J Transp Secur (2010) 3:197–211
DOI 10.1007/s12198-010-0047-y

Container transportation as an interdependent security problem

Konstantinos G. Gkonis · Harilaos N. Psaraftis

Received: 20 June 2010 / Accepted: 26 July 2010 / Published online: 10 August 2010

Abstract This paper concerns container shipping transportation viewed as an interdependent security system. The methodological background is the use of game-theory in the investigation of how interdependence affects individual choices about security expenditures in so-called interdependent systems (IDS problems). Any agent's incentive to adopt security measures depends on the actions of others because of the negative externalities created among them. In this context, we examine security questions in container transportation and more specifically we focus on investments in container checking systems at ports, considering the currently much debated 100% scanning requirement of containers destined to USA. It is obvious, that in such analysis there is a demand to balance the cost of investing in (installing) and operating such a system and the reduction in the risk of a potential damage from a "dangerous" container from a security point of view. A transferred "dangerous container", which may pass through another agent / port (screening point), introduces an additional dimension of risk. Useful suggestions are reached from such a treatment of the subject and policy dimensions emerge, such as the potential need for coordinating mechanisms among ports.

Keywords Container transportation · Interdependent security · Game theory

Introduction

This paper presents part of a broader research work providing a preliminary identification of the relevance to shipping security of concepts and insights developed in other security settings. The rationale of this work is to explain why

K. G. Gkonis (✉) · H. N. Psaraftis
Laboratory for Maritime Transport, National Technical University of Athens, 9,
Iroon Polytechneiou str, 157 73 Zografou, Greece
e-mail: cgonis@naval.ntua.gr

H. N. Psaraftis
e-mail: hnpsar@mail.ntua.gr

game theory is suitable to support such an analysis, and following a literature review of relevant security and counter-terrorism models to adapt them to the merchant shipping context.

In the same research framework also belong the papers by Gkonis et al. (2009) and by Gkonis et al. (2010). The first one applied a game theoretic model to a port security setting, where "port" and "ship" targets must decide on the level of their security measures against potential attack by terrorists. The second paper concerned game theoretic modelling of piracy threats and counteractions, in a setting where the defender is a naval force command and the attacker the pirates, while two potential target areas for the pirates (and respective areas for the deployment of the naval forces) are considered. Security is different from safety as, for one reason, there are at least two decision makers, and therefore a different approach is needed. Game theory allows the treatment of players as rational decision-making agents with interdependent interests.

The present paper concerns container shipping transportation viewed as an interdependent security system. The methodological background is the use of game-theory in the investigation of how interdependence affects individual choices about security expenditures in so-called interdependent systems (IDS problems) and has been adopted from Kunreuther and Heal (2003), and Heal and Kunreuther (2005). Any agent's incentive to adopt security measures depends on the actions of other agents because of the negative externalities created among them. It is for example the risk that a "dangerous parcel" will be transferred from an unsecured link of the transportation chain to the others that creates such negative externalities. The members of the group are interdependent and investing in protection produces positive externalities, while not investing produces negative externalities.

In this context, we will examine security questions in container transportation and more specifically we will focus on investments in container checking systems at ports, considering the currently much debated 100% scanning requirement of containers destined to the US. It is obvious, that in such analysis there is a demand to balance the cost of investing in (installing) and operating such a system and the reduction in the risk of a potential damage from a "dangerous" container from a security point of view. A transferred "dangerous container", which may pass through another agent / port (screening point), introduces an additional dimension of risk.

In a few words, the present modeling approach employs game theory to investigate how interdependence affects individual choices about security expenditures in container transportation, the latter viewed as an interdependent system in terms of security associated with potential terrorist threats.

The rest of this paper is divided into the following sections. "Methodological approach: game theory" is a general discussion of the methodological approach of game theory in the present research framework. "Literature review on methodological approach" is a literature review of game theoretic contributions to security/terrorism questions. "The security setting examined in this paper" describes the security setting to be examined. "Methodological analysis" presents the methodological approach to the problem. "Illustrations—numerical examples" provides illustrations/numerical examples of the modeling application. "Conclusions" concludes this paper with an assessment of the results and proposed extensions of the analysis.

Methodological approach: game theory

Terrorism is the premeditated use or threat of use of violence or force by individuals or sub-national groups against non-combatants to obtain a political or social objective through the intimidation of a large audience beyond that of the immediate victim (Sandler and Siqueira 2006). Game theory analyses of terrorism and security issues provide policy insights that do not follow from non-strategic analyses.

There are many reasons why game theory is an appropriate methodology for the study of terrorism and associated security questions (see for example Sandler and Arce 2003). First of all, it is clear that "safety" and "security" have a common high-level objective, to take measures that either avoid events that put at risk human life, a ship, a port, or a transport system, or mitigate their consequences. This is true whether the event is a ship collision, or a terrorist act. However, the fundamental difference between safety and security is that in the former setting the events we want to avoid are not intentional, while in the latter setting they are intentional. This difference is significant enough for security to require a methodological approach different from traditional risk analysis. In fact, if in safety there is a single decision maker whose decisions are the measures to be taken to enhance safety, in security the decision makers are two, those who aim to inflict damage (e.g. the terrorists) and those who want to avoid it (the potential target). In that sense, the objectives of the two are in direct conflict with one another. Both attackers and defenders must choose strategies based on how they anticipate the other side will react to their choices (Lapan and Sandler 1993).

A second reason why game theory is appropriate is that a game-theoretic framework captures the notion that security / terrorist scenarios concern interactions among rational agents that are trying to act according to how they think their counterparts will act and react. These players are rational in the sense that they optimize an objective subject to constraints.

A third reason is that game theory allows adversaries to issue threats and promises for strategic advantage. Last but not least, game theory incorporates the uncertainty and learning in a strategic environment. In a terrorism scenario, many agents interact with asymmetric information. Terrorists can exploit asymmetries to gain advantage e.g. exploit their informational asymmetries, thereby leaving a target uncertain about the requisite level of defence. They may also gain a second-mover advantage by identifying soft targets after defensive expenditures have been allocated.

Thus, addressing security problems is not a usual problem of estimating a risk, such as natural disaster events or accidents. It requires the determination of the outcome of a game between attackers and defenders. In this context, game theory allows an analyst to consider the adversaries' goals and take into account the actual purposes of a terrorist attack, not just the potential plans of terrorists such as in other analysis approaches.

Literature review on methodological approach

The interested reader can refer to a number of publications on the growing issue of shipping security and terrorism (an indicative review can be found in Gkonis et al.

2009). Therefore the following literature review will only refer to the game theoretic treatment of security / terrorism issues.

Sandler and Siqueira (2006) discuss transnational terrorism. Each country is vulnerable at home and abroad, insofar as an attack anywhere may involve residents or foreigners. Deterrence measures refer to actions that transfer the terrorist threat abroad, where a country may have no interests (extreme case 1: no collateral damage) or equal concerns as at home (extreme case 2: globalized terrorism). Pre-emption measures refer to actions that a targeted government must independently decide, such as launching an attack against a terrorist group or its sponsor, and which confer public benefits on targeted countries. An increase in a country's pre-emption efforts reduces the probability of terrorist attack / success not only for this country, but also for other countries.

Sandler and Lapan (1988) apply formal modelling to study a terrorist group's choice of whether to attack or not, and, in the case of an attack, which of two potential targets to strike. Also they show that increased information about terrorists' preferences may prove inefficient when deterrence efforts are not coordinated.

Lapan and Sandler (1993) examine the interaction between a terrorist group and the target (government) in a setting of incomplete information. Information is asymmetric as the government is not informed about the terrorist group's capabilities, while the terrorist group is fully informed, even for the strategy of the government.

Sandler and Arce's (2003) literature review covers the use of game theory for the analysis of hostage-takings by terrorists and negotiations, bargaining games, the rationale for terrorist hosting by some countries in order to gain some benefit, information and signalling games between governments and terrorist groups, as well as terrorists' choice of targets. The authors summarize the different proactive and reactive policies and analyze them with associated game modelling forms.

Bier et al. (2007) examine the strategic interaction between a defender and an attacker, whose choice of target is unknown. Questions concerning optimal policies of strategic deterrence are addressed, such as whether strategic defensive decisions should be centralized or decentralized.

Zhuang and Bier (2007) show that increased defensive investment can lead the attacker to either increase or decrease his level of effort, so that the effectiveness of investments in protection are either decreased or increased. The paper stresses, among other, the importance of intelligence in counter-terrorism, in order to anticipate not only the attacker's choice of targets, but also the likely attacker responses to defensive investments.

Azaiez and Bier (2007) examine optimal investments in the security of systems comprising various components. Based on the assumption that the defender is interested primarily in preserving the functionality of the overall system and preventing catastrophic failures, useful conclusions are reached, such as that defending the stronger elements in a parallel subsystem is preferable to hardening the weaker ones. Bier et al. (2005) examine similar settings with emphasis on the defence of series and parallel component systems.

Basuchoudhary and Razzolini (2006) focus on the interaction between two rational players, namely a governmental security agency and a terrorist organization, where the agency must infer whether a visa applicant or an airline passenger is a terrorist or not,

and must base this decision only on some easily observable signal—thus saving on information gathering costs.

Wein et al. (2006) resort to game theory to address security considerations in shipping and ports. They develop a mathematical model to find the optimal inspection strategy for detecting a nuclear weapon (or nuclear material to make a weapon) in a shipping container, subject to constraints of port congestion and an overall budget. The multi-agent nature of the problem leads to the use of a game-theoretic approach as part of a complex optimization problem. Bakshi and Gans (2010) also employ a game-theoretic framework in an economic analysis of the so-called Customs-Trade Partnership Against Terrorism (C-TPAT) program. The interested reader can find more references regarding the applications of game theory to security and counter-terrorism for example in Bier (2006).

The present paper methodologically is based on Heal and Kunreuther (2005) and Kunreuther and Heal (2003), who use game-theory to investigate how interdependence affects individual choices about security expenditures in so-called interdependent systems (IDS problems). Any agent's incentive to adopt risk-reducing measures depends on the actions of others because of the negative externalities created by not investing in protection. Airline security is examined as an example, while other IDS-kind problems include computer security, fire protection, and theft protection.

The security setting examined in this paper

The present modeling task has as reference the 100% scanning requirement of containers destined to the US. A bill was passed in USA in 2007, under the title "Implementing Recommendations of the United States 9/11 Commission Act of 2007", mandating overseas radiation scanning and Non-Intrusive Inspection of 100% of all cargo containers destined to USA by 2012 (Donner and Kruk 2009). Following a series of concerns expressed by several stakeholders, it was decided in 2009, and while this paper was written, to delay the enforcement of the above law for 2 years to 2014.

Indeed, concerns were expressed from the moment the bill was passed—on the grounds mainly of resulting costs, delays, and staff requirements—even from US stakeholders (see for example AmChamEU 2007), and US agencies (see e.g. Straw 2008). Several studies enhanced such concerns (see e.g. NDIA 2009) and examined the US law impacts on a macro- and a micro- economic level, such as the one commissioned by the World Customs Organisation (Carluer et al. 2008). Fears included the possibility that the European Union might go down the same regulatory route as the US. European Commission assessments saw in such measures an unnecessary economic burden for European ports, an expensive disruption of European transport, and a potential new trade barrier, suggesting that implementing 100% scanning would require sizable investments, increase transport costs significantly and entail massive welfare losses (see EC 2010).

In the following analysis, the primary actors (players) are considered to be the ports (outside USA) participating in the international movement of containers destined to USA.

The ports have to choose whether or not to invest in security measures in relation to the screening of their incoming containers. This choice is taken to be discrete:

invest or not invest in a 100% scanning system for containers that are entering the port from land. It is assumed that a 100% scanning of containers that a port receives from the landside supply chain will ensure the detection of a "dangerous container" (e.g. a "container carrying a nuclear bomb" and referred to as dangerous container from now on), but there could still be such a dangerous container in transit (i.e. transferred) from another port by sea. We also assume that, for reasons of cost, timing and resources, it is not possible for a port to examine the containers in transit (i.e. coming from another port by sea), before they are dispatched to USA. Indeed, there exists a practical difficulty of scanning at ports where containers are transferred between ships via cranes and shuttle vehicles (Straw, 2008). There is thus an additional risk originating in another port which has not invested in the security measures in question.

The loss, when the port is found to be dispatching a dangerous container to USA following inspection at US border crossing points, is quantified as L. This loss is the result of trade sanctions imposed on this port and/or its inclusion in a "black list" of ports by the US authorities, actions which result in economic losses for the port.

In accordance with the above, there are two possible ways in which this loss can occur. It can either be the result:

a) of a container dispatched from the specific port to USA after it was received at the port by land (dangerous container entering directly the port's system), or
b) of a container dispatched from the specific port to USA after this container was received (i.e. originating) from another port.

The probability of a loss in case (a) if the port has not invested in the security measures in question (scanning) is p, so that the expected loss from this event is pL. If the port has invested in security precautions (100% scanning) then this risk is assumed to be zero, as already explained. Regarding case (b), the probability that a port sends a dangerous container to another port is q, so that the latter's expected loss from the detection of that container at US borders is qL.

Methodological analysis

The analysis in this section will examine first the 2-agent problem, before moving to the n-agent problem. The methodological analysis has been adopted from Kunreuther and Heal (2003), and Heal and Kunreuther (2005).

The case of 2 ports

We consider two ports P1 and P2. Let Mi be the income for a period of time (e.g. annual) of each port before any expenditure on security or any security-related losses. The cost of investing in and operating the 100% security scanning measures (as described above) is c (for the same period of time; the following analysis will have this same time period reference).

If both ports invest in security (choice "I"), then each one incurs a cost of c (security investment and operational cost) and faces no losses from any dispatch of a dangerous container to USA, so that their net incomes are Mi-c.

If P1 invests (choice "I") and P2 does not (choice "N"), then P1 incurs a cost of c and also runs the risk of a loss originating from P2. The probability that P2 sends a dangerous container to P1 is q, so that P1's expected loss from the detection of that container at US borders is qL. This cost represents the negative externality imposed by P2 on P1. P2 incurs no costs from investment in security and faces no risk of loss from P1, but it does face the risk of loss originating from receiving a dangerous container from the landside (which is destined to the US where it is detected), which is pL. The case when P2 invests (choice "I") and P1 does not (choice "N") is an exact mirror case.

If neither port invests in security (choice "N"), then each will have an expected payoff of Mi-pL-(1-p)qL. The latter term is suggesting that the possibility that a dangerous container (e.g. carrying a nuclear bomb) arrives at a port from both land and sea during the considered time period is 0.

The above cases (outcomes) and the respective payoffs for the ports P1 and P2 are given in Table 1, where for each outcome (cell) of the table, the first term is P1's payoff and the second term P2's payoff.

The conditions for both ports to invest in security (100% scanning), as suggested in Table 1, i.e. for investing in security (I) to be a dominant strategy, are:

a)

$$\mathrm{Mi} - \mathrm{c} > \mathrm{Mi} - \mathrm{pL} \Rightarrow \mathrm{c} < \mathrm{pL}$$

and

b)

$$\mathrm{Mi} - \mathrm{c} - \mathrm{qL} > \mathrm{Mi} - \mathrm{pL} - (1 - \mathrm{p})\mathrm{qL} \Rightarrow \mathrm{c} < \mathrm{pL} - \mathrm{pqL} \Rightarrow \mathrm{c} < \mathrm{pL}(1 - \mathrm{q})$$

The first inequality indicates that the cost of investing in security must be less than the expected loss, which is straightforward for an isolated agent. The second tighter inequality reflects the possibility of contagion with the dangerous container from one port to the other. This possibility reduces the incentive to invest in security, because in isolation, investment in security ensures a port from the risk of loss (as defined above), however with the possibility of contagion it does not. Even after investment, there remains a risk of loss from a dangerous container originating from the other port. "Investing in security buys you less when there is the possibility of contagion from others" (Kunreuther and Heal 2003).

The above setting corresponds to a non-cooperative game, where both players make decisions simultaneously and the optimal behavior of each port can be determined. If c < pL(1-q), then both ports will want to invest in 100% scanning

Table 1 Outcomes and payoffs associated with investing (I)/not investing (N) in security.

Payoffs		Port 2 (P2)	
		I	N
Port 1 (P1)	I	M1-c, M2-c	M1-c-qL, M2-pL
	N	M1-pL, M2-c-qL	M1-pL-(1-p)qL, M2-pL-(1-p)qL

Figure 1 A different decision (I) or (N) is impossible for ports with same costs of investing in security (axis in figure is "cost")

(I,I); if c > pL then neither port will want to invest (N,N). If pL(1-q) < c < pL then there are two Nash equilibria (I,I) and (N,N) and the solution to this game is indeterminate (any of the above inequalities becoming equality, corresponds to the case of indifference between investing or not investing).

For (N,I)[1] to be a Nash equilibrium it is necessary that M1-pL > M1-c or c > pL and also that M2-c-qL > M2-pL-(1-p)qL or c < pL(1-q) which is impossible (see Figure 1). So the only Nash equilibria are where both ports invest (I,I) or both do not invest (N,N).

If the ports have different costs of investing in security measures, then there may be a Nash equilibrium where one port invests in security and the other does not. Specifically, let c1 and c2 be the costs of the two ports P1 and P2 respectively. Then (N,I) will be a Nash equilibrium if $c_1 > pL$ and $c_2 < pL(1-q)$. This mixed equilibrium requires that the two costs differ by at least pqL (see Figure 2).

An extension of the above with $p_1 \neq p_2$ and $q_{12} \neq q_{21}$ (where qij is the probability of transfer of a dangerous container from port i to port j) is straightforward (see Heal and Kunreuther 2005). For i,j=1 or 2:

1. (I, I) will be Nash equilibrium as the outcome of dominant strategies if $c_i < p_iL(1 - q_{ji})$
2. (N, N) will be Nash equilibrium as the outcome of dominant strategies if $c_i > p_iL$
3. (I, I) and (N, N) will both be Nash equilibria if $p_iL(1 - q_{ji}) < c_i < p_iL$
4. (N, I) will be a Nash equilibrium if $c_1 > p_1L$ and $c_2 < p_2L(1 - q_{12})$
5. (I, N) will be a Nash equilibrium if $c_2 > p_2L$ and $c_1 < p_1L(1 - q_{21})$

It should be noted that equilibria resulting from dominant strategies are also Nash equilibria. On the other hand, Nash equilibria are not necessarily unique or the outcome of dominant strategies, such as in the 3rd case above where (I, I) and (N, N) are both Nash equilibria (the solution is indeterminate, as there are no dominant strategies in this case). All the above Nash equilibria are graphically depicted in Figure 3.

The case of n ports

In the general case of the above setting, n risk-neutral players (the ports) exist designated by Pi, i=1…n. First we consider the case of three ports, Pi, i=1, 2, 3. If only P1 has placed a container 100% security scanning system, then it can suffer loss from a dangerous container transferred from P2, before sending it to USA. This event occurs with probability q/2 since we assume that the container from P2 has an equal chance of being transferred to either P1 or P3. A dangerous container transferred from P3 can also damage P1[2] with probability (1-q/2)q/2.

[1] (I,N) is a mirror case.
[2] This can occur when P2 does not transfer a dangerous container to P1 but P3 does.

Figure 2 A different decision (I) or (N) is possible for ports with different costs of investing in security (axis in figure is "cost")

According to the analysis by Kunreuther and Heal (2003), we define X(3, 0) as the expected negative externality to any port i that has installed a security system, if there are three ports and none of the others have invested in the security measures in question. Then:

$$\mathrm{X}(3,0) = (\mathrm{q}/2)[1 + (1 - \mathrm{q}/2)]\mathrm{L}$$

When one other port has invested in security, then the expected negative externality is[3]:

$$\mathrm{X}(3,1) = (\mathrm{q}/2)\mathrm{L}$$

If there are four ports then the expected negative externalities become:

$$\mathrm{X}(4,2) = (\mathrm{q}/3)\mathrm{L}$$
$$\mathrm{X}(4,1) = (\mathrm{q}/3)[1 + (1 - \mathrm{q}/3)]\mathrm{L}$$
$$\mathrm{X}(4,0) = (\mathrm{q}/3)[1 + (1 - \mathrm{q}/3) + (1 - \mathrm{q}/3)2]\mathrm{L}$$

In general, for $n>1$ ports:

$$X(n,0) = \frac{q}{n-1}\sum_{t=0}^{n-2}\left(1 - \frac{q}{n-1}\right)^{t} L = \left[1 - \left(1 - \frac{q}{n-1}\right)^{n-1}\right] L \qquad (1)$$

So it is proposed that if there are n ports and none has invested in security, then the expected loss inflicted on any port by all others is given by (1) above. In accordance with the previous analysis (see e.g. Table 1), the payoff to P1 from not investing in security (N) when the other n-1 ports are also not investing will be:

$$\mathrm{M} - \mathrm{pL} - (1 - \mathrm{p})\mathrm{X}(\mathrm{n},0) \qquad (2)$$

The payoff to P1 from investing (I) will be:

$$\mathrm{M} - \mathrm{c} - \mathrm{X}(\mathrm{n},0) \qquad (3)$$

So, from (2) and (3), investing (I) will be preferable if:

$$\mathrm{c} < \mathrm{p}[\mathrm{L} - \mathrm{X}(\mathrm{n},0)]$$

This means that the higher the negative externalities from the rest of the ports, the lower the cost of investing in security should become, for (I) to be the preferable choice, and so there is less incentive to invest in security. It is therefore implied that as we add to the analysis context more ports who do not invest in security, the externality on any other port increases, and the condition for them to want to invest in security becomes more demanding, i.e. such investment becomes less likely.

For the n-port case, in accordance with the two ports case examined before, (I,I,…I) will be a dominant strategy if $\mathrm{c} < \mathrm{p}[\mathrm{L} - \mathrm{X}(\mathrm{n},0)]$ and (N,N. . .N) will be a dominant

[3] There is only one port without a security system and it transfers a dangerous container to port i with probability q/2

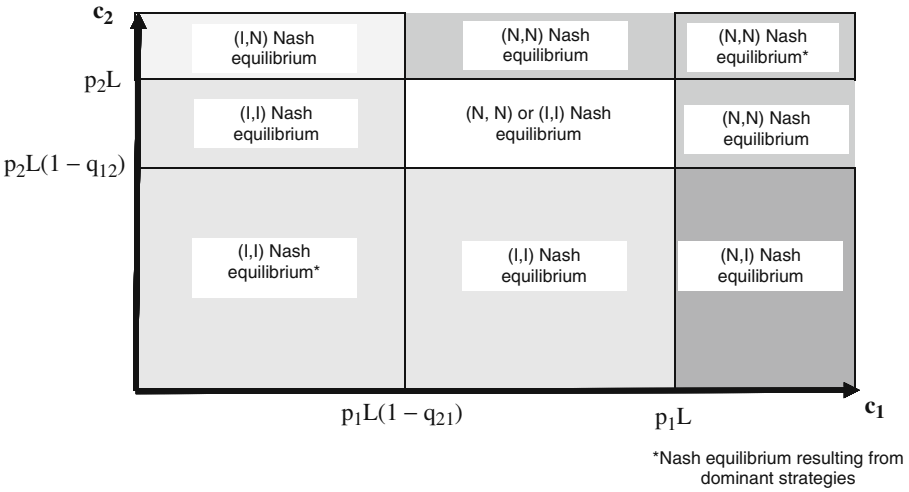

Figure 3 Various Nash equilibria depending on costs c1 and c2 (adapted from Heal and Kunreuther 2005)

strategy if c > pL. When c is between these two values there will be two Nash equilibria, i.e (I,I,…I) and (N,N. . .N). Moreover, if all ports are identical (same c), they will all choose the same strategy (the only Nash equilibria are the ones where all ports choose the same strategy, just as in the 2-port case—proof can be found in Kunreuther and Heal, 2003).

An extension of the above for various pi and qij (port i≠port j) is straightforward (see Heal and Kunreuther 2005).

Illustrations—numerical examples

In this section, we will demonstrate the results of the previous analysis through illustrations giving (theoretical, not real) values to the parameters in question. The case of two ports and then of n-ports will be discussed.

A case of 2 ports

Let's first examine two ports, both exporting containers directly to USA but also transferring containers between them before dispatching them to USA. Their annual income is M1 and M2 respectively.

Case I

Let's assume that the cost for each port of investing and operating a 100% scanning system at its gates is 100 mUSD[4] per year. Also that the loss each one will experience if a dangerous container is detected at the US borders (originating from the port) is L=4,000 mUSD (annually again). Without any security measures, it is

[4] Million US dollars. The monetary amounts used in these examples are only illustrative. Rough cost estimates can be found for example in EC (2010).

Table 2 Case I payoffs.

Payoffs		Port 2 (P2)	
		I	N
Port 1 (P1)	I	M1-100, M2-100	M1-140, M2-80
	N	M1-80, M2-140	M1-119.2, M2-119.2

also assumed that p=0.02 (i.e. there is a 2% probability that a port receives a dangerous container from the landside and then dispatches it directly to the US) and q=0.01 (i.e. there is a 1% probability that a port sends a dangerous container to the other one, before it is dispatched to the US from the latter).

From Table 1, we derive the payoffs of the two ports as shown in Table 2. It is obvious that both P1 and P2 have (N) as dominant strategy (see underlined payoffs), i.e. the equilibrium is where neither port invests in the scanning system. This outcome was expected according to the previous analysis as c > pL (it is pL=80 mUSD).

Case I has the structure of a "prisoner's dilemma" game, as outcome (I,I) is advantageous for both ports (players), but does not constitute a Nash equilibrium, as none of them has an economic incentive to invest in security on its own. Indeed, each port has a cost incentive not to invest in security, but if there were a coordinating mechanism to induce both ports to invest there would be a shared benefit.

Case II

For (I) (i.e. investing in security) for both ports to be a dominant strategy, then the cost of the scanning system should be c < pL(1-q) = 79.2 mUSD. Indeed, for c=40 m USD. we get Table 3, where the values suggest that (I,I) is the only equilibrium.

Case III

If $pL(1-q) < c < pL$, i.e. if 79.2 mUSD<c<80 mUSD) then there will be two Nash equilibria (I,I) and (N,N) and the solution to this game is indeterminate. Indeed, for c=79.5 mUSD we get Table 4.

In this case, we have two Pareto ranked Nash equilibria, where the ports have an interest in moving to the highest-ranked equilibrium, which is (I,I), as it corresponds to higher payoffs than (N,N) for both players. These are so-called coordination games. Port 1 could somehow convince port 2 to invest in security, as they both have an economic incentive to do so. Institutional mechanisms may ensure that the best outcome is attained, and this aspect is further discussed later on.

Table 3 Case II payoffs.

Payoffs		Port 2 (P2)	
		I	N
Port 1 (P1)	I	M1-40, M2-40	M1-80, M2-80
	N	M1-80, M2-80	M1-119.2, M2-119.2

Table 4 Case III payoffs.

Payoffs		Port 2 (P2)	
		I	N
Port 1 (P1)	I	M1-79.5, M2-79.5	M1-119.5, M2-80
	N	M1-80, M2-119.5	M1-119.2, M2-119.2

Other cases

According to the above analysis, there will be a Nash equilibrium where one agent invests in security and the other does not, if the ports have different costs c1 and c2 of investing in security measures. Specifically, (N,I)[5] will be a Nash equilibrium (i.e. P1 will not invest in scanning and P2 will invest in scanning) if c1 > pL and c2 < pL (1-q), i.e. c1>80 mUSD and c2<79.2 mUSD.

For example for c1=100 mUSD and c2=40 mUSD, we get Table 5, where (N,I) is the equilibrium.

A case of n ports

Let's consider now the case of n ports through an illustration. We keep the previous values, i.e. L=4,000 mUSD, p=2%, q=1%. Also, we consider six ports, which dispatch containers to USA, while containers are also transferred among them in this trade.

According to the previous analysis, the critical values for the cost c for each port (of investing and operating a 100% scanning system), which will determine the ports' decision to invest in security or not i.e. (I) or (N), will be:

$$c^* = p(L - X(6,0)) \text{ and } c^{**} = pL$$

and

- if c < c* then the equilibrium will be (I,I,…I) (i.e. invest in security for all six ports)
- if c > c** then the equilibrium will be (N,N,…N) (i.e. not invest in security for all six ports)

For the above values, we get X(6,0)=39.84 mUSD and c*=79.20319 mUSD[6] and c**=80 mUSD.

So

- if c<79. 20319 mUSD then the equilibrium will be (I,I,…I) (i.e. invest in security for all six ports)
- if c>80 mUSD then the equilibrium will be (N,N,…N) (i.e. not invest in security for all six ports)
- if 79.20319 mUSD<c<80 mUSD, then the equilibrium will be either (N,N,…N) or (I,I,…I). In this latter case, what each port will do is influenced by the decision of the rest of the ports.

[5] (I,N) will be a mirror case.

[6] We note that there is difference of only 3,190 USD compared to the case of two ports for the respective critical value.

Table 5 Case with c1 > pL and c2 < pL(1-q).

Payoffs		Port 2 (P2)	
		I	N
Port 1 (P1)	I	M1-100, M2-40	M1-140, M2-80
	N	M1-80, M2-80	M1-119.2, M2-119.2

It is interesting to note that the above calculations for $n=10$ or $n=100$ ports gave changes only in the 4th decimal of the c* value, i.e. insignificant changes of the order of hundreds of US dollars.

It is derived from the above that for sufficiently low values of c, ports will want to invest in security even if they can experience loss from dangerous containers originating from other ports, because they are able to reduce losses originating from containers received directly at their own facilities. If c is sufficiently high, then it is not worthwhile for any port to invest in container scanning. For c values in between the critical limits, what each port will do is influenced by the decision of the rest of the ports in the context of a coordination game.

Conclusions

The previous analysis examined security in container transportation and more specifically focused on investments in container checking systems by ports, considering the currently much debated 100% scanning requirement of containers destined to USA. A "dangerous container" transferred from port to port introduces an additional dimension of risk. Game theory was employed to investigate how interdependence affects individual port choices regarding security investments in container transportation, the latter viewed as an interdependent system in terms of security, an approach adopted from Kunreuther and Heal (2003), and Heal and Kunreuther (2005). Security measures depend on the actions of others because of the negative externalities created by those not investing in security upon the rest.

The examination of the case of two ports provided the main intuitions, before proceeding to the analysis of the case of n ports. The choices of the ports (invest or do not invest in a 100% container scanning system) are interdependent and result in different equilibria depending on parameters such as the cost c of investing in and operating the security measures and the probability of receiving a dangerous container during a given period of time.

For sufficiently low values of c, ports will want to invest in security even if they can experience loss from dangerous containers originating from other ports, because they are able to reduce losses originating from containers received directly at their own facilities. If c is sufficiently high, then it is not worthwhile for any port to invest in container scanning. For c values in between the critical limits, what each port will do is influenced by the decision of the rest of the ports.

In this latter case, there may be an economic rationale for a coordinating mechanism among the ports to induce them to invest in security. Other cost structures under which there is a need for coordination mechanisms to induce ports to invest in security for

their common benefit were also identified in the analysis (e.g. a Prisoner's dilemma game setting).

This coordinating role could be played by an industry association, such as the International Association of Ports and Harbors. Institutions or trade associations may encourage or force members to take measures by requiring security investments as a condition for membership. Inspections could enforce such regulatory requirements through the threat of fines.

In this rationale, international institutional requirements expressed through government intervention could take several forms, such as insurance, taxation and subsidies (see Kunreuther and Heal 2003; Heal and Kunreuther 2005). A form of "social" (common) insurance could internalize the above-mentioned externalities since it could provide coverage to all those players facing risks. A port adopting a security measure would be given premium reductions. A government could also employ corrective taxes and subsidies, i.e. tax non-investment or subsidize investment. As already commented, enforced standards or regulations could require certain security standards as a condition for operation.

Heal and Kunreuther (2005) also develop other dimensions of the problem, which in our context would concern the incentive for any port to invest in security, as a function of how many others have already done so. It might be expected that once a critical mass has invested, then all other ports will want to do the same. In a similar rationale, the change in the behavior of one port (change of strategy by one port or a small set of ports) may tip under certain conditions the whole system from one equilibrium to another, i.e. from an equilibrium with no investment in security to an equilibrium with improved security and improved profits. This phenomenon is referred to as tipping (Heal and Kunreuther 2005). An associated phenomenon is cascading (or domino effect), which refers to a situation in which one agent (here port) changes its policy, and this leads another to follow suit. The fact that two ports have changed now persuades a third to follow, and so on. It would be interesting to study the conditions under which the above phenomena may occur in the context examined in the present paper.

Acknowledgments This paper is based on a research work undertaken at the Laboratory for Maritime Transport of the National Technical University of Athens (NTUA), which is partially financed by Det Norske Veritas under the topic "Effective Bulk Transport" in the context of a strategic research and development collaboration with NTUA.

References

AmChamEU (2007) Comments on the US Legislation to require 100% container scanning. American Chamber of Commerce to the European Union, December 6th 2007 (www.amchameu.eu)

Azaiez M, Bier V (2007) Optimal resource allocation for security in reliability systems. Eur J Oper Res 181:773–786

Bakshi N, Gans N (2010) Securing the containerized supply chain: analysis of government incentives for private investment. Manage Sci 56(2):219–233

Basuchoudhary A, Razzolini L (2006) Hiding in plain sight—using signals to detect terrorists. Public Choice 128:245–255

Bier VM (2006) Game-theoretic and reliability methods in counterterrorism and security. In: Wilson AG, Wilson GD, Olwell DH (eds) (2006) Statistical methods in counterterrorism. Springer

Bier VM, Nagaraj A, Abhichandani V (2005) Protection of simple series and parallel systems with components of different values. Reliab Eng Syst Saf 87:315–323
Bier V, Oliveros S, Samuelson L (2007) Choosing what to protect: strategic defensive allocation against an unknown attacker. J Public Econ Theory 9(4):563–587
Carluer F, Alix Y, Joly O (2008) Global logistic chain security: economic impacts of the US 100% container scanning law. University of Le Havre study commissioned by the World Customs Organization (WCO), June 2008
Donner M, Kruk C (2009) Supply chain security guide. The International Bank for Reconstruction and Development/The World Bank
EC (2010) Secure trade and 100% scanning of containers. European Commission Staff Working Paper, Brussels, 11.2.2010, SEC(2010) 131 final
Gkonis KG, Psaraftis HN, Ventikos NP (2009) Game theory contributions to terrorism in merchant shipping: an application to port security. Proceedings of IAME 2009 Conference, June 24–26, Copenhagen, Denmark
Gkonis KG, Psaraftis HN, Ventikos NP (2010) Modelling security aspects of merchant shipping: a piracy setting, Proceedings of IAME 2010 Conference, July 7–9, Lisbon, Portugal
Heal G, Kunreuther H (2005) IDS models of airline security. J Confl Resolut 49(2):201–217
Kunreuther H, Heal G (2003) Interdependent security. J Risk Uncertain 26(2/3):231–249
Lapan H, Sandler T (1993) Terrorism and signaling. Eur J Polit Econ 9:383–397
NDIA (2009) Study blasts container scanning process. National Defense online magazine (www.nationaldefensemagazine.org), March 2009
Sandler T, Lapan HE (1988) The calculus of dissent: an analysis of terrorists' choice of targets. Synthese 76:245–261
Sandler T, Arce D (2003) Terrorism & game theory. Simul Gaming 34(3):319–337
Sandler T, Siqueira K (2006) Global terrorism: deterrence versus pre-emption. Can J Econ 39(4)
Straw J (2008) Outlook for container scanning. Security Management magazine online (www.securitymanagement.com), October 2008
Wein L, Wilkins A, Baveja M, Flynn S (2006) Preventing the importation of illicit nuclear materials in shipping containers. Risk Anal 26(5)
Zhuang J, Bier VM (2007) Balancing terrorism and natural disasters—defensive strategy with endogenous attacker effort. Oper Res 55(5):976–991