GAME THEORY CONTRIBUTIONS TO TERRORISM ANALYSIS IN MERCHANT SHIPPING: AN APPLICATION TO PORT SECURITY

Konstantinos G. GKONIS[1], Harilaos N. PSARAFTIS, Nikolaos P. VENTIKOS
Laboratory for Maritime Transport, School of Naval Architecture and Marine Engineering,
National Technical University of Athens
9 Heroon Polytechniou Str. 157 79 Zografou, Greece
[1]Corresponding author, email: cgonis@naval.ntua.gr, tel.: +30 6977 302427

Abstract

This paper concerns merchant shipping security and proposes a game theory framework for modelling terrorism threats and counteractions. First, the security considerations associated with merchant shipping in the post 9/11 era are reviewed, as well as the main current issues in maritime security, and the approaches developed in the academic literature. It is argued that game theory is suitable to address such security issues and its contributions to counter-terrorism in other security settings are reviewed. The purpose is to identify the relevance to merchant shipping security of concepts and insights developed in other security settings, and then accordingly apply them to the former.

In this context, such a game theoretic model is applied to a port security setting, where "port" and "ship" targets must decide on the level of their security measures and their associated costs, in order to respond to a potential attack by terrorists. The interaction settings involve the actors, their available options, their preferences and strategic goals, and other important parameters and assumptions. Defensive measures and potential damages are associated with cost variables.

The analysis considers on one hand the case where the targets decide independently about the deterrence measures each one will take, wishing to minimise its expected overall costs. This may result to an attack being diverted from one target to the other. On the other hand, the targets may reach defence measures decisions in coordination with each other, in order to achieve the game's social optimum. In this case, the aim is the collective best, while the players' actions may not be in their best private interests. Useful conclusions and suggestions are reached from such treatment of the subject through an appropriate numerical example.

Key words

Game Theory, Merchant Shipping, Security, Terrorism, Deterrence measures

GAME THEORY CONTRIBUTIONS TO TERRORISM ANALYSIS IN MERCHANT SHIPPING: AN APPLICATION TO PORT SECURITY

1. INTRODUCTION

Maritime security is an integral part of the International Maritime Organization's (IMO) responsibilities (IMO, 2008). Even though security was not absent from the international regulatory agenda before 2001, 9/11 provided an important push. Two months after the 9/11 attacks, IMO's 22nd Assembly adopted a resolution on "Review of measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships". The Assembly agreed to hold a diplomatic conference on maritime security in December 2002, to adopt any new regulations that might be deemed necessary to enhance ship and port security and prevent shipping from becoming a target of international terrorism.

The mandatory security measures, adopted in December 2002, include a number of amendments to the 1974 Safety of Life at Sea Convention (SOLAS), and mainly the International Ship and Port Facility Security Code (ISPS Code), which were developed by IMO's Maritime Safety Committee (MSC) and its Maritime Security Working Group. The ISPS Code is a comprehensive set of measures to enhance the security of ships and port facilities. The new security regime for international shipping entered into force on 1 July 2004.

Furthermore, many pieces of national and international legislation are based on the ISPS Code, and many more are based on similar concepts. For instance, EC Regulation 725/2004 on enhancing ship and port security transposes the ISPS Code into EU law, and EC Directive 2005/65/EC on enhancing port security provides additional requirements as regards port security, not only for the ship-port interface but also for the port perimeter. The US has a comprehensive arsenal of legislation on maritime security, including the SAFE[1] Port Act, the Container Security Initiative (CSI), the 24-hour rule, the C-TPAT[2], etc (see Psaraftis (2007) for more details). Looking at the legislative aspects of maritime security is outside the scope of this paper.

The threat of terrorist acts against the shipping and port industry is the major security concern. The purpose of the ISPS Code is to provide a standardized, consistent framework for evaluating risk. The idea is to reduce the vulnerability of the industry to attack, thus countering the threat and reducing the risk.

Terrorism is not a matter of concern to one country or a group of countries, it is a global issue. Eliminating the source of the threat, which in this case is those that would commit acts of terrorism or otherwise threaten the security of ships or of the port facilities, is essentially a government function. The maritime security provisions of SOLAS chapter XI-2 and the ISPS Code are part of a wider initiative to counter terrorism, including action by the Counter Terrorist Committee of the UN Security Council, co-operation with the World Customs Organization (WCO) on container security, joint initiatives with the International Labour Organization (ILO) on port security and identification documents etc.

[1] Security and Accountability for Every Port Act.
[2] Customs-Trade Partnership Against Terrorism.

This paper provides a preliminary identification of the relevance to shipping security of concepts and insights developed in other security settings, and it is explained why game theory is suitable to address them. A literature review of relevant security and counter-terrorism work is undertaken, before adapting such a model to the merchant shipping context, and more specifically concerning deterrence security measures in a port. The purpose of this paper is to analyse a port security problem with the use of game theory, in order to reach practical suggestions for the involved stakeholders. For one reason, security is different from safety (as there are at least 2 decision makers) and a different approach is needed. Game theory allows the treatment of players as rational decision-making agents with interdependent interests. The added value of our analysis, apart from the application context, is found in a numerical example, where the above suggestions were further elaborated by giving values to the model's parameters.

The models proposed in the context of this broader research work are in the stage of conceptual development and are not directly amenable to real world applications. Still, in this paper it is demonstrated how they can be useful to port authorities and shipping companies, in order to reach, propose, and support in the shipping community positions with a clear practical value backed by a robust methodological analysis, rather than intuition or a disputable policy viewpoint.

The rest of this paper is divided into the following sections. Section 2 discusses the methodological approach of game theory to merchant shipping security questions. Section 3 is the literature review. Section 4 continues with the actual modelling of security. Section 5 presents a numerical example of the previously developed model, and finally section 6 concludes the paper and briefly refers to further research.

2. 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 & Siqueira, 2006). Game theory analyses of terrorism provide policy insights that do not follow from non-strategic analyses, such as (in titles): Proactive vs. defensive policies; Interdependent security choices; Interaction of agents with asymmetric information (authorities / terrorists); First and second mover advantages; Authorities defensive measures (with budget constraints); Allocation of resources among antiterrorism measures; Terrorists' choice of targets; and security checkings.

There are many reasons why game theory is an appropriate methodology for the study of terrorism (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, formal safety assessment, and so on. In fact, if in safety there is a single decision maker whose decisions are the measures to be taken to enhance safety (these

are typically the Risk Control Options), in security the decision makers are two, those who aim to inflict damage (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. Game theory can capture the strategic interplay between terrorists and targets, where actions are interdependent as each side responds to its adversary's action. Both the terrorists and the target agents 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 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 defense or whether resistance is the most appropriate response. They may also gain a second-mover advantage by identifying soft targets after defensive expenditures have been allocated.

Thus, addressing terrorism 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 terrorists 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.

3. LITERATURE REVIEW

The first part of the literature review in this section is rather brief, as the interested reader can refer to a number of publications on the growing issue of shipping security and terrorism. The second part refers to the game theoretic treatment of terrorism issues.

3.1 Shipping security and terrorism

King (2005) provides an introduction to the security of transportation in general and shipping in particular. He draws attention to the most significant measures adopted to strengthen security and prevent terrorism, especially after the destruction of the World Trade Center in the United States.

Pinto and Talley (2006) study the security incident cycle of a port by investigating how ports and governments have addressed prevention, detection, response and recovery of port security incidents. They discuss several types of potential port security incidents and give examples of prevention strategies in US ports. A risk-based return-on-investment (RROI) approach is proposed that may be used to determine if enough security resources are being spent in light of the reduction in security risk afforded by resources (e.g. additional perimeter cameras, tighter ID and document authentication, higher fences, etc.).

Technological improvements are indeed a means of providing extra security. Stibe (2006) provides such examples, in face of the fact that only a small percentage of containers are

actually inspected in any given year. A current problem with container scanning are considerable delays, while it is spreading outside North America for the detection of nuclear and radioactive materials (Lloyd's List, 2008).

In the United States, a 24-Hour Rule requires that importers report the contents of their containers to customs inspectors one day before the boxes are loaded on ships bound for the United States (Flynn & Wein, 2005). Still, more than 90 percent of containers arrive without such checking and determined terrorists could easily take advantage of the knowledge that customs inspectors routinely designate certain shipments as low risk.

Brooks & Button (2006) discuss shipping security issues in the aftermath of the events of September 11th, 2001. The focus of the paper is on potential terrorist threats, rather than more traditional matters of piracy, smuggling or stowaways. This distinction is important because "the immediate aim of terrorism is essentially destruction, either of physical property or of social cohesion, whereas the others are acts in which damage is purely a collateral byproduct". "Safety" is essentially "technical" in its nature, rather than being a conscious act to cause damage. Security, in contrast, has always been "a gaming problem entailing acts designed to deliberately steal or damage individuals or property".

The paper also reviews the approach of international agencies such as the IMO. This has largely been one of suggesting generic measures, rules initiation and of an oversight role. Such an example is the ISPS Code. The Container Security Initiative (CSI) is a US-led effort which involves bilateral agreements that allow the nations involved to send inspectors to each other's ports. The Customs-Trade Partnership Against Terrorism (C-TPAT) is another US programme that seeks to develop cooperative relationships between firms in the global supply chain and the US authorities.

The EU brought out Regulation (EC) No725/2004 in 2004, just before the implementation date for the amendments to Solas and the ISPS Code. This regulation, which is the law for all EU member countries, ensures that the ISPS Code is implemented consistently across member states, and establishes inspection regimes, among other. In fact, the EU voted a second piece of legislation in 2005 for this last purpose, namely Regulation (EC) No884/2005 "Laying Down Procedures for Conducting Commission Inspections in the Field of Maritime Security" (Lloyd's List, 2008). Also, the 2005/65 Directive concerns safety issues up to the perimeter of ports, while Regulation 725/2004 covers mainly the ship-port interface. Moreover, the European Commission presented a Green Paper in 2005 titled "European Programme for Critical Infrastructure Protection-EPCIP", which also discusses Maritime Infrastructure Protection (Psaraftis, 2007).

Obviously, a number of regulatory interventions have been made around the world concerning shipping security. A great challenge is that these regulations become efficient on a practical and cost level, and that additional layers of bureaucracy are avoided. Also, any unnecessary overlapping of laws and authorities' responsibilities should be avoided (Psaraftis, 2007). For more on shipping security aspects, the reader can refer for example to Emerson & Nadeau (2003), Price (2004), Banomyong (2005), Bichou (2004).

3.2 Game theoretic contributions to terrorism questions

Sandler & 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 & 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 & 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 & 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, Oliveros, and Samuelson (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 & 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 & 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.

Heal & Kunreuther (2005) and Kunreuther & Heal (2003) 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.

Basuchoudhary & 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. The interested reader can find more references regarding the applications of game theory to security and counter-terrorism for example in Bier (2006).

4. MODELLING SECURITY IN MERCHANT SHIPPING

In the section, a model is presented, which has been adapted from the security and counter-terrorism literature to a security setting of merchant shipping.

4.1 Deterrence security measures in a port setting

In general, antiterrorism policies are either proactive or reactive. A proactive or pre-emptive policy involves aggressively going after the terrorists, in order to eliminate their resources and attack potential. A reactive or deterrence policy concerns protective measures either to divert the attack or limit its consequences. This model concerns deterrence measures taken by certain targets, in order to respond to potential terrorist attacks.

The structure of this model is based on Sandler and Lapan (1988) and Sandler and Arce (2003). As adapted here, it discusses deterrence security measures to be taken in a port area, in order to respond to a potential terrorist attack. The potential players are the port authority and the shipping firms (whose ships call at the port), on one hand, and a terrorist group planning an attack, on the other. The targets are of two kinds: (i) a ship moored at a port berth (denoted S) and (ii) port facilities (buildings, warehouses etc) (denoted P). An attack on target S results in collateral damage to P as well (as berths are also damaged or become unavailable for service for certain time). On the other hand, it is assumed that the opposite does not hold, i.e. an attack on target P has no collateral damage for S. Also, it is assumed that the terrorists are determined to place an attack at either one of the two targets.

In Figure 1, the deterrence game tree for the above described setting is shown (as adapted from Sandler and Arce, 2003). Initially, the levels of deterrence measures are chosen for the two targets (P and S), which are actually translated to costs D. These deterrence levels are associated with the terrorists' perceived likelihood of failure f following an attack at one of the two targets (P or S). Obviously, $1 - f$ are the probabilities of success following an attack at one of the two targets respectively.

Deterrence costs increase at an increasing rate with respect to the associated failure probability (these costs are assumed to be convex). Deterrence could be considered as an insurance policy, as it is paid regardless of the outcome.

The terrorists move next and decide which of the two targets to attack. The probability in each case is π_i , where i = {P, S}, which depends on their perceived failure probabilities i.e., $\pi_i(f_i, f_j)$ for i, j = {P, S} and $i \neq j$. The probability function is assumed continuous with:

$$\frac{\partial \pi_i}{\partial f_i} < 0 \ \ and \ \ \frac{\partial \pi_i}{\partial f_j} > 0 \qquad (0)$$

The meaning of these partial derivatives for the π functions is that there exists target transference, i.e., efforts by target i to limit terrorist success displaces the attack to target j.

The terrorists have a second-mover advantage in the sense that they place their attack after the deployment of the defensive measures, so that they can choose the softer target. The game has four outcomes depending on failure or success when each of the two targets is attacked.

The payoffs to the involved players are indicated at the bottom of Figure 1. The targets wish to minimize their costs, while the terrorists to maximize their benefits. More specifically, the terrorists' payoffs are L_i and H_i , i = {P, S}, for failure and success respectively, so that $L_i < H_i$. The collateral damage to P when S is attacked is *ld* when the attack on S is a failure and *hd* when it is a success. In the former case, the damage (cost) is expected to be lower so that *ld* < *hd*. Also, a symmetry of damage costs is assumed between the two targets. More specifically, when any of the targets is attacked with success the resulting damage is *HD* that is higher, than the damage cost *LD* when the attack is a failure (i.e. *HD* > *LD*).

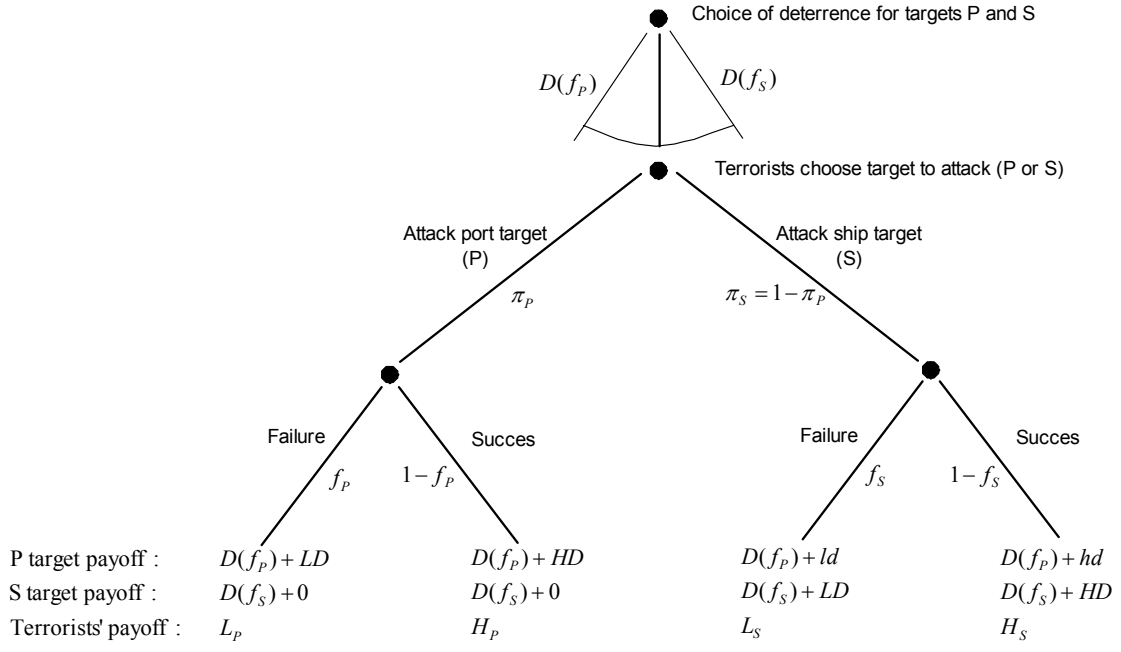

Figure 1: Game tree

In the following analysis, it is assumed that the terrorist threat is an exogenous parameter, and the focus is placed on the decision-making of players S target and P target. Two cases will be examined:

Case I: Simultaneous-move Nash equilibrium

The players P and S decide independently about the defence measures each one will take and so we are in search of a Nash Equilibrium of the game. Each of the players P and S wishes to minimise his expected costs and under the Nash Equilibrium they do so simultaneously, because it is at their best interest, and no player has unilaterally an incentive to deviate from such an equilibrium.

Case II: Social optimum cooperative equilibrium

The players P and S decide in coordination with each other about the defence measures each one will take as they want to achieve the game's social optimum. In this case, P and S aim at the collective best and their actions may not be in their best private interests (see for example the discussion on collective-action games in Dixit & Skeath, 2004). The social optimum is attained when the sum of the players' payoffs is minimised, i.e. a Pareto optimum cooperative equilibrium, which does not necessarily coincide with the Nash non-cooperative equilibrium.

4.2 Analysis

Given the above context, the expected costs to the port target (P) from an attack is (neglecting for the moment the cost of deterrence measures D):

$$EC(f_P) = f_P \cdot LD + (1 - f_P) \cdot HD \tag{1}$$

and the respective expected costs to the ship target (S):

$$EC(f_S) = f_S \cdot LD + (1 - f_S) \cdot HD \tag{2}$$

The expected collateral damage cost to P because of an attack on S is:

$$ECD(f_S) = f_S \cdot ld + (1 - f_S) \cdot hd \tag{3}$$

Given the setting and the assumptions of the model, $EC(f_i)$ decreases when f_i increases for i = {P, S} and also $ECD(f_S)$ decreases when f_S increases.

Overall, the port target P has an expected payoff (cost):

$$EP_P = D(f_P) + \pi_P \cdot EC(f_P) + \pi_S \cdot ECD(f_S) \tag{4}$$

Similarly, the ship target S has an expected payoff (cost):

$$EP_S = D(f_S) + \pi_S \cdot EC(f_S) \tag{5}$$

Case I

In Case I (see assumptions above), a Nash equilibrium corresponds to each target group minimizing its expected costs. The first-order condition for minimizing the ship target S's expected cost is:

$$\begin{aligned} &\frac{\partial EP_P}{\partial f_P} = 0 \\ &\Rightarrow \frac{dD(f_P)}{df_P} + \frac{\partial \pi_P}{\partial f_P} \cdot EC(f_P) + \pi_P \cdot \frac{dEC(f_P)}{df_P} + ECD(f_S) \cdot \frac{\partial \pi_S}{\partial f_P} = 0 \end{aligned} \tag{6}$$

This last expression includes the marginal deterrence costs (left side, 1st term), the marginal benefits of diverting an attack and limiting damage to P (2nd and 3rd terms), and the potential harm to P from an attack deflected to S (4th term), because of the assumed collateral damage.

In a similar fashion, the first-order condition for minimizing the port target P's expected cost is:

$$\frac{\partial EP_S}{\partial f_S} = 0$$
$$\Rightarrow \frac{dD(f_S)}{df_S} + \frac{\partial \pi_S}{\partial f_S} \cdot EC(f_S) + \pi_S \cdot \frac{dEC(f_S)}{df_S} = 0 \qquad (7)$$

The solution $f_P = f_P{}^N$ and $f_S = f_S{}^N$ to the set of equations (6) and (7) corresponds to the deterrence levels adopted by targets P and S under the Nash Equilibrium, i.e. $D(f_P{}^N),\ D(f_S{}^N)$.

Case II

In Case II (see assumptions in the description of the problem), the social optimum is the goal, i.e. when the sum of P and S's expected payoffs is minimized. This aggregate expected cost is [by adding (4) + (5)]:

$$P = D(f_P) + D(f_S) + \pi_P \cdot EC(f_P) + \pi_S \cdot [EC(f_S) + ECD(f_S)] \qquad (8)$$

The first-order condition for a minimum to (8) with respect to f_P is examined:

$$\frac{\partial P}{\partial f_P} = \frac{dD(f_P)}{df_P} + 0 + \frac{\partial \pi_P}{\partial f_P} \cdot EC(f_P) + \pi_P \cdot \frac{dEC(f_P)}{df_P} + [EC(f_S) + ECD(f_S)] \cdot \frac{\partial \pi_S}{\partial f_P} \qquad (9)$$

In order to compare with the results in Case 1, we set $f_P = f_P{}^N$, i.e. when (6) holds, and expression (9) becomes:

$$\left.\frac{\partial P}{\partial f_P}\right|_{f_P = f_P{}^N} = EC(f_S) \cdot \left.\frac{\partial \pi_S}{\partial f_P}\right|_{f_P = f_P{}^N} < 0 \qquad (10)$$

as $EC(f_S) < 0$ and $\frac{\partial \pi_S}{\partial f_P} > 0$.

The expression in (10) represents the external costs that the independent deterrence decision of target P imposes on target S by transferring more attacks to S. In other words, when the targets decide on their defense measures independently, the social outcome is not achieved as the first-order condition - under which expression in (9) equals 0 - is not met. Instead, (10) implies that target P spends too much on deterrence, i.e. "P over-deters".

The first-order condition for a minimum to (8) with respect to f_S is also examined:

$$\frac{\partial P}{\partial f_S} = 0 + \frac{dD(f_S)}{df_S} + \frac{\partial \pi_P}{\partial f_S} \cdot EC(f_P) + \frac{\partial \pi_S}{\partial f_S} \cdot [EC(f_S) + ECD(f_S)] + \pi_S \cdot [\frac{dEC(f_S)}{df_S} + \frac{dECD(f_S)}{df_S}] \quad (11)$$

By setting $f_S = f_S{}^N$, i.e. when (7) holds, expression (11) becomes:

$$\left.\frac{\partial P}{\partial f_S}\right|_{f_S = f_S{}^N} = \left.\frac{\partial \pi_P}{\partial f_S}\right|_{f_S = f_S{}^N} \cdot EC(f_P) + \left.\frac{\partial \pi_S}{\partial f_S}\right|_{f_S = f_S{}^N} \cdot ECD(f_S{}^N) + \pi_S \cdot EC'(f_S{}^N) \quad (12)$$

The sign of expression (12) depends on the signs and values of each of its 3 terms, which are elaborated in Appendix 1. If the overall sum (term 1 + term 2 + term 3) is positive then the S target under-deters, because terms 2 and 3 dominate term 1 and the impact on S and its collateral damage to P, is higher than the impact from a possible diversion of the attack to P. While when expression (12) is negative, then the S target over-deters, as the impact from the diversion of the attack to P is more important than the impact on S and its collateral damage to P (see Appendix 1 for further details).

For the two players P and S to achieve the social optimum, their respective deterrence levels must be $D(f_P{}^O)$, $D(f_S{}^O)$, given the solution $f_P = f_P{}^O$ and $f_S = f_S{}^O$ to the set of equations that we get, when (9) and (11) are set equal to 0.

4.3 Assessment of results

The previous analysis examined two cases. In Case I, the players P and S decide independently about the defense measures each one will take with the goal of minimizing their expected costs. The Port Authority can be considered on one hand, which decides on the measures to be taken to protect the port infrastructure from a potential terrorist attack. A Shipowner can be considered on the other hand, who also decides about the security measures for his ship moored at a port's berth. Both players know (common knowledge) the game's structure, e.g. the fact that the choices of one player influence the choices of the other player, as attacks may be diverted from one target to the other. An important insight of the presented model is that as alternative targets divert attacks, those least able to do so become the victims. In this context, the Nash Equilibrium of the game was found, under which both P and S act to their best interests simultaneously and no player has unilaterally an incentive to deviate from it.

The above results where assessed in the context of another Case II, where the players P and S's goal is the social optimum or collective best. In the considered setting, the social optimum is attained when the sum of the players' expected costs is minimized. It was shown, that their decisions under a Nash Equilibrium (Case 1) do not satisfy the social optimum goal (i.e. the social optimum security measures do not coincide with the Nash Equilibrium). Instead, a P target over-deters (when the social optimum is considered), while the S target's choice ranges from over-deterrence to under-deterrence.

So, the above results are suggesting that when a Port Authority and a calling Ship are left to act independently regarding their security measures, the former is inclined to over-deter and thus divert potential terrorist attacks to the ship target. The latter, may either under-deter or

over-deter depending on the anticipated damages from such an attack, any collateral damage etc. The overall result may be over-spending. These inefficiencies are attributed to the externalities associated with the involved actors' decisions, i.e. the impact they have on each other. These externalities can be internalized by an overseeing authority. In this case, decentralized decision-making will be replaced by a central coordinating authority having under its umbrella all the involved actors. Obviously, an adequate legislative framework is required for such purpose in the service of the social optimum.

5. NUMERICAL EXAMPLE

Next, we will illustrate the above-presented model and its results through a numerical example. We set the values *LD*=-10 mEUR[3], *HD*=-100 mEUR, *ld*=-2 mEUR, *hd*=-10 mEUR (which are of course assumptions, and not real data), so that:

$$(1) \Rightarrow EC(f_P) = f_P \cdot (-10) + (1 - f_P) \cdot (-100)$$

$$(2) \Rightarrow EC(f_S) = f_S \cdot (-10) + (1 - f_S) \cdot (-100)$$

$$(3) \Rightarrow ECD(f_S) = f_S \cdot (-2) + (1 - f_S) \cdot (-10)$$

Also, we set:

$$\pi_P = (1 - f_P) \cdot f_S = f_S - f_P \cdot f_S$$
$$\pi_S = (1 - \pi_P) = 1 - f_S + f_P \cdot f_S$$

which meet the conditions (0).

Moreover, the deterrence measures costs for the Port and Ship target are set respectively to (in mEUR):

$$D(f_P) = -100 \cdot f_P^{\,2}$$
$$D(f_S) = -30 \cdot f_S^{\,2}$$

So:

$$(4) \Rightarrow EP_P = -100 \cdot f_P^{\,2} + (f_S - f_P \cdot f_S) \cdot [f_P \cdot (-10) + (1 - f_P) \cdot (-100)] + (1 - f_S + f_P \cdot f_S) \cdot [f_S \cdot (-2) + (1 - f_S) \cdot (-10)]$$

$$(5) \Rightarrow EP_S = -30 \cdot f_S^{\,2} + (1 - f_S + f_P \cdot f_S) \cdot [f_S \cdot (-10) + (1 - f_S) \cdot (-100)]$$

Case I: Nash equilibrium

The relevant calculations are shown in Appendix 2, which give the Nash equilibrium:

$$f_P^{\,N} = 0.47 \Rightarrow D(f_P^{\,N}) = -22.09\, mEUR$$
$$f_S^{\,N} = 0.92 \Rightarrow D(f_S^{\,N}) = -25.39\, mEUR \qquad \text{(Nash equilibrium)}$$
$$\pi_P = 0.49,\ \pi_S = 0.51$$

[3] cost unit, e.g. mEUR = million EURO

So the Port target takes deterrence measures which cost 22.09 mEUR, while the Ship target deterrence measures of 25.39 mEUR. The probability of an attack placed on either P or S is almost equal.

Case II: Social optimum

The relevant calculations are shown in Appendix 3, which give the social optimum:

$$f_P^{\,O} = 0.28 \Rightarrow D(f_P^{\,N}) = -7.84\,mEUR$$
$$f_S^{\,O} = 0.61 \Rightarrow D(f_S^{\,N}) = -11.16\,mEUR \qquad \text{(Social optimum)}$$
$$\pi_P = 0.44,\ \pi_S = 0.56$$

So the Port target takes deterrence measures which cost 7.84 mEUR, while the Ship target deterrence measures of 11.16 mEUR. The probability of an attack placed on P is 44%, while of an attack placed on S is 56%.

Comparison

A comparison of the Nash equilibrium (Case I) with the Social optimum results (Case II) (see also Table 1 below) suggests that under the former both P and S over-deter, i.e. they over-spend in deterrence measures. Indeed, in Case I total deterrence measures (i.e. $D(f_P) + D(f_S)$) cost about 47 mEUR, while in Case II only about 19 mEUR.

Table 1: Comparison of Case I & Case II results

	Case I	**Case II**
Probabilities		
failure prob. fp	47%	28%
failure prob. fs	92%	61%
attack prob. πp	49%	44%
attack prob. πs	51%	56%
Costs	*mEUR (rounded)*	
deterrence D(fp)	-22	-8
deterrence D(fs)	-25	-11
expected damage EC(fp)	-58	-75
expected damage EC(fs)	-17	-45
expected damage ECD(fs)	-3	-5
expected payoff EPp	-52	-44
expected payoff EPs	-34	-36
aggregate cost P	-86	-80

In Case I, where both players' aim is to serve their private interests, the possibility of attack on either of them is almost equal. In Case II, the possibility of attack on P has been reduced and equally increased for S, as the benefit of the whole is the goal, i.e. the minimization of the aggregate expected cost. In this context, S accepts to become a more likely target (the probability of an attack on S, $\pi_S = 1 - \pi_P$, has increased to 56%). Indeed, while in Case I the expected payoff for P and S (calculated from (4) and (5) respectively) is approximately -52 mEUR and -34 mEUR, in Case II the respective payoffs are approximately -44 mEUR and -36 mEUR, i.e. the P target has reduced its expected payoff, while S has increased it. Overall,

in Case I the aggregate expected cost P is approximately -86 mEUR, while in Case II it has been decreased to -80 mEUR (the minimum).

Another interesting remark is that in Case II the players manage to minimize the aggregate expected cost by decreasing their deterrence measures costs and thus increasing the possibility of success following an attack on either of them (compare the values of f_P and f_S in the two cases). So, the expected damage costs (calculated from (1), (2) and (3)) have actually increased in Case II, but the lower deterrence measures costs result in an overall lower aggregate expected cost. This result is acceptable given the model's assumptions about costs and probabilities, however in a real setting the damage costs may involve the loss of human life and any increase of such losses may be just unacceptable. This must be taken into account and accordingly represented in the values of the model's parameters.

6. CONCLUSIONS AND FURTHER RESEARCH

This paper examined the potential contributions of game theory to security and counter-terrorism problems in merchant shipping and forms part of a broader research work. Security is different from safety (as there are at least 2 decision makers) and a different approach is needed to analyse it. Game theory allows the treatment of players as rational decision-making agents with interdependent interests.

The literature review referred to other works related to shipping security and terrorism, but mainly focused on game theoretic contributions to terrorism questions in other security settings. The main and innovative contribution of the present research and this paper is attempting to bridge the game theoretic methodological approach with the security and terrorism problems in merchant shipping. In this context, a relevant model from the literature was adapted to the merchant shipping context, and more specifically concerning deterrence security measures in a port setting.

The analysis examined the interrelated decision-making of an appropriately defined Port and Ship target vis-à-vis the attack choice of a terrorist group and focused on two cases. Namely, a so-called simultaneous-move Nash equilibrium case and a Social optimum cooperative equilibrium case. The analysis' results demonstrated the inefficiencies (translated e.g. to overspending) when the defending decision-makers act independently, which are derived from the externalities associated with their decisions, i.e. the impact they have on each other. These inefficiencies can be overcome with a centralized decision-making structure, as it was accordingly proposed. The added value of our analysis, apart from the application context, is found in a numerical example, where the above suggestions were further elaborated by giving values to the model's parameters.

In other words, what this paper shows about port and shipping security is that when a Port Authority and a calling Ship are left to act independently regarding their security measures, the former is inclined to over-deter and thus divert potential terrorist attacks to the ship target. The latter, may either under-deter or over-deter depending on the anticipated damages from such an attack, any collateral damage etc. The overall result may be over-spending, and therefore decentralized decision-making needs to be replaced by central coordination having under its umbrella all the involved actors. In this respect it is suggested that an adequate

legislative framework may be the missing element, and this suggestion is the outcome of a quantitative methodological analysis, rather than intuition or a disputable policy viewpoint.

Extensions to the presented model that can be considered include: the examination of the decision-making from the terrorists point of view; the introduction of incomplete information about terrorists preferences; the introduction of more targets; and the consideration of budget constraints for the allocation of defensive measures.

Other models considered in the context of the broader research work concern: transnational port security choices, where two international ports with commerce relationships face similar terrorist threats; security considerations for a logistical port system, where a defender is responsible for the functionality of the logistical system of a port infrastructure, against terrorist attacks (the system comprises as components sea transport, port berths / facilities, storage facilities, intermodal transport); container transportation as an interdependent security system, where the transport of a potentially contaminated container is considered, along several links (agents) of a transport chain, who may either invest in a security system or not (the adoption of security procedures by one agent / container transporter may not mitigate the risks faced as the result of the transfer from other agents); piracy threats, precautions, deterrence measures and counter-actions and modelling of relevant interaction settings; and passenger checking.

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

Azaiez, M. and V. Bier (2007), "Optimal resource allocation for security in reliability systems", European Journal of Operational Research, 181: 773–786

Banomyong, R. (2005), "The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management", Maritime Policy and Management, 32: 3–13

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

Bichou, K. (2004), "The ISPS Code and the Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management", Maritime Economics and Logistics 6:322–348

Bier V. M. (2006), "Game-Theoretic and Reliability Methods in Counterterrorism and Security" in A. G. Wilson, G. D. Wilson and D. H. Olwell (eds) (2006) "Statistical Methods in Counterterrorism", Springer

Bier V. M., A. Nagaraj, and V. Abhichandani (2005), "Protection of simple series and parallel systems with components of different values", Reliability Engineering and System Safety 87: 315–323

Bier, V., S. Oliveros, and L. Samuelson (2007), "Choosing what to protect: Strategic Defensive Allocation against an unknown attacker", Journal of Public Economic Theory, 9 (4), 2007, pp. 563–587

Brooks, M. and K. Button (2006), "Market Structures and Shipping Security", Maritime Economics & Logistics, 8: 100–120

Dixit, A. and S. Skeath (2004), Games of Strategy, 2nd edition, W.W. Norton & Company

Emerson, S.D. and J. Nadeau (2003), "A Coastal Perspective on Security", Journal of Hazardous Materials, 104:1-13

Flynn, S.E. and L.M.Wein (2005), "Think Inside the Box", The New York Times, November 29, 2005

Heal, G. and H. Kunreuther (2005), "IDS Models of Airline Security", Journal of Conflict Resolution, Vol. 49 No. 2, 201-217

IMO (2008), International Maritime Organization website, http://www.imo.org/

King, J. (2005), "The security of merchant shipping", Marine Policy, 29 (2005) 235–245

Kunreuther, H. and G. Heal (2003), "Interdependent Security", The Journal of Risk and Uncertainty, 26:2/3; 231–249

Lapan, H. and T. Sandler (1993), "Terrorism and signaling", European Journal of Political Economy, 9 (1993) 383-397

Lloyd's List (2008), Special Report on Maritime Security, 18 August 2008, http://www.lloydslist.com

Pinto, C.A. and W. K. Talley (2006), "The Security Incident Cycle of Ports", Maritime Economics & Logistics, 8: 267–286

Price, W (2004), "Reducing the Risk of Terror Events at Seaports", Review of Policy Research, 21: 329–349

Psaraftis, H.N. (2007), "Port security", course material, Laboratory for Maritime Transport, National Technical University of Athens

Sandler, T. and D. Arce (2003), "Terrorism & Game Theory", Simulation & Gaming, 34:3, 319-337

Sandler, T. and H.E. Lapan (1988), "The calculus of dissent: an analysis of terrorists' choice of targets", Synthese, 76: 245-261

Sandler, T. and K. Siqueira (2006), "Global Terrorism: deterrence versus pre-emption", Canadian Journal of Economics, Vol. 39, No. 4

Stibe, M. (2006), "Shipping security—all at sea?", Infosecurity Today, March/April 2006

Wein, L., A. Wilkins, M. Baveja, and S. Flynn (2006), "Preventing the Importation of Illicit Nuclear Materials in Shipping containers", Risk Analysis, Vol. 26, No. 5

Zhuang, J. and V. M. Bier (2007), "Balancing Terrorism and Natural Disasters - Defensive Strategy with Endogenous Attacker Effort", Operations Research, 55: 5, 976–991.

APPENDIX 1

The sign of the expression in (12) depends on the signs and values of each of its 3 terms.

Term 1, i.e. $\frac{\partial P}{\partial f_S} = \left.\frac{\partial \pi_P}{\partial f_S}\right|_{f_S = f_S{}^N} \cdot EC(f_P)$, is negative (as the product of a positive partial derivative and a negative - cost - expected payoff) and it corresponds to the external transference costs on P (for example when f_S increases, π_P also increases and the attack is diverted to target P from target S, with an associated expected cost on P).

Term 2, i.e. $\left.\frac{\partial \pi_S}{\partial f_S}\right|_{f_S = f_S{}^N} \cdot ECD(f_S{}^N)$, is positive (as the product of a negative partial derivative and a negative - cost - expected payoff) and it corresponds to the collateral damage costs on P from an attack on S or a potential external benefit to P (for example when f_S increases, π_S decreases and, while the attack is diverted to P, the expected collateral damage on P from an attack on S decreases).

Term 3 is $\pi_S \cdot EC'(f_S{}^N) = \pi_S \cdot (LD - HD)$ (from (2)) and it is positive (as the product of a positive probability and a positive incremental cost term). It corresponds to the incremental damage costs on S from an attack on S (when f_S increases, $EC(f_S)$ decreases).

APPENDIX 2

In order to find the Nash equilibrium we need to find the solution to the set of equations (6) and (7):

$$(6) \Rightarrow \frac{\partial EP_P}{\partial f_P} = 0$$

$$\xrightarrow{(4)} -200 \cdot f_P - 180 \cdot f_P \cdot f_S + 180 \cdot f_S + 8 \cdot f_S{}^2 = 0 \qquad (6')$$

$$(7) \Rightarrow \frac{\partial EP_S}{\partial f_S} = 0$$

$$\xrightarrow{(5)} -240 \cdot f_S + 180 \cdot f_S \cdot f_P - 100 \cdot f_P + 190 = 0 \qquad (7')$$

The solution to (6'), (7') gives the Nash equilibrium.

APPENDIX 3

The aggregate expected cost is:

$$(8) \xrightarrow{(4),(5)}$$

$$P = -100 \cdot f_P{}^2 + -30 \cdot f_S{}^2 + (f_S - f_P \cdot f_S) \cdot (90 f_P - 100) + (1 - f_S + f_P \cdot f_S) \cdot (98 f_S - 110) \qquad (8')$$

The first-order condition for a minimum to the aggregate expected cost with respect to f_P gives:

$$\frac{\partial P}{\partial f_P} = -200 f_P - 180 f_P \cdot f_S + 80 f_S + 98 {f_S}^2 \qquad (9')$$

which for $f_P = {f_P}^N$ gives:

$$\left.\frac{\partial P}{\partial f_P}\right|_{f_P = {f_P}^N} = -94 - 4.6 \cdot f_S + 98 {f_S}^2 < 0, \; as \; 0 \le f_S \le 1$$

as expected (see (10)). Similarly, the first-order condition for a minimum to the aggregate expected cost with respect to f_S gives:

$$\frac{\partial P}{\partial f_S} = -256 f_S + 80 f_P - 90 {f_P}^2 + 196 f_P \cdot f_S + 108 \qquad (11')$$

which for $f_S = {f_S}^N$ gives:

$$\left.\frac{\partial P}{\partial f_S}\right|_{f_S = {f_S}^N} = -127.52 + 260.32 f_P - 90 {f_P}^2$$

whose sign is undetermined. Setting $f_P = {f_P}^N$ (i.e. for the Nash equilibrium) gives to $\frac{\partial P}{\partial f_S}$ a negative value, which means that the S target over-deters (see the analysis section). Overall, the Nash equilibrium does not serve the social optimum. The latter we get by finding the solution $f_P = {f_P}^O$ and $f_S = {f_S}^O$ to the set of equations derived from setting (9') and (11') equal to 0.