MANAGEMENT SCIENCE
Vol. 56, No. 2, February 2010, pp. 219–233
ISSN 0025-1909 | EISSN 1526-5501 | 10 | 5602 | 0219

informs®

DOI 10.1287/mnsc.1090.1105
© 2010 INFORMS

Securing the Containerized Supply Chain: Analysis of Government Incentives for Private Investment

Nitin Bakshi
London Business School, Regent's Park, London NW1 4SA, United Kingdom, nbakshi@london.edu

Noah Gans
The Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania 19104, gans@wharton.upenn.edu

To mitigate the threat that terrorists smuggle weapons of mass destruction into the United States through maritime containers, the U.S. Bureau of Customs and Border Protection (CBP) inspects containers upon entry to domestic ports. Inspection-driven congestion is costly, and CBP provides incentives to firms to improve security upstream in the supply chain, thereby reducing the inspection burden at U.S. ports. We perform an economic analysis of this incentive program, called Customs-Trade Partnership Against Terrorism (C-TPAT), modeling in a game-theoretic framework the strategic interaction between CBP, trading firms, and terrorists. Our equilibrium results highlight the possibility that a properly run program can efficiently shift some of CBP's security burden to private industry. These results also suggest that CBP may have the opportunity to use strategic delay as an incentive for firms to join. Analysis of comparative statics shows that, with increasing capacity, membership in C-TPAT systematically declines.

Key words: game theory; nuclear weapons; container inspections; homeland security; queueing theory; terrorism; principal-agent models
History: Received November 28, 2007; accepted September 18, 2009, by Linda V. Green, public sector applications. Published online in *Articles in Advance* December 14, 2009.

1. Introduction

The volume and value of containerized goods entering the United States through ports is enormous, and it continues to grow.[1] In 2004, $423 billion in goods entered the United States in 15.8 million containers (U.S. Government Accountability Office (GAO) 2007). Almost half of the $2 trillion in international goods transported through the United States in 2000 was shipped in containers, and the international tonnage of trade through the United States is expected to double by 2020 (Greenberg et al. 2006).

Given the large numbers and value of containers entering U.S. ports each year, concern about their use by terrorists is high. Only one of millions of containers need be compromised to cost the United States billions of dollars in lost trade and to endanger thousands of lives. For instance, Abt (2003) estimates that the detonation of a nuclear device in a port may lead to losses in the range of $55–$220 billion. Abt et al. (2003) estimate the economic losses from a similar bio-terrorist attack to be in the range of $15–$40 billion. Using a simulated war game, Gerencser et al. (2003) estimate the economic losses stemming from a coordinated "dirty bomb" attack on U.S. ports to be $58 billion.[2] The reported loss figures do not include the value of lives lost.

The U.S. Bureau of Customs and Border Protection (CBP) is responsible for ensuring the security of U.S. ports against these types of attacks. To promote port security, CBP uses risk management techniques to screen containerized cargo for potential anomalies. Its Automated Targeting System (ATS) assigns a risk score to each container entering U.S. waters and, based on these scores, a fraction of incoming containers is marked for rigorous inspection (GAO 2004). Containers may be subject to inspection at the port of origin, outside the United States, as well as at the port of entry into the United States. The focus of this paper is on the latter.

CBP is charged with securing ports with the least possible hindrance to commerce, and there are inherent economic trade-offs between the frequency and rigor with which containers can be inspected and the speed with which they can be turned around. The more containers inspected and the more time

[1] A container is a sealed, reusable metal box (generally 20′ or 40′ long) in which goods are shipped by vessel, rail, or truck.

[2] A dirty bomb, also called a "radiological dispersal device," combines a conventional explosive, such as dynamite, with radioactive material. When the conventional explosive detonates, it disperses the radioactive material, and the dispersion contaminates the surrounding area.

spent inspecting each container, the smaller the probability of a hazard, such as a nuclear bomb or biological weapon, going undetected. The congestion that results from increased inspection can also be detrimental to trade. In the short run, unanticipated container delays can cause costly supply chain disruptions. For example, Spencer (2004) estimates the cost of delay per day to approach 0.5% of the value of a container. Even in the long run, when inspection-induced delays can be anticipated, the extra pipeline inventory required to accommodate delays can be costly. For example, given an annual flow of $423 billion in goods, a day of pipeline inventory is worth $1.16 billion. At a cost of capital of 15%, that day of pipeline inventory would, in turn, require $174 million per year to finance.

Customs-Trade Partnership Against Terrorism (C-TPAT) is a federal initiative intended to induce private companies to help address this trade-off. Companies that join C-TPAT agree to take specific steps to improve the security of the containers they ship to U.S. ports (GAO 2004). By improving the risk profile of these containers, CBP aims to reduce the number of containers it needs to inspect and, at the same time, reduce the overall level of terrorism-related risks associated with containers entering the United States. Thus, members of C-TPAT bear out-of-pocket security expenses that allow CBP to reduce costs and risks associated with container hazards and inspections.

C-TPAT membership is voluntary, and a central economic incentive for joining the program is the reduction in inspection burden to which members are entitled (C-TPAT Strategic Plan 2004). Another (more speculative) benefit is the prospect that, in the event of a disaster, C-TPAT members would be "at the head of the line" once the target port were to resume operations.

For many companies, the program's benefits appear to outweigh its costs. More than 7,000 companies have joined C-TPAT since its inception in November, 2001 (Basham 2007). A survey of 1,756 C-TPAT members (953 of which were importers), conducted by the University of Virginia on behalf of CBP, found that among the importers, the respondents spent, on average, about $66,353 per year in compliance costs in 2005, as compared to about $35,006 in security-related expenditures during the last full year before joining C-TPAT (Diop et al. 2007). The survey also found that 35.4% of the 814 importers who responded to the question on number of CBP inspections experienced a reduction in inspection frequency, whereas 44.1% reported no change, and 6.6% reported an increase. The remaining 13.9% either did not know the answer or indicated that the question did not apply to them. CBP is encouraged by these results because it has increased inspection levels considerably since September 11, 2001.

At the same time, both trade magazines and federal government reviews of C-TPAT cite widespread dissatisfaction with the program (Keane 2005, GAO 2005). These reviews consistently cite two sets of concerns: (1) the benefits to participating members have not been clearly outlined; and (2) effective validation of security profiles, and regular audit of members to ensure compliance, is lacking.

Even more alarming is the apparent lack of rigor with which security inspections themselves can be conducted. For example, on two occasions journalists from ABC News have managed to ship nuclear material into the United States in cargo containers (Kurtz 2003). Similarly, the GAO reports that its investigators have twice used forged documents to import radioactive material through inland borders (GAO 2006a).

The goal of this paper is to provide a modeling framework to understand the economic trade-offs embedded in container-inspection decisions and to use this framework to analyze policy initiatives such as C-TPAT. For a private company there exists a trade-off between the cost of compliance with C-TPAT and the benefit of reduced congestion costs associated with the inspection of its containers. The United States government faces a trade-off between the security benefit derived from increased inspection of incoming containers and the adverse impact of the resulting congestion. The government must also consider the financial burden stemming from the need for additional security infrastructure. Given the actions of CBP and of trading firms, terrorists trade off the costs and benefits of attempting to infiltrate a container.

We model the interaction between CBP, trading firms, and terrorists as a multiplayer sequential game, using the principal-agent framework. CBP (the principal) acts first, followed by the trading firms (agents) and subsequently the terrorists. CBP first sets the levels of inspection frequency and intensity (rigor), as well as parameters for the audit of members. Trading firms then decide whether or not to join C-TPAT, based on their idiosyncratic costs of complying with the security guidelines laid out in the program. Finally, terrorists choose which set of containers to target for infiltration.

Elementary considerations within our modeling approach imply that members' potential for moral hazard (shirking) requires CBP to audit them for compliance. Further analysis demonstrates that an equilibrium outcome exists and has the following properties:

- A threshold cost of compliance that separates firms that join and do not join C-TPAT.
- An optimal audit policy that can be determined independently of the optimal inspection policy. CBP

imposes the highest permissible penalty on a noncompliant member firm.

We model firms' tolerance for delay using a participation constraint that places an upper bound on a container's expected system wait time. Given this representation, our equilibrium results also include the following:

- The intensity of container inspections drives the surplus of nonmember firms to zero.
- The expected cost to member firms, because of security measures under C-TPAT, varies with their firm-specific compliance costs, and nonmembers end up with a higher expected cost than members.
- For any given (fixed) level of inspection capacity, implementation of C-TPAT results in a reduction in the costs incurred by both CBP and trading firms, relative to a base-case scenario, without C-TPAT.

An analysis of the game's equilibrium outcome also suggests that there may exist cases in which CBP deliberately inspects some containers more frequently than is required for security purposes. This overinspection increases congestion levels and is a means of inducing *strategic delay*. The delay benefits CBP by providing a stronger incentive for trading firms to join C-TPAT.

Comparative statics with respect to inspection capacity show the following:

- An increase in inspection capacity results in lower expected cost of disaster for CBP.
- Surprisingly, increased capacity results in lower C-TPAT membership levels in equilibrium.

The remainder of this paper is organized as follows. Section 2 presents a literature review. Section 3 describes a base-case scenario, without C-TPAT, against which the outcomes of the C-TPAT program can be compared. Section 4 models the principal-agent interactions between CBP and the trading firms and develops our equilibrium results. The role of inspection capacity is analyzed in §5. Finally, we present a brief discussion of the general scope and limitations of our work in §6.

2. Literature Review

Government documents are a comprehensive source for background information on port-security measures, such as C-TPAT, as well as inspection considerations related to border security. Details on C-TPAT can be found in the C-TPAT Strategic Plan (2004). More documents are available on CBP's website. A comprehensive treatment of inspection issues at the various ports of entry into the United States can be found in Wasem et al. (2004). The GAO reports on maritime security (GAO 2004, 2005, 2006a, b) highlight implementation challenges.

Issues relating to port security and container inspections lie in the overlap between public policy and operations management (OM), and researchers from both sides have contributed to the growing literature in the field. Examples of policy work on this issue include Greenberg et al. (2006), Martonosi et al. (2006), and Boske (2006). Examples of the OM approach can be found in Wein et al. (2006, 2007). Our work is closest in spirit to Wein et al. (2006).

Wein et al. (2006) develop and analyze a mathematical model of the entire multilayered port-security system. The paper takes a computational approach to evaluating CBP's optimal inspection strategy when faced with the risk of importation of illicit nuclear material into the United States. Its aim is to prescribe the level of investment (in radiation detection equipment and personnel) required to meet a safety target, given a *predefined* flow of containers to be inspected.

In contrast, ours is an analytical treatment of the strategic interaction—between CBP, trading firms, and terrorists—that *generates* the flow of containers to be inspected. Our treatment is stylized and is at a higher level: it is not concerned with the specific details of the detection of nuclear threats, and our results apply to a broad range of risks, including nuclear, biological, and chemical threats.

Our model has three key components: risk assessment of containers, the impact of inspections on the economics of terrorist activity, and the effectiveness of inspections. We discuss each in turn.

CBP performs a risk assessment for terrorist threats for the entire population of incoming containers and assigns a score, that we refer to as the ATS score, to each individual container.[3] This score is a probabilistic representation of the threat posed by a container. It is generated using manifest information as well as targeting rules that are based on strategic intelligence and anomalies (GAO 2004, Wasem et al. 2004, Bettge 2006). Statistics has a rich literature in screening and classification methodology, including the use of techniques such as ROC (receiver operating characteristic) curves (Fawcett 2006, Marshall and Olkin 1968). For a related treatment in OM, see Shumsky and Pinker (2003). Ours is also an example of a classification problem in which the ATS score is the screening variable used to segment the container population into "high-risk" and "low-risk" categories.

The decision regarding whether or not to inspect a container at the U.S. domestic port is a function of its ATS score. The effectiveness of a container inspection can be measured through the residual probability of risk, post inspection. We use a speed-accuracy tradeoff (SAT) function to associate the expected inspection time with CBP's capacity choice and the residual

[3] ATS is the software used by CBP to help in risk assessment.

risk. Literature on SAT functions includes McClelland (1979), Ghylin et al. (2006), and Hopp et al. (2007).

Finally, we mention three related but distinct streams of literature. First is research on security. Martonosi and Barnett (2006) study airline and passenger security, in which passengers are the analogues of shipping containers. Pinker (2007) studies the interplay between warnings and resource deployment when defending against terrorist attacks. Second is more traditional work on the optimization of container-terminal operations. Steenken et al. (2004) provides a comprehensive survey of this literature. Third is the evolving body of work on managing supply chain disruptions. A few notable contributions on this front include Kleindorfer and Saad (2005), Sheffi (2005), and Tomlin (2006). Lee and Whang (2005) highlight the parallels between quality management and the creation of supply chain security.

3. Port Security and Congestion

In this section, we lay out the key features of port security that are relevant to our analysis. We also discuss the form of the container-inspection policy and its impact on terrorist activity and congestion at ports. The model presented in this section is an abstraction of reality that helps us to generate insights into the trade-offs inherent in the container-inspection problem, as well as to provide a benchmark against which we can judge the effectiveness of C-TPAT.

3.1. Shipping and Inspection Process

The flows of containers belonging to different firms follow a similar pattern. After leaving the shipper's premises, containers are brought to the port of embarkation. From there, they are sent on an ocean-going vessel that visits a U.S. port of debarkation. At this port of debarkation, all containers undergo some form of "passive" screening, a nonintrusive inspection that may include neutron and gamma-ray radiation monitoring. We refer to this stage as *primary inspection*.[4] Based on prior information on the source and handling of the container, as well as the results of these tests, a fraction of these containers is tagged by CBP for more intensive, *secondary inspection*. Secondary inspection can include tests such as gamma and x-ray radiography, as well as a *devanning* of the container for a comprehensive manual inspection. For more details on inspection strategies see, Wein et al. (2006). Finally, when a container is determined to be safe, it is allowed into the country.

3.2. Terrorist Considerations

We model terrorists as rational agents who have the means to infiltrate a container with weapons of mass destruction (WMD). Given that we are considering only large-scale acts of terrorism, we posit that terrorists have the wherewithal to launch only one such attack in the period of interest, e.g., one year.[5] They select a target only among those containers that offer the greatest chance of success. In choosing a container, they trade off the expected benefit from an attack with the cost of planning and execution. In the context of CBP's inspection problem, we model the cost of mounting an attack, c_a, as exogenously specified.

The benefit that terrorists derive from their efforts depends on the eventual disposition of the container. If the contraband *escapes* detection, then it may be used for a large-scale terrorist attack, at which point the United States suffers loss L_e (e for escapes detection). If the contraband is *found* inside a container before it crosses the U.S. borders, then the United States suffers losses L_f (f for found). We note that the discovery of WMD in a maritime container can, itself, trigger economic losses.[6] To avoid trivial results, we assume that $L_e > L_f$.

We also assume that the U.S.'s loss is the terrorists' gain. Note that this is not literally true. For example, if an attack is thwarted, then terrorists may incur a loss of morale and additional costs because of subsequent difficulty in recruitment, effects that may not show up in the computation of L_f. Nevertheless, for the sake of simplicity and analytical tractability, we proceed with this zero-sum assumption.

3.3. Risk Scoring

CBP's Automated Targeting System uses manifest information and targeting rules, based on expert judgment and historical shipment information, to determine the probability that a container poses a high risk, and should be scrutinized thoroughly. ATS scores drive inspection decisions at the port of entry.

We model the ATS score as the product of two factors. First, we let b denote the (exogenously specified) base-rate probability of a terrorist attack in the period of interest. For instance, a recent congressionally mandated report (Graham et al. 2008) estimates a higher than 50% chance of a WMD attack launched by terrorists, over the next five years. Previous estimates include the work by Lugar (2005). We then define the *risk score*, x, to be the conditional probability that,

[4] Recent initiatives suggest that, in the future, primary inspection for most U.S.-bound containers may be completed at the port of embarkation itself (Bakshi et al. 2009).

[5] A different choice for the period of interest would not have a qualitative impact on the insights generated. Because the U.S. security budget is determined annually, working with a one-year horizon seems natural.

[6] For example, there may be a port slowdown or lockdown until the source of the security breach is discovered.

given that a terrorist targets a container for infiltration, the attempt would escape detection by security precautions in place up through the primary inspection at the port of debarkation: $P\{\text{no alarm} \mid \text{threat}\}$. Thus, the ATS score equals bx.

In the analysis that follows, we do not vary the base rate, b, across containers. Our assumption presumes that terrorists have not exogenously decided which containers are more or less likely to be successfully infiltrated. Rather, we explicitly model the terrorists' decision regarding which containers might be most profitably compromised, a decision that depends on the risk score, x. If there were only primary inspection of containers at U.S. shores, the expected benefit to terrorists from targeting a container with risk score, x, would be $xL_e + (1-x)L_f$. The set of containers that the terrorists target for possible infiltration emerges through the equilibrium outcome determined by our analysis, after we have accounted for CBP's inspection strategy at the U.S. ports.

In the exposition that follows, we will assume that $L_e > c_a > L_f$, so that CBP's aim is to eliminate the terrorist threat by reducing terrorists' expected gains to c_a. If $c_a < L_f$, then no amount of inspection will deter terrorists from attempting to infiltrate a container, and the best outcome that CBP could attain would be to find an infiltrated container with probability one. In this case, CBP would analogously aim to reduce terrorists' expected gains to L_f.

If security measures up through primary inspection do not trigger an alarm, then the container is not inspected further. If, however, this condition does not hold, then CBP tags the container for a more intensive secondary inspection.

We define the cumulative distribution function (cdf) of risk scores to be $G_n(x)$, with $x \in [0,1]$. We denote the associated density function as $g_n(x)$. For simplicity, we assume that $g_n(x) > 0$, $\forall x \in [0,1]$. Here, the subscript n is used to signify firms that are not members of C-TPAT. In this section, which analyzes a "base case" without C-TPAT, all firms are nonmembers. In §4, we identify members by using the subscript m.

3.4. Secondary-Inspection Time and Residual Risk

Huizenga (2005) notes that, even though current technology is quite effective in detecting most nuclear material, it is less effective in detecting certain configurations of shielded highly enriched uranium. The diversity of the nuclear threat, in conjunction with often hard-to-detect threats from chemical and biological weapons, requires CBP to determine not only which containers to inspect, but also the rigor of the inspection process for containers identified as risky.

The effectiveness of inspections depends on the time and care with which they are conducted. As we noted in the introduction, Kurtz (2003) and GAO (2006a) report instances in which lax inspections allowed nuclear materials to be clandestinely slipped into the United States. *USA Today* (2007) and Ghylin et al. (2006) note analogous problems with the screening of passengers and baggage at airports.

For containers, the time required for secondary inspections can range widely. For example, the time needed to properly interpret x-ray images may vary. More significantly, the rigor with which a container is "devanned" can extend broadly: from a cursory look inside the back doors, to a more thorough emptying out of a center "aisle" through which inspectors move, to the removal of all contents stored within the container, even to the opening and inspection of the cartons or flats that have been removed.

Thus, a key decision that CBP makes is the extent or rigor of inspection of high-risk containers. We let S denote the time required to perform a secondary inspection and ε denote the residual probability that there exists a hazard that remains undetected after secondary inspection. We then use an SAT function to model expected inspection time as a function of capacity choice and ε:

$$S = \psi(\varepsilon, \kappa) + \phi, \tag{1}$$

where κ represents the appropriately scaled inspection capacity. The random variable, ϕ, has mean zero and variance σ^2, which captures the randomness introduced by container-specific characteristics, such as the type of goods being shipped and the quality of documentation of manifest information. From (1) we have $E(S) = \psi$, and $E(S^2) = \psi^2 + \sigma^2$.

The inspection capacity is meant to represent a composite of equipment and human resources devoted to the secondary-inspection process. In this section and in §4, we assume that κ is fixed. In §5, we then analyze the impact of capacity, κ, on the equilibrium outcome.

We make two mild sets of assumptions concerning the form of $\psi(\varepsilon, \kappa)$. First, time spent on inspection is strictly decreasing in both the residual risk and capacity: $\psi_\varepsilon \equiv \partial\psi/\partial\varepsilon < 0$ and $\psi_\kappa \equiv \partial\psi/\partial\kappa < 0$. To appreciate the motivation for the latter, consider the scenario wherein two inspectors would be able to examine a devanned container faster than just one inspector acting alone, while maintaining the same residual risk, ε, across the two scenarios. Second, for any finite capacity level, κ, we assume that $\psi(1, \kappa) = 0$ and $\lim_{\varepsilon \to 0} \psi(\varepsilon, \kappa) = \infty$.

Remark 1. As an example, consider the following specific functional form for ψ:

$$S = -\frac{\ln \varepsilon}{\kappa} + \phi. \tag{2}$$

This functional form satisfies both of our assumptions. It also is consistent with the classic model for SATs presented in McClelland (1979), as well as with recent higher-level models of speed-accuracy trade-offs used in the OM literature (see Hopp et al. 2007). Similar trade-offs are observed by Ghylin et al. (2006) for the problem of passenger–baggage screening.

3.5. Container Inspection Policy and Congestion

We model a policy in which CBP inspects containers with risk score x, with probability $p(x)$.[7] We represent the fraction of containers that are tagged for secondary inspection by θ_n and observe that

$$\theta_n = \int_0^1 p(x) g_n(x)\, dx. \tag{3}$$

Let Λ denote the "raw" (or "base") arrival rate of containers into a port. Given that containers are marked for secondary inspection with probability θ_n, the resulting effective arrival rate for secondary inspection is $\lambda = \Lambda\theta_n$.

We model the process of secondary inspections as an $M/G/1$ queue, with Poisson arrival rate $\Lambda\theta_n$, service times S, as determined by (1), and expected delay in queue:

$$E(D) = \frac{\lambda E(S^2)}{2(1-\lambda E(S))} = \frac{\lambda(\psi^2+\sigma^2)}{2(1-\lambda\psi)}. \tag{4}$$

The queueing discipline followed is first-come, first-served.

The $M/G/1$ queueing model is an approximation of the real world, where more than one station might process the containers tagged for secondary inspection. This assumption allows us to include an analytically tractable expression for expected delay within our broader economic analysis. Furthermore, in the current context—in which a small number of servers is highly utilized—the single-server assumption is reasonable, as is explained in Kollerstrom (1974) and Wolff (1989, p. 518).

Suppose that firm i incurs an idiosyncratic per-container delay cost, d_i, per unit of time and that the average dollar value per container is r_i for firm i. Then we assume that waiting cost per dollar of revenue, $w = d_i/r_i$, is a constant, for all i. To the extent that delay costs are driven by the cost of capital (and other value-driven factors) such a constant ratio is a natural assumption (for example, see Martonosi et al. 2006).

3.6. Analysis of the Base Case

The base case refers to the scenario without C-TPAT. Containers come into a port at arrival rate Λ and are picked up for secondary inspection at a rate $\lambda = \Lambda\theta_n$. We model the interaction between CBP and terrorists as a Stackelberg game (Laffont and Martimort 2001). CBP acts as the leader and decides its inspection policy first: $\{p(x) \mid x \in [0,1]\}$ and ε_b, the base-case residual risk. Terrorists act next to determine which container to target for infiltration. We assume that CBP and terrorists are risk neutral.

As is typical in the backward induction process that leads to the characterization of an equilibrium outcome in a Stackelberg game, we first determine the "best response" of terrorists. From the terrorists' point of view, it is optimal to target the container that offers them the most favorable prospects. If there is more than one such container, then the terrorists' equilibrium strategy will be to target any one of these containers for infiltration, with equal likelihood. Given a container with risk score x, inspection probability $p(x)$, and residual risk ε_b, the expected benefit to the terrorists from targeting it is

$$x\{p(x)[\varepsilon_b L_e + (1-\varepsilon_b)L_f] + (1-p(x))L_e\} + (1-x)L_f. \tag{5}$$

We next determine CBP's equilibrium strategy. Given capacity, κ, CBP's choice of residual risk, ε_b, then yields an expected inspection time, $\psi(\varepsilon_b, \kappa)$. CBP's objective is to choose an inspection policy, $\{p(x) \mid x \in [0,1]\}$ and ε_b, to minimize the expected losses due to a container harboring a terrorist threat entering a port. Therefore, its objective is

$$\min_{\varepsilon_b, \{p(x) \mid x\in[0,1]\}} \Big[O_P = \max_{x\in[0,1]} x\{p(x)[\varepsilon_b L_e + (1-\varepsilon_b)L_f] \\ + (1-p(x))L_e\} + (1-x)L_f\Big]. \tag{6}$$

Although this objective naturally leads CBP to make ε_b as small as possible, for any choice of $p(x)$, concern for the economic viability of the trading firms that use the port prevent it from simply setting $\varepsilon_b = 0$.

Specifically, firm i is willing to participate in ocean trade as long as, on a per-container basis, the expected cost incurred from inspection-induced congestion is bounded above by some fraction ($\Delta > 0$) of the container's dollar value, r_i: $\theta_n d_i(E(D) + E(S)) \le \Delta r_i$. Because $d_i/r_i = w$, we can rewrite the inequality as

$$\theta_n w(E(D) + E(S)) \le \Delta. \tag{IR$_\text{b}$}$$

The above constraint acts as an upper bound on the expected cost that a firm is willing to bear. It is the natural analogue of the participation or "individual rationality" constraint used in economic theory. We note that one might also consider adding the LHS of (IR$_\text{b}$) to CBP's objective function. In this case, CBP

[7] Another potential degree of freedom is offered by modeling risk-score-specific inspection protocols, $\varepsilon(x)$, but our limited experience with inspection systems suggests that this scheme would be very difficult to operationalize.

would be optimizing social welfare rather than simply minimizing the expected cost of disaster.

The effective arrival rate at the secondary-inspection facility is $\lambda = \Lambda\theta_n$. From (4) we see that ($\text{IR}_\text{b}$) requires that $\lambda(\psi^2+\sigma^2)/(2(1-\lambda\psi))+\psi \le \Delta/(w\theta_n)$, which implies that $\lambda \le 2\Delta/(\sigma^2 w\theta_n)$ must be satisfied for the mean service time to be nonnegative. A sufficient condition for this to be the case is $\Lambda \le 2\Delta/(w\sigma^2)$, and we assume that this condition is met. Similarly, (4), (IR_b), and $\Delta < \infty$ imply that, if $\theta_n > 0$, then $\rho \equiv \lambda\psi < 1$. Thus, any feasible solution, with $\theta_n > 0$, must have a stable inspection queue.

If CBP had enough inspection capacity, then it would inspect each container down to a residual probability, ε_b, that eliminates terrorist threat, or equivalently, $O_P = c_a$, without creating excessive congestion for trading firms. We rule out this possibility by assuming that CBP has limited inspection capacity. This assumption is consistent with the conclusion in the various GAO and media reports that review maritime security. So, for a given inspection capacity (or budget), the optimization problem faced by CBP is as follows:

$$O_P^* = \min_{\varepsilon_b,\,\{p(x)\,|\,x\in[0,1]\}} \{O_P \mid \theta_n w(E(D) + E(S)) \le \Delta;\ 0 \le \varepsilon_b \le 1\}. \quad (7)$$

Our first result characterizes basic properties of the optimal solution.

Lemma 1. *Suppose* $\Lambda \le 2\Delta/(w\sigma^2)$.

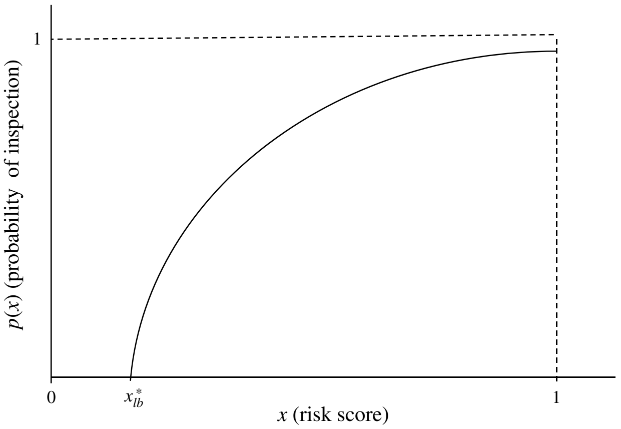
(i) *If* $\exists\, \varepsilon < 1$ *such that* $\psi(\varepsilon, \kappa) < \infty$, *then any optimal solution to* (7) *has* $0 < \varepsilon_b < 1$ *and* $\theta_n > 0$.

(ii) *If, in addition,* $O_P^* > c_a$, *then the* (IR_b) *constraint is binding in the optimal solution.*

Proof. All proofs are in Online Appendix A (provided in the e-companion).[8] □

Part (i) shows that we can always assume that, at optimum, the residual risk, ε_b, and the inspection frequency, θ_n, are interior to the problem boundaries. That is, if CBP has inspection capacity, then it will use it. Part (ii) shows that if CBP does not have enough capacity to drive its expected losses—and the terrorists expected gains—down to c_a, then it will inspect as intensively as possible, consuming all of the trading firms' surplus. To see this, note that for a given level of container traffic, λ, determined by a certain choice of the inspection probabilities, $p(x)$, the LHS of (IR_b) is monotonically decreasing in ε_b. Because the objective function in (6) is increasing in ε_b, for a fixed λ, it would be optimal for CBP to set ε_b to be as low as possible, i.e., to drive the expected cost incurred by a trading firm up to its upper bound.

Figure 1 Optimal Form of the Inspection Probability, $p(x)$, for the Base Case



The fact that (IR_b) is binding in equilibrium allows us to precisely characterize the optimal form of $p(x)$:

Proposition 1. *Let* $\mathscr{A}_b^* \overset{\Delta}{=} \{x \mid x$ *offers the maximum expected benefit to terrorists*$\}$ *and* $x_{lb}^* \overset{\Delta}{=} \inf \mathscr{A}_b^*$. *Suppose* $O_P^* > c_a$ *and that* $\Lambda \le 2\Delta/(w\sigma^2)$. *Then the optimal form of* $p(x)$ *is given by the following*:

(i) $p(x) = \begin{cases} 0 & x \in [0, x_{lb}^*], \\ \dfrac{1 - x_{lb}^*/x}{1-\varepsilon_b^*} & x \in [x_{lb}^*, 1]; \end{cases}$

(ii) $O_P^* = x_{lb}^* L_e + (1 - x_{lb}^*) L_f$;

(iii) $\varepsilon_b^* \le x_{lb}^*$.

If there are multiple solutions that satisfy the conditions in Lemma 1 and Proposition 1, then the solutions with the smallest value of x_{lb}^* are the relevant candidate optimal solutions. This is because we know from Proposition 1 that $O_P^* = x_{lb}^* L_e + (1 - x_{lb}^*) L_f$, which is strictly increasing in x_{lb}^*. Indeed, if the candidate optimal solutions are such that ε_b varies continuously in x_{lb}^*, then, with limited inspection capacity, the optimal solution is unique, with $\varepsilon_b^* = x_{lb}^*$ and $p(1) = 1$.[9] As it stands, we find that the optimal $p(x)$ takes the form depicted in Figure 1.

The intuition behind the choice of the optimal form of $p(x)$ is that CBP tries to equalize its risk exposure across containers, such that the expected benefit offered to terrorists is the same for every container. If the terrorists were not indifferent among the containers, then CBP could lower its expected cost by reducing the value of $p(x)$ for containers that offer lower than maximum expected benefit (and hence would be ignored by terrorists in equilibrium) until either the expected benefit increases to the maximal value, or $p(x) = 0$.

[8] An electronic companion to this paper is available as part of the online version that can be found at http://mansci.journal.informs.org/.

[9] For sufficient conditions under which ε_b varies continuously in x_{lb}^*, see Online Appendix B (provided in the e-companion).

The results of this base case serve as a benchmark with which we compare and contrast the results of the security scenario with C-TPAT, as described in §4.

4. C-TPAT

4.1. Background on C-TPAT

CBP asks C-TPAT members to ensure the integrity of their supply chain security practices and to communicate and verify the security practices of their supply chain partners (GAO 2005). CBP specifies standards, such as infrastructure requirements and procedures to be followed, while preparing a container for shipping. For example, a C-TPAT member may be required to secure its premises with patrols and video surveillance, undertake an extensive exercise in risk assessment and take remedial measures based on the results, use electronic tamper-proof seals on its containers, verify the background of all employees and contractors working for it, and adhere to other guidelines in the program.

4.1.1. C-TPAT and Security-Related Effort. Whether or not a firm joins C-TPAT, it may perform some due diligence of its own accord, to prevent pilferage, ensure visibility of the container during its journey to its destination, or facilitate reconciliation of contents upon delivery. To ensure compliance with C-TPAT guidelines, a firm may need to exert additional effort. We normalize the effort exerted by nonmember firms to be zero and define $\gamma_i \in [0, \infty)$ to be the extra cost per container that firm i incurs to comply with C-TPAT guidelines.

4.1.2. Risk Profile of Members. As in §3, the cdfs $G_m(x)$ and $G_n(x)$ (m for members and n for nonmembers) describe the distribution of risk scores in the container population. The distribution $G_n(x)$ is the same as that in the base case. We assume that the cdfs are differentiable, with corresponding density functions $g_m(x)$ and $g_n(x)$. Once again, we assume that $g_n(x), g_m(x) > 0$, $\forall x \in [0, 1]$.

Given C-TPAT's aim of motivating companies to reduce container risk, we expect the distribution of G_m and G_n to differ, and we assume that $G_m(x) > G_n(x)$, for all $x \in [0, 1)$. This relationship is referred to as a strict first-order stochastic dominance (FOSD) ordering (Shaked and Shanthikumar 1994).

4.1.3. Fraction of Containers Inspected. Whether or not a firm joins C-TPAT, the flow of its containers follows a similar pattern. The fraction of a C-TPAT member's containers that undergo more intensive secondary inspection is represented by θ_m. Likewise, θ_n represents the fraction of a nonmember's containers that are tagged for secondary inspection. The values of θ_m and θ_n are functions of $p(x)$—the probability of tagging a container with risk score x, for secondary inspection—and the density functions $g_m(x)$ and $g_n(x)$, respectively. The value of θ_n is as described in (3), and the value of θ_m is similarly defined as follows:

$$\theta_m = \int_0^1 p(x) g_m(x)\, dx. \tag{8}$$

Observe that, for nondecreasing $p(x)$, the strict FOSD ordering implies that $\theta_m < \theta_n$. We will verify in §4.2 that this is indeed the case for the optimal choice of $p(x)$. Thus, by joining C-TPAT, a firm improves its risk profile, and the improvement leads to a reduction in the fraction of its containers that undergo secondary inspection. The savings associated with this reduction are an important incentive to join.

4.1.4. Audit of Members. To prevent C-TPAT members from shirking (i.e., not exerting the extra security effort required of members), CBP may conduct an audit of member firms. The audit determines whether or not the guidelines laid out in C-TPAT are being diligently followed. Use of damaged electronic container seals, use of contract labor without background checks, and absence of video surveillance at facilities are examples of the types of lapses that might be encountered during an audit. We assume that, once an audit has been undertaken, it can be determined with certainty whether or not a firm has shirked.

CBP audits member firms with an annual relative frequency, q, and it then imposes a penalty if a deviation is discovered. The audit frequency can also be thought of as the fraction of C-TPAT members that are audited in any given time period. We denote the per-container cost of auditing a member firm i as $c_i(q)$, with $c_i'(q) \geq 0$. For example, a firm with an annual volume of container traffic, V_i, incurs an expected cost of audit of $qc_i(q)V_i$, which translates to a per-container expected cost of $qc_i(q)$. Similarly, we let P_i represent the per-container allocation of the penalty assessed should firm i be found to be shirking. (The total penalty is assessed on the firms's container traffic, from the start of the period until the time shirking is discovered, because this is the set of containers that benefited from a lower inspection frequency.) This allows us to account for all costs on a per-container basis. A shirking firm is also relegated to nonmember status for the remainder of the period.[10]

We model audit costs as being borne by trading firms. Specifically, the SAFE Port Act (2006) mandates a pilot for a third-party audit program. Under this scheme, CBP-authorized third-party auditors conduct

[10] An equivalent penalty scheme would be to penalize all of the deviating firm's container traffic in the period of interest, but then allow the firm to sign up as a member again, immediately after failing the audit.

audits, and C-TPAT participants pay for the audits. The third parties need to be audited by CBP in turn. Because only a small fraction of the staff resources are required to audit the auditors, relative to auditing the member firms directly, we make the simplifying assumption that the cost associated with the auditing of third-party auditors is fixed, i.e., it is independent of the membership level in C-TPAT. Hence, we do not explicitly include it in our model.

Such a third-party scheme is attractive to CBP for two reasons. First, with an increasing number of firms signing up for C-TPAT, CBP is falling short of staff required to effectively validate membership and later audit firms (GAO 2005).[11] Second, for political and sovereignty reasons, CBP's auditors do not have access to certain trade lanes in the international supply chain. CBP launched its pilot program for third-party audits in June 2007 (Basham 2007).[12]

4.2. A Principal-Agent Model of C-TPAT

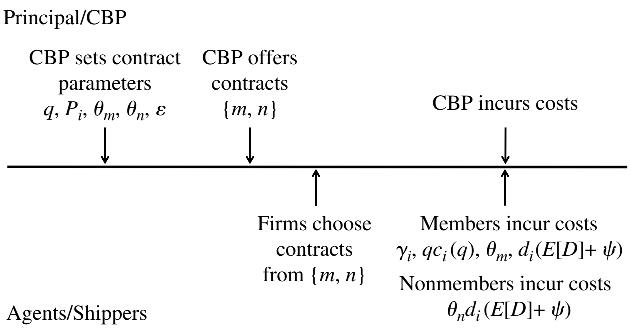
We model the interaction between CBP, trading firms, and terrorists as a multiplayer sequential game. The terrorists act last and their equilibrium strategy is to target one of the containers that offers maximum expected benefit, as explained in the base-case analysis in §3.6. Incorporating the best response of terrorists in this manner, the interaction between CBP and the trading firms can thereafter be thought of as a Stackelberg game in which CBP (the principal) acts as the leader and the trading firms (agents) are followers. Both CBP and the trading firms are assumed to be risk neutral.

CBP first decides on the secondary-inspection frequencies, $\theta_m = \int_0^1 p(x) g_m(x)\,dx$ and $\theta_n = \int_0^1 p(x) g_n(x)\,dx$, the inspection intensity or residual risk, ε, and the audit frequency, q, and penalty, P_i. It then offers the contract $\{q, P_i, \varepsilon, \theta_m\}$ to members and $\{\varepsilon, \theta_n\}$ to nonmembers who use the port facilities.

The inspection parameters are set to minimize the expected cost of disaster from a terrorist attack. The audit parameters are set to ensure that member firms comply with the security-related guidelines prescribed in the agreement. In our model, CBP ensures compliance by conducting audits and then penalizing firms that are found in violation. For every member firm, the expected penalty cost associated with shirking is stiff enough that it outweighs the benefit.

A firm decides whether or not to join C-TPAT, based on its cost of compliance and the expected congestion costs due to secondary inspection. If these costs are not greater than some threshold value that the firm can tolerate, then it will sign up as a member. Moreover, to create appropriate incentives for participation, the total cost incurred by a member firm should be lower than what it would incur as a nonmember.

Figure 2 **Dynamics of the Principal-Agent Stackelberg Game**


Principal/CBP
CBP sets contract parameters q, P_i, θ_m, θ_n, ε
CBP offers contracts $\{m, n\}$
CBP incurs costs
Firms choose contracts from $\{m, n\}$
Members incur costs γ_i, $qc_i(q)$, θ_m, $d_i(E[D]+\psi)$
Nonmembers incur costs $\theta_n d_i(E[D]+\psi)$
Agents/Shippers

A pictorial representation of the sequence of events is presented in Figure 2. The remainder of this section is devoted to a formal mathematical treatment of the interaction described above.

4.2.1. Agent's Problem. The decision of whether or not to join C-TPAT is largely governed by the agents' cost of compliance with the program. Firms with cost of compliance, $\gamma_i \in [0, \infty)$, are faced with two choices: either sign up for C-TPAT at an expected per-container expense of $\gamma_i + qc_i(q)$ and experience an expected system waiting time of $E(D) + E(S)$ with probability θ_m, or remain a nonmember and experience an expected wait of $E(D) + E(S)$ with probability, θ_n. The condition that must be satisfied for a firm to sign up for C-TPAT is therefore

$$\gamma_i + qc_i(q) + \theta_m d_i(E(D)+E(S)) \le \theta_n d_i(E(D)+E(S)). \quad (9)$$

The above condition necessarily requires that $\theta_n \ge \theta_m$. Observe that the expected sojourn time, $E(D) + E(S)$, is the same on both sides of the inequality. Implicitly, we are assuming that each firm is an infinitesimal player, whose individual decisions do not impact the overall congestion levels in the system. This assumption is similar in spirit to the treatment in a Wardrop equilibrium (Altman et al. 2006).

Recalling that the dollar value of revenue associated with a container is r_i for firm i, we now define $\alpha(q) \equiv (\gamma_i + qc_i(q))/r_i$, as member i's cost of compliance per dollar of revenue, or simply the compliance cost. For $\gamma_i \in [0, \infty)$, we see that $\alpha(q) \in [qc_i(q)/r_i, \infty)$. For fixed q, we can also define the cdf $F(\alpha)$ to be the fraction of the total volume of containers shipped to the United States that come from firms with a compliance cost of no more than α. We assume that for any fixed q, $F(\alpha)$ is differentiable everywhere, and $dF(\alpha) = f(\alpha)d\alpha$ represents the relative likelihood that

[11] In CBP's parlance, "revalidation" of C-TPAT membership is equivalent to an audit, as described in this paper.

[12] Similar third-party audit mechanisms have been used successfully in other contexts, such as the promotion of industrial safety and the enforcement of environmental regulations (Kunreuther et al. 2002).

a container comes from a firm with compliance cost α. Implicit here, again, is the assumption that each firm contributes an infinitesimal amount to the cumulative volume of container trade.

For a given $E(S)$ and $E(D)$, let α_t denote a threshold compliance cost (t for threshold), below which (9) is satisfied and above which it is not. In turn, for a given α_t, the fraction of C-TPAT certified containers is $F(\alpha_t)$, which yields the effective arrival rate at the secondary-inspection queue:

$$\lambda = \Lambda[F(\alpha_t)\theta_m + (1 - F(\alpha_t))\theta_n]. \qquad (10)$$

For a given $E(S)$, the substitution of this value of λ into (4) yields the corresponding expression for expected delay, $E(D)$.

As described above, the definitions of α_t and $E(D)$ are circular, because each depends on the other. Nevertheless, we can show that, for given q, θ_m, θ_n, and ε, these two equilibrium quantities are well defined.

Proposition 2. *For given q, θ_m, θ_n, and ε, the threshold compliance cost exists, is unique, and is given by*

$$\alpha_t = (\theta_n - \theta_m)w(E(D) + E(S)). \qquad (11)$$

4.2.2. The Principal's Problem. As before, the principal tries to minimize the expected cost of a disaster:

$$\min_{\varepsilon,\, P_i,\, q,\, \{p(x)\,|\,x\in[0,1]\}} \Big[\max_{x\in[0,1]} x\{p(x)[\varepsilon L_e + (1-\varepsilon)L_f] + (1-p(x))L_e\} + (1-x)L_f\Big]. \qquad (12)$$

The solution to the principal's problem should be such that it provides the appropriate incentives for the agents to participate without shirking.

Participation Constraint for Agents. The participation constraint for nonmembers remains the same as described in condition ($\mathrm{IR_b}$) in the base case. Satisfying ($\mathrm{IR_b}$) is also sufficient to ensure participation of member firms, as is apparent from (9), provided $\theta_n \geq \theta_m$.

Incentive-Compatibility Constraint for Agents. A firm that has signed up for membership in C-TPAT may find it beneficial to shirk by not putting in the effort required for compliance with C-TPAT guidelines while, at the same time, continuing to enjoy reduced congestion costs afforded to members only. An incentive-compatibility constraint ensures that such a situation does not arise. The principal uses audit as a means to achieve incentive compatibility: a member firm i that fails an audit is penalized an amount P_i, which is bounded above by some $B_i < \infty$.

The upper bound, B_i, is set to the benefit accruing to the participating firm from joining C-TPAT. This captures the idea that the penalty cannot be larger than the noncompliant agent's benefit from its false announcement (see Laffont and Martimort 2001, p. 123). We consider a more general upper bound, a constant multiple $\beta(\geq 1)$ of the benefit from noncompliance, minus the cost of the audit itself.[13] A member firm that fails an audit, no matter when it is conducted, forgoes the benefit accrued due to member status and is relegated to nonmember status for the rest of the period. Thus, for $\alpha(q) \in [0, \alpha_t]$, where $\alpha(q) = (\gamma_i + qc_i(q))/r_i$, condition (9), along with incentive-compatibility considerations, implies that for each member firm i:

$$\begin{aligned}\gamma_i + qc_i(q) + \theta_m d_i(E(D) + E(S)) \\ \leq (1-q)[\theta_m d_i(E(D) + E(S))] \\ + q[\theta_n d_i(E(D) + E(S)) + c_i(q) + P_i],\end{aligned} \qquad (13)$$

where

$$0 \leq P_i \leq B_i = \beta(\theta_n - \theta_m)d_i(E(D) + E(S)) - c_i(q). \qquad (14)$$

We assume that β is large enough so that $B_i \geq 0$. Dividing (13) by r_i, we observe that, without audit, $q \equiv 0$, and (13) can be satisfied only for $\alpha = 0$. Thus, without some form of audit (or analogous mechanism), CBP cannot prevent shirking among member firms.

In fact, CBP has an incentive to make the audit penalty, P_i, as large as possible.

Proposition 3. *In equilibrium, $P_i^* = B_i$.*

Thus, at optimum, P_i will achieve its upper bound B_i, or in other words, the penalty for failing an audit is that which recovers any monetary benefit that the firm has enjoyed on account of its membership. In the economics literature, this is known as the *principle of maximal punishment* (see Laffont and Martimort 2001, pp. 121–126). Indeed, a finite upper bound B_i is required to make the audit mechanism reasonable, lest CBP impose an infinite penalty with probability zero.

Using (11), (13), and (14) to simplify the incentive-compatibility (IC) constraint, we obtain

$$\frac{\gamma_i + qc_i(q)}{r_i} \equiv \alpha(q) \leq q(1+\beta)\alpha_t(q) \quad \forall\, \alpha(q) \leq \alpha_t(q). \qquad \text{(IC)}$$

In turn, we have the following:

Proposition 4. *In the Stackelberg game between CBP and trading firms, the optimal fraction of members to be audited is*

$$q^* = \frac{1}{1+\beta} \quad \text{if } \alpha_t(q^*) > 0, \qquad q^* = 0 \quad \text{if } \alpha_t(q^*) = 0.$$

[13] Once a firm is audited, it has to incur the audit cost irrespective of whether or not it failed the audit. This expected cost is already accounted for in the compliance cost.

Proposition 4 implies that the value of the optimal audit frequency, q^*, is independent of the choice of inspection probabilities, $p(x)$, and residual risk, ε. Thus, CBP can fix q^* and then optimize over $p(x)$ and ε alone. Also, given q^*, we have $\alpha \equiv (\gamma_i + q^* c_i(q^*))/r_i$, and the compliance-cost distribution function $F(\alpha)$ is well defined.

Proposition 4 also provides insight into the effectiveness of audit practices. For example, suppose $\beta = 1$, so that the penalty for shirking equals the expected benefit from joining the program. This implies that $q^* = 0.5$, in which case a 50% chance of audit is optimal.

Thus, the optimization problem faced by the principal is

$$O_P^* = \min_{\varepsilon, \{p(x) \mid x \in [0,1]\}} \Big[\max_{x \in [0,1]} x\{p(x)[\varepsilon L_e + (1-\varepsilon)L_f] + (1-p(x))L_e\} + (1-x)L_f\Big],$$

$$\text{s.t.} \quad \theta_n w(E(D)+E(S)) \le \Delta, \qquad \text{(IR)}$$

$$\theta_n \ge \theta_m, \qquad \text{(IC}')$$

$$0 \le \varepsilon \le 1, \qquad \text{(FEAS)}$$

and we obtain an initial characterization of the equilibrium behavior induced by C-TPAT that parallels that of the base case.

Lemma 2. *Suppose $\Lambda \le 2\Delta/(w\sigma^2)$.*

(i) *If $\exists\, \varepsilon < 1$ such that $\psi(\varepsilon, \kappa) < \infty$, then any equilibrium solution has $0 < \varepsilon < 1$ and $\theta_n > 0$.*

(ii) *If, in addition, $O_P^* > c_a$, then the* (IR) *constraint is binding in equilibrium.*

The intuition for this result is similar to that for the result in Lemma 1, and with it we can more completely characterize the optimal form of $p(x)$. To do so, we first define the following quantity:

$$\zeta = \frac{f(\alpha_t)\alpha_t + F(\alpha_t)}{f(\alpha_t)\alpha_t(1-\alpha_t/\Delta) + F(\alpha_t) - 1 - (\Delta\lambda(1-\lambda\psi)/(\theta_n^2 w \Lambda E(D)))}. \qquad (15)$$

Proposition 5. *Suppose $\Lambda \le 2\Delta/(w\sigma^2)$. Let $\mathcal{A}^* \overset{\Delta}{=} \{x \mid x$ offers the maximum expected benefit to terrorists$\}$, and let $x_l^* \overset{\Delta}{=} \inf \mathcal{A}^*$. If $O_P^* > c_a$ then we have the following:*

(i) *$\forall\, x \in \mathcal{A}^*$, $p(x)$ is strictly increasing in x, and*

$$x\{p(x)[\varepsilon L_e + (1-\varepsilon)L_f] + (1-p(x))L_e\} + (1-x)L_f = k, \quad \textit{a constant}. \qquad (16)$$

(ii) *If $\zeta \le 0$, then*

(a) *$\forall\, x \in [0, x_l^*]$, we have $p(x) = 0$;*

(b) *$\forall\, x \in [x_l^*, 1)$, we have $x \in \mathcal{A}^*$;*

(c) *$\forall\, x \in (x_l^*, 1)$, we have $p(x) \in (0,1)$, and the relationship in* (16) *is satisfied.*

(iii) *If $\zeta > 0$, then $\forall\, x \in [0,1)$:*

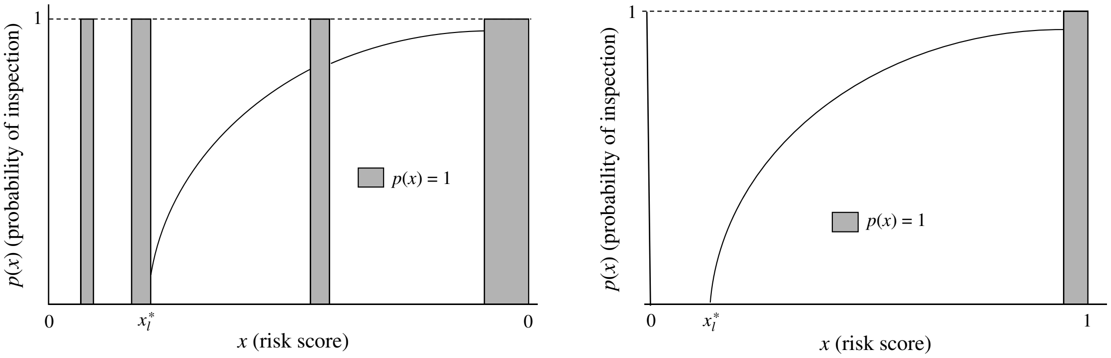
(a) *If $g_n(x)/g_m(x) < \zeta$, then $p(x)$ behaves as in* (ii).

(b) *If $g_n(x)/g_m(x) \ge \zeta$, then $p(x) = 1$.*

(iv) *$\theta_n > \theta_m$.*

The left panel of Figure 3 provides an illustration of the general form of the optimal $p(x)$. Once again, the intuition behind the nature of the optimal form of $p(x)$ is similar to that in the result for the base case in Proposition 1: CBP tries to equalize its risk exposure across all containers to minimize its expected cost of disaster. However, in this case it is possible that CBP makes strategic use of its inspection capacity to influence the membership level in C-TPAT. When $g_n(x)/g_m(x) > \zeta$, an increase in the corresponding $p(x)$ drives up congestion costs for nonmembers relative to members (by increasing $(\theta_n - \theta_m)$ as well as system wait time) by an amount that is large enough to result in a higher threshold compliance cost, α_t, and therefore additional participation (see Equation (11)). If the condition is satisfied, $p(x) = 1$, even though these containers offer less than the maximum expected benefit to terrorists. In this case, the additional membership would benefit CBP enough to offset the additional burden of inspecting containers that are not the terrorists' preferred targets. This would be an instance of the use of strategic delay by CBP (Afèche 2006).

Figure 3 **Optimal Form of Inspection Probability, $p(x)$**



Note. The left panel shows the general case, and the right panel depicts the case in which $g_n(x)/g_m(x)$ has an MLR ordering.

Corollary 1. *Suppose $F(x) > 0$, $\forall x > 0$. If $O_P^* > c_a$, then implementation of C-TPAT results in a strictly lower cost of disaster for CBP and weakly lower costs for the trading firms, relative to the base case.*

This result confirms the economic intuition behind C-TPAT. The main purpose of the program is to transfer the burden of securing the containerized supply chain, in a cost-effective manner, from the congestion-causing step of secondary inspections to security investments by importers further upstream in the supply chain. If implemented judiciously, it ought to be a win-win solution for CBP and the trading community.

Even though we have made progress toward characterizing the optimal solution for the case with strict FOSD ordering between the distribution $G_n(x)$ and $G_m(x)$, we can obtain sharper results if we assume the stronger condition of strict monotone likelihood ratio (MLR) ordering; i.e., $g_n(x)/g_m(x)$ is strictly increasing in x (Shaked and Shanthikumar 1994). The MLR property implies that compliance with C-TPAT *systematically* reduces the distribution of risk across a given company's containers. Assuming that there is not enough inspection capacity to eliminate terrorist threat completely, the nature of the optimal solution is formalized as follows:

Corollary 2. *Suppose $\Lambda \le 2\Delta/(w\sigma^2)$ and that $g_n(x)$ and $g_m(x)$ obey a strict MLR ordering. If $O_P^* > c_a$, at the optimal solution to the principal's problem, the results in Proposition 5 hold, and the following applies:*

(i) *If $\zeta > 0$, then there is at most a single value, x_u^*, such that $0 \le x_l^* < x_u^* \le 1$, and $\forall x \in (x_u^*, 1]$, $g_n(x)/g_m(x) > \zeta$.*

(ii) $O_p^* = x_l^* L_e + (1 - x_l^*) L_f$.

(iii) $\varepsilon^* \le x_l^*$.

The optimal form of $p(x)$ is depicted in the right panel of Figure 3. Here, the set of risk scores for which $p(x)$ might equal 1 is restricted to $x \in (x_u^*, 1]$, i.e., for containers with risk scores such that $g_n(x)/g_m(x) > \zeta$. The intuition for the latter condition is the same as that provided after Proposition 5. Thus, when $g_n(x)$ and $g_m(x)$ follow an MLR ordering, the possible use of over inspection as a means of inducing strategic delay is limited to only the riskiest containers.

Because $O_P^* = k = x_l^* L_e + (1 - x_l^*) L_f$, the principal's objective function is strictly increasing in x_l^*. If there are multiple solutions that satisfy the conditions in Corollary 2, then we can restrict attention to the candidate solutions with the smallest value of x_l^*. Indeed, if ε^* varies continuously in x_l^*, then, assuming $O_P^* > c_a$, the optimal solution is unique, with $\varepsilon^* = x_l^*$, $p(1) = 1$ and $(x = 1) \in \mathscr{A}^*$.[14]

From Corollary 1, we know that implementation of C-TPAT results in lower costs for CBP, relative to the base case, i.e., $x_l^* L_e + (1 - x_l^*) L_f < x_{lb}^* L_e + (1 - x_{lb}^*) L_f$, or effectively, $x_l^* < x_{lb}^*$. This suggests that, when the sufficiency conditions for $\varepsilon^* = x_l^*$ and $\varepsilon_b^* = x_{lb}^*$ hold, C-TPAT results in lower residual risk, $\varepsilon^* < \varepsilon_b^*$, and hence allows for more intensive (longer) secondary inspections, $\psi(\varepsilon^*) > \psi(\varepsilon_b^*)$.

5. Comparative Statics with Capacity

Installed inspection capacity is a crucial determinant of overall security in the containerized supply chain. It can be thought of in terms of the number of customs inspectors available for container inspections at ports, along with the technology infrastructure in place, such as x-ray and gamma-ray scanners. Both more inspectors and better technology can allow for quicker and more precise inspections and thereby enable lower inspection times for a given ε. Although greater capacity can provide for greater security, it is expensive, and a key decision CBP must make is how much to invest.

In this section, we characterize the impact of changes in capacity, κ, on the equilibrium outcome. Using a mix of analytical and numerical approaches, we analyze the sensitivity of our optimal solution to the installed inspection capacity. We use the results of Proposition 5 and Corollary 2 as our starting point. Our first analytic result states the following:

Proposition 6. *Suppose $\Lambda \le 2\Delta/(w\sigma^2)$ and that $g_n(x)$ and $g_m(x)$ obey a strict MLR ordering. If $O_P^* > c_a$, then greater inspection capacity results in a lower expected cost of disaster for CBP, and a lower x_l^*. Furthermore, if for any x_l and x_u that are candidates for the optimal solution in Corollary 2, the corresponding ε varies continuously with x_l, then greater capacity results in*

(i) *higher θ_n and θ_m;*

(ii) *lower C-TPAT membership, $F(\alpha_t)$; and*

(iii) *higher effective arrival rate of containers to inspection facility, λ.*

Online Appendix B characterizes sufficient conditions under which the optimal ε is continuous in x_l. In this case, $\varepsilon^* = x_l^*$ and $x_u^* = 1$. In all of our numerical tests, reported in Online Appendix C (provided in the e-companion), we found that these equalities held.

Thus, for this special case, we find a somewhat surprising outcome: An increase in inspection capacity results in lower C-TPAT membership. The intuition for this result is that greater capacity provides CBP with the ability to inspect a higher volume of containers at the secondary-inspection facility, thereby reducing the need for upstream security measures, as encompassed in C-TPAT.

The gain from the reduction in CBP's expected cost of disaster, due to greater inspection capacity, could be offset by the cost of installing this additional capacity. This notion gives us some insight into how the

[14] For details, refer to Online Appendix B.

optimal capacity can be determined. Given a linear cost of capacity, h, CBP would choose capacity to optimize the following objective: $\min_\kappa[bO_P^* + h\kappa]$. If O_P^* is strictly convex in κ, as with the case in our numerical study, then the overall objective is strictly convex as well, and the first-order condition will specify the optimal capacity level, κ.

6. Discussion and Future Research

We have used a stylized model of port-security operations to obtain insights into the strategic considerations of CBP, trading firms that participate in C-TPAT, and terrorists. Our analysis suggests that, within the context of our model, for any given level of capacity, the program results in an improvement in the costs incurred by CBP and trading firms. Therefore, we can conclude that, even though security mandates might seem to be the easiest way to bolster homeland security, a creative use of economic mechanisms—ones that provide the right incentives for private sector (and individual) participation in security initiatives—may yield important benefits.

At the same time, it is important to remember that C-TPAT's effectiveness is critically dependent on the improvement in the risk profile induced by the supply chain practices included in the program, as well as the efficacy of ATS. These aspects are treated as exogenous to our model. Prospective changes on both of these fronts may lead to new operational challenges and to new opportunities for analysis.

Ideally, we would also consider the case in which CBP optimizes welfare and incorporates trading firms' delay costs directly into its objective function. However, owing to tractability considerations we have left this extension to be analyzed as part of future work with possibly alternative formulations. Another simplification that we have made for analytical tractability is the assumption that the loss accruing to CBP from a terrorist attack (successful or otherwise) is equal to the gain to terrorists from the same attack, thus effectively making the interaction a zero-sum game. The reader would do well to bear in mind these assumptions while interpreting the results of the analysis.

From the trading firms' point of view, the benefits of joining C-TPAT must offset the additional investment required to comply with the security guidelines. In this paper, we focus our attention on the benefit related to reduced inspection frequency. An additional level of benefits pertains to a proposed tiered membership of C-TPAT. The highest performing members of C-TPAT would be eligible to have access to an inspection-free shipping process. This use of expedited processing has been referred to as the "green lane" concept (C-TPAT Strategic Plan 2004). However, implementation of this scheme is contingent on R&D advances and successful rollout of "smart" containers. Challenges remain, and it is yet to be ascertained whether green lanes will ever become a reality (Downey 2006). Also on the horizon is the benefit associated with "restart priority" in the event of port closure due to a disaster. An economic analysis of both of these benefits present further opportunities for future work.

Our analysis generates useful high-level insights by characterizing the nature of the equilibrium outcome. However, the contrasting of our findings with reality presents a challenge in terms of accurately estimating model parameters: the distributions G_n, G_m, and F; the cost of capacity h; etc. Nevertheless, the numerical study in Online Appendix C illustrates how our model might be used to determine an optimal inspection policy. The current inspection frequency for nonmembers is about 5%–6% (Marine Link 2004, McClure 2007), and our numerical results highlight the possibility that the optimal θ_n could be much larger, although not necessarily close to 100%. The current membership level of C-TPAT is about 30% in terms of container traffic (GAO 2008), but it is hard to draw a meaningful comparison with our model results, owing to the estimation problems described above.

Because the audit-policy parameters are determined independently of the optimal inspection policy, these are less affected by difficulty in estimating the true value of the model primitives. Here, we find that a 50% annual audit rate is optimal given $\beta = 1$, which assumes that the only benefit obtained from the program is via reduced inspection. In contrast, CBP plans to revalidate (or audit) the security profile of member firms only once every three years (GAO 2008). It is possible that our ignoring of other benefits of C-TPAT, besides reduced inspection frequency, leads us to find a higher optimal audit rate in our analysis; however, the GAO has also raised concerns pertaining to the inadequacy of CBP's revalidation strategy.

It is also worth noting that the idea of reduced inspections of trusted entities crossing U.S. borders is applicable to other domains besides port security. CBP has trusted traveler programs (e.g., SENTRI, NEXUS) for frequent, low-risk border crossers. The program entitles trusted travelers to expedited inspection at the ports of entry (SENTRI 2006). Analogous to the compliance cost for C-TPAT, these trusted travelers incur a disutility from subjecting themselves to an extensive background check, a prerequisite for enrollment in the program. Similar ideas may be applicable to international mail as well. Although the scope of CBP's mandate for inspections covers international mail (Wasem et al. 2004), it has not yet become a priority issue.

This paper represents one of the first efforts to conduct an economic analysis of the container security problem. This type of analysis may have implications for other inspection problems, though these need not be limited to the context of security alone. We hope that our research encourages further work that not only generalizes our model but explores analogous areas of application as well.

7. Electronic Companion

An electronic companion to this paper is available as part of the online version that can be found at http://mansci.journal.informs.org/.

Acknowledgments

The authors gratefully acknowledge the financial support for this research from the Wharton Risk Management and Decision Processes Center and the U.S. Department of Transportation's intermodal containerized freight security program in partnership with Oklahoma University.

References

Abt, C. C. 2003. The economic impact of nuclear terrorist attacks on freight transport systems in an age of seaport vulnerability. Report, Abt Associates, Cambridge, MA.

Abt, C. C., W. Rhodes, R. Casagrande, G. Gaumer. 2003. The economic impacts of bioterrorist attacks on freight transport systems in an age of seaport vulnerability. Report, Abt Associates, Cambridge, MA.

Afèche, P. 2006. Incentive-compatible revenue management in queueing systems: Optimal strategic delay and other delay tactics. Working paper, Rotman School of Management, University of Toronto, Toronto.

Altman, E., T. Boulogne, R. El-Alzouzi, T. Jimenez, L. Wynter. 2006. A survey of networking games in telecommunications. *Comput. Oper. Res.* **33**(2) 286–311.

Bakshi, N., S. E. Flynn, N. Gans. 2009. Estimating the operational impact of container inspections at international ports. Working paper, The Wharton School, University of Pennsylvania, Philadelphia.

Basham, W. R. 2007. Remarks by CBP Commissioner W. Ralph Basham on Container Security at the Center for Strategic and International Studies. http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/commish_remarks_csc.xml.

Bettge, J. 2006. Private conversation with the authors, November 3. Wharton Risk Management and Decision Processes Center, Philadelphia.

Boske, L. B. 2006. Port and supply chain security initiatives in the United States and abroad. Report, Lyndon B. Johnson School of Public Affairs, The University of Austin, Austin, TX.

C-TPAT Strategic Plan. 2004. Securing the global supply chain: Customs-trade partnership against terrorism. http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf.

Diop, A. D., D. Hartman, D. Rexrode. 2007. C-TPAT: Cost/benefit survey. Report, Center for Survey Research, Weldon Cooper Center for Public Service, University of Virginia.

Downey, L. 2006. International cargo conundrum: How much investment in security is enough? *RFID J.* (Feburary 6).

Fawcett, T. 2006. An introduction to ROC analysis. *Pattern Recognition Lett.* **27**(8) 861–874.

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

Ghylin, K. M., C. G. Drury, A. Schwaninger. 2006. Two-component model of security inspection: Application and findings. 16th World Congress of Ergonomics, IEA, Maastricht, The Netherlands.

Graham, B., J. Talent, G. Allison, R. Cleveland, S. Rademaker, T. Roemer, W. Sherman, H. Sokolski, R. Verma. 2008. World at risk. Report of the Commission on the Prevention of WMD Proliferation and Terrorism. http://www.preventwmd.gov/report/.

Greenberg, M. D., P. Chalk, H. H. Willis, I. Khilko, D. S. Ortiz. 2006. Maritime terrorism, risk and liability. Report, RAND Center for Terrorism Risk Management Policy, Santa Monica, CA.

Hopp, W. J., G. Yuen, S. M. R. Iravani. 2007. Operation systems with discretionary task completion. *Management Sci.* **53**(1) 61–77.

Huizenga, D. 2005. Detecting nuclear weapons and radiological materials: How effective is available technology? Testimony before the House Committee on Homeland Security. http://ftp.resource.org/gpo.gov/hearings/110h/25356.pdf.

Keane, A. G. 2005. Where's the incentive? *Traffic World* (April 11) 12.

Kleindorfer, P. R., G. H. Saad. 2005. Managing disruption risks in supply chains. *Production Oper. Management* **14**(1) 53–98.

Kollerstrom, J. 1974. Heavy traffic theory for queues with several servers I. *J. Appl. Probab.* **11**(3) 544–552.

Kunreuther, H. C., P. J. McNulty, Y. Kang. 2002. Third-party inspection as an alternative command and control regulation. *Risk Anal.* **22**(2) 309–318.

Kurtz, H. 2003. ABC ships uranium overseas for story. *Washington Post* (September 11) A21.

Laffont, J. J., D. Martimort. 2001. *The Theory of Incentives, the Principal-Agent Model*. Princeton University Press, Princeton, NJ.

Lee, H. L., S. Whang. 2005. Higher supply chain security with lower cost: Lessons from total quality management. *Internat. J. Production Econom.* **96**(3) 289–300.

Lugar, R. G. 2005. The lugar survey on proliferation threats and responses. Report by the Chairman, Senate Foreign Relations Committee. http://lugar.senate.gov/reports/NPSurvey.pdf.

Marine Link. 2004. The 5% myth. Accessed August 29, 2008, http://www.marinelink.com/Story/The+5%25+Myth-15423.html.

Marshall, A. W., I. Olkin. 1968. A general approach to some screening and classification problems. *J. Roy. Statist. Soc. Series B* (*Methodological*) **30**(3) 407–443.

Martonosi, S. E., A. Barnett. 2006. How effective is security screening of airline passengers? *Interfaces* **36**(6) 545–552.

Martonosi, S. E., D. S. Ortiz, H. H. Willis. 2006. Evaluating the viability of 100 percent container inspection at America's ports. Report, RAND Corporation, Santa Monica, CA.

McClelland, J. L. 1979. On the time relations of mental processes: An examination of systems of processes in Cascade. *Psycho. Rev.* **86**(4) 287–330.

McClure, G. 2007. How safe are our ports? Accessed August 14, 2008, http://www.todaysengineer.org/2007/Sep/port-security.asp.

Pinker, E. J. 2007. An analysis of short-term responses to threats of terrorism. *Management Sci.* **53**(6) 865–880.

SAFE Port Act. 2006. HR 4954, 109th Congress, http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.4954:.

SENTRI. 2006. Secure electronic network for travelers rapid inspection. U.S. Customs and Border Protection, Washington, DC.

Shaked, M., G. J. Shanthikumar. 1994. *Stochastic Orders and Their Applications*. Academic Press, San Diego.

Sheffi, Y. 2005. *The Resilient Enterprise*, MIT press, Cambridge, MA.

Shumsky, R. A., E. J. Pinker. 2003. Gatekeepers and referrals in services. *Management Sci.* **49**(7) 839–856.

Spencer, C. 2004. International supply chain security regulatory programs presented at McCombs School of Business, University of Texas at Austin, October 16, 2003, IMS Worldwide. http://mba.mccombs.utexas.edu/plus/Academies/BAB/CurtisSpencer.ppt.

Steenken, D., S. Voß, R. Stahlbock. 2004. Container terminal operation and operations research—A classification and literature review. *OR Spectrum* **26**(1) 3–49.

Tomlin, B. 2006. On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Sci.* **52**(5) 639–657.

U.S. Government Accountability Office. 2004. Summary of challenges faced in targeting oceangoing cargo containers for inspection. Report GAO-04-557T. GAO, Washington DC.

U.S. Government Accountability Office. 2005. Homeland security: Key cargo security programs can be improved. Report GAO-05-466T. GAO, Washington DC.

U.S. Government Accountability Office. 2006a. Border security: Investigators transported radioactive sources across our nation's borders at two locations. Report GAO-06-583T. GAO, Washington DC.

U.S. Government Accountability Office. 2006b. Cargo container inspections: Preliminary observations on the status to efforts to improve the automated targeting system. Report GAO-06-591T. GAO, Washington DC.

U.S. Government Accountability Office. 2007. Maritime security: Observations on selected aspects of the SAFE port act. Report GAO-07-754T. GAO, Washington DC.

U.S. Government Accountability Office. 2008. Supply chain security: U.S. customs and border protection has enhanced its partnership with import trade sectors, but challenges remain in verifying security practices. Report GAO-08-240. GAO, Washington DC.

USA Today. 2007. Most fake bombs missed by screeners. (October 17), http://www.usatoday.com/news/nation/2007-10-17-airport-security_N.htm.

Wasem, R. E., J. Lake, L. Seghetti, J. Monke, S. Vina. 2004. Border security: Inspection practices, policies, and issues. Congressional Research Service Report. The Library of Congress, http://fpc.state.gov/documents/organization/33856.pdf.

Wein, L. M., Y. Liu, Z. Cao, S. E. Flynn. 2007. The optimal spatiotemporal deployment of radiation portal monitors can improve nuclear detection at overseas ports. *Sci. Global Security* **15**(3) 211–233.

Wein, L. M., A. H. Wilkins, M. Baveja, S. E. Flynn. 2006. Preventing the importation of illicit nuclear materials in shipping containers. *Risk Anal.* **26**(5) 1377–1393.

Wolff, R. W. 1989. *Stochastic Modeling and the Theory of Queues*. Prentice Hall, Upper Saddle River, NJ.