Topic: Shipping
Sub- Topic: Maritime security

CARGO Edições, Lda

MODELLING SECURITY ASPECTS OF MERCHANT SHIPPING: A PIRACY SETTING

Konstantinos G. Gkonis[1]
Email address: cgonis@naval.ntua.gr

Harilaos N. Psaraftis
Email address: hnpsar@mail.ntua.gr

Nikolaos P. Ventikos
Email address: niven@deslab.ntua.gr

Laboratory for Maritime Transport, National Technical University of Athens
Address: 9, Iroon Polytechneiou str, 157 73 Zografou, Greece
Phone: +30 210 77 21 410 / Fax: +30 210 77 21 408

Abstract:

This paper concerns merchant shipping security and proposes a game theoretic model for modelling piracy threats and counteractions. Piracy has become a central concern for the international maritime community, especially after the recent tremendous increase in the number of piracy attacks in the Gulf of Aden and adjacent waters, off Somalia and the eastern coasts of Africa. This phenomenon has forced governments around the world into political and military action. However, the pirates appear to have adapted their operations to these developments. The piracy phenomenon is basically a security problem, where on one side the international community is seeking for measures to restrain attacks on merchant ships, while on the other side, pirates develop tactics and assess the existing situation in order to successfully place hijacking attacks.

An interaction setting (game) is examined in the present approach between two players, a defender and an attacker. The defender (player 1) is a naval force command and the attacker (player 2) is the pirates "headquarters" (where their leaders plan their attacks). Two potential target areas for the pirates (and respective areas for the development of the naval forces) are considered, each of which is defined within certain geographical limits. Technically, this is an incomplete information game with information asymmetry.

Following a number of assumptions, the analysis reaches interesting suggestions for the side of the defender, given the behaviour of the attacker. For example, regarding the target areas which should be defended and the level of defense measures, as a function of the expected damage costs that the shipping community might suffer, budget considerations, and damage expectations for any given defense strategy. In general, parametric analyses can be performed to reach useful results, regarding the optimal allocation of ships - defense measures, for given expectations (and not knowledge) for piracy activity.

Keywords:

Shipping security, piracy, game theory

[1] Author for correspondence and presenting the paper

MODELLING SECURITY ASPECTS OF MERCHANT SHIPPING: A PIRACY SETTING

1. INTRODUCTION AND BACKGROUND

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 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. Security is different from safety as, for one reason, there are at least 2 decision makers, and therefore a different approach is needed. Game theory allows the treatment of players as rational decision-making agents with interdependent interests. In this framework also belongs the paper by Gkonis et al. (2009) presented at the IAME 2009 Conference and Gkonis & Psaraftis (2010).

The present paper adopts a game theoretic model developed in Bier et al. (2007) to address interesting aspects of a piracy setting with the purpose of producing some useful suggestions. So the added value of our analysis is mainly associated with the application context and the demonstration of the relevance of such modelling tasks to a field of utmost concern for the shipping community nowadays. More specifically, the present analysis is about the deployment of naval forces in a sea area with the objective of optimal protection from piracy attacks.

It is useful to note for the reader who is unfamiliar with the present methodological approach, that game theory analyses of terrorism and security issues provide policy insights that do not follow from non-strategic analyses, and there are many reasons for this (see for example Sandler and Arce, 2003). First of all, 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 and those who want to avoid it. 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 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. 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.

The interested reader can refer to a number of publications on the growing issue of shipping security, piracy and terrorism. Therefore the following indicative reference to the literature only concerns a game theoretic treatment of security and terrorism issues, that introduce the reader to the rationale of the present approach.

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. Pre-emption measures refer to actions that a targeted government must independently decide, such as launching an attack against a terrorist group. 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.

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 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.

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.

The present paper is based on Bier et al. (2007), who 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. The interested reader can find more references regarding the applications of game theory to security and counter-terrorism for example in Bier (2006).

The rest of this paper is divided into the following sections. Section 2 describes the model which serves as a basis for the following analysis. Section 3 proceeds with the analysis of the model. Section 4 presents the application of the model to a piracy setting. After some background discussion of the piracy phenomenon, which justifies the use of the proposed methodological approach, a numerical example is presented which provides the main suggestions of the proposed treatment of the subject. Section 5 concludes the paper.

2. MODEL DESCRIPTION

The model adopted in this paper from Bier et al. (2007) is about deterrence measures in a security interaction setting (game) between two players, a defender and an attacker. Moreover, in this setting the defender defends two targets called P and S.

The interaction is represented as in Figure 1. The defender chooses initially the levels of deterrence measures for the two targets (P and S), which are actually translated to costs *Di , i = {P, S}*. These deterrence levels are associated with the attackers' perceived likelihood of failure *fi* following an attack at one of the two targets (P or S) (obviously, $1 - f_i$ are the respective probabilities of success).

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.

It is assumed for simplification that $L_i=0$, $i = \{P, S\}$, which are the attackers' payoffs for failure. The terrorists' payoffs for success are H_i , $i = \{P, S\}$, so that the pair (H_P, H_S) can be regarded as the attacker's preferences, which define the "type" of the attacker. In the general case, the type of the attacker (H_P, H_S) is not known by the defender (uncertainty about attacker's valuation), and so there exists information asymmetry (the attacker obviously knows his own type) and we have an incomplete information game. In this case, it can be considered that the type of the attacker is drawn (by Nature) from a known cumulative distribution function $F(H_P, H_S)$, with density $f(H_P, H_S)$.

Also, it is assumed that there is no collateral damage following an attack to either target, so that *ld=hd=0*. Moreover, when an attack is a failure, the damage cost is assumed *LD=0*. However, when an attack is a success, the damage cost (loss) is HD_i , $i = \{P, S\}$.

So, the defender does not know the attacker's preferences (H_P, H_S), while the attacker observes the defender's resource allocation (D_P , D_S) and chooses which target to attack. The probability of placing an attack on either target *i* is π_i, which does not depend only on the perceived failure probabilities f_i, f_j (i.e. the defender's strategy (D_P , D_S)), but also on the attacker's strategy, as it will be explained next.

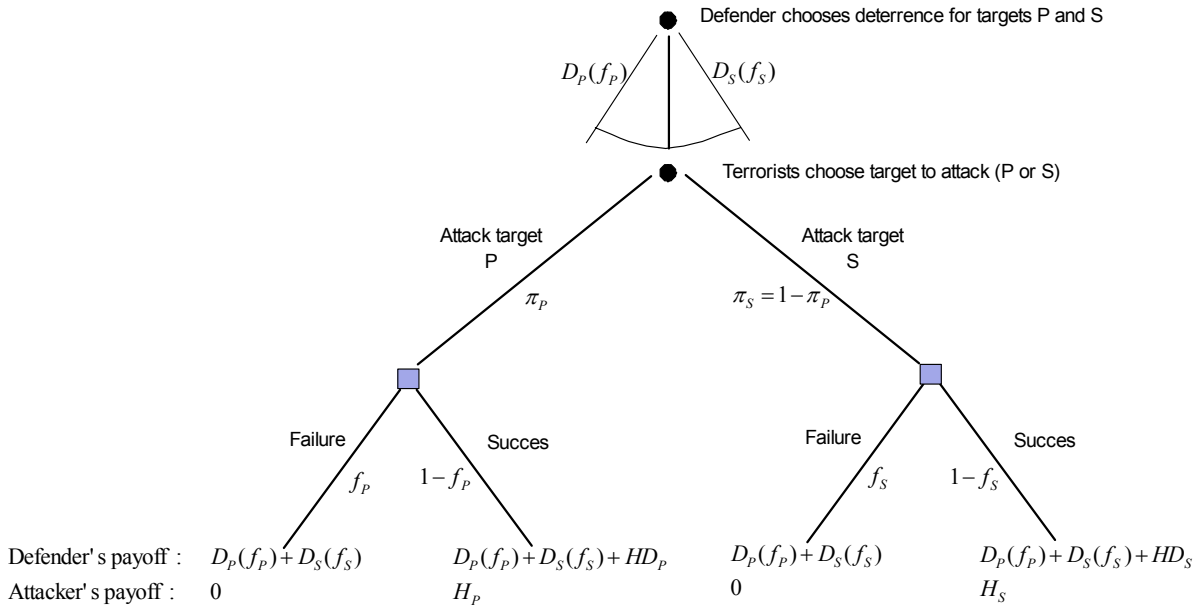

Figure 1: Interaction representation (game tree)

3. MODEL ANALYSIS

3.1 Strategies – Payoffs

Given the above interaction formulation, the defender's (pure) strategies are represented by pairs *($D_P(f_P)$, $D_S(f_S)$)*, while the attacker's strategy space will be defined as binary, with available strategy choices $s(H_P, H_S, D_P, D_S) = \{0,1\}$, where s=1 for attack at P, and s=0 for attack at S.

In the general case (under uncertainty about the attacker's valuation, as explained above), the probability that P will be attacked is:

$$\pi_P(D_P, D_S, s) = \int_{H_P} \int_{H_S} s(H_P, H_S D_P, D_S)\, f(H_P, H_S)\, dH_P\, dH_S \quad (1)$$

while the probability that S will be attacked is $\pi_S = 1 - \pi_P$.

The attacker's expected payoff (or gain that he wishes to maximize) will be:

$$U(D_P, D_S, s) = \int_{H_P} \int_{H_S} [s(.)(1-f_P)H_P + (1-s(.))(1-f_S)H_S]\, f(H_P, H_S)\, dH_P\, dH_S \quad (2)$$

The defender's expected payoff (or damage/cost that he wishes to minimise) will be:

$$L(D_P, D_S, s) = \pi_P(1-f_P)HD_P + \pi_S(1-f_S)HD_S + D_P(f_P) + D_S(f_S) \quad (3)$$

3.2 Equilibrium

The equilibrium solution consists of the optimal strategy choices for the two players, denoted (D_P^*, D_S^*) and s^*. It is proved in Bier et al. (2007) that there always exists a pure equilibrium, i.e. mixed strategies[1] are not required to attain an equilibrium outcome.

Attacker's optimal strategy

From Eq. (2), and in order to maximize the attacker's expected payoff, it will be *s*=1 if $(1-f_P)H_P > (1-f_S)H_S$ and *s*=0 in the opposite case. So, overall:

- If $\frac{H_S}{H_P} < \frac{1-f_P}{1-f_S} \Rightarrow s^* = 1$, while if $\frac{H_S}{H_P} > \frac{1-f_P}{1-f_S} \Rightarrow s^* = 0$
- In case, $(1-f_P) = (1-f_S)$ then the attacker will choose the target with the higher value to him.

The above are represented in Figure 2. If $(1-f_P) = (1-f_S)$, then the two areas representing attack on either S or P have the same surface. If the ratio $\frac{1-f_P}{1-f_S}$ takes a value other than 1, then the attack on P or S becomes more likely.

[1] Mixed-strategies refer to the choice of strategies by players at random (but according to specific and optimal probabilities that can be determined), so that the other player cannot know which strategy will be used.

It is interesting to note, that if (for example) target S is undefended, then the possibility of success for an attack on S will be 100%, i.e. $1-f_S=1$. However, S will be attacked (i.e. s=0) only if $H_S > (1-f_P)H_P$ (i.e. the target will not be attacked for sure, if left undefended).

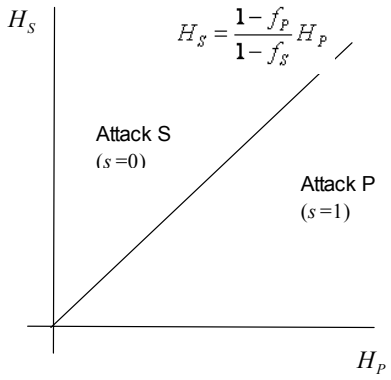

Figure 2: Optimal choice of target for attacker[1]

Defender's optimal strategy

The defender is in search of an optimal strategy (D_P^*, D_S^*) which minimizes his expected payoff, given the attacker's optimal strategy s^*. From Eq. (3), we get the following optimization problem:

$$\min_{D_P, D_S} L(D_P, D_S, s^*) =$$
$$\min_{D_P, D_S} [\pi_P(1-f_P)HD_P + \pi_S(1-f_S)HD_S + D_P(f_P) + D_S(f_S)]$$

which has as first order conditions:

$$\frac{\partial L}{\partial f_P} = 0$$
$$\xrightarrow{\pi_S = 1-\pi_P} \frac{\partial \pi_P}{\partial f_P}(1-f_P)HD_P - \pi_P HD_P - \frac{\partial \pi_P}{\partial f_P}(1-f_S)HD_S + D_P'(f_P) = 0 \qquad (4)$$
$$\Rightarrow \frac{\partial \pi_P}{\partial f_P}[(1-f_P)HD_P - (1-f_S)HD_S] - \pi_P HD_P + D_P'(f_P) = 0$$

and

[1] adapted from Bier et al. (2007)

$$\frac{\partial L}{\partial f_S} = 0$$

$$\xrightarrow{\pi_S = 1-\pi_P} \frac{\partial \pi_P}{\partial f_s}(1-f_P)HD_P - \frac{\partial \pi_P}{\partial f_S}(1-f_S)HD_S - (1-\pi_P)HD_S + D_S{}'(f_S) = 0 \quad (5)$$

$$\Rightarrow \frac{\partial \pi_P}{\partial f_S}[(1-f_P)HD_P - (1-f_S)HD_S] - (1-\pi_P)HD_S + D_S{}'(f_S) = 0$$

The solution f_P^*, f_S^* to the system of Eq. (4) and (5) defines the optimal strategy $(D_P^*(f_P), D_S^*(f_S))$ of the defender. Obviously this solution depends on the optimal strategy of the attacker s^* through π_P.

4. APPLICATION TO A PIRACY SETTING

4.1 Application background: Piracy

An international problem

Piracy has become a central concern for the international maritime community, especially after the recent tremendous increase in the number of piracy attacks in the Gulf of Aden and adjacent waters, off Somalia and the eastern coasts of Africa. Specifically, in 2008 took place in that region 111 piracy attacks, 42 ship hijackings, and 815 seafarers were held as hostages. As of early April 2009, 9 ships were in captivity and 153 seamen were kept as hostages (Naftemporiki, 2009).

According to a report by the International Chamber of Commerce's International Maritime Bureau (IMB[1]) (ICC Commercial Crime Services, 2009), the result is a worldwide dramatic increase in the number of ships attacked during the year's first quarter compared with the same period in 2008 (102 incidents reported in the first three months of 2009 compared to 53 incidents in the first quarter of 2008). Also, attacks worldwide increased by almost 20% over the last quarter of 2008.

In fact, the increase in the first quarter of 2009 is due almost entirely to increased Somali pirate activity off the Gulf of Aden and the east coast of Somalia. The two areas accounted for 61 of the 102 attacks during the first quarter compared to six incidents for the same period in 2008.

This phenomenon has had repercussions beyond the maritime sphere, forcing governments around the world into political and military action more commonly seen in times of war (LL, 2009). As indicatively reported, Germany and Japan have been forced to consider the revision of pacifist constitutions, while China and India have extended their military power beyond their normal spheres. In the end, the European Union organised in December 2008 and currently operates a naval force (EU Navfor taskforce) in this rather distant sea from Europe, while naval ships from USA, Russia, China and Japan also patrol the dangerous waters (Naftemporiki, 2009).

[1] The IMB is part of ICC Commercial Crime Services, which is a specialised division of the International Chamber of Commerce.

Attack relocation and pirates' tactics

However, the pirates appear to have adapted their operations to these developments. While in 2008 they mainly attacked ships in the Gulf of Aden, in 2009 and after the deployment of security naval forces, it has been observed that they reach waters more distant from the African shores using larger mother ships in their operations (Naftemporiki, 2009). Indeed, "if naval forces leave an area prematurely, either in the mistaken belief they have accomplished their mission or because they are needed elsewhere, the pirates may quickly re-emerge" (LL, 2009).

A fear has been expressed by the International Maritime Bureau (IMB) that piracy will simply shift to another region, "Somalia today, Nigeria tomorrow, the next day somewhere else" (LL, 2009). The world is too focused on Somalia when there are similar problems off Nigeria. Indeed, deadly attacks on vessels in Nigerian waters are witnessed, while the IMB believes most attacks go unreported.

Pirates in the 21st century have access to sophisticated means of communication and use modern digital tools to hunt down the next victims. For example, there is a widely held view that the hijackers used such tools to track the Saudi-owned, 318,000 dwt Sirius Star as it headed fully-laden towards the Mozambique Channel and round the Cape of Good Hope for a Caribbean transshipment. The seizure of such a large ship 400 nautical miles from Kenya's Mombasa, far south of the Gulf of Aden, shocked the shipping as well as military and intelligence communities (LL, 2009). Moreover, as demonstrated during negotiations with pirates, they understand the "dynamics of both shipping and insurance" (LL, 2009).

Existing measures for an ongoing problem

"When seafarers hear someone mention the International Ship and Port Facility Security (ISPS) Code, a typical reaction is a resigned shrug of the shoulders". A victims of a piracy incident used the phrase "failing rules and failed people" — from Somalia to the Malacca Strait — to describe the current situation in which crews find themselves in a "triangle" of economics, conflict and complex politics which in a particular region guarantee piracy. Overall, ISPS has proved virtually redundant during the wave of hijackings and attacks on ships in areas like the Gulf of Aden and off the coast of Nigeria (LL, 2009).

Calls for the training of crews in resisting hijackers to be included in international regulations suggest the militarisation of merchant shipping. On the other hand, a "sound and common sense strategy" is not to arm merchant ships and to teach crews "not to undertake hazardous actions against the pirates" (LL, 2009).

Officials have suggested that naval operations should continue (e.g. IMB Director, see ICC Commercial Crime Services, 2009). Apart from the deployment of naval forces in the areas of concern by individual countries or the EU, the possible arrival in the Gulf of Aden of mercenary firms (military / security professionals) is not seen as a desirable solution by many, such as BIMCO whose members are advised not to hire them (for example a gunboat operated by a US mercenary firm has a reported hire rate of $85,000 a day (LL, 2009)).

The practical security issues concern, primary, the lives of crews and, secondary, the security of ships and cargoes, the financial losses for companies, and the operational and economic effects on maritime trade, yet this new challenge has also raised a number of complex international law issues. These are related to insurance, to who pays associated costs, such as

lawyers' fees, under what and whose law hijackers are to be prosecuted, some of which depend on whether hijackers should be considered terrorists or just criminals. Indeed, one such problem is the legality of any payment to pirates. For the moment, and for the most part, the hijackers in the Gulf of Aden and wider area are not regarded as terrorists because, if they were, payment would be illegal in many countries. Some countries, however, make payment for criminal activities also illegal. It depends on whether the country concerned is the flag-state or the home of the organisation making payment (owner, operator or insurer) (LL, 2009).

The modeling setting

From the above short overview, it is rather obvious that, although technicalities may complicate the piracy phenomenon, it is basically a security problem, where on one side the international community is seeking for measures to restrain attacks on merchant ships, while on the other side, pirates develop tactics and assess the existing situation in order to successfully place hijacking attacks. They also appear to possess modern communication means and adapt to the defenders moves by diverting their attacks accordingly.

Although central decision-making for diverting piracy attacks from the Gulf of Aden to as far as the Nigerian waters is not realistic, this is not the case for the waters off the eastern African coasts, where pirates are reported to relocate attacks within a vast sea surface. Defense measures can also be assumed to be defined by central decision-making, if not for the overall naval forces (which would be even more efficient), at least regarding the EU naval taskforce as an example. Moreover, any such defender has limited resources (ships and budget) to deploy.

Therefore, in an initial (yet quite realistic) approach, this interaction setting can be associated with the previously developed model setting and this is the basis for the numerical example presented next and adapted from Bier et al. (2007).

4.2 Definition of parameters and analysis

The following illustration is based on a generic numerical example found in Bier et al. (2007) and it serves demonstration purposes, given the computational demands of such a modelling task. Two players are considered in the following illustration. The defender (player 1), which is the EU Navfor Command (see above) and the attacker (player 2), which is the Somalian pirates "headquarters" (where their leaders plan their attacks).

Two potential target areas for the pirates (and respective areas for the development of the naval forces) are considered, each of which is defined within certain geographical limits (Figure 3). Target area S covers waters off the east coast of Somalia, and is crossed mainly by routes of large size ships (VLCCs, containerships etc.) traveling around Africa. Target area P is located at the Gulf of Aden, is smaller in surface than target area S (and therefore easier for the naval forces to patrol), comprises waters closer to the coast and is frequented by smaller in size merchant vessels and those passing from Suez Canal.

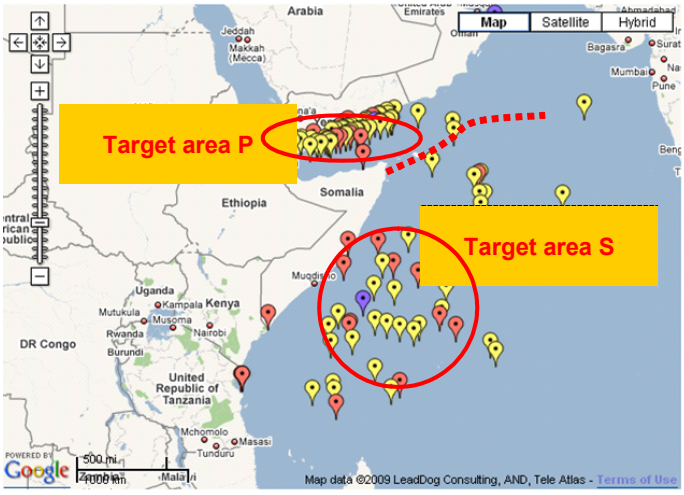

Figure 3: Target areas (source: IMB Live Piracy Map 2009, http://www.icc-ccs.org)

In this illustration, the analysis' reference time-period is one month. So, the allocation of defense measures (naval ships) to the respective areas is decided upon and reviewed on a monthly basis, and also the considered costs (expected damages, expenditures etc.) are aggregations for a 1-month period.

It is assumed that the deterrence (levels) costs (naval force deployment costs in our illustration) D_i for the two target areas, $i = \{P, S\}$, are associated with the pirate's perceived likelihood of failure f_i following an attack at one of the two areas as: $D_i = \ln(1 - f_i)$, where D_i in m.USD[1]. This relationship is illustrated in Figure 4.

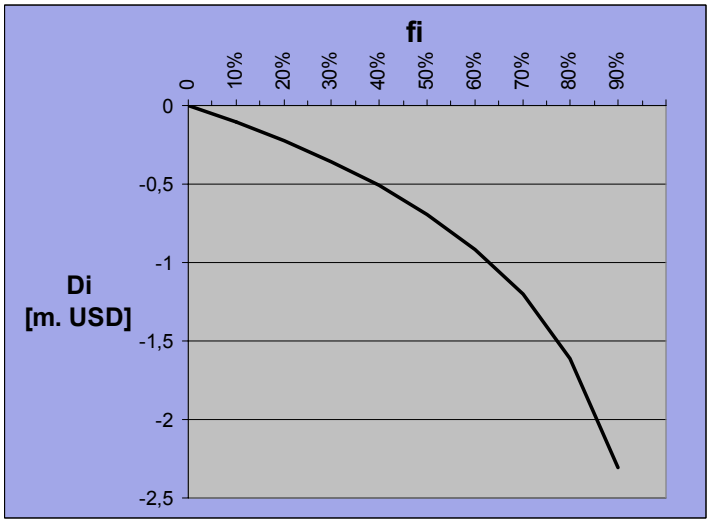

Figure 4: Deterrence expenditures as a function of attack failure probability f_i

As there is information asymmetry, it is assumed that the "type" of the pirates (see description section) is defined (drawn by Nature) from cumulative distributions of the type

[1] The same function is assumed for both target areas, and so there is a symmetry assumption in this respect.

$F_i(H_i) = 1 - e^{-4Hi}$, where H_i , i = {P, S}, are the pirates' preferences or payoffs for success (see Figure 5).

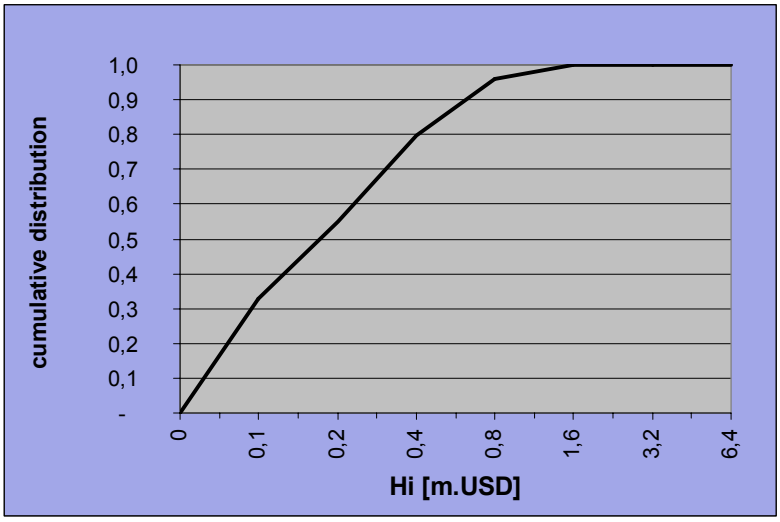

Figure 5: Cumulative distribution of pirates' preferences (success payoffs H_i)

With the above input, the target areas which will be defended can be determined as a function of the level of the expected damage costs (loss) HD_i for the defender (i.e. in our illustration, the losses that the shipping community will suffer following successful attacks at area P or S). An area will be defended when $f_i>0$ and undefended when $f_i=0$. These results are shown in Figure 6.

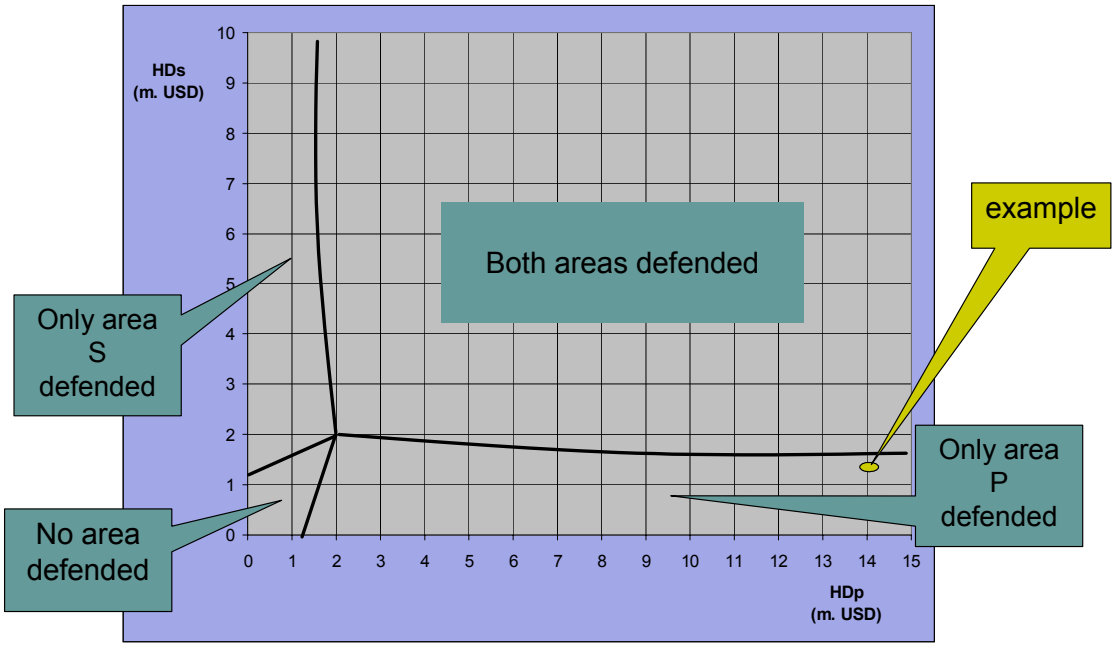

Figure 6: Defense allocation as a function of anticipated damage *HDi* in each target area

Figure 6 demonstrates that the defender's valuation regarding the damage to be incurred (here expressed in monetary value terms in m. USD) following successful piracy attacks at area P or S determine (as should be expected) the allocation of defense measures in the respective areas. For low expected losses in both areas, no defense is allocated in either area. When expected losses in one area are considerably larger than those in the other area, then only the

first one will be defended. When expected losses in both areas are above certain levels, then both areas are defended.

In this example, the boundary curve that separates the "both areas defended" surface from the "only area P defended" surface in Figure 6 "decreases" as HD_P increases, with low limit value that of HD_S=1.5 m.USD when $HD_P \rightarrow \infty$ (symmetrically there is a low limit value for this curve of HD_P=1.5 m.USD when $HD_S \rightarrow \infty$).

For every combination of expected damage costs (loss) HD_i (for i=P and S) the optimal defense allocation can be determined. For the example combination pointed in Figure 6 and corresponding to defender valuations HD_S=1.6 m.USD and HD_P=14 m.USD, only area P is defended (i.e. ships will be patrolling and defending only area P), whereas $fs=0$, $Ds=0$ (translated to no defense for area S).

We can draw iso-damage / iso-cost (budget) curves for these values of HD_S, HD_P. An iso-damage curve corresponds to a damage level equal to ISD (see Eq. 3):

$$\pi_P(1-f_P)HD_P + \pi_S(1-f_S)HD_S = ISD$$

while an iso-cost curve corresponds to a total cost level (budget) equal to ISC (see Eq. 3):

$$D_P(f_P) + D_S(f_S) = ISC$$

For HD_S=1.6 m.USD, HD_P=14 m.USD (above example point) and if moreover we assume ISC=1.4 m.USD (i.e. the total budget of defense expenditures), then in Figure 7 we see the corresponding iso-cost curve. For $fs=0\%$ (no defense for area S), we get $fp=75\%$ and D_P=1.4 m.USD (i.e. all defense allocated in area P).

Moreover, the intersection of ISC=1.4 m.USD and $fs=0\%$ corresponds to the iso-damage curve ISD=2 m.USD, i.e. we have an expected damage of 2 m.USD.

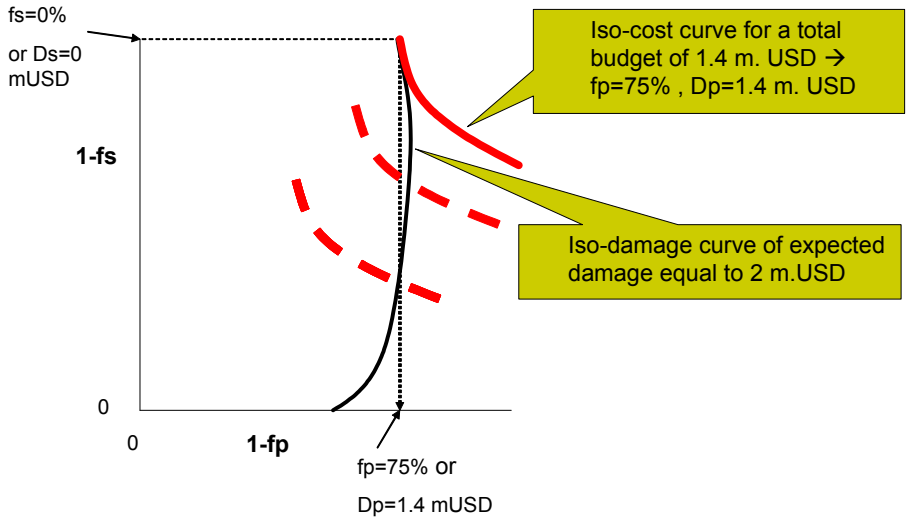

Figure 7: Iso-cost and iso-damage curves as a function of success probabilities $1\text{-}f_P$, $1\text{-}f_S$

Other parametric analyses can also be performed to reach useful results, such as the influence of the defender's valuations HD_S, HD_P (i.e the anticipated damage costs from piracy attacks at

each location) on the optimal allocation of ships - defense measures (translated to cost expenditures) in the two areas. For example, if we set HD_S=1.7 m.USD, we can determine the equilibrium outcomes for various levels of HD_P along the dotted line in Figure 8.

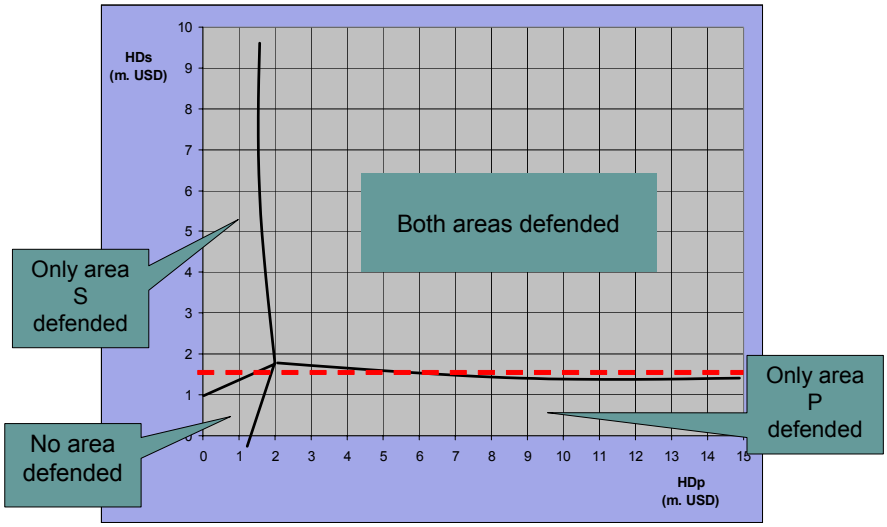

Figure 8: Equilibrium points for fixed HD_S and various levels of HD_P

In Figure 9 we see the various levels of defense allocation D_S, D_P (expressed in cost expenditures) in areas S and P, and also the respective success probabilities of an attack placed on them as a function of HD_P (for the given HD_S=1.7 m.USD).

When HD_P is very small, only area S is defended. As HD_P increases, defending area S becomes less valuable and so D_S decreases, as attacks are diverted to an increasingly valuable area P. The defender does not allocate ships to any area for HD_P between 1.6 and 1.8 m. USD. As HD_P further increases, area P (only) is defended and for HD_P above 5 m. USD, expenditures on defending area P make area S an attractive target for the pirates, and so it becomes optimal to defend both areas. The optimal success probabilities (1- *fi)* for attacks at both areas move according to the levels of defense allocations D_S, D_P.

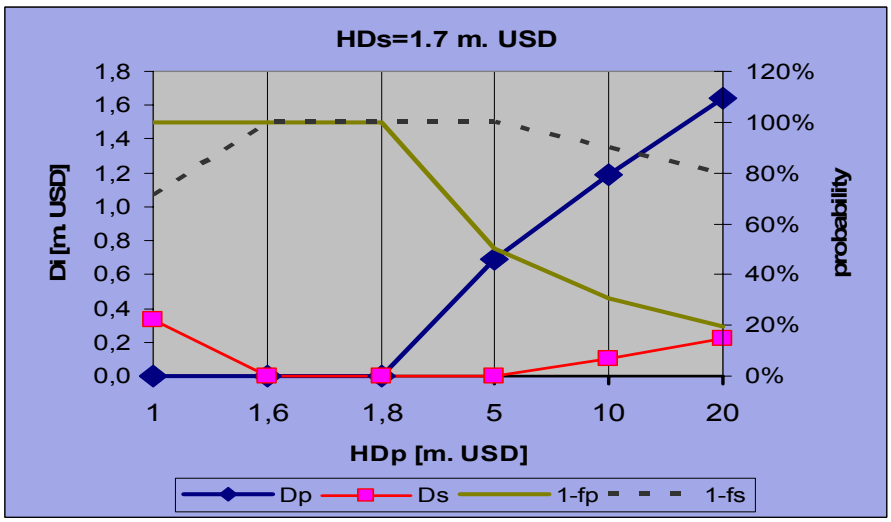

Figure 9: Defense allocation & attack success probabilities as a function of anticipated damage HD_p in area P

5. CONCLUSIONS

The model presented in this paper was adopted from Bier et al. (2007). It introduces to the security analysis the attacker as an active player, whose optimal choices must be examined in order to reach equilibrium outcomes. Two potential targets were considered, while the defender was only one agent. So, an interaction setting (game) was examined between two players, a defender and an attacker.

The attacker's preferences, which define the "type" of the attacker, were not known by the defender (uncertainty about attacker's valuation), and so an incomplete information game was modeled (with information asymmetry), transformed to an imperfect information game with Nature as a pseudo-player (who assigns the attacker's type).

The model was adapted to a piracy setting. Piracy is an important concern for the international maritime community, especially after the recent tremendous increase in the number of attacks. Several dimensions of this phenomenon were discussed, in order to show the relevance and potential applicability of the theoretical modeling setting to this practical problem.

The illustration referred, more specifically, to the waters off the eastern African coasts. The defender (player 1) was the EU Navfor Command and the attacker (player 2), the Somalian pirates "headquarters" (where their leaders plan their attacks). Two potential target areas for the pirates (and respective areas for the development of the naval forces) were defined within certain geographical limits.

Following a number of assumptions, the analysis reaches interesting suggestions for the side of the defender, given the behaviour of the attacker. For example, regarding the target areas which should be defended and the level of defense measures, as a function of the expected damage costs that the shipping community might suffer, budget considerations, and damage expectations for any given defense strategy. The above illustration demonstrated that parametric analyses can be performed to reach useful results, regarding the optimal allocation of ships - defense measures in a given geographical sea area, for given expectations (and not knowledge) for piracy activity.

In the same research framework, briefly outlined in the introduction section of this paper, game theory is applied to security scenarios that cover "cargo sensitive" ships such as Ro-Pax, Cruise vessels etc (Metaxas, 2009). Through game theory an alternative approach for threat assessment is provided to overcome the deterministic nature of current practices and introduce a methodology capable of providing a realistic assessment of the danger of specific threats, e.g. terrorism, piracy, sabotage etc. Since the focus is placed upon specific scenarios regarding security threats to ships (set up with certain characteristics, well defined conditions and estimated consequences) this effort can be filed as part of a tactical level approach. Tactical level applications deal with the probability and consequences of a certain incident or a selected scenario (the ship, the ship to port interface and the conditions/strategies regarding this combination) and therefore they cover a highly interesting part of the map of operations and possible outcomes.

ACKNOWLEDGMENTS

The authors are grateful to Professor Vicki Bier, University of Wisconsin–Madison, for kindly providing further information and explanations on the model, which formed the methodological basis of this paper.

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

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

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.

Gkonis, K.G. and H.N. Psaraftis (2010), "Container transportation as an Interdependent Security problem", National Technical University of Athens, Laboratory for Maritime Transport, working paper

Gkonis, K.G., H.N. Psaraftis, N.P. Ventikos (2009), "Game Theory contributions to Terrorism in Merchant Shipping: an Application to Port Security", Proceedings of IAME 2009 Conference, June 24-26, Copenhagen, Denmark

ICC Commercial Crime Services (2009), "Piracy attacks almost doubled in 2009 first quarter", http://www.icc-ccs.org, accessed April 29

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

Lloyd's List newspaper (2009), Special Report on Piracy & Security, March 03, http://www.lloydslist.com

Metaxas, P. (2009), "Study of Threat Assessment for Ships with the Usage of Game Theory", NTUA Diploma Thesis, Athens, Greece (in Greek)

Naftemporiki newspaper (2009), "New tactics employed by pirates in Somalia" article, April 2 (in Greek)

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

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.