Securing Containerized Supply Chain through Public and Private Partnership

Mohammad E. Nikoofal
Ted Rogers School of Management, Ryerson University, Toronto, Canada, M5B 2K3, m.nikoofal@ryerson.ca

Morteza Pourakbar
Rotterdam School of Management, Erasmus University Rotterdam, Rotterdam, mpourakbar@rsm.nl

Mehmet Gümüş
Desautels Faculty of Management, McGill University, Montreal, Quebec, H3A 1G5, mehmet.gumus@mcgill.ca

Global trade is seafaring commerce: 90% of traded goods are carried by maritime transport that has become vulnerable to security risks. This has led governments to initiate security programs serving tens of thousands of members worldwide. This paper studies the government's incentive design and the interaction between Customs inspection capacity and the incentives offered in security programs. Using the theory of incentives, we examine the value of a partnership elevating containerized supply chain security. We have developed a sequential game featuring the government, firms, and an adversary. The government selects the inspection capacity and incentives to foster the partnership, namely, an operational benefit in the form of reduced inspection rate, and a security benefit obtained through reductions in the risks of adversarial infiltration. Firms subsequently decide on collaboration level, followed by a strategic adversary's decision to infiltrate. Using the adversary's best response, we show that, in equilibrium, the government ranks all the firms and induces collaboration with only a subset of them. We demonstrate that, in equilibrium, while security incentives may benefit all participants, tailored operational incentives should be offered strictly to foster collaboration. The required condition to implement the inspection-free lane for members is also characterized. Our results also inform practice to help security policymakers understand the underlying interaction between Customs inspection capacity and incentive design in forging collaboration with private firms. In particular, since firms opting for collaboration experience lower inspection rate, this further reduces overall congestion that, in turn, creates positive externality for nonmember firms. Therefore, having excess inspection capacity may yield briefer wait times that could dissuade firms from collaborating.

Key words:
History: Current version: April 23, 2022

1. Introduction

Transporting over 90% of the world's cargo, maritime containers play a massive role in today's global supply chains. This huge volume creates enormous opportunities for illicit actors to infiltrate and abuse this mode of transport. Examples of bad actors include terrorists, smugglers, traffickers and counterfeiters that pose health, security and safety risks to people, firms and infrastructures. With containers undergoing Customs inspections several times throughout their journeys, Customs administrations are at the front line battling these illicit activities. However, Customs alone cannot ensure container safety and security since the physical flow of goods and its related information rest in the hands of companies and supply chains who own the shipments, containers and vessels. Therefore, government agencies must collaborate with private sector firms to improve the security of supply chains. Private companies also rely on intelligence and enforcement resources owned by governments in reducing the probability of disruption in their supply chains, marking the salience of public-private partnerships for risk and security management of global maritime supply chains.

In this paper, we study the World Customs Organization's (WCO) Framework of Standards to Secure and Facilitate Trade (SAFE) as an example of such partnership. The SAFE framework stresses security measures enhancement by prescribing a set of standards for participating firms. These standards entail fulfilling requirements aimed at managing risk and security issues in cargo, processes, personnel and physical assets, among many others (World Customs Organization 2021). This framework for one member state of the European Union is called AEO (Authorized Economic Operator) and has more than 10,000 certified partners (European Committee Taxation and Customs Union 2015). In the U.S. this is known as C-TPAT (Customs-Trade Partnership Against Terrorism) with over 11,000 members (US Customs and Border Protection 2021). The ultimate goal here is to collaboratively establish supply chain security for all parts of the supply chain, from container origin to destination. These programs aim to mitigate the risk of *serious infringements* that include smuggling, those related to Intellectual Property Rights, counterfeiting, terrorist activities, and others (European Commission 2016). Throughout this paper, we refer to the infiltrating party as an *adversary* perpetrating different types of serious infringements.

Because of the voluntary nature of these programs, one of the main challenges is designing an incentive mechanism that encourages parties to implement and comply with the standards laid out in the program guidelines. Carrying out these dictates is costly for companies. One Customs survey found that the three greatest implementation costs exceeding $55,000 arise from: (i) establishing and improving physical security, (ii) setting up and tightening information technology systems and database development, and (iii) paying the salaries and expenses of personnel hired or contracted specifically to implement and manage the program (The Journal of Commerce 2017). Firms thus

seek apparent incentives and immediate benefits to justify the costs of certification and compliance. The benefits accruing to participants could be broadly categorized as two types. First, a certified member is assigned a lower risk score that may reduce the number of Customs checks carried out on their documents and goods at ports of entry (European Commission 2016). Our model calls this *operational benefit*. Second, through regular audits and training offered by governments, certified members benefit from state-owned intelligence resources that better guard their supply chains against possible adversarial infiltration. We call this *security enhancement benefit* in our model.

Operational incentives yield lower waiting and processing times for containers at ports of entry. However, processing time also depends on the availability of inspection capacity. Thus, in order to ensure the effectiveness of these security programs, it is vital to align the Customs' strategic capacity decisions with operational incentives offered to member firms. Too much inspection capacity renders membership operational incentives less effective since all parties, regardless of membership status, enjoy rapid processing at ports of entry. However, a lack of Customs capacity may delay timely cargo clearance while degrading the effectiveness of security programs in detecting and deterring shipments as to serious infringements (The Journal of Commerce 2016).

Strategically, the degree of collaboration between the government and the firm determines the risk of infiltration by adversaries. Specifically, a high level of collaboration between the state and the firm may deter the strategic adversary from infiltration. Meanwhile, low-level collaboration could make a supply chain more susceptible to adversaries. This is supported by evidence-based studies suggesting that adversaries are purposeful agents engaging in adaptive decision processes (Jaspersen and Montibeller 2020, Arin et al. 2011). The main research questions that we strive to address in this paper are:

- How should the operational and security enhancement incentives be best designed to foster collaboration between governments and supply-chain firms? Additionally, how can Customs inspection capacity be optimized to support the incentive mechanism without hindering trade?
- Which firms, and with what characteristics, should be given priority inducement by the government toward collaboration? How should limited public resources be assigned to assist firms for enhancing security status and reducing the likelihood of adversary infiltration?
- How does such collaboration generate value for all public and private parties?

To answer these research questions, we have designed a game-theoretic model with Customs, firms and adversaries as players. Here, Customs first makes a decision on inspection capacity, and the prescription of security requirements that a firm should meet to become a member. Customs also offers both operational and security enhancement incentives to induce compliance with the security program. Then, firms opt whether to become a member or remain a non-member. Member

firms may also enlist security enhancement aid, such as training, offered by Customs. Once the membership status and security level of firms are known, an adversary then decides which firms' containers to infiltrate and with how much effort. Through inspection, Customs can detect and confiscate containers suspicious of serious infringements. When a container escapes detection, this incurs harm to both society and the firm owning the shipment.

A brief preview of our main results is as follows. First, using adversary's best-response function, our developed algorithm finds the optimal subset of firms induced for collaboration based on volume, sensitivity to delay, security level and the impact of successful infiltration. This subset is identified minimizing the total expected cost of congestion plus risk of adversary's infiltration. Second, our results show that the *security incentive*, which is a combination of a firm's investment in security compliance (same cost for all firms) plus the government's security enhancement assistance (may vary by firm), is applied mainly to satisfy member *participation* constraints. Meanwhile, the *operational incentive* acts more as a *screening* tool to help the government induce collaboration on a selective set of firms whenever the security incentive fails to induce. Third, our analyses detect an underlying interaction between inspection capacity and incentive effectiveness. In particular, collaborating firms experience lower inspection rates, further reducing overall congestion that, in turn, creates positive externality for firms declining security partnership. Therefore, if the government wants to induce collaboration from a larger cluster of firms, it must consider cost-benefit implications of inspection capacity versus security and operational incentives. We show that excessive inspection capacity with briefer wait times may dissuade firm membership. Finally, our modeling approach enables the government to assess the scenario of inspection-free shipping for certified members, dubbed the *green lane* concept in the U.S. Customs and Border Protection's strategic plan (The Journal of Commerce 2005). We characterize the conditions leading to firms being so securely defended against adversary infiltration, thus allowing Customs to set the inspection rate equal to zero for them. Our results shed light on the value of security partnership for all firms, including members, non-members and the government.

The rest of this paper is structured as follows. In Section 2, we review the relevant literature. Sections 3 and 4 feature our model and the Customs container risk-scoring process, respectively. Section 5 next models the benchmark problem with no partnership between the government and the firms. In Section 6, we analyze the partnership model, and in Section 7, we compare results of these two sections to generate insights on the value of partnership. Section 8 further extends the model to two other cases, and Section 9 concludes the paper.

2. Literature Review

Globalization of supply chains has increased vulnerabilities to man-made and security disasters. Yet, security management has not received sufficient attention in the academic SCM/OM literature.

Extant literature addresses problems mainly related to terrorist attacks. We refer to Gupta et al. (2020) for a comprehensive review of OM-based research related to the prevention of terrorism. Evidently, *supply chain security management* has become a major concern for both public and private sectors after the disastrous terrorist attack of September 11, 2001. The public is extremely concerned with the susceptibility of transport abuse by illicit actors that might embed weapons of mass destruction in the shipments. The private sector is further concerned with the costs of both assuring the security of supply chains and avoiding potential disruptions associated with actual and threatened activities of adversaries such as terrorists (Lee and Whang 2005).

When it comes to supply chain security, maritime shipment suffers from a huge exposure to security-related risks since its massive volume of container transport offers ample opportunities for illicit actors to infiltrate this mode. Since September 11, 2001, emphasis on boosting port and maritime security has led to responses from many national and international public and governmental agencies such as International Maritime Organization (IMO), World Customs Organization, U.S. Customs and Border Protection (CBP), among others (Willis and Ortiz 2004).

A stream of literature has examined the *role of government* and its associated decisions in securing the containerized supply chains in the presence of a *passive* adversary that is not strategic responding to policies and decisions of public and private parties. Bakshi and Gans (2010) developed an economic model where the state offers firms incentives to improve security upstream in their supply chains in exchange for reduced inspection at ports. Assuming that the adversary may infiltrate into any container, the authors characterized optimal inspection rates of containers as a function of the container risk score. Subject to a limited budget for screening containers under linear modeling of the problem, McLay and Dreiding (2012) aimed to identify the primary security outcome where detection probability is maximized. Other studies have investigated the role of the government in security management, but not necessarily in the context of maritime transport, such as Hausken and Zhuang (2013) and Hausken and Zhuang (2016). Assuming a passive adversary, they have studied problems regarding how the government and firms should form their relationships by exerting safety efforts when exposed to risk of a disaster, including terrorist attacks. In these papers, the likelihood of the disaster hinges on the efforts of both parties mobilized to reduce the negative impact of disaster.

A more relevant stream of literature to our paper has cast the adversary as *strategic* in responding to the decisions and strategies of the securing party, whether public or private. In this line of work, a growing body of literature has studied mainly the logistic problem of resource allocation faced by governments defending themselves against terrorism – often framed as defender/attacker games (Powell 2007, Zhuang and Bier 2007, Golany et al. 2009, Hausken et al. 2009, Shan and Zhuang 2013, Nikoofal and Gümüs 2015, Baron et al. 2018). In this stream of research (Bakir 2011)

and (Bier and Haphuriwat 2011) have featured defender/attacker configurations in the context of maritime transportation. Bakir (2011) presented a game-theoretic model where the government (defender) must allocate resources to secure the container transportation in the presence of a strategic adversary who subsequently observes the actions of the government before opting how to conduct its attack. Results advise how to balance security between non-intrusive inspection capabilities at foreign seaports and the physical security at the destination port.

Bier and Haphuriwat (2011) have examined a similar problem aimed at identifying the right proportion of containers to be screened so that loss to the government (defender) is minimized, highlighting that it may be suboptimal to inspect all containers when lower-level inspection may suffice to deter an attack. Haphuriwat et al. (2011) next extended that model (Bier and Haphuriwat 2011) to identify the required percentage of containers that must be inspected to deter a terrorist from attempting a nuclear attack via container transport. Bagchi and Paul (2017) recently probed the design of the C-TPAT program where the government sets the required program standards and inspection rates for members and non-members, as well as the level of costly espionage effort to detect terrorist activities. They examined the government's allocation of resources between espionage and inspection in securing critical infrastructure, such as a port. Their main results indicated that the government under-spends in espionage relative to the level that could have minimized congestion. Also, membership rate (size) of the program has been shown to depend non-monotonically on the government's policies, such as expenditure on espionage or inspection rates.

To summarize, our paper contributes to the literature in supply chain security by developing a game-theoretical model featuring the government, firms, and a strategic adversary. In our setting, the public and private sectors collaborate under decentralized decision-making to invest in the security of containerized supply chain, with the adversary then endogenously opting on its infiltration plan. We consider compliance requirements and resources needed to enhance security (to characterize optimal *security* incentives), as well as the inspection rate and optimal capacity (to characterize optimal *operational* incentives), as levers for the government to foster collaboration with the firms. To the best of our knowledge, no prior research has developed a game-theoretical model of security partnership against an adversary threat featuring these three strategic players.

3. Model Framework

We model the problem as an interaction among the government, firms (supply chain stakeholders), and an adversary in a sequential game. The orderly timing of events and decisions shown in Figure 1 is described below. We list the notation for all parameters and decisions in Table 1.

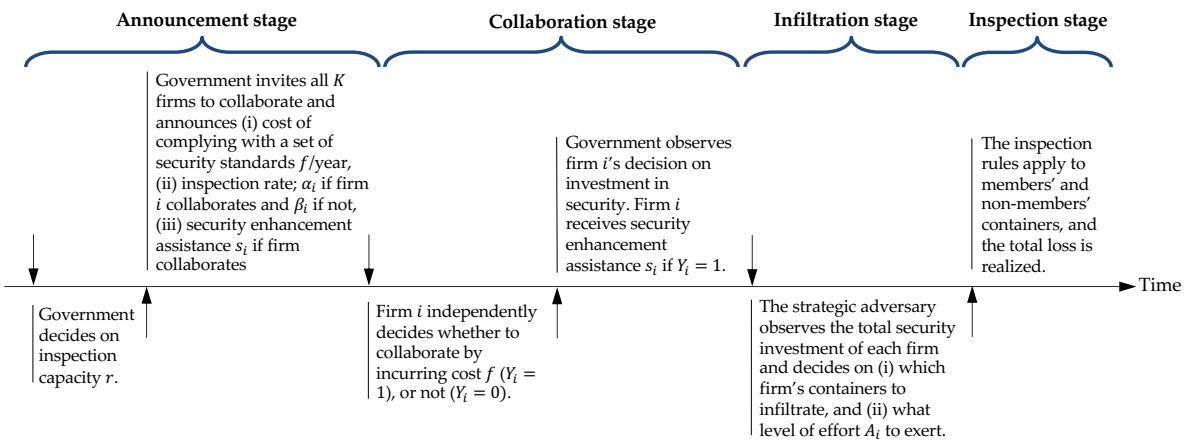

Figure 1 Timing of events and decisions

Table 1 Table of Notation

Decisions	
A_i:	Adversary's level of infiltration on firm i's containers
f:	Annual cost of complying with the security program
s_i:	Government's annual security assistance level allocated to firm i
$Y_i \in \{0,1\}$:	Binary decision variable that takes 1 if firm invests in security to become a member and 0 otherwise
α_i:	Inspection rate for firm i if it becomes a certified member
β_i:	Inspection rate for firm i if it remains a non-member
r:	Capacity of inspection facilities
Parameters	
F:	The annual operational cost of an inspection facility
S:	Government total security assistance budget
λ_i:	Firm i's annual arrival rate
μ:	Service rate of inspection facility
$\mathcal{L}_i$:	Expected loss suffered by firm i if adversary successfully infiltrates through its containers
L:	Expected nationwide loss from adversary attack if an infiltrated container escapes detection
ω:	Waiting cost per container per unit of time to the government
κ_i:	Firm i's delay cost per container per unit of time
γ:	The probability that an infiltrated container escapes detection
z_i:	The inherent security level of firm's supply chain before any security investment
η_i:	Firm i's risk factor
t_r:	Expected waiting time of a container calculated as a function of α_i and β_i for inspection capacity r
Sets	
K:	Set of all firms
M:	Set of all member firms
N :	Set of all non-member firms

– *Announcement stage:* At time zero, the government selects inspection capacity. This broadly comprises, for example, inspection facilities and staff needed to conduct inspection processes. We let r and F, respectively, indicate the inspection capacity and the annual cost per each unit of capacity. In our model, the decision on inspection rate (i.e., operational incentive) is taken after quantifying inspection capacity. This aligns with real-world practice and governmental maritime security strategy. Namely, the priority mission of Customs is to guard the borders and ensure that products entering countries are safe and secure. Still, Customs has limited resources to control borders; inspection capacity and rates should be set so as to not incur onerous burdens on trading firms. In other words, as stated in the U.S. National Strategy for

Maritime Security, securing the supply chains should not result in transportation processes that impair free trade (Department of Homeland Security 2005). Although setting inspection capacity is a long-term strategic decision, inspections rates may need to adjust within abbreviated time spans (e.g., annually) in response to changes in the flow of containers, as well as security and membership enrollment status of firms. We capture these elements using a sequential decision-making process.

The government sets two types of incentives, namely, *security* and *operational* incentives, to lure firms for collaboration. Security incentives embody two components. The first requires firms to incur annual cost f in improving their security levels and becoming certified members. This cost covers the implementation of physical security, the development of information technology systems and databases, and the salaries of personnel hired or contracted to set up and manage the security program. We assume that upon investing f, the security level of the firm improves proportionally to make it more difficult for the adversary to infiltrate its cargo. Thus, a firm benefits from security enhancement by becoming more firmly defended against infiltration compared with a non-member. The second component of the security incentives embodies security assistance offered by the government to member firms. Denoted by s_i, this comprises training, as well as shared expertise and information, offered by the government to member firms. The second incentive type (operational) offers a *reduced inspection rate* for collaborators. Here, the inspection policy for member firm i means inspecting a fraction α_i of its containers, while policy dictates inspecting a fraction β_i of containers should firm i remains non-member, $\alpha_i < \beta_i$.

– *Collaboration stage:* Each firm independently opts whether to enroll under security guidelines or not. We let $Y_i \in \{0, 1\}, i \in K$ be assigned 1 when firm i opts to invest f and become a member, and 0 otherwise. We assume each firm decides on collaboration simultaneously. We define M and N as the sets of member and non-member firms. To capture the collaborative relationship between government and firm, we assume that security incentive s_i is conditional on the firm's decision Y_i through the constraint $0 \leq s_i \leq GY_i$, where G is a big number. In other words, the government may assign s_i to help firm i enhance its supply chain security only when firm i becomes a member, $Y_i = 1$.

– *Infiltration stage*: The adversary responds strategically by observing the security level of each firm, both member and non-member, and then selecting which firm's container to infiltrate. The membership status of firms is public knowledge and can be observed by the adversary as reported in company documents or in related government websites. For instance, the European Commission offers a public query page where the AEO status of companies can be verified. The adversary next decides the level of infiltration effort A_i in order to maximize

its payoff. Rising A_i reflects lower likelihood of Customs detecting infringement. Our model assumes that the adversary chooses the effort level A_i to infiltrate any container of the target firm, aligning with the common assumption in defender-attacker literature (see Bier et al. 2007, Powell 2007, Zhuang and Bier 2007, Nikoofal and Zhuang 2015, Shan and Zhuang 2020, and references therein).

– *Inspection stage*: To carry out container inspection, an inspection rule is executed differentiating inspection rates for members versus non-members. We model the inspection process as $M/M/r$ queuing where the service time for each facility follows an exponential distribution having a service rate μ. Modeling the inspection process as $M/M/r$ queuing offers analytical tractability to compute wait time t_r, given inspection capacity r. Figure 2 illustrates the inspection process.

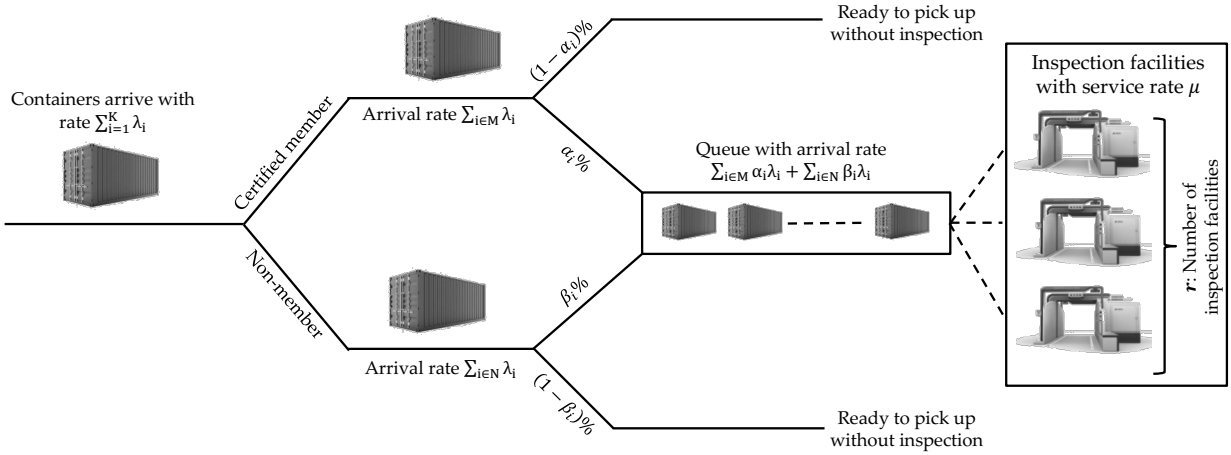

Figure 2 Inspection process and congestion with security partnership

Finally, expected loss for both firms and the government is evaluated. This will be demonstrated in Sections 5 and 6.

4. The Risk Scoring

Once container information such as manifest, bill of lading and invoice are received, Customs performs a risk assessment and assigns a *risk score* to each individual container as a probabilistic representation of the threat posed for that container per U.S. CBP's Automated targeting system (ATS), as well as the World Customs Organization's Cargo Targeting System (CTS). In our model, risk score captures the vulnerability of a container to infiltration considering the government, firms and adversary decisions as a function of the: (i) collaboration level between firm and government, $Y_i \in \{0,1\}$, (ii) firm's investment f in the security program, (iii) government's security assistance s_i in firm i, (iv) inherent security level of firm i's supply chain before joining the security program,

z_i, (v) adversary's infiltration effort on firm i's containers, A_i, and, (vi) firm's risk factor, $\eta_i \in [0,1]$. This risk factor captures the risk level of a container belonging to firm i based on its origin, content, expert opinion, and available intelligence. We let $P_i(Y_i, f, s_i, A_i)$ denote the probability of infiltration, i.e., risk score, given that the adversary targets firm i's container. Thus, any firm's container assigned a positive risk score, i.e., $P_i(Y_i, f, s_i, A_i) > 0$, could be inspected.

We assume that $P_i(Y_i, f, s_i, A_i)$ increases with A_i, but decreases with both f and s_i. Also, $P_i(Y_i, f, s_i, A_i)$ has the following regularity properties: (i) $P_i(Y_i, f, s_i, A_i)$ is twice differentiable with respect to A_i; (ii) $\lim_{A_i \to 0} P_i(Y_i, f, s_i, A_i) = 0$; and (iii) $\lim_{(f+s_i)\to\infty} P_i(Y_i, f, s_i, A_i) = 0$. An appropriate candidate for the probability of infiltration function satisfying the above properties is the cumulative exponential function (Nikoofal and Gümüs 2015, Bier et al. 2008, Gerchak and Safayeni 1996):

$$P_i(Y_i, f, s_i, A_i) = 1 - \exp\left(\frac{-\eta_i A_i}{Y_i(f + s_i) + z_i}\right) \tag{1}$$

Note in Equation (1) that the adversary may infiltrate a non-member's container with less effort than for member cargo, explaining why the state may set stricter inspection rules for non-members. This is also addressed in the US Customs and Border Protection (2021) as the benefits of C-TPAT where security partners are assigned *reductions in their overall cargo risk score*. Such reductions, in turn, translate into fewer examinations at import and export facilities.

5. A Benchmark: Model Analysis without Partnership

Before analyzing the partnership model, we study the problem as a benchmark where the government and firms do *not* form a security partnership and thus firms play a passive role. Figure 3 depicts the inspection process of this problem. The government sets inspection capacity and rates; then, the adversary decides which container to attack. Since the game is played sequentially, we need to work backwards and first solve for the adversary's optimal decision.

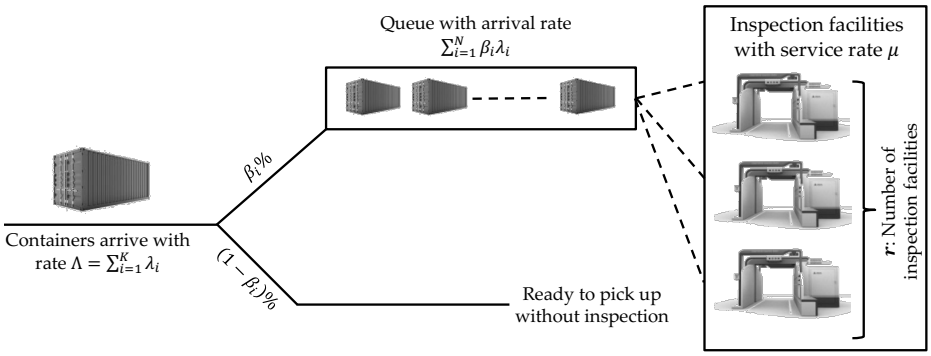

Figure 3 **Inspection process and congestion without security partnership**

5.1. Adversary's Optimization Problem

Suppose the government and firms do not form a partnership; i.e., $Y_i = 0$. Then, firm i's risk score in Equation (1) becomes as follows: $P_i(Y_i, f, s_i, A_i) = P_i(A_i) = 1 - \exp\left(\frac{-\eta_i A_i}{z_i}\right)$. Consequently, the government sees all firms as non-members and sets an inspection rate β_i for each firm i. The adversary next chooses which firm's containers to infiltrate and at what levels of effort A_i to maximize its payoff. Note that the adversary's payoff increases with the: (i) probability of successful infiltration $P_i(A_i)$, (ii) probability of an infiltrated container escaping detection after inspection, γ, and (iii) expected societal loss when an infiltrated container escapes detection, L, all offset by the level of infiltration effort A_i. Given the inspection rate β_i, the strategic adversary seeks to maximize his payoff by launching an attack through firm j's supply chain, where j solves the following equation:

$$j = \arg\max_{i \in K} \Big\{ P_i(A_i) \big[\beta_i \gamma + (1 - \beta_i)\big] \lambda_i L - A_i \Big\}. \tag{2}$$

An infiltrated container can remain undetected with probability $\beta_i\gamma + (1 - \beta_i)$. The first term, $\beta_i\gamma$, is the probability of not being detected during the inspection arising from type II error, γ, of the inspection process. The second term, $(1 - \beta_i)$ is the probability of the container escaping inspection. Here, the expected loss when an infiltrated container escapes detection is $P_i(A_i)\big[\beta_i\gamma + (1 - \beta_i)\big]\lambda_i L$. We normalize the adversary's marginal cost of infiltration effort to 1 and assume that the total cost of attack linearly increases in A_i. By optimizing the adversary's payoff function with respect to A_i, the best response of the adversary to the government's inspection rate is expressed in Lemma 1.

LEMMA 1. *There is a threshold, $\bar{\beta}_i = \frac{\eta_i \lambda_i L - z_i}{(1-\gamma)\eta_i \lambda_i L}$, on the customs inspection rate β_i where the adversary's best response function A_i^{br} is*

$$A_i^{br} = \begin{cases} \frac{z_i}{\eta_i} \ln\left[\frac{\eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)] L}{z_i}\right] & \text{if } \beta_i < \bar{\beta}_i \\ 0 & \text{if } \beta_i \geq \bar{\beta}_i \end{cases} \tag{3}$$

From Lemma 1, we observe that the lone strategic tool for the government to deter an infiltration is through adjusting the inspection rates. Specifically, there is a threshold inspection rate of containers for firm i, $\bar{\beta}_i$, where the government can deter the adversary from infiltrating firm i's containers by setting an inspection rate exceeding the threshold, $\beta_i \geq \bar{\beta}_i$. Here, $\bar{\beta}_i$ increases with λ_i, η_i and L but decreases with z_i. In other words, to effectively deter an adversary, Customs must elevate the inspection rate for a rising arrival rate of containers, risk factor of firm i, or societal loss from infringement. As intuition suggests, the inspection rate should drop as the inherent security of firm i tightens.

5.2. Government's Optimization Problem

Absent security partnership and per the timing of decisions in Figure 1, the government makes two sequential decisions: (i) the inspection capacity r, and (ii) the inspection rate β_i for firm $i \in K$. We use backward induction to frame the government optimization problem.

Given inspection capacity r, inspection rate, β_i, should fulfill the inspection capacity utilization constraint, $\sum_{i \in K} \beta_i \lambda_i < \mu \times r$. This ensures that the expected arrival rate of containers to the inspection facility does not exceed its expected processing rate. The optimal inspection rate of firm i, β_i^*, minimizes the expected loss due to infringement and can be obtained by solving the following Equation (4):

$$\beta_i^* = \arg \min_{\beta_i | \sum_{i \in K} \beta_i \lambda_i < \mu \times r} \underbrace{\left\{ \left[1 - \exp\left(\tfrac{-\eta_i A_i}{z_i}\right)\right] \left[\beta_i \gamma + (1 - \beta_i)\right] L \times I_{i=j} \right\}}_{Z_t\text{: loss due to infringement}} \tag{4}$$

where $I_{i=j}$ is the binary indicator function assigned 1 when firm i's container is attacked by the adversary, i.e., $i = j$, and 0 otherwise (see Equation (2)). A_i is the adversary optimal infiltration effort for target i (see Equation (3)). To minimize the loss due from infringement, i.e., Z_t in Equation (4), the government needs to increase β_j. Note that increasing inspection rate β_j has two effects on Z_t: one indirect and the other direct. First, higher inspection rate β_j reduces adversary effort level A_j^{br} which leads to a decrease in P_j (see Equation (1)). Increasing β_j thus indirectly reduces loss Z_t. Second, high β_j directly reduces the expected damage through $[\beta_j \gamma + (1 - \beta_j)]L$. Therefore, as long as the capacity utilization constraint is met, the government increases β_j for each firm j just enough to either deter the adversary from infiltration completely, or at least minimize the expected damage when it cannot be completely deterred.

Finding the optimal level of inspection rate $\beta_i^*, i \in K$ and plugging them into Equation (5), we can find the optimal level of inspection capacity, r, that minimizes the total cost from congestion. The optimal inspection capacity should be set to minimize loss due to congestion, i.e.,

$$\min_r \underbrace{\underbrace{\sum_{i \in K} \beta_i^* \lambda_i t_r \omega}_{\text{waiting cost to the government}} + \underbrace{\sum_{i \in K} \beta_i^* \lambda_i \kappa_i t_r}_{\text{delay cost to firms}} + \underbrace{r \times F}_{\text{Operational cost}}}_{Z_c\text{: cost of congestion}}. \tag{5}$$

The first and second terms calculate the government's cost of waiting and the delay to firms, respectively. *Waiting cost* is denoted by ω per container per time and includes the generic waiting cost to Customs due to congestion at the terminal, i.e., the costs related to trucks waiting to be loaded at the container terminal. *Delay cost* is firm specific and may depend on the content of a container for firm i being denoted as κ_i per container per unit of time. This delay cost includes,

among others, shortage cost, spoilage cost for perishable goods, and obsolescence cost of fashion products. Government, as a social planner, should minimize these costs. The last term calculates the investment cost toward inspection capacity. Proposition 1 characterizes the equilibrium absent a security partnership:

PROPOSITION 1. *Let* $\bar{\beta}_i = \frac{\eta_i \lambda_i L - z_i}{(1-\gamma)\eta_i \lambda_i L}$ *if* $z_i \geq \gamma L \eta_i \lambda_i$ *and* $\bar{\beta}_i = 1$ *otherwise. Without a security partnership, given inspection capacity* r*, the equilibrium characterization is as follows:*

- *If* $\sum_{i \in K} \bar{\beta}_i \lambda_i < \mu \times r$ *then the optimal inspection rate is* $\beta_i^N = \bar{\beta}_i$*, and* $Z_t = \max_{i|\beta_i=1} \{\gamma L - \frac{z_i}{\eta_i \lambda_i}\}$.
- *If* $\sum_{i \in K} \bar{\beta}_i \lambda_i \geq \mu \times r$ *then*
  - *rank the firms with respect to adversary's preference score* $\mathscr{T}_i^{NP}$ *where* $\mathscr{T}_i^{NP} = L - \frac{z_i}{\eta_i}\left[\frac{1}{\lambda_i} + \ln\left(\frac{\eta_i \lambda_i L}{z_i}\right)\right]$ *such that* 1 *and* H *indicate firm with the highest and the lowest adversary's preference score, respectively. Let* $q = \arg \min_{J=1,\ldots,H} \{\sum_{i=1}^{J} \bar{\beta}_i \lambda_i \geq \mu \times r\}$.
  - *The optimal inspection rate is* $\beta_i^N = \bar{\beta}_i$ *for* $i < q$ *and* $\beta_i^N = 0$ *for* $i \geq q$ *and* $Z_t = L - \frac{z_q}{\eta_q \lambda_q}$.
- *Let* $\mathbf{r} = \min_{r>1} \{r \mid (t_{r-1} - t_r) \sum_{i \in K} \beta_i^N \lambda_i (\omega + \kappa_i) \leq F\}$*. The optimal level of inspection capacity is* $r^N = \mathbf{r} - 1$.

The results of Proposition 1 indicate that when the utilization constraint is not binding, inspection policy is effective in deterring infringement only for firms with a sufficiently high inherent security level, i.e., $z_i \geq \gamma L \eta_i \lambda_i$. For ample inspection capacity, however, a firm's low inherent security level, $z_i \leq \gamma L \eta_i \lambda_i$, makes it susceptible to infiltration where even 100% inspection by Customs may not effectively deter an adversary, i.e. $Z_t > 0$. This emphasizes the importance of the government's design of incentive mechanisms to enhance firms' security levels. Furthermore, where inspection capacity is limited to the point of capacity utilization constraint being binding, then inspection will never effectively deter an adversary. It is because the adversary can always identify and target containers not inspected at a sufficiently high rate. This makes critical the aligning of capacity and inspection policy decisions. This result confirms practical evidence suggesting that a lack of resources has made it difficult for Customs to guarantee cargo security (The Journal of Commerce 2016).

Therefore, as expressed in Proposition 1, the inspection capacity should be set by increasing its level where operational gains from reduced waiting and delay times outweigh the investment costs for greater inspection capacity. This characterization of the equilibrium reveals another interesting insight: inspection rate and capacity reinforce each other since a higher inspection rate demands greater inspection capacity. Therefore, all factors that increase the optimal inspection rate (such as arrival rate, firm-specific risk factor, or expected loss from adversary attack) or decrease this rate, i.e., firm-specific inherent security level, likewise affect the optimal inspection capacity.

6. Analysis of Partnership Model

In this section, we analyze the case where the state and firms may partner to enhance security. In the benchmark model, the government's security policy includes setting only inspection rate β_i. With partnership, however, a government's security policy is redefined as $\mathbf{P} = (\alpha_i, \beta_i, f, s_i)$ where α_i indicates the inspection rate for member firm i (β_i for nonmembers), f is the invested level of security compliance by members, and s_i is the security enhancement assistance assigned to firm i after being certified as a member.

To analyze the model proposed in Figure 1, we apply the Stackelberg equilibrium concept where the government moves first, followed by the firm and finally the adversary. For a sequential game, we can solve the problem backward. We first solve the adversary's decision on which container to infiltrate and at what effort (A_i^{br}) to exert. We then solve the firm's decision ($Y_i \in \{0,1\}$) on whether or not to become a member. Given inspection capacity, r, we then characterize the government's optimal security policy. Finally, we analyze the government's strategic decision to obtain the optimal inspection capacity, r.

6.1. Adversary's Optimization Problem

The adversary strategically responds to actions taken by the government and firms by planning to infiltrate any of firm i^*'s containers that maximizes its payoff:

$$i^* = \arg\max_{i \in K} \left\{ P\left(Y_i, f, s_i, A_i\right) \left[Y_i \left(\alpha_i \gamma + (1-\alpha_i)\right) + (1-Y_i)\left(\beta_i \gamma + (1-\beta_i)\right) \right] \lambda_i L - A_i \right\} \tag{6}$$

The best-response function of the adversary, denoted by A_i^{br}, can be obtained by solving the first-order condition for its payoff function (6) with respect to the infiltration effort A_i:

LEMMA 2. *Given the collaboration level $Y_i \in \{0,1\}$, there are thresholds on the inspection rates of member and non-member firms, respectively, $\bar{\alpha}_i = \frac{\eta_i \lambda_i L - (f + s_i + z_i)}{(1-\gamma)\eta_i \lambda_i L}$ and $\bar{\beta}_i = \frac{\eta_i \lambda_i L - z_i}{(1-\gamma)\eta_i \lambda_i L}$, where the adversary's best response function, A_i^{br}, is given by*

$$A_i^{br} = \begin{cases} \frac{z_i}{\eta_i} \ln\left[\frac{\eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)] L}{z_i}\right] & \text{if } Y_i = 0, \beta_i < \bar{\beta}_i \\ 0 & \text{if } Y_i = 0, \beta_i \geq \bar{\beta}_i \\ \frac{f + s_i + z_i}{\eta_i} \ln\left[\frac{\eta_i \lambda_i [\alpha_i \gamma + (1-\alpha_i)] L}{f + s_i + z_i}\right] & \text{if } Y_i = 1, \alpha_i < \bar{\alpha}_i \\ 0 & \text{if } Y_i = 1, \alpha_i \geq \bar{\alpha}_i \end{cases} \tag{7}$$

From Lemma 2, we note that the adversary's infiltration effort depends mainly on the collaboration level Y_i between the government and firm i, as well as inspection rates α_i and β_i. In addition, Equation (7) indicates that the government can deter adversary infiltration (i.e., inducing A_i^{br} to zero) by raising inspection rates. Specifically for a non-member firm (i.e., $Y_i = 0$), the minimal inspection rate that deters infiltration echoes that in the benchmark case where no collaboration forms. Where

the firm is a member (i.e., $Y_i = 1$), however, the government can impede adversary infiltration with a lower inspection rate than that set for nonmembers, i.e. $\alpha_i \leq \beta_i$ as collaboration boosts the defense level of member firm i by $f + s_i$. This essentially means that collaboration not only helps the government reduce the risk of an adversary infiltrating firms (i.e., security enhancement benefits), but it also streamlines the container flow for the member firms (i.e., operational benefits).

6.2. Firm's Optimal Collaboration Level

Given the best-response function of the adversary, firm i next decides whether to comply with the security program and become a member (see Figure 1) or remain non-member. This decision is made solving the following optimization problem:

$$\min_{Y_i \in \{0,1\}} \; Y_i \Big[\underbrace{f}_{\substack{\text{cost of} \\ \text{compliance}}} + \underbrace{\alpha_i \lambda_i t_r \kappa_i}_{\text{delay cost}} + \underbrace{[\alpha_i \gamma + (1-\alpha_i)] P(Y_i = 1, f, s_i, A_i) \mathcal{L}_i}_{\text{loss to the firm due to adversary infiltration}} \Big] + (1 - Y_i) \Big[\underbrace{\beta_i \lambda_i t_r \kappa_i}_{\text{delay cost}} + \underbrace{[\beta_i \gamma + (1-\beta_i)] P(Y_i = 0, f, s_i, A_i) \mathcal{L}_i}_{\text{loss to the firm due to adversary infiltration}} \Big] \quad (8)$$

where the probability of infiltration $P(Y_i, f, s_i, A_i)$ can be expressed by substituting the adversary's best-response function characterized from Lemma 2 into Equation (1) as follows:

$$P(Y_i, f, s_i, A_i) = \begin{cases} 1 - \frac{z_i}{\eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)] L} & \text{if } Y_i = 0, z_i < \eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)] L \\ 0 & \text{if } Y_i = 0, z_i \geq \eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)] L \\ 1 - \frac{f + s_i + z_i}{\eta_i \lambda_i [\alpha_i \gamma + (1-\alpha_i)] L} & \text{if } Y_i = 1, f + s_i + z_i < \eta_i \lambda_i [\alpha_i \gamma + (1-\alpha_i)] L \\ 0 & \text{if } Y_i = 1, f + s_i + z_i \geq \eta_i \lambda_i [\alpha_i \gamma + (1-\alpha_i)] L \end{cases} \quad (9)$$

For ease of exposition, we define $\delta_i = [\beta_i \gamma + (1-\beta_i)] P(Y_i = 0, f, s_i, A_i) - [\alpha_i \gamma + (1-\alpha_i)] P(Y_i = 1, f, s_i, A_i)$ as measuring the reduction in expected loss due to adversary infiltration of firm i's containers when it becomes a member and invests in security compliance. The following proposition characterizes firm i's optimal collaboration decision:

PROPOSITION 2. *Given the government's announcement on α_i, β_i, s_i, and f, then*

– *Firm i's optimal collaborative level is:*

$$Y_i^* = \begin{cases} 1 & \text{if } f \leq \underbrace{(\beta_i - \alpha_i) \lambda_i t_r \kappa_i}_{\text{Operational benefit}} + \underbrace{\delta_i \mathcal{L}_i}_{\text{Security enhancement benefit}} \\ 0 & \text{otherwise} \end{cases} \quad (10)$$

– *Given the compliance decision by all firms, then, in equilibrium, there is no profitable deviation for firm i by unilaterally changing his compliance decision Y_i.*

From proposition 2, we note that firm i opts whether to collaborate or not by comparing the cost of collaboration (i.e., f) versus its benefit (i.e., $(\beta_i - \alpha_i)\lambda_i t_r \kappa_i + \delta_i \mathcal{L}_i$). There are two types of benefits: (i) *operational benefit* that is proportional to the relative difference between waiting costs with and

without collaboration, and (ii) *security enhancement benefit* yielded through improved security. Once a member adheres to the standards outlined in the security program, then expected future damage from security incidents is reduced. This security enhancement benefit is captured by $\delta_i \mathcal{L}_i$.

6.3. Government's Optimization Problem

Beyond the non-partnership benchmark analysis where the only security decision is to select inspection rate β_i, the government's optimization problem under a security partnership means solving for the optimal values of the following interrelated decisions that induce the best level of collaboration among firms: the optimal levels of inspection rate for members (α_i) versus non-members (β_i)[1], the security compliance level (f), and the government security enhancement assistance (s_i) that minimize loss due to adversary's infiltration threat, all given by:

$$\begin{aligned} \mathbf{P} = \arg \min_{\alpha_i, \beta_i, f, s_i} & \underbrace{P\left(Y_i, f, s_i, A_i\right)\left[Y_i\left(\alpha_i \gamma + (1-\alpha_i)\right) + (1-Y_i)\left(\beta_i \gamma + (1-\beta_i)\right)\right] L \times I_{i=j}}_{Z_{\mathrm{t}}\text{: loss due to adversary infiltration}} \\ s.t. \quad & \sum_{i \in M} s_i \leq S \\ & \sum_{i \in N} \beta_i \lambda_i + \sum_{i \in M} \alpha_i \lambda_i < r \times \mu \end{aligned} \tag{11}$$

where $I_{i=j}$ is the binary indicator variable that takes 1 if firm i's container is chosen by the adversary, and 0 otherwise, and where $P\left(Y_i, f, s_i, A_i\right)$ can be determined from Equation (9). Note that the key step in characterizing the government's security policy is to determine the subset of firms that may be induced for collaboration. To start, let us assume that there is no firm who opts for collaboration. This can be easily achieved by setting $\alpha_i = \beta_i$ with f sufficiently large. In order to characterize which firm would be induced for collaboration, we must first identify adversary's most preferred target. This is characterized in the following Lemma:

LEMMA 3. *Among all non-member firms, N, the adversary targets firm $j = \arg\max_{i \in N} \{\mathscr{T}_i^P\}$, where*

$$\mathscr{T}_i^P = [\beta_i \gamma + (1-\beta_i)] L - \frac{z_i}{\eta_i}\left[\frac{1}{\lambda_i} + \ln\left(\frac{\eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)] L}{z_i}\right)\right] \tag{12}$$

Note Lemma 3 provides a score $\mathscr{T}_i^P$, namely, "*adversary preference score*", that enables the government to rank non-member firms for collaboration in decreasing order in terms of $\mathscr{T}_i$. As we will later see, this yields an efficient iterative procedure where at each step the government may cut the expected infringement loss by inducing collaboration with the most preferred target. With rankings set for candidate firms to be induced by the government, we next identify the conditions where a partnership between firms and the government can be established. With j indicating the

[1] For expositional purpose, we detail the relationship among t_r, α_i, β_i, and the firms' collaboration decisions in the appendix.

firm with the highest adversary preference score, the government's policy decision should satisfy the following two constraints to induce collaboration on firm$j$:

$$f \leq (\beta_j - \alpha_j)\lambda_j t_r \kappa_j + \delta_j \mathcal{L}_j \tag{13}$$

$$f + s_j \geq \eta_j \lambda_j [\alpha_j \gamma + (1 - \alpha_j)]L - z_j \tag{14}$$

The first constraint (13) is a *participation constraint* to ensure that collaborating firm j's payoff is larger than that without collaboration as characterized in Proposition 2. Constraint (14) is a *deterrence constraint* derived from Equation (9) ensuring that the both level of security assigned to firm j (i.e., $f + s_j$) and the inspection rate α_j suffice to deter adversary infiltration of firm j cargo. Since the state's security budget is limited, we can show that both the participation and deterrence constraints are binding in equilibrium, thus allowing us to characterize the cost of compliance f and security enhancement assistance s_j for firm j. The level of security compliance f that satisfies firm j's participation may also incentivize other firms to participate. According to Proposition 2, a non-member firm i will have an incentive to collaborate as long as the total benefit of collaboration exceeds the cost of compliance, i.e., $f \leq (\beta_i - \alpha_i)\lambda_i t_r \kappa_i + \delta_i \mathcal{L}_i$. In this regard, two types of firms arise. The first type enjoys a high security benefit from collaboration regardless of operational benefit. The second type corresponds to the firms where the security benefit is too small to cover the cost of compliance, casting the decision to collaborate on sufficiently value-added operational benefit. Proposition 3 below characterizes the government's decisions required to induce firm j for collaboration, as well as the subset of firms (denoted by M_j) whose participation constraints would also be satisfied once firm j is induced for collaboration:

PROPOSITION 3. *Let $j \leftarrow \arg\max_{i \in N} \{\mathscr{T}_i\}$ denote the firm with the highest adversary preference score among all the non-members. Given inspection capacity r, find $\beta_i = \beta_i^N$ in proposition 1. Then, in equilibrium,*

- *The government security policy that induces firm j for collaboration is as follows:*
  - *If $\kappa_j \leq \frac{\eta_j L(1-\gamma)}{t_r}$ then $f = \delta_j \mathcal{L}_j$, $\alpha_j = \beta_j$, and $s_j = [\eta_j \lambda_j [\beta_j \gamma + (1 - \beta_j)]L - z_j - f]^+$.*
  - *If $\kappa_j > \frac{\eta_j L(1-\gamma)}{t_r}$ then $f = \beta_j \lambda_j t_r \kappa_j + \delta_j \mathcal{L}_j$, $\alpha_j = 0$, and $s_j = [\eta_j \lambda_j L - z_j - f]^+$.*
- *The list of firms who opt for collaboration, i.e., M_j is as follows:*
  - *If $\mathcal{L}_i \geq \eta_i \lambda_i [\beta_i \gamma + (1 - \beta_i)]L$ then firm i opts for collaboration (i.e., $i \in M_j$), receives inspection rate $\alpha_i = \beta_i$, and security enhancement assistance $s_i = [\eta_i \lambda_i [\beta_i \gamma + (1 - \beta_i)]L - z_i - f]^+$.*
  - *If $\mathcal{L}_i < \eta_i \lambda_i [\beta_i \gamma + (1 - \beta_i)]L$ then firm i opts for collaboration (i.e., $i \in M_j$) iff $\kappa_i \geq \frac{f - \delta_i \mathcal{L}_i}{\beta_i \lambda_i t_r}$, under which the firm receives inspection rate $\alpha_i = \beta_i - \frac{f - \delta_i \mathcal{L}_i}{\lambda_i \kappa_i t_r}$, and security enhancement assistance $s_i = [\eta_i \lambda_i [\alpha_i \gamma + (1 - \alpha_i)]L - z_i - f]^+$.*

The government's security policy prescribes the adversary's deterrence for: (i) the firm with the highest adversary preference score, i.e. firm j, and (ii) others joining the security program,

firm i, $i \in M_j$. Proposition 3 characterizes conditions in terms of incentive type, delay cost, and infiltration loss for both firm j, and firm i, $i \in M_j$ where these conditions suffice to deter the adversary. For firm j, the deterrence condition depends on its delay cost, κ_j. A sufficiently small κ_j makes a firm indifferent to the inspection rate. Here, the only relevant incentive is the security enhancement benefit where firm j invests f to harvest the security enhancement benefit $\delta_j \mathcal{L}_j$. Next, the government must assign security assistance s_j to ensure adversary deterrence for this firm. Yet, when κ_j is sufficiently high, firm j invests f to benefit from both operational and security enhancement benefits. When the government assigns s_j to securely defend this firm, we have $\alpha_j = 0$.

Next considering other members, i.e., firm i, $i \in M_j$, the deterrence condition depends mainly on the loss incurred due to successful infiltration. These firms are offered an inspection rate lower than that for non-members only when this loss is sufficiently low and the delay cost is sufficiently high. When the loss is sufficiently low, the merit of security enhancement benefit for the firm decreases. Under sufficiently high delay cost, the firm would prefer to benefit from a reduced inspection rate.

Further results can be drawn from Proposition 3. First of all, when the level of security benefit exceeds the cost of compliance, the firm collaborates and the government need not offer any operational benefit: $\alpha_i = \beta_i$. Note that providing operational benefit here (i.e., $\alpha_i < \beta_i$) may lower t_r, making it costly for the state to incentivize non-member firms to collaborate. Per Proposition 2, lower t_r curtails f. Consequently, additional security assistance s_i is required to make member firms safe. This same argument applies to inspection capacity r: elevated r reduces t_r, and the consequent value of operational benefits accrued by member firms also fades. To counter, the government must increase the level of security assistance to incentivize firms to collaborate on making the maritime supply chain more secure. Therefore, as long as the security benefit covers the cost of compliance, the state is better off not offering the operational benefit, i.e., $\alpha_i = \beta_i$. However, if the amount of security benefit due to collaboration is less than the cost of compliance, then the firm would collaborate only when the unit delay cost κ_i is relatively high. Here, the state may provide operational benefit to make the collaboration break-even for the participant. This latter observation helps characterize the required conditions to implement the inspection-free lane where the member can ship with no inspection, i.e., $\alpha_i = 0$. We detail such conditions in the next corollary:

COROLLARY 1. *A firm would qualify for inspection-free lane if it is*
- *firm j, with the highest adversary preference score, and $\kappa_j > \frac{\eta_j L(1-\gamma)}{t_r}$.*
- *firm $i \in M_j$ with $\mathcal{L}_i < \eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)] L$ and $\delta_i \mathcal{L}_i + \beta_i \lambda_i \kappa_i t_r = f$.*

Clearly, there are two types of members who may qualify to ship using the inspection-free lane. The first is the firm with the highest adversary preference score (i.e., firm j in Proposition 3) having

sufficiently high delay cost. Note that inducing collaboration with firm j having high delay cost lets the government also set a high value of f (according to Proposition 3 where $f = \beta_j \lambda_j t_r \kappa_j + \delta_j \mathcal{L}_j$). Not only does this yield a higher contribution of firm j in its security investment, it also reduces the government's total contribution to membership security investment since f is a common cost that every participant incurs. Hence, astutely offering the inspection-free lane to firm j curbs the government's total investment in security $\sum_{i \in M_j} s_i$. The second member type is firm i who sees a low level of security enhancement benefit from collaboration when $\mathcal{L}_i$ is sufficiently low. To convince such a firm to collaborate and invest f in costly security compliance, the government must therefore offer a significant amount of operational benefit by setting $\alpha_i = 0$.

6.4. Optimal Clustering Algorithm

For members clustered in set M_j per proposition 3, the government must allocate security assistance resources S to ensure that the adversary is deterred. This means that the adversary would launch its container attack on a non-member firm belonging to $M_j^c = K - M_j$. To further reduce loss due to adversary infiltration, the state should next induce collaboration on the adversary's most preferred firm among non-members, namely $j+1 \leftarrow \arg\max_{i \in M_j^c} \{\mathscr{T}_i\}$. This requires adjusting cost of compliance f to make collaboration beneficial for firm $j+1$. Similar to our earlier discussion, the level of new security compliance f that satisfies firm $j+1$'s enrollment may incentivize other firms to join; this specifically includes firm j with its higher adversary preference score based on the original cluster roster. Considering the limit of available security assistance resources S, one can further adjust the security compliance f to lure a larger cluster of firms finding it beneficial to collaborate. Repeating the same process until all firms are induced for collaboration yields the next Algorithm:

Algorithm 1. Clustering Algorithm for Collaboration:

1. **(Initiation)** Let $N = K$. Find $\beta_i, \forall i \in N$ from Proposition 3.
2. **(Prioritization)** Let $j = 1$, $j \leftarrow \arg\max_{i \in N} \{\mathscr{T}_i\}$.
3. **(Clustering)** Find the security compliance f, the list of participants M_j and the inspection rate $\alpha_i, i \in M_j$ from proposition 3. Let $M_j^c = N - M_j$.
   - **If** $M_j^c = \emptyset$ **then** Let $\zeta = j$ and stop. The clusters are $M_1, M_2, ..., M_\zeta$.
   - **else** Let $j = j+1$, $j \leftarrow \arg\max_{i \in M_j^c} \{\mathscr{T}_i\}$, and go to **Clustering** step.

The above algorithm helps significantly trim the number of potential clusters that can be induced for collaboration in equilibrium. Accordingly, one must rank all firms with respect to $\mathscr{T}_i$, induce them one-by-one for collaboration in decreasing order, and identify others prone to collaborate. Once we identify all the clusters, we can then find the government's total damage as the summation of loss due to adversary infiltration Z_t, plus that due to congestion Z_c. Given inspection capacity r, the *optimal* cluster is thus the one that minimizes total cost:

PROPOSITION 4. *Given the inspection capacity r, and the clusters $M_1, M_2, ..., M_\zeta$ constructed by Algorithm 1, the optimal cluster $\mathscr{M}^r$ can be found by solving the following minimization problem:*

$$\mathscr{M}^r = \arg\min_{i=1,\dots,\zeta} \{Z_{t|M_i} + Z_{c|M_i}\}$$

where $Z_{t|M_i} = [\gamma L - \frac{z_j}{\eta_j \lambda_j}]$ *and* $j \leftarrow \arg\max_{i \in M_i^c} \{\mathscr{T}_i\}$, *and*

$$Z_{c|M_i} = \underbrace{t_r \omega \Big[\sum_{i \in M_i} \alpha_i \lambda_i + \sum_{i \in M_i^c} \beta_i \lambda_i \Big]}_{\text{waiting cost}} + \underbrace{t_r \Big[\sum_{i \in M_i} \alpha_i \lambda_i \kappa_i + \sum_{i \in M_i^c} \beta_i \lambda_i \kappa_i \Big]}_{\text{delay cost}} + \underbrace{r \times F}_{\text{Operational cost of inspection capacity}} \quad (15)$$

Note that Proposition 4 characterizes the optimal cluster of firms to be induced for collaboration for a given inspection capacity r. Here, an upper bound for the optimal inspection capacity in the partnership model echoes the optimal inspection capacity in the non-partner benchmark model, i.e., r^N characterized in proposition 1. Since the inspection rate for all firms in the partnership model is less than that without partnership ($\alpha_i \leq \beta_i$). We can now find the optimal inspection capacity in a partnership model:

COROLLARY 2. *In the partnership model, the optimal level of inspection capacity is*

$$r^P = \arg \min_{r=1,\dots,r^N} \{Z_{t|\mathscr{M}^r} + Z_{c|\mathscr{M}^r}\}.$$

Before characterizing the value of a security partnership, we next apply our clustering algorithm to an instance constructed based on container transport data for a number of firms entering the U.S.

6.5. An Illustrative Numerical Example

In this section, we apply Algorithm 1 to the data for the top 10 U.S. importers that transport via ocean container (The Journal of Commerce 2018) as presented in Table 2. We use the estimates provided in Martonosi et al. (2007) for the costs of delay κ_i per TEU-hour. Specifically, we assign \$6 per TEU-hour to represent 0.5 percent value per day costs of a \$30,000/TEU shipment, and \$60 per TEU-hour to reflect time-sensitive (perishable) cargo. We use the average abnormal stock returns as reported in Hendricks and Singhal (2005) to estimate a firm's loss from adversary infiltration. Hendricks and Singhal (2005) have shown over three-year time periods the average abnormal stock returns of firms that experience disruptions to be near -40%. We further assume the same level of inherent security for all firms equal to $z_i = \$200,000\ \forall i$, which is the amount that Hasbro spent to become C-TPAT compliant (Rice and Caniato 2003). Using these estimates, we next operated Algorithm 1 for two values of inspection capacity r, where r is set low $(r = 1)$ and high $(r = 5)$, to generate potential clusters. We present results in Table 3 where we identify cluster firms, as well as which receive security enhancement benefits (denoted in column SB) and/or operational benefits (denoted in column OB). The following observations emerge:

Table 2 Top 10 US Importers, 2017 (The Journal of Commerce 2018)

Firm	Category of Import	Volume (TEUs)	Delay Cost ($/TEU-hour)	Stock Price ($)
Wal-Mart	Apparel and footwear	874,800	6	99
Target	Clothing, health and beauty, electronics	590,300	6	81
Home Depot	Home renovation and construction	388,000	0	177
Lowe's	Home improvement and appliance	287,500	0	94
Dole Food	Fruit and vegetables	220,200	60	13
Samsung	Electronics	184,800	6	2,200
Dollar Tree	Housewares, Toys, Food and Snacks	168,400	6	86
LG Group	Electronics	161,600	6	70,800
Philips Electronics NA	Electronics	142,900	6	38
Chiquita	Fresh fruit and vegetables	117,500	60	14

Table 3 Clustering top 10 US importers for different values of inspection capacity

$r = 1$

Cluster 1			Cluster 2			Cluster 3			Cluster 4		
Firm	SB	OB	Firm	SB	OB	Firm	SB	OB	Firm	SB	OB
Walmart*	✓	✓+	Walmart	✓	✓	Walmart	✓	–	Walmart	✓	–
Dole Food	✓	✓	Dole Food	✓	✓	Dole Food	✓	–	Dole Food	✓	–
Samsung	✓	–	Samsung	✓	–	Samsung	✓	–	Samsung	✓	–
LG Group	✓	–	LG Group	✓	–	LG Group	✓	–	LG Group	✓	–
Chiquita	✓	✓	Chiquita	✓	✓	Chiquita	✓	–	Chiquita	✓	–
			Target*	✓	✓+	Target	✓	–	Target	✓	–
						Home Depot*	✓	–	Home Depot	✓	–
						Dollar Tree	✓	–	Dollar Tree	✓	–
						Philips	✓	–	Philips	✓	–
									Lowe's*	✓	–

$r = 5$

Cluster 1			Cluster 2			Cluster 3		
Firm	SB	OB	Firm	SB	OB	Firm	SB	OB
Walmart*	✓	–	Walmart	✓	–	Walmart	✓	–
Home Depot	✓	–	Home Depot	✓	–	Home Depot	✓	–
Lowe's	✓	–	Lowe's	✓	–	Lowe's	✓	–
Samsung	✓	–	Samsung	✓	–	Samsung	✓	–
Dollar Tree	✓	–	Dollar Tree	✓	–	Dollar Tree	✓	–
LG Group	✓	–	LG Group	✓	–	LG Group	✓	–
			Target*	✓	–	Target	✓	–
						Dole Food*	✓	✓
						Philips	✓	–
						Chiquita	✓	✓

Notes: In the above table, "SB" and "OB" indicate security enhancement benefit and operational benefit, and whether the firm receives any benefit "✓" or not "–", respectively. The sign "*" in each cluster indicates firm "j" in algorithm 1; firm with the highest adversary preference score. The sign "+" indicates firm who would be qualified to ship under inspection-free lane. System parameters: $\frac{\sum_{i=1}^{N} \lambda_i}{\mu} = 3$; $z = \$200,000$; $\gamma = 0.1$; $\eta = 0.1$.

- Regardless of inspection capacity, the firm joining a security partnership is always entitled to receive the security benefit (SB). Note that a compliance decision requires the firm to invest f in its supply chain security. This investment, along with the security enhancement assistance allocated by the government, plus inspection rate α_i make the member's containerized supply chain a tough target for adversary infiltration. This aligns with our earlier discussion indicating that compliance enrollment yields an *immediate* security benefit for the member firm.

We note that firms with a high expected security benefit may collaborate even when not offered operational benefits (Samsung and LG groups with high $\mathcal{L}_i$). Beyond the security benefit offered to every participant, the decision to provide the operational benefit (OB) may vary depending on: (i) the inspection capacity and (ii) cluster size. Namely, when the inspection capacity is low, i.e., r =1, (or high, i.e., r =5), the number of participants who enjoy operational benefit drops (or increases) when clusters grow in size, i.e., from cluster 1 to cluster 4.

The rationale behind this observation when inspection capacity is low $(r = 1)$ is as follows. To induce other compliant firms, the state must provide: (i) security benefit by increasing security assistance resources allocated to members, and/or (ii) operational benefit by reducing wait time via lower inspection rate. Each member firm receives the security benefit itself, thus not impacting a non-member firm's partnership decision. However, a reduced inspection rate for a member firm curtails wait time t_r to benefit both members and non-members. This implies that larger cluster size may favor non-members more, thus making participation less attractive. Hence, the government may stop offering operational benefit to members in order to indirectly make the non-compliance decision more costly for non-members. That said, when the size of the cluster is small, reducing the inspection rate becomes more effective and acts as a *screening tool* to differentiate firms especially under a high delay cost. This corresponds to the last part of Proposition 3 where the potential member demands a reduced inspection rate (Dole Food and Chiquita in clusters 1 and 2).

- Apart from the case of low inspection capacity $(r = 1)$, the government may fare better offering the operational benefit (OB) to participants of large clusters (e.g., cluster 3) where inspection capacity is high $(r = 5)$. Ample capacity makes operational benefit less attractive for firms since the wait time of containers at the inspection facility, t_r, is already shortened. Thus, a limited incentive generated via operational benefit makes it less appealing here for firms to comply. To boost the attractiveness of partnership, the government strategically increases the difference in inspection rates for members versus non-members to yield operational benefit for members. Note the firm's participation condition in Proposition 2 capping such cost (i.e., f) at $(\beta_i - \alpha_i)\lambda_i t_r \kappa_i + \delta_i \mathcal{L}_i$. This cap is decreasing in r while increasing in $\beta_i - \alpha_i$. Therefore, in order to retain the firm's contribution to security investment (i.e., keeping f as high as possible when r is high), the government offers a reduced inspection rate to members.
- Finally, the government offers inspection-free lane only when inspection capacity is low. Also, when the inspection-free lane policy is offered, it is offered for the relatively small clusters. Note that the inspection-free lane policy is an extreme version of operational benefit. Therefore, it is most effectiveness when there are fewer number of member firms in the cluster and the inspection capacity is relatively low (i.e., Clusters 1 and 2 with $r = 1$).

7. Value of Security Incentives

In §5 and §6, we respectively characterized equilibria both without and with security partnership. To understand the value of partnership for the government, we need to compare the government's total loss under each scenario. We use the superscripts "P" and "N" to define equilibrium outcomes with and without security partnership, respectively. As discussed in §5, absent security partnership, there is no opportunity for collaboration as the government thus sets the inspection rate for all firms to minimize expected loss due to adversary infiltration (indicated by Z_t^{N}). The government next finds the optimal inspection facility capacity (indicated by r^{N}) to minimize the total cost of congestion (indicated by Z_c^{N}). With security partnership, however, the government can reduce expected losses from adversary infiltration and congestion to Z_t^{P} and Z_c^{P}, respectively, by inducing collaboration with an optimal cluster of firms per Proposition 4. The next proposition characterizes the value of security partnership for the government, member, and non-member firms.

PROPOSITION 5. *Let r^N denote the optimal inspection capacity without security partnership. Given r^P, let M denote the optimal cluster of firms induced for collaboration in Proposition 4. Then,*

– *The value of security partnership for government is*

$$V_g = \underbrace{\left[Z_c^N - Z_c^P\right]}_{\Delta Z_c\text{: Congestion term}} + \underbrace{\left[Z_t^N - Z_t^P\right]}_{\Delta Z_t\text{: Security term}} - \underbrace{\sum_{i\in M} s_i}_{\text{Security enhancement assistance}} \tag{16}$$

– *Let $j \leftarrow \arg\max_{i\in M}\{\mathscr{T}_i\}$. The value of security partnership for member $i \in M$ is*

$$V_m = \begin{cases} \beta_i\lambda_i\kappa_i(t_{r^N} - t_{r^P}) & \text{if } i = j \\ \beta_i\lambda_i\kappa_i(t_{r^N} - t_{r^P}) + \underbrace{\delta_i\mathcal{L}_i - f}_{\geq 0} & \text{if } i \neq j, \mathcal{L}_i \geq \eta_i\lambda_i[\beta_i\gamma + (1-\beta_i)]L \\ \beta_i\lambda_i\kappa_i(t_{r^N} - t_{r^P}) & \text{if } i \neq j, \mathcal{L}_i < \eta_i\lambda_i[\beta_i\gamma + (1-\beta_i)]L, \kappa_i \geq \frac{f-\delta_i\mathcal{L}_i}{\beta_i\lambda_i t_{r^P}} \end{cases} \tag{17}$$

– *The value of security partnership for non-member $i \in N$ is*

$$V_n = \beta_i\lambda_i\kappa_i(t_{r^N} - t_{r^P}) \tag{18}$$

We next discuss how the security partnership yields value for the government and for the firms, starting with each firm type.

Value of security partnership for member firms: The government can induce collaboration with firms by offering security (through lowered risk of adversary infiltration) and/or operational (through lower inspection rate) incentives. The former is always offered to the members (incurring investment cost f for the firm). However, the latter would be offered only where the security benefit *alone* fails to compensate the cost of compliance f for the member firms (refer to Proposition

3). Now if the firm induced for collaboration is the most preferred target for the adversary (i.e., $i = j$ in Equation (17)), then the government, depending on delay cost κ_j (see proposition 3)), may offer just security or both security and operational benefits. Irrespective of the benefit composition, the government always satisfies the participation constraint of member firm j and sets the compliance cost f equal to the total incentives. Therefore, the value of security partnership for member firm j is the expected waiting cost difference with versus without the security partnership.

This can be positive or negative since inspection capacity (i.e., r^{P} and r^{N}) can differ at optimality. That said, for the same level of inspection capacity, i.e., $r^{\mathrm{P}} = r^{\mathrm{N}}$, the value of security partnership is always positive since some members may ship under lower inspection rates when the security partnership is implemented, thus curtailing total congestion, i.e., $t_{r^P} \leq t_{r^N}$. For all other firms in the cluster ($i \neq j$), the value of security partnership depends on whether the cost of compliance f exceeds the security benefit $\delta_i \mathcal{L}_i$. If the cost of compliance is less than the security benefit, then firm i in the cluster enjoys a positive value of security partnership as long as the positive portion (i.e., $\delta_i \mathcal{L}_i - f > 0$) is not consumed by the difference in expected waiting cost $\beta_i \lambda_i \kappa_i (t_{r^N} - t_{r^P})$. Otherwise, where the cost of compliance is not covered by the security benefit, the government provides just enough operational benefit to make the firm's participation constraint binding, and the value of security partnership for the member thus arises from the difference in expected waiting cost with versus without the security partnership.

Value of security partnership for non-member firms: The value of security partnership for a non-member is simply the difference in expected waiting cost with versus without the partnership. Note that the optimal capacity of inspection facility may differ with versus without the partnership; therefore, the value of security partnership is positive for the non-member firm when $r^{\mathrm{P}} \geq r^{\mathrm{N}}$. Otherwise, i.e., $r^{\mathrm{P}} < r^{\mathrm{N}}$, it would be positive only if the reduced inspection rate for members under the security partnership results in a lower wait time at the inspection facility (i.e., $t_{r^P} < t_{r^N}$).

Value of security partnership for the government: Note from equation (16) that the value of security partnership for the government consists of three terms. The first is the congestion term capturing its impact on the total congestion cost. Since the optimal number of inspection facilities with security partnership differs from that without security partnership, the congestion term is not necessarily positive for the government. That said, for identical inspection capacity (i.e., $r^{\mathrm{P}} = r^{\mathrm{N}}$) we can verify the congestion term to be non-negative, i.e., $\Delta Z_c \geq 0$. The rationale is as follows. With the help of security partnership, some cluster firms may receive the operational benefit that reduces the total expected wait time. Here, the total waiting cost with security partnership is less than or equal to that in its absence.

The second component is the security term arising from the partnership helping the government deter adversary infiltration for cluster firms, but at the expense of security enhancement assistance

(i.e., the third component). Recall that the total security allocated to the members' supply chain (which is $f + s_i$), together with the inspection rate (α_i), suffices to deter adversary infiltration of member containers. This implies that under security partnership, the government can expect an adversary attack only for a non-member container that is less likely to occur versus no collaboration. Therefore, the security term is always non-negative for the government, i.e., $\Delta Z_t \geq 0$.

To summarize, assessing the value of security partnership for the government requires applying a holistic approach that weighs the impact of all three terms.

8. Other Cases

8.1. Role of Security Enhancement Assistance

Here, we analyze a partnership model under only operational incentives. In this case, firms can benefit from shipping under a reduced inspection rate (i.e., $\alpha_i \leq \beta_i$) when they become a partner by complying with security standards outlined in the program. Details of this model can be found in Appendix **??**. This serves as a benchmark to compare with our partnership model presented in §6, allowing us to generate insights on the value of the government's offering security enhancement assistance S. Let superscript "O" denote a partnership model under only operational incentives.

PROPOSITION 6. *Let $j \leftarrow \arg\max_{i \in N} \{\mathscr{T}_i\}$. Given the inspection capacity r, in equilibrium,*

- *The government security policy that induces firm j for collaboration requires $f^O = \eta_j \lambda_j L - z_j$, $\alpha_j^O = 0$, $\beta_j^O = \frac{f^O - \delta_j \mathcal{L}_j}{\lambda_j t_r \kappa_j}$.*
- *If $\delta_i \mathcal{L}_i \geq f^O$ then firm i opts for collaboration, i.e., $i \in \mathscr{M}^O$, and ships under inspection rate $\alpha_i^O = \frac{[\eta_i \lambda_i L - z_i - f^O]^+}{\eta_i \lambda_i (1-\gamma) L}$.*

The first part of Proposition 6 characterizes the deterrence condition for the adversary's most preferred target j. This implies that the security compliance level f^O invested by firm j is enough to secure its cargo and thus ship via the *inspection-free lane* ($\alpha_j = 0$). This differs from prior results in Proposition 3 where the government offers security enhancement assistance. Proposition 3 showed that the most preferred target j may or may not be qualified for the inspection-free lane depending on delay cost κ_j (first part of proposition 3). When delay cost is sufficiently low, in lieu of offering a reduced inspection rate (i.e., operational incentives), the government uses security enhancement assistance S to fortify the security of firm j. This readily means that the: (i) operational benefit for firm j (the adversary's most preferred target) is higher in the model with only operational incentives (i.e., $\alpha_j^O \leq \alpha_j$), and (ii) security compliance level f^O here exceeds that in Proposition 6 (i.e., $f^O \geq f$).

The second part of proposition 6 characterizes the optimal cluster of firms for whom investing in security compliance is economically beneficial. Given here inspection capacity r, Proposition 6

indicates only one cluster of firms, $\mathscr{M}^O$, enrolling to collaborate. This markedly differs from the partnership model in §6, where, under security enhancement assistance, the government may form *various* clusters (see Algorithm 1) to then choose the optimal one per Proposition 4. To summarize, the availability of security enhancement assistance S helps the state contribute toward a firm's total security level (i.e., $f+s$) which, in turn, reduces the firm's own security contribution (i.e., $f^O \geq f$). This fosters a firm's collaboration level, thus luring more firms to collaborate. This also equips the government more options in offering a tailored mix of operational-security incentives depending on a firm's specific parameters. As a result, expected wait time at an inspection facility may drop (i.e., $t_r^P \leq t_r^O$) to benefit both members and non-members.

8.2. Cost of failure to the adversary

Customs enforces law by targeting and penalizing adversaries through monetary policies and legal actions. When the adversary is caught and fails to escape inspection, we here assume it to incur cost Γ. In our baseline model, we excluded Γ to simplify exposition and interpretation using a streamlined number of variables and parameters. In this extension, we investigate the impact of considering this cost to the adversary on our results and analysis. Given inspection rate β_i, one can verify that Equation (2) would be written as follows:

$$j = \arg\max_{i \in K} \Big\{ P_i(A_i) \Big[\big[\beta_i \gamma + (1-\beta_i)\big] \lambda_i \big[L+\Gamma\big] - \Gamma \Big] - A_i \Big\}.$$

By optimizing the adversary's payoff function with respect to A_i, the adversary's best response to the government's inspection rate is expressed in Lemma 4.

LEMMA 4. *Let* $\bar{\beta}_i = \frac{\eta_i \lambda_i (L+\Gamma) - z_i - \eta_i \Gamma}{(1-\gamma)\eta_i \lambda_i (L+\Gamma)}$ *if* $z_i \geq \gamma(L+\Gamma)\eta_i\lambda_i - \eta_i\Gamma$ *and* $\bar{\beta}_i = 1$ *otherwise. The adversary's best response function* A_i^{br} *is*

$$A_i^{br} = \begin{cases} \frac{z_i}{\eta_i} \ln \left[\frac{\eta_i \lambda_i [\beta_i \gamma + (1-\beta_i)](L+\Gamma) - \eta_i \Gamma}{z_i} \right] & \text{if } \beta_i < \bar{\beta}_i \\ 0 & \text{if } \beta_i \geq \bar{\beta}_i \end{cases} \tag{19}$$

Lemma 4 indicates that considering the cost of failure in the adversary's payoff function affects the inspection rate required to deter its infiltration threat. We can then verify all the theoretical results with this new characterization of $\bar{\beta}_i$.

9. Concluding Remarks

9.1. Summary and Discussion

In view of the burgeoning volume of containerized transport facing imminent risk of infiltration, port security emerges as the Achilles' heel in many national economies. This paper examines the value of a public-private partnership in elevating the security of containerized supply chains

to minimize the risk of adversary infiltration. We have developed a game-theoretical model featuring three strategic players: government, firms, and adversary. The government first selects inspection capacity to next offer the firms incentives to form a public-private partnership. Firms respond to these incentives by determining their levels of collaboration. Finally, the overall level of collaboration induced by the incentives determines the level of threat from a strategic adversary that ultimately decides on its attack level.

By comparing equilibrium characterizations with versus without security partnership, we extract the value of partnership for the state, as well as for members and non-members. In general, security partnership yields security and operational benefits exerting different cost-benefit implications for these stakeholders. In terms of security, partnership offers benefits mainly for member firms as it helps curb the risk of attack from an adversarial infiltrator. On the other hand, security partnership operationally reduces congestion for the whole inspection facility. This means shorter wait times for port operations. Although this benefits all firms – members and non-members – our analyses show the government needing to account for the cost of providing security and operational benefits when maximizing security partnership value. Specifically, operational benefits merged with security benefits become more cost-effective for the government when inducing smaller clusters as the screening power of the former is amplified when used selectively. That said, a smaller cluster size may degrade the value of security partnership. Indeed, according to a recent article posted on The Journal of Commerce 2017, firms react to security and operational benefits differently depending on program size. Therefore, the government must find a way to sustain a large security partnership such as C-PTAT without incurring excessive costs. Equilibrium characterization under security partnership enables us to distill the required conditions for exploiting an inspection-free lane where a member can ship with no inspection. Here, offering the inspection-free lane to a most preferred firm for the adversary helps the government reduce its total cost of security investment incurred in all member supply chains.

9.2. Recommendations for Policymakers

Based on our analysis, the following recommendations can be made for policymakers:

Align capacity decision and security programs. The endgame in developing and implementing security programs is to deter adversaries from abusing the flow of maritime container transport while ensuring the security, health and safety of people, firms and infrastructures without imposing a barrier to oceanic trade. However, as our analysis shows, the effectiveness of such programs deteriorates where inspection capacity is scarce. In other words, if state supervision and inspection capabilities toward container flow proves lacking, then it becomes impossible to deter adversaries from infiltration. Hence, it is of utmost importance to align inspection capacity decisions with security standards and incentives.

Diligently set the inspection rates for members and non-members. As mentioned earlier, available inspection capacity plays a salient role in ensuring the effectiveness of security programs. Still, this is a double-edged sword and must be handled very carefully for the following reasons. Inadequate capacity harms the effectiveness of security programs, while overcapacity dissuades firm membership since the availability of ample inspection capacity reduces everyone's inspection processing time. Thus, firms may not see operational value in becoming a member by investing to enhance their security level. Here, Customs must strategically tailor inspection rates for members and non-members. This becomes especially relevant with modernized inspection tools and the availability of fast, effective technologies.

When advertising security programs, emphasize the security enhancement benefits. Membership lets firms enjoy security enhancement benefits and (perhaps) operational benefits. Security enhancement benefits are hidden and intangible while operational benefits are overt for instant realization by member firms. As our analysis shows, all member firms individually enjoy security enhancement benefits while operational benefits supplement to incentivize firms where security enhancement benefits do not suffice to induce collaboration. This could impede inducing firms to invest in security standards and measures when they may not realize operational benefits at all, or when these benefits alone may not cover the cost of program compliance. Thus, greater emphasis should feature security enhancement benefits when communicating to firms the advantage of complying with security programs.

Make security benefits (partially) tangible by offering security enhancement assistance or security subsidies. As our results show, deterring adversaries with inspection – even under a 100% inspection rate – may not suffice. Developing partnership mechanisms may raise effectiveness, but firms may not readily experience tangible benefits. Governments can address this by offering overt, tangible benefits such as subsidizing investment cost or offering security assistance to members. These can better incentivize firms to join these programs. By offering security assistance, part of the security investment costs is borne by the government, making it more attractive for firms, particularly ones not highly appreciating the operational benefits.

9.3. Future Research

The model presented in this paper can extend in multiple directions. Since our work assumes that the adversary is strategic and responds optimally to the government and to firms' decisions, such behavior does not represent all adversarial activities in recent history. Indeed, the container selection criteria of a nonstrategic adversary may be influenced by factors not readily available or measurable government-wise. Therefore, one possibility could develop a model that considers two different types of adversary: strategic and *nonstrategic*. A strategic adversary chooses a container

by accounting for the total security assigned during the collaboration stage, while a nonstrategic adversary of preference unknown by the government and firms may select a container irrespective of its assigned security level. This may result in a model featuring information asymmetry where the type of adversary (strategic, nonstrategic) goes undetected by government. Another extension may analyze a model under information asymmetry where the government's security assistance level assigned to a member's supply chain is not observable by the adversary.

Second, for the sake of analytical tractability, we have considered only a *single* inspection stage. This might deviate from the inspection process in reality. For example, under C-TPAT membership compliance, all containers undergo a primary inspection stage demanding non-intrusive inspection that may include neutron and gamma-ray radiation monitoring. Furthermore, based on the results of this primary inspection, a fraction of these containers may be tagged for secondary inspection, corresponding to our single-stage inspection. This second inspection may include tests such as gamma and x-ray radiography, as well as a comprehensive manual inspection. Although we have not analyzed a two-stage inspection model, we expect that considering two stages of inspection in our model may foster collaboration since this may increase wait times at the inspection facility where firms have more incentives to collaborate in order to benefit from inspection-free shipping.

References

Arin KP, Lorz O, Reich OF, Spagnolo N (2011) Exploring the dynamics between terrorism and anti-terror spending: Theory and uk-evidence. *Journal of Economic Behavior & Organization* 77(2):189–202.

Bagchi A, Paul JA (2017) Espionage and the optimal standard of the customs-trade partnership against terrorism (C-TPAT) program in maritime security. *European journal of operational research* 262(1):89–107.

Bakir NO (2011) A stackelberg game model for resource allocation in cargo container security. *Annals of Operations Research* 187(1):5–22.

Bakshi N, Gans N (2010) Securing the containerized supply chain: Analysis of government incentives for private investment. *Management Science* 56(2):219–233.

Baron O, Berman O, Gavious A (2018) A game between a terrorist and a passive defender. *Production and Operations Management* 27(3):433–457.

Bier VM, Haphuriwat N (2011) Analytical method to identify the number of containers to inspect at us ports to deter terrorist attacks. *Annals of Operations Research* 187(1):137–158.

Bier VM, Haphuriwat N, Menoyo J, Zimmerman R, Culpen AM (2008) Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis* 28(3):763–770.

Bier VM, Oliveros S, Samuelson L (2007) Choosing what to protect: Strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory* 9(4):563–587.

Department of Homeland Security (2005) Maritime commerce security plan for the national strategy for maritime security. Technical report, Department of Homeland Security, URL https://www.dhs.gov/sites/default/files/publications/HSPD_MCSPlan_0.pdf.

European Commission (2016) Authorised economic operators guidelines. Technical report, European Commission, URL https://ec.europa.eu/taxation_customs/system/files/2017-03/aeo_guidelines_en.pdf.

European Committee Taxation and Customs Union (2015) Authorised economic operators (aeo). Technical report, European Commission, URL http://ec.europa.eu/taxation_customs/dds2/eos/aeo_consultation.jsp?Lang=en.

Gerchak Y, Safayeni F (1996) Perfect information with potentially negative value: an intriguing war story and a possible explanation. *Journal of the Operational Research Society* 710–714.

Golany B, Kaplan EH, Marmur A, Rothblum UG (2009) Nature plays with dice–terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research* 192(1):198–208.

Gupta S, Starr MK, Zanjirani Farahani R, Ghodsi MM (2020) Prevention of terrorism–an assessment of prior POM work and future potentials. *Production and Operations Management* 29(7):1789–1815.

Haphuriwat N, Bier VM, Willis HH (2011) Deterring the smuggling of nuclear weapons in container freight through detection and retaliation. *Decision Analysis* 8(2):88–102.

Hausken K, Bier VM, Zhuang J (2009) Defending against terrorism, natural disaster, and all hazards. *Game theoretic risk analysis of security threats*, 65–97 (Springer).

Hausken K, Zhuang J (2013) The impact of disaster on the strategic interaction between company and government. *European Journal of Operational Research* 225(2):363–376.

Hausken K, Zhuang J (2016) The strategic interaction between a company and the government surrounding disasters. *Annals of Operations Research* 237(1-2):27–40.

Hendricks KB, Singhal VR (2005) An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. *Production and Operations management* 14(1):35–52.

Jaspersen JG, Montibeller G (2020) On the learning patterns and adaptive behavior of terrorist organizations. *European Journal of Operational Research* 282(1):221–234.

Lee HL, Whang S (2005) Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of production economics* 96(3):289–300.

Martonosi SE, Ortiz DS, Willis HH (2007) Evaluating the viability of 100 per cent container inspection at america's ports. *The economic impacts of terrorist attacks* 218.

McLay LA, Dreiding R (2012) Multilevel, threshold-based policies for cargo container security screening systems. *European Journal of Operational Research* 220(2):522–529.

Nikoofal ME, Gümüs M (2015) On the value of terrorist's private information in a government's defensive resource allocation problem. *IIE Transactions* 47(6):533–555.

Nikoofal ME, Zhuang J (2015) On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. *European Journal of Operational Research* 246(1):320–330.

Powell R (2007) Allocating defensive resources with private information about vulnerability. *American Political Science Review* 101(4):799–809.

Rice JB, Caniato F (2003) Supply chain response to terrorism: Creating resilient and secure supply chains. *Report by MIT Center for Transportation and Logistics* .

Shan X, Zhuang J (2013) Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. *European Journal of Operational Research* 228(1):262–272.

Shan XG, Zhuang J (2020) A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. *Reliability Engineering & System Safety* 195:106683.

The Journal of Commerce (2005) C-TPAT importers get 'green lane' clearance. Technical report, JOC.com, URL https://www.joc.com/maritime-news/c-tpat-importers-get-green-lane-clearance_20051006.html.

The Journal of Commerce (2016) Lack of us customs funding endangers timely cargo clearance. Technical report, JOC.com, URL http://www.joc.com/regulation-policy/customs-regulations/us-customs-regulations/lack-resources-endangers-customs-efficiency-report-says_20160711.html.

The Journal of Commerce (2017) Us watchdog: No way to tell if importers gain from C-TPAT. Technical report, JOC.com, URL https://www.joc.com/regulation-policy/customs-regulations/us-customs-regulations/us-watchdog-no-way-tell-if-importers-gain-c-tpat_20170214.html.

The Journal of Commerce (2018) Top 10 us importers, 2017. Technical report, JOC.com, URL https://www.joc.com/regulation-policy/trade-data/united-states-trade-data/tariffs-trucking-top-threats-top-100-us-importers-and-exporters_20180521.html.

US Customs and Border Protection (2021) C-TPAT: Customs trade partnership against terrorism. https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat.

Willis HH, Ortiz DS (2004) Evaluating the security of the global containerized supply chain. Technical report, Rand Corporation.

World Customs Organization (2021) Aeo implementation and validation guidance. Technical report, wcoomd.org, URL http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/aeo-implementation-guidance.pdf?la=en.

Zhuang J, Bier VM (2007) Balancing terrorism and natural disasters: Defensive strategy with endogenous attacker effort. *Operations Research* 55(5):976–991.