INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document ▼](#)

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore [RAND Infrastructure, Safety, and Environment](#)

View [document details](#)

This product is part of the RAND Corporation reprint series. RAND reprints reproduce previously published journal articles and book chapters with the permission of the publisher. RAND reprints have been formally reviewed in accordance with the publisher's editorial policy.

12. Evaluating the viability of 100 per cent container inspection at America's ports

**Susan E. Martonosi, David S. Ortiz
and Henry H. Willis**

INTRODUCTION

The US and the global economy are wholly dependent on overseas trade and the integrated transportation system that moves cargo around the world and throughout the US. Six million cargo containers, equivalent to over 11 million 20-foot equivalent units (TEUs),¹ of goods arrive at United States seaports (Maritime Administration, 2002; Bureau of Transportation Statistics, 2003). Approximately 90 per cent of global trade, including 75 per cent by value of non-North American trade to and from the US, is shipped via cargo container (Stana, 2004; Willis and Ortiz, 2004). The multi-modal structure of the containerized supply chain permits containers entering via a seaport to exploit the US road and rail network to penetrate deeply into the country.

Any disruption to the steady flow of containers into and out of the United States can have a devastating economic impact. Estimations of the costs from a ten-day West Coast port lock-out ranged from \$500 million to as high as \$19 billion (Crist, 2003), and a simulation conducted by the consulting firm Booz-Allen-Hamilton estimated that the discovery of proposed attacks on selected ports could lead to nationwide shutdown of ports carrying economic effects up to \$58 billion (Gerencser et al., 2003). Though these estimates are highly dependent upon underlying assumptions and subject to debate, the fact remains that there are many port disruption scenarios that would result in billions of dollars in damages.

The volume of containers and the pervasiveness of the delivery system reveal two distinct vulnerabilities: an attack on a port could carry a devastating economic impact and also the system itself could be used to deliver a weapon to any location in the country. These vulnerabilities are not new. The efficiency and anonymity of the containerized supply chain have also made

it a useful target of smugglers and vulnerable to theft. Stephen Flynn of the Council on Foreign Relations has long warned that the vulnerability of this system and consequences of attacks on it, or using it, make the containerized shipping system an attractive terrorist target (Flynn, 2000, 2002, 2004).

Prior to the terrorist attacks of 11 September 2001, the primary focus of port security was to prevent theft and to ensure that illegal or undeclared goods were not brought into the United States. The United States and international responses to the terrorist threat has expanded the focus of port security. Within the Department of Homeland Security (DHS), Customs Service and Border Patrol functions were merged to become US Customs and Border Protection (CBP). The International Maritime Organization updated the Convention for the Safety of Life at Sea and issued the International Ship and Port Facility Code. The United States passed the Maritime Transportation Security Act of 2002, instituting new protocols for the declaration of cargo, and has stationed customs inspectors at overseas ports. The private sector is now encouraged to participate in voluntary programs for securing their supply chains through the Customs–Trade Partnership Against Terrorism (Crist, 2003). The Smart and Secure Tradelanes consortium funds pilot projects to demonstrate new technology to make the supply chain more transparent ('SST Phase One Report', 2003). Despite this extensive response, there is little evidence that enough has been done to secure US ports or that what has already been done is effective.

We argue that the goal of transportation security initiatives, focused on the ports of entry for cargo containers, is to balance the costs of providing increased security with the reduction of risks from the unintended use of the container supply system. While unintended uses include the movement of any dangerous or illegal goods, we focus on the reduction of risks from terrorist attacks at a port or deriving from cargo arriving at a port. To this end, we propose that cost–benefit analysis be used to assess security initiatives directed at preventing terrorist attacks. This chapter provides a case study for a specific proposal: 100 per cent scanning of containers at US ports. Container scanning and inspection are essential steps in the process of ensuring a secure containerized shipping system. These processes may reduce the risk of an attack on the port itself through deterrence or by increasing the likelihood that terrorist weapons will be detected.²

Previous work by the authors has developed a framework for assessing and evaluating the security of the containerized supply chain (Willis and Ortiz, 2004). Here we present an extension of that work focused on technological requirements for implementing the specific policy of inspecting all incoming containers via scanners.

We begin by defining some terms. Homeland Security Presidential Directive HSPD-11 defines 'terrorist-related screening' in a general context

as ‘the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security’ (Bush, 2004). Accordingly we call ‘screening’ the initial assessment of the risk of a container based on manifest, shipper, carrier, consignee and other information associated with the shipment. ‘Primary inspection’ or ‘scanning’ is the radiographical scanning of a container via an X-ray or a gamma-ray scanner to identify its contents. ‘Secondary inspection’ is the hand-inspection of the contents of a container by a team of CBP inspectors.³

The small fraction of containers that currently undergo primary inspection has motivated calls for complete scanning: US House of Representatives minority leader Nancy Pelosi called for complete inspection of containers in the Democratic response to the 2004 State of the Union address (Pelosi and Daschle, 2004). At the 2004 Democratic National Convention in Boston, former president Bill Clinton highlighted the need for dramatically increased scanning at our nation’s ports (Clinton, 2004). Stephen Flynn proposes electronic scanning of containers at departure and arrival, comparing images to verify security (Flynn, 2004). A recent study (Wein et al., 2003) examined potential container inspection policies against nuclear materials from a game-theoretic standpoint, where the government would like to choose an inspection scheme that falls within budgetary constraints and maximizes detection probabilities over a range of possible terrorist responses. In this chapter, we perform a cost–benefit analysis of implementing a policy of scanning 100 per cent of incoming containers at US ports, exploring issues of technological cost and performance, and we examine the minimum threat required to justify the costs of particular inspection proposals.

In this context, we present three questions:

1. Given current technological effectiveness, how does changing the percentage of containers selected for scanning alter the cost and effectiveness of the containerized supply chain? In particular, under what situations is 100 per cent scanning cost-effective?
2. What are the implications of policy decisions for small versus large ports?
3. What technological improvements would be required to make increased scanning of incoming ocean containers effective?

The remainder of the chapter is organized as follows. We follow the introduction with an overview of proposals for increasing container inspection processes and associated technology issues. We then describe a cost–benefit approach for assessing the viability of increased inspections of containers

using a queuing model to simulate the inspection process. Limitations because of simplifications in the model and estimates of parameters are discussed. We conclude by presenting results from this modeling approach and the implications of these results on policy efforts to secure US ports.

CONTAINER INSPECTION PROCESSES AND TECHNOLOGY ISSUES

Overview of Container Screening, Scanning and Inspection Process

A container arriving at a US port is subjected to several checks. The 24-hour advanced manifest rule requires carriers to submit manifest information 24 hours before cargo is loaded onto a US-bound vessel. In this time, CBP performs a background screen on the manifest, carrier and shipper to determine if the shipment poses a risk to the United States. In some cases, the container is denied permission to be loaded on the vessel. CBP performs additional manifest screening prior to shipment arrival via a computerized targeting system. Currently, approximately 5 per cent of incoming containers from the sea are selected for additional scrutiny, which consists of a two-stage inspection process. Primary inspection consists of scanning via an X-ray or a gamma-ray scanner. Gamma-ray scanners tend to be less expensive and faster than X-ray scanners; gamma-ray scanners however operate at lower power and therefore have difficulty producing clear images of densely packed containers. Scanning occurs by passing a container through a fixed scanner, or by moving the scanner over a fixed container. Inspectors examine the scanned image for discrepancies with the manifest and other signs of risk.

In some cases, actual physical inspection is required. Of these already suspicious containers, it is estimated that roughly 5 per cent show irregularities in the image, or are so densely packed that the image is not clear; these containers require a hand-search in which the container is opened and its contents removed and examined (Schiesel, 2003, Krikorian, 2004). This is a time-consuming process involving as long as four hours using 15 to 20 inspectors (Bowser and Husemann, 2004) or three days for five agents (Johnson, 2004). Neither of these estimates has been statistically studied.

Proposed Policies for Increased Scanning and Inspection of Containers

Any proposed policy change requiring increased primary inspection of containers raises several issues. Additional scanning equipment would need to be purchased, operated and maintained. Competing technologies have

different costs and performance, measured by detection capability and scanning rate. Increased scanning of containers would also require more teams of inspectors to complete secondary inspections by hand. These factors form the basis of alternative policies for increased inspection of containers, described below. The alternative policies are compared against a 'base policy', which is modeled on the current scanning regime.

- *Base policy, 'current' scanning processes:* The base policy randomly⁴ selects 5 per cent of incoming containers to be scanned via deployed X-ray scanners. Of these containers, 5 per cent require additional inspection by hand. The costs for this policy are annual operations and maintenance costs for the scanning equipment and salaries for the inspectors.

To assess the viability of 100 per cent inspection of containers at US ports, we present three alternative policies (see also Table 12.1).

- *Policy 1 – 100 per cent inspection using current technology:* This policy mandates the scanning of 100 per cent of arriving containers with current technology. More scanning machines are required than for the base policy. The costs of this policy include capital, operations, maintenance and inspection costs.
- *Policy 2 – 100 per cent inspection using faster and cheaper technology:* This policy requires the scanning of 100 per cent of arriving containers, but with improved equipment. The new scanning technology is assumed to be gamma-ray based, but improved from currently available gamma-ray equipment. The improved scanning equipment is characterized by a faster scanning rate and lower equipment costs than the current technologies in the base policy and Policy 1, but carries the same 5 per cent false positive rate. Additionally, we assume a faster hand-inspection rate, because of improved training for inspectors or improved signaling from the scanning equipment as to the region of the container requiring scrutiny.
- *Policy 3 – 100 per cent inspection with greater accuracy:* This case improves on Policy 2 by reducing the false positive rate to 1 per cent.

APPLYING COST-BENEFIT ANALYSIS TO CONTAINER INSPECTION POLICIES

The goal of increasing container inspection is to reduce the risks from terrorist attacks on or using the containerized shipping system. Any

Table 12.1 The three policies considered in the case study of 100 per cent scanning of incoming containers are each characterized by 11 parameters. These parameters are based on assessments of current technology and possible performance characteristics of future technology. The three alternative cases are based on a simplification of the current policy

Parameter	Base policy	100% scanning same technology (Policy 1)	100% scanning slightly improved technology (Policy 2)	100% scanning greatly improved technology (Policy 3)
Fraction containers screened	0.05	1.00	1.00	1.00
Targeting method	Random	N/A	N/A	N/A
Detection rate	0.95	0.95	0.95	0.95
Scanning rat (TEU/hr)	20	20	30	30
False positive rate	0.05	0.05	0.05	0.01
Equipment unit cost (\$M)	\$4.5	\$4.5	\$1.0	\$1.0
Annual maintenance costs (\$)	\$200 000	\$200 000	\$90 000	\$90 000
Operators per scanner	4	4	4	4
Hand searching rate (containers per day)	1	1	4.8	4.8
Number of inspectors per team	5	5	5	5
Annual operator/inspector salary (\$)	\$50 000	\$50 000	\$50 000	\$50 000

proposals for increasing container inspection must be compared to current policies. Cost–benefit analysis provides a normative approach to evaluate proposals for increased container scanning. Using this approach, a new policy should be adopted if the marginal costs the policy achieves are less than the expected marginal decrease in risk due to terrorist attacks.

A cost–benefit analysis requires defining the scope of costs and benefits considered. We have defined the direct benefits of the policy to be associated with stopping the damage of a terrorist attack, both to the port and to the economy in general. These benefits are a result of deterrent effects of scanning and the potential to detect and remove or disarm a weapon before it is used. The indirect benefits of a policy are more difficult to determine; for example 100 per cent scanning might allow CBP to more readily intercept misrepresented cargo and thus collect additional tariff revenue. The direct costs that we will consider are the equipment and personnel costs associated with 100 per cent scanning. There are also indirect costs associated with increased scanning, delays being the most important. We do not estimate other indirect costs associated with allocation of real estate at the port for inspections, nor expenses associated with inspector training.

It is important to account for uncertainty in parameters of the model for container inspections. For costs, this uncertainty can be reduced through surveys of relevant data and sensitivity analysis of results to this uncertainty. There is greater uncertainty about benefits, since the benefits of container inspection depend upon the probability that attacks would be stopped if they were attempted, the consequences of such an attack, and also the probability that a terrorist attack might be attempted in the first place. The last issue introduces a high level of uncertainty. Terrorist motivations and capabilities can be studied and understood through intelligence gathering, though at some level, this uncertainty is irreducible. Nevertheless, cost–benefit analysis is a useful framework for this decision context.

For each policy, a threshold attack probability defines conditions for adoption of the policy to be cost-effective. Calculating the threshold probability of attack provides bounds that can inform comparisons of competing policy alternatives. The methodology is similar to that used by Barnett and Martonosi (2003) to evaluate aviation security policies. The threshold annual probability of an attack on the United States on or using a cargo container may be derived as:

$$P(\text{Attack}) = \frac{(\text{Cost of Proposed Policy}) - (\text{Cost of Baseline Policy})}{\text{Attack Cost} \left(\frac{P(\text{Proposed Policy Prevents Attack}) - P(\text{Baseline Prevents Attack})}{P(\text{Baseline Prevents Attack})} \right)}$$

The difference in costs and detection capabilities between the base and proposed policies can be both positive and negative. This creates several cases to consider, two of which are degenerate since they would produce negative threshold probabilities. First, note that when the denominator is positive, the new policy improves detection capability, and when it is negative, it degrades the detection capability. The first degenerate case occurs when the new policies improve detection capability and decrease costs; then it is always beneficial to switch to the new policy. The second degenerate case occurs when the detection capability decreases and the costs rise; then it is never beneficial to switch to the new policy.

For other cases, the decision to switch policies is more interesting. If the new policy improves detection capability but increases costs, it makes sense to switch if the threat is sufficiently high to justify the increased costs. In this case, the threshold probability is a lower bound: the proposed policy is cost-effective if the perceived probability of a terrorist attack is greater than this threshold. However if in decreasing detection capability, costs also decrease, then it might still be beneficial to switch to the new policy if the probability of a terrorist attack is believed to be sufficiently low.

Finally, there are two trivial cases to consider. If the policies have the same detection performance, the function is undefined as the denominator equals zero and switching depends only on relative costs, so the cheaper policy is better. If policies have the same costs, the numerator equals zero and the decision to adopt depends only on the relative detection probabilities, so the higher-performing policy is better.

CALCULATING COSTS AND BENEFITS OF CONTAINER INSPECTION

We develop a queuing model to estimate the cost and performance of each policy. The model takes into account scanning equipment technology, performance, acquisition requirements, depreciation and operation. The number of scanning machines and hand-inspection stations required is calculated as a function of the container arrival, scanning and inspection rates. We also consider incurred costs due to cargo delays. The benefit of any policy is the averted financial damages due to a terrorist attack on the system. All parameters are based on estimates from publicly available literature, though considerable uncertainty remains with respect to the advancement of scanning technology, the variability in arrival and service rate and the estimation of costs.

Cost and Performance of Container Inspection

Our base technology scenarios assume the technology most widely available and applicable currently is X-ray scanning. The X-ray scanners in use today cost approximately \$4.5 million with estimated annual operating costs of approximately \$200 000 (Frankle, 2004). We converted fixed equipment costs into annual costs by amortizing evenly over ten years. For the case of X-ray scanners, the total annual equipment costs are \$650 000. We assume that X-ray scanners are 95 per cent effective at detecting dangerous materials, though this value is a function of both the technology and the operator. It is estimated that approximately 5 per cent of scanned containers require additional inspection and that few carry dangerous materials (Schiesel, 2003); hence we estimate the false positive rate to be equal to the total positive rate, 5 per cent.

Estimates for scanning rates vary. X-ray scanners can scan a 20-foot container in 30 seconds (ARACOR, 2004). But an operator may take up to 15 minutes to review the image. Having more operators per machine would reduce the average time a container spends being scanned. For simplicity, we have assumed that each machine requires four inspectors – one to operate the machine and three to examine the images – and that the total inspection rate is 20 TEUs per hour, or equivalently three minutes for scanning and reviewing the image of each container.

Though gamma-ray scanners are currently being used at some ports, we choose it to model policies employing improved technology. Operational concerns regarding gamma-ray scanners remain: their ability to scan densely packed containers is less than that of X-ray devices, which could cause them to have a high false positive rate; and truck drivers have expressed concerns about gamma-ray scanners because of potential radiation exposure. Gamma-ray scanners such as SAIC's Vehicle and Cargo Inspection System (VACIS) cost approximately \$1 million, again amortized over ten years, and require \$90 000 in annual maintenance costs, including the cost of replacing the radioisotopes once every five years (McDaniel, 2004; Schiesel, 2003). VACIS literature estimates a total inspection time of one to three minutes per TEU – an average of 30 TEU per hour – and we again assume a team of four inspectors per scanner.⁵ We assume a 95 per cent rate of detection.

There are also parameters that do not rely on the type of scanning equipment used. The annual salary of a port inspector is assumed to be \$50 000, based on an estimate by the Bureau of Labor Statistics (Bureau of Labor Statistics, 2004). Times for hand-inspections vary, ranging from four hours using 15 to 20 inspectors (Bowser and Husemann, 2004) to as high as three days for five agents (Johnson, 2004). We have thus chosen a value of one container per day for a team of five agents for the current case. For the cases

considering improved technology, we reduced the search time to roughly five hours per container, or 4.8 containers per day, for a team of five people. While this reduction is not necessarily associated with improvements in technology, new technology might provide the inspectors with more information regarding the exact location of the material instigating a search.

Container Arrivals, Scanning and Hand-Inspection Service Rates

The model for container arrival, scanning and hand-inspection is that of a tandem queue. We assume that containers arrive at the port according to a Poisson process with rate λ containers per hour, which is easily calculated for any particular port.⁶ The average arrival rate for the United States is 1 474 TEUs/hour over 157 ports, and arrival rates for prototypical large (for example Los Angeles)⁷ and small ports (for example Miami) are 365 TEUs/hour and 50 TEUs/hour, respectively. The containers that arrive at a port are selected for scanning according to a Bernoulli random process with parameter p . For the base case, p will be 0.05, or 5 per cent of containers; for the case of 100 per cent scanning, p will be 1. A certain percentage of containers that are machine scanned will be selected for secondary inspection by hand; we assume that this selection process follows a Bernoulli process with parameter f representing the false-positive rate associated with the scanning technology. We assume that the scanning time per machine is exponentially distributed with parameter μ_S containers (TEU) per hour and that the rate for hand scanning is μ_H containers (TEU) per hour.⁸ We assume that a port has M_S scanning machines and M_H hand-inspection stations, which are chosen to be the minimum number guaranteeing that the queue of containers to be scanned remains finite. This value is given by constraining the arrival rates ($p\lambda$ and p/λ for primary and secondary inspection, respectively) to be strictly less than the total service rates ($M_S\mu_S$ and $M_H\mu_H$, respectively).⁹

Inspection Costs: Equipment and Man Hours

The costs of scanning are equivalent to equipment purchase, maintenance and operation costs. Therefore if C_S is the purchase price of each primary scanning machine, and A is the period over which the cost of the machine will be amortized, then the purchase price per year is C_S/A assuming straight-line depreciation. Furthermore each machine will require maintenance and repairs, R_S , per year. Lastly, each machine will require N_S operators at any time, and we assume that these operators earn a salary, S , per year and work in three shifts per day. Thus the annual cost for primary (machine) scanning per port is $M_S(C_S/A + R_S + 3N_S S)$. Because not all

ports operate three full shifts a day, this assumption will underestimate somewhat the machine and staffing requirements per shift, yielding conservative estimates.

For hand inspection, the calculation is similar. Let M_H be the number of hand-inspection teams required at a port as calculated above. Since each hand-inspection team consists of N_H workers, again requiring a salary S and working in three different shifts daily, the total cost associated with hand inspections is $M_H(3N_HS)$.

Thus each port contributes a total of $M_S(C_S/A + R_S + 3N_S S) + M_H(3N_H S)$ to the total equipment and labor costs of the scanning and inspection policy. We have calculated this value exactly for the top 30 ports representing 99.5 per cent of container imports based on data from the Maritime Administration. We apportion the remaining costs equally among the 127 remaining seaports.

Delay Costs per Container

Increased delays for containerized freight are cited as one of the principal concerns associated with increased scanning. For any given container, the delay time is probabilistically distributed based on the arrival and service processes (see Burke, 1968, 1972; Bertsekas and Gallager, 1972; and Larson and Odoni, 1981, among others). Therefore with knowledge of the delay costs per container per hour of delay, it would be a straightforward calculation to determine the total delay costs. Unfortunately the costs per hour of delay are exceptionally difficult to estimate.

The sensitivity of a shipment to a delay varies according to the contents. Short delays – from minutes to hours – most likely have little economic effect so long as delivery falls within a prescribed window. Delays of perishable items, such as fresh fruit, might incur no cost for a delay of several hours, but may incur a total loss if the delay is several days. Items critical to manufacturing supply chains might incur large costs almost immediately, and induce exponentially growing costs as assembly lines close due to lack of parts. The cost per hour of delay is certainly a non-linear function. Some scholars have attempted to estimate the costs of supply chain delays: Spencer (2004) for example cites a Fortune 100 estimate that a delay of one day adds 0.5 per cent of the product value to its cost, implying a linear relationship between delay time and incurred cost.

Rather than propose an estimate of the distribution of delay costs, we have chosen to use in our analysis several values for the costs of the delay: \$0, \$6 and \$60 per TEU-hour. In these scenarios, \$0 per TEU-hour represents the delay costs of time-insensitive cargoes, \$6 per TEU-hour represents 0.5 per cent value per day costs of a \$30 000/TEU shipment

using Spencer's estimate, and \$60 per TEU-hour represents extremely time-sensitive cargo – for example 5 per cent loss of value per day.

Direct and Indirect Attack Costs

Estimates of the cost of a terrorist attack vary widely. We are concerned with an attack on a port, nearby infrastructure, or a remote destination facilitated by using a shipping container. The cost of the attack includes loss of life, infrastructure damage and residual repercussions through the economy. We are assuming that increased scanning could eliminate the costs of an attack by allowing authorities to isolate the container from port facilities and other areas in which it may cause damage. We consider a range of attack costs from \$1 billion to \$1 trillion.

It is possible to place these figures into the context of other terrorist attacks and natural disasters. The 1993 attack on the World Trade Center was estimated to inflict a cost of \$510 million, and the bombing of the Murrah Federal Building in Oklahoma City in 1995 was estimated to inflict a cost of \$125 million (CNNMoney, 2004). The Booz–Allen–Hamilton simulation estimated the total cost of sequential port shutdowns at \$58 billion. Estimates for the costs of the attacks of 11 September 2001 begin at \$100 billion (Looney, 2002). Natural disasters, too, carry large price tags: Hurricane Andrew caused damages in the range of \$100 billion (Looney, 2002), initial estimates for damages to Florida from Hurricane Ivan are \$50 billion (Treaster, 2004), and an economic analysis of a hypothetical magnitude 7.1 earthquake on the Elysian Park Fault estimated costs up to \$94 billion (Cho et al., 2001). The cost of a terrorist nuclear attack on the United States could begin at approximately \$600 billion (Abt, 2003). Therefore our estimates for the costs of an attack via a container fit into the range of costs related to other attacks and natural disasters.

Expected Benefits of Policy

The expected benefit of increasing scanning at the nation's ports is the expected averted cost of attack. No scanning protocol is perfect: if only a fraction p of the containers are scanned, then if any of the $1 - p$ per cent of containers that are not scanned is dangerous – for example contains a weapon of mass destruction – it will enter the country. Furthermore the scanning systems do not have perfect detection rates. If d is the probability of detection, then the probability that a dangerous container is prevented from entering the country is the product of the probability of scanning and the probability of detection: pd . We assume that hand-searching has a 100 per cent detection rate. The expected benefit therefore is the product

of the probability that a container is dangerous, the probability of detection and the cost of an attack: $P(\text{Attack}) \cdot (pd) \cdot C_A$.

Case Parameters

The parameters for the base policy and the three alternative policies were listed earlier. The scanning equipment and staffing requirements were determined as follows. For each of the top 30 incoming ports, we calculated average container arrival rates to determine equipment and staffing requirements (Maritime Administration, 2002). For the remaining 127 ports that handle container traffic – 0.5 per cent of the annual total – we allocated container traffic equally over all of these ports, determined equipment and staffing requirements for a single port, and replicated it 127 times to estimate nationwide requirements.

RESULTS

The decision to switch to a new scanning and inspection policy is based on the probability of an attack within a year and the costs of delay, attack, equipment acquisition and labor. Figure 12.1 illustrates how the threshold probability of attack depends on delay and attack costs. Looking first at the policy using current technology and the curve corresponding to a \$1 billion attack, we see that as delay costs increase from \$0 per TEU-hour to \$60 per TEU-hour, the estimated annual probability of attack required to switch to 100 per cent scanning varies from 80 per cent to almost 100 per cent. Thus unless an attack of that magnitude is very likely to occur within a year, it is not cost-effective to switch to 100 per cent screening using current technology. For an attack costing up to \$10 billion, the switching probability varies from 15 to 45 per cent. For attacks inflicting costs from \$100 billion to over \$1 trillion, the switching threshold probability is less than 10 per cent. The graphs for the other policies show that when technology is improved, the switching probability declines precipitously. For an attack inflicting \$1 billion of costs, the probability of attack required to make 100 per cent scanning beneficial varies from 23 per cent for \$0-per-hour delays, to 60 per cent for \$60-per-hour delays. For \$10 billion in inflicted costs, the probability of attack required to switch varies from approximately 3 per cent to approximately 10 per cent. Therefore the use of improved technology in scanning reduces the threshold probability of attack by an order of magnitude. New technology offers performance gains causing the decision to switch to 100 per cent scanning to be beneficial even when the estimated probability of attack is very low.

Figure 12.1 The threshold probability of attack required to switch to a new scanning policy for a range of attack costs

While estimating the likelihood of an attack within a year is difficult, it is somewhat easier to decide whether our perceived likelihood of attack is higher or lower than a threshold. For instance we might be very confident a \$1 billion attack will not occur every year, particularly since it has been several years since the 11 September attacks. However it is harder to determine whether or not a large-scale attack such as a nuclear attack would occur roughly every 1000 years. This model does not help estimate the probability of attack, but it provides bounds to help decision makers understand what factors might cause them to switch from a position of adopting a policy to one of not. While the estimated threshold probability of attack might be low enough to recommend the implementation of 100 per cent scanning, other details in the analysis show that the decision is more complicated. For example though the benefit of preventing a large attack might offset the costs of machines, land requirements and personnel considerations may lead us to another conclusion.

Figure 12.2 illustrates the number of machines and hand-search stations required at typical ports for 100 per cent scanning per shift. With current technology, a large port like Los Angeles alone would require over 400 hand-search stations (or 2000 inspectors) per shift¹⁰ to inspect containers to maintain a stable queue. Improved technology is not necessarily a panacea: improved technology would still require close to 100 hand-search stations per shift at a port the size of Los Angeles. Port space is optimized for throughput and any regime of 100 per cent scanning would require significant changes to port operations. Thus the costs excluded from our model likely make 100 per cent inspection infeasible using the technology of the base policy.

Even if space constraints do not make inspection policies infeasible, the costs of equipment and labor also influence the decision to switch to 100 per cent scanning. Figure 12.3 illustrates the equipment and labor costs per TEU for the three policies versus the base case. We see that the average cost per TEU increases significantly when 100 per cent scanning is performed with current technology, but that improvements in technology can decrease this cost. If false positive rates are reduced, then the costs of 100 per cent scanning under improved technology would be comparable to those estimated for the current scanning and inspection regime. Note that the thresholds shown above already consider these cost changes, and indicate that it can still be worthwhile to implement the new policies if the threat of attack is sufficiently high.

Of course the institution of 100 per cent scanning would impose a delay. Figure 12.4 illustrates this delay for the three proposed policies. The expected delay increases from approximately 0.5 hour per TEU for the base case to approximately 5.5 hours for the case of 100 per cent scanning using

Figure 12.2 The number of scanning machines and hand-search stations required at prototypical ports per shift for 100 per cent scanning versus the base case for different levels of technology

current technology. This is the worst-case scenario, which could be tolerated with appropriate coordination among land-based carriers and shippers. Improved technology reduces this delay to approximately an hour, and greatly improved technology, offering a low false positive rate, has an inspection-induced delay comparable to that of the current 5 per cent scanning regime. Because the majority of a container's inspection time comes from the very long hand-searches, reducing the fraction of containers needing to be hand-searched causes a steep reduction in the average inspection time over all containers.

In summary, with currently available technology, 100 per cent scanning of arriving containers at US seaports may be cost-effective, but only if the land and personnel constraints prove feasible. To justify the switch to such a regime from a cost-benefit perspective would require at least a minimum

Figure 12.3 Equipment and labor costs per TEU for 100 per cent scanning versus the base case for different levels of technology

of a 14 per cent chance of an attack with consequences of \$10 billion within a year, or a minimum of 80 per cent for an attack with consequences of \$1 billion. However at high-traffic ports 100 per cent inspections may demand personnel increases of more than an order of magnitude beyond current staffing levels. Most of the inspection-related delays and labor costs stem from the vast number of containers that would require hand-searches. If advances can be made toward less-expensive and faster technologies with a lower false positive rate, then costs of inspection would not rise if 100 per cent scanning were employed and could make 100 per cent scanning a viable option at all ports. Nonetheless if our threat of attack is sufficiently high, then 100 per cent scanning could be justified with current technology.

Figure 12.4 The expected delay because of inspection per TEU compared to the base case

LIMITATIONS

The results presented in this chapter are subject to model and data assumptions. This section discusses the limitations of our analysis stemming from the idealized queuing model, the algorithm for assigning machines and inspection teams to ports, and excluded costs and benefits.

Limitations of the Queuing Model

This model employed a tandem queue with Poisson arrivals and exponential service times. The inter-arrival times are independent and memoryless: the probability at any instant that an arrival occurs is independent of how long it has been since the last arrival. The assumption allows a closed-form solution for the distribution of waiting times in the queue, but overlooks the reality that container arrivals are coordinated with ship arrivals, which would tend to bunch container arrivals in batches. The assumption of exponential service times is justifiable, because scanning and inspection of

containers can be expected to have a range of values distributed around a mean value, with certain rare containers having a long service time. It is possible to model arrival and service times at ports empirically; we recommend this before further development of the model or application of the results.

Possible Suboptimal Estimation of Equipment and Personnel Requirements

The model assigned the number of machines and the number of hand-inspection stations to be the minimum required to guarantee a stable queue. More detailed analysis would minimize the total costs associated with scanning, including equipment, labor – for example number of operators per machine and hand inspectors per station – and delay costs at individual ports. Additionally, certain ports handle more valuable or time-sensitive goods than others and would require a machine and staffing allocation that reflected this distribution. The result of this more detailed analysis would be to reduce the threshold probability of attack by some unknown amount.

Infrastructure and Operational Costs

As discussed above, the model did not consider infrastructure and operational costs that would be incurred to provide space for drayage, scanning and additional personnel. Additionally, we excluded scanning machine failure rates and the possibility that many small ports would need at least two scanners: one for normal operations and one to be used when the primary scanner fails or is undergoing maintenance. Inclusion of such costs would make 100 per cent scanning even less desirable than what was estimated in this analysis.

Marginal Analysis

In this chapter, we compared the total costs of implementing 100 per cent screening at all ports to the total benefits of such screening. Another strategy would have been to conduct this analysis incrementally, on a port-by-port basis. Starting with those ports that offer the greatest benefit of screening on a 'per dollar spent' basis, implement 100 per cent screening at those ports, and continue adding ports until the marginal costs of the next best port outweigh the marginal benefits. We have chosen not to use this method however because such analysis would require estimating the threat of attack on each port separately. While we may have some idea of the general level of threat facing our nation, the implementation of

100 per cent screening on a dynamic basis could very well shift the target away from those ports conducting the screening to those ports that do not screen, causing the results to vary at each increment. Furthermore if we believe those ports that are most desirable to attack are the very large ports, then our analysis has shown that these are the same ports for which 100 per cent screening is not currently feasible. Another problem is the potential political repercussions of choosing some ports for 100 per cent screening while ignoring others. Our study chooses to focus on the feasibility of a policy affecting all ports rather than on the incremental decision of which ports to protect before others. In addition, our research acknowledges marginal analysis in two other ways: considering alternative probabilities of an attack and mentioning, if not modeling, screening rates intermediate between the 5 per cent base case and 100 per cent screening.

CONCLUSIONS AND RESEARCH DIRECTIONS

This chapter has presented a cost–benefit analysis of 100 per cent scanning of incoming sea containers at US ports. The model uses cost estimates associated with equipment acquisition, operations and maintenance, inspector pay and the delay in delivery of goods. The benefits of the policy are the expected averted costs due to prevention of a terrorist attack. The analysis does not consider the costs of allocating space for the scanning equipment and inspection stations at ports, nor the benefits due to increased interception of illegal or misrepresented goods likely to occur from the imposition of 100 per cent scanning. We draw the following conclusions:

- Adopting a policy of 100 per cent scanning with current technology is not viable because of restrictions on land and personnel. If port land and personnel considerations are negligible – an unlikely case – then scanning 100 per cent of all incoming containers is cost-effective for attacks with direct and indirect consequences greater than \$10 billion. For an attack inflicting a cost of \$1 billion, the minimum annual probability of attack to switch to a policy of 100 per cent scanning is close to 0.80. However the threshold probability of attack is considerably smaller when attacks inflicting costs of \$10 billion or more are considered. When slightly improved scanning technology is deployed, personnel and land area requirements remain significant at high-volume ports when 100 per cent scanning is imposed. If these improvements manifest themselves as a reduction in the false positive rate, reduced land costs would make adoption of a 100 per cent scanning policy cost effective and could prompt

a policy discussion regarding risk tolerance at America's ports. Technology developers should seek to reduce the false positive rate of their technology as they improve scanning rate, reliability and other performance characteristics.

- An area ripe for future study is the impact of 100 per cent scanning on deterrence. Complete scanning and subsequent inspection of containers at ports would most likely deter terrorists and smugglers under particular circumstances. A sufficiently high detection rate would render irrational an attempt to employ a container in an attack on an interior target, since it would have little chance of reaching the desired location. Of course the ability to attack a port via a container would remain. There are different ways to model deterrence. For example Martonosi and Barnett (2004) assign a threshold probability of success below which a terrorist will decide not to attack; the probability of a successful attack in their model is a function of the security measures in place and the deterrence threshold. Such a deterrence threshold could be incorporated in our model; however since there is little empirical evidence regarding successful deterrence of terrorists, any policy decision would require making assumptions regarding terrorist behavior. Incorporating deterrence into our model would embolden the case for 100 per cent scanning, because it would reduce the likelihood of an attack.
- The base policy assumed that 5 per cent of incoming containers were selected at random for scanning. However there is a broad range of scan rates between 5 and 100 per cent that may be employed to a certain degree of success, especially if such a policy mitigates needs for large parcels of land at ports. Any policy scanning less than 100 per cent of incoming containers would likely employ a targeting algorithm to increase the rate of detection. GAO concluded that there was no empirical evidence that US Customs and Border Protection's Automatic Targeting System identified dangerous cargo more readily than random scanning (Stana, 2004). Therefore to implement a policy scanning less than 100 per cent of containers, empirical demonstration of the ability of automatic targeting algorithms to detect dangerous cargo would be required.
- We found that port area for scanning and inspection was a critical driver of a policy's viability. The same issues in the case of air cargo may not be as serious: air cargo pallets are smaller than standard intermodal containers, are more readily scanned and inspected, and airport operations already require ferrying cargo around an airfield. A similar analysis could be applied directly to airfreight to evaluate policies requiring increased scanning of air cargo.

NOTES

1. The standard container is a 20 ft equivalent unit, which is a sturdy steel box measuring $20 \times 8 \times 8$ ft, although containers are often 40 ft long and can come in various configurations to support different kinds of cargo.
2. Further protection of US ports as targets would require detection prior to port arrival.
3. CBP 'screens' 100 per cent of incoming containers. Manifest information for US-bound containers must be communicated electronically to CBP 24 hours before being loaded on a US-bound vessel. Ninety-six hours prior to arrival at a US port, a vessel must declare crew and manifest information. Based on this information, CBP operates an automated targeting system to assess the risk each container may pose, and select some – roughly 5 per cent (Wasem et al., 2004) – to be radiographically scanned and/or hand-inspected.
4. Currently, containers are selected for targeting based on an automated targeting algorithm. The US General Accounting Office (Stana, 2004) determined that the Automated Targeting System (ATS) used by Customs and Border Protection has not undergone the rigorous testing that have similar systems. Furthermore, the GAO reported that industry experts believe that the data used by ATS to identify suspicious containers, including manifest declarations, are often unreliable and do not provide a sound basis for targeting. Hence it is unclear if the ATS performs better than random selection. It is also possible that terrorists could outwit the targeting system (Chakrabarti and Strauss, 2002).
5. It should be noted however that current scanning rates reported by those ports already using VACIS are approximately 8–10 per hour because of unfamiliarity with the technology (Schiesel, 2003).
6. A Poisson process is a stochastic counting process often used to simulate arrivals at a service queue such as a bank teller or bus stop. It has several characteristics that make it attractive for modeling such systems: the times between successive arrivals are independent and exponentially distributed with parameter λ ; if two Poisson processes are combined, the resulting process is also Poisson; if a Poisson process is split into two processes by assigning a probability, p , to each arrival, then the resulting two processes are Poisson with rates λp and $\lambda(1-p)$ respectively (Bertsekas and Gallager, 1992). Poisson processes are considered good approximations for aggregate arrival processes, but might not be so well suited to the batch-like characteristics of a ship discharging cargo. As such, our use of a Poisson process will serve as a lower bound on the required equipment to achieve a certain level of container scanning.
7. All references in this chapter to the Port of Los Angeles consider this port individually and do not combine its traffic with that of the adjacent port of Long Beach.
8. It is traditional to assume that the service times of a queuing system follow an exponential distribution. This assumption and that of a Poisson arrival process guarantee that the scanning and hand inspection queues are $M/M/M_s$ and $M/M/M_H$ queues, for which probability distributions for the queuing delays are well understood (Bertsekas and Gallager, 1992). Future research may entail empirical estimation of the arrival and service processes at ports.
9. By choosing the smallest number of screeners satisfying this requirement, we minimize the equipment and labor cost, but perhaps do not minimize the total cost, which includes the inspection-related delay a container experiences at the port. Optimizing the number of machines with respect to total costs could alter somewhat the results of the analysis.
10. As a point of reference, the total CBP personnel at the Ports of Los Angeles and Long Beach increased to a total of about 500 after 9/11 (Fleming, 2004). Inspectors make up a portion of this staff.

REFERENCES

- Abt, C.C. (2003), 'The economic impact of nuclear terrorist attacks on the freight transport systems in an age of seaport vulnerability', Cambridge, MA: Volpe National Transportation Center.
- ARACOR (2004), 'ARACOR Eagle Product Information', Sunnyvale, CA: ARACOR, Inc.
- Barnett, A.I. and S.E. Martonosi (2003), 'A cost-benefit risk analysis of three airport security measures', working paper, Cambridge, MA: Massachusetts Institute of Technology.
- Bertsekas, D. and R. Gallager (1992), *Data Networks*, 2nd edn, Englewood Cliffs, NJ: Prentice Hall.
- Bowser, G.F. and R.C. Husemann (2004), 'Full cargo inspection possible through recent technology advances', Port Technology International, http://www.porttechnology.org/journals/ed11/downloads/pt11_69-72.pdf, 27 September.
- Bureau of Labor Statistics (2004), 'Occupational employment and wages, May 2003: 53-6051 transportation inspectors', US Department of Labor, <http://www.bls.gov/oes/2003/may/oes536051.htm>, 5 October.
- Bureau of Transportation Statistics (2003), 'US international trade and freight transportation statistics', BTS03-02, Washington, District of Columbia: US Department of Transportation.
- Burke, P.J. (1968), 'The output process of a stationary M/M/s queuing system', *Annals of Mathematical Statistics*, **399**, 1144-52.
- Burke, P.J. (1972), 'Output processes and tandem queues', *Proceedings of the Symposium on Computer-Communications, Networks, and Teletraffic*.
- Bush, G.W. (2004), 'Comprehensive terrorist-related screening procedures', Homeland Security Presidential Directive/HSPD-11, 27 August.
- Chakrabarti, S. and A. Strauss (2002), 'Carnival booth: an algorithm for defeating the computer-assisted passenger screening system', *First Monday*, **7** (10).
- Cho, S., P. Gordon, H.W. Richardson, M. Shinozuka and S.E. Chang (2001), 'Integrating transportation network and regional economic models to estimate the costs of a large urban earthquake', *Journal of Regional Science*, **41**, 39-65.
- Clinton, W.J. (2004), 'Text of former president Clinton's Remarks to the Democratic National Convention', *Washington Post*, <http://www.washingtonpost.com/wp-dyn/articles/A16929-2004Jul26.html>, 4 October.
- CNNMoney (2004), 'Insurance claims to reach billions: the WTC attack could be the costliest manmade disaster', CNN, <http://money.cnn.com/2001/09/12/worldbiz/ins/index.htm>, 9 August.
- Crist, P. (2003), 'Security in maritime transport: risk factors and economic impact', Paris: OECD Directorate for Science, Technology and Industry, Maritime Transport Committee.
- Federal Highway Administration (2004), 'FHWA freight management and operations: Los Angeles Port', US Department of Transportation, http://ops.fhwa.dot.gov/freight/freight_analysis/state_info/california/pb_lax.htm, 27 September.
- Fleming, M. (2004), Public Affairs Officer, Port of Long Beach, personal correspondence, 17 December 2004.
- Flynn, S.E. (2000), 'Beyond border control', *Foreign Affairs*, **79** (6), 57.
- Flynn, S.E. (2002), 'America the vulnerable', *Foreign Affairs*, **81** (1), 60.
- Flynn, S.E. (2004), *America the Vulnerable: How Our Government is Failing to Protect Us from Terrorism*, New York: Harper Collins Publishers.

- Frankle, R.S. (2004), 'Discussion regarding ARACOR products, services and costs', Arlington, VA, July.
- Gerencser, M., J. Weinberg and D. Vincent (2003), 'Port security war game: implications for US supply chains', McLean, VA: Booz Allen Hamilton.
- Johnson, E. (2004), 'Cargo is reviewed several times', *Long Beach Press Telegram*, 11 July.
- Krikorian, G. (2004), 'Ports called "enormous target": about 12 000 containers arrive daily in LA. On average, 43 of them are inspected by hand under the "layered" system of Homeland Security', *L.A. Times*, 26 November.
- Larson, R.C. and A.R. Odoni (1981), *Urban Operations Research*, New York: Prentice-Hall.
- Looney, R. (2002), 'Economic costs to the United States stemming from the 9/11 attacks', Center for Contemporary Conflict, National Security Affairs Department, Naval Postgraduate School.
- Maritime Administration (2002), 'US waterborne foreign trade: containerized cargo, Top 30 US ports, calendar year 2002', Washington, District of Columbia: US Department of Transportation.
- Martonosi, S.E. and A.I. Barnett (2004), 'How effective might security profiling of airline passengers be?', Cambridge, MA: Massachusetts Institute of Technology, submitted for publication.
- McDaniel, B. (2004), 'SAIC's vehicle and cargo inspection system cost and performance', Arlington, VA, July.
- Pelosi, N. and T. Daschle (2004), 'Pelosi and Daschle deliver pre-buttal to State of the Union Address', United States Senate, Office of the Democratic Leader, <http://democrats.senate.gov/~dpc/releases/2004116B38.html>, 4 October.
- Schiesel, S. (2003), 'Their mission: intercepting deadly cargo', *New York Times*, 20 March, G1.
- SST Phase One Report (2003), 'Smart and secure tradelanes Phase One report. Network visibility: leveraging security and efficiency in today's global supply chains', SST Initiative.
- Spencer, C. (2004), 'International supply chain security regulatory programs' presented at McComb School of Business, University of Texas at Austin, 16 October 2003, IMS Worldwide, <http://mba.mcombs.utexas.edu/plus/Academies/BAB/CurtisSpencer.ppt>, 17 August.
- 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, GAO-04-557T, Washington, District of Columbia: General Accounting Office.
- Treaster, J.B. (2004), 'After being bounced around Florida is bouncing back', *New York Times*, 18 September.
- Wasem, E., J. Lake, L. Seghetti, J. Monke and S. Viña (2004), 'Border security: inspections practices, policies, and issues', Washington, District of Columbia: Congressional Research Service, Library of Congress.
- Wein, L.M., A.H. Wilkins, M. Baveja and S.E. Flynn (2003), 'Preventing the importation of illicit nuclear materials in shipping containers', submitted for publication.
- Willis, H. and D. Ortiz (2004), 'A framework for evaluating the security of the global containerized supply chain', TR-214-RC, Santa Monica, CA: RAND Corporation.