International Journal of Performability Engineering Vol. 5, No. 1, January, 2009, pp. 31- 43.

Printed in India

Secrecy in Defensive Allocations as a Strategy for achieving more Cost-effective Attacker Deterrence

NIKHIL S. DIGHE[2], JUN ZHUANG[1]* and VICKI M. BIER[2]

[1]*Department of Industrial & Systems Engineering, University at Buffalo, SUNY, 403 Bell Hall, Buffalo, NY 14260, USA*
[2]*Department of Industrial & Systems Engineering, University of Wisconsin-Madison, 3234 Mechanical Engineering Building, 1513 University Ave., Madison, WI 53706, USA*

(Received on September 18, 2007)

Abstract: We discuss strategic interactions between an attacker and either centralized or decentralized defenders, and identify conditions under which centralized defender decision making is preferred. One important implication of our results is that partial secrecy about defensive allocations (disclosure of the total level of defensive investment, but secrecy about which resources are defended) can be a strategy for achieving more cost-effective attack deterrence. In particular, we show that such partial secrecy can be potentially beneficial when security investments are discrete (*e.g.,* as in the use of air marshals to counter threats to commercial aviation).

Keywords: *Non-cooperative games; deterrence; terrorism; centralization; secrecy.*

1. Introduction

The increased threat of terrorism against the U.S. in the 21st century has forced the nation to spend more on defenses. With increasing demands for protection and a limited defense budget, important tradeoffs have to be made; see [3] for a discussion of the use of game theory to study to such questions. Note that many game-theoretic models (*e.g.*, [4]; [19]) recommend making the defensive allocations public. Here, we consider a problem in which keeping the defensive allocation secret, and releasing only partial information, helps the defender deter attacks at lower levels of investment than would be possible if the defensive allocation were disclosed. Our model accounts for the strategic behavior of both the defender(s) and the attacker. Other examples of models with strategic interactions include [1], [4], [14], and [18].

In this paper, we consider a game between an attacker, and either one or two defenders. There are two resources to be defended. The attacker is trying to maximize his payoff, which is the total loss he inflicts on the defender(s), minus the cost of any attack. The attacker has partial information — he can observe how many resources are defended, but not which ones. The attacker then has to decide whether it is worth attacking at all, and if so, which resources to attack. A practical example of this phenomenon is the use of Lojack, which can be used to track down stolen cars. Ayres and Levitt [2] describe the results of an empirical study of the benefits of Lojack not only to car owners who have installed Lojack systems, but also to other car owners (due to positive externalities). Consistent with the findings of this paper, the results of Ayres and Levitt [2] suggest

* Corresponding author's email: jzhuang@buffalo.edu

that the availability of information regarding the approximate market penetration of Lojack can help to reduce car thefts by deterring potential attackers, as long as the installation of Lojack on any given car is kept secret.

The game proposed and analyzed in this paper can be used to model a number of security decisions in which the decision maker has to allocate her defense budget among various resources, and wishes to avoid over-investment. The decision maker can protect all, some, or none of her resources, and wants to make an optimal decision. One novel feature of this model is that knowing how many resources are defended may deter the attacker even if not all resources have been defended, so there are both externalities between decentralized defenders, and an endogenous choice on the part of the attacker. Our model shows that under centralized decision making, the defender can sometimes achieve the social optimum by coordinating (mixed) defenses to ensure that one asset is always defended, making it more feasible and less costly to achieve attack deterrence. Thus, a centralized defender can sometimes achieve more cost-effective deterrence than decentralized defenders.

In their model, Bier *et al*. [4] find public disclosure of defenses to be an optimal strategy. This need not always be the case, as shown by our model. In particular, in order to deter the attacker, if defenses are publicly disclosed, the defender would have to defend all of her resources, as any undefended resource would be susceptible to an attack. By contrast, we show that in some cases, defense of a subset of resources will be sufficient to deter attack if the defended resources are kept secret, leading to more cost-effective defenses. In particular, terrorist groups like Al-Qaeda are known to avoid targets where the defense levels or chances of success are uncertain [18]; this can be exploited to deter attacks.

Section 1 presents the notation and assumptions for our model. Section 2 presents and compares the centralized and decentralized resource-allocation models. Section 3 discusses some insights from the results of this game, and Section 4 gives directions for future work.

1. Notation and assumptions

There are two types of players in this version of the game: an attacker (he); and either one defender (she) attempting to protect two resources, or two defenders (both she), each attempting to protect one resource.

- V = Value of both resources
- C_{di} = Cost of defending resource i, where i = 1, 2; we assume without loss of generality that the cost of defense for resource 1 is greater than that for resource 2 (*i.e.*, $C_{d1} \geq C_{d2}$), and both are less than the target valuation (*i.e.*, $0 < C_{d2} \leq C_{d1} < V$)
- C_a = Cost of attacking either resource; we assume, $0 < C_a < V$

We assume that:

- All parameter values are common knowledge to both the attacker and the defender(s).
- If a resource is defended, the success probability of an attack on that resource is zero. If not defended, the success probability of an attack on that resource is one.

- The attacker can attack at most one resource.[1]
- The defender(s) and the attacker all maximize their own payoffs. For the attacker, the payoff is the expected value of any resource successfully attacked, minus the cost of the attack. For the defender, the payoff is the loss of expected value of any resource that is successfully attacked, minus the cost of defense.
- The attacker can observe how many resources are defended, but not which ones. In other words, in cases where the defender adopts a mixed strategy, we assume that the attacker observes the actual number of resources defended as a result of the defender's (random) choice, not merely the mixing probability.[2]

We recognize that our model and the assumptions above are somewhat limiting. Other work ([19]) allows for more general attacker and defender characteristics, including differences in target valuations between the attacker and the defender, more general contest success functions, *etc*. However, those models address somewhat different research questions. Zhuang and Bier [19] focus on balancing protection from terrorism and natural disasters, and does not even find defender secrecy at equilibrium. Zhuang and Bier [20] do explore defender secrecy and deception, but in a rather different context. In particular, they find secrecy emerging from attacker uncertainty about defender types, even in a model with only a single defender resource, where the defensive investment is continuous and the success probability of an attack is a convex function of the defensive investment (unlike here). By contrast, here we find secrecy emerging from the existence of multiple defender resources and the discrete nature of defensive investment (so that the success probability of an attack is a non-convex function of defensive investment). Therefore, this paper identifies a fundamentally different reason for defender secrecy that that in [20], and provides unique insights into both one potential reason for secrecy, and a possible benefit of defender centralization.

2. Centralized and decentralized resource allocation

In the centralized model, the defender moves first by investing in security for (some subset of) her two resources. The pure strategies for the two players are given below.

- For the defender: Defend both resources (D_1, D_2); Defend resource 1 only (D_1, ND_2); Defend resource 2 only (ND_1, D_2); and Don't defend either resource (ND_1, ND_2)
- For the attacker, given that i resources are defended (i = 0, 1, 2): Attack resource 1 (A_1); Attack resource 2 (A_2); and Don't attack either resource (A_0)

The game is represented in its extensive form in Figure 1. See Appendix A for the calculation of equilibrium payoffs and strategies, which are summarized in Table 1 (including the possibility of multiple equilibria when the attack cost is small and $V = C_{d1} + C_{d2}$).

By contrast, in the decentralized model, two independent defenders each individually invest in security for their respective resources. The pure strategies of the players are given below:

[1] This assumption is of course limiting, but may be fairly realistic for some of the most demanding attack strategies, due to attacker budget constraints.

[2] This is clearly realistic in some situations (*e.g.*, the attacker might know the market penetration of Lojack). However, there obviously also exist cases in which the attacker can infer the defender's mixing probability (or observe a signal disclosed by the defender), but cannot observe the number of resources actually defended. See [20] for an example.

- For defender 1: Invest in security (D_1); Don't invest in security (ND_1)
- For defender 2: Invest in security (D_2); Don't invest in security (ND_2)
- For the attacker, given that i resources are defended (i = 0, 1, 2): Attack resource 1 (A_1); Attack resource 2 (A_2); Don't attack any resource (A_0)

This game is presented in Figure 2. See Appendix B for the calculation of equilibrium payoffs and strategies, which are summarized in Table 2 (including again the possibility of multiple equilibriums). Note that there cannot be a pure-strategy equilibrium in which only one defender chooses to defend. For example, if defender 1 chooses strategy D_1 and defender 2 chooses strategy ND_2, then the attacker's best response is to choose A_2, in which case defender 2 would prefer to switch to D_2, and so on.

Comparing the equilibrium payoffs of both models (as shown in Tables 1 and 2), we can see that the defender payoff in the centralized case is sometimes strictly better than the sum of the defender payoffs achieved in the decentralized case. In particular, when the centralized defender defends only one resource, the payoff is $- C_{d1}$, which is less negative than either $- C_{d1} - C_{d2}$ or $- V$ (the achievable payoffs in the decentralized case). In fact, for all parameter values, the centralized payoff is always (at least weakly) better than the sum of the two defender payoffs in the decentralized case.

3. Discussion and interpretation

Our model shows that attacker deterrence can sometimes be achieved with only partial defense. In particular, if the cost of an attack is high enough ($C_a \geq 0.5V$ in the centralized model), a centralized defender can successfully achieve at least partial attack deterrence (a non-zero probability of no attack) by probabilistically mixing defenses (see Table 1); by contrast, complete deterrence (a zero attack probability) with partial defense is possible only when $C_{d1} = C_{d2}$. By contrast, in the decentralized model, each defender chooses her individual optimal action, instead of the social optimum. This can either drive up the total level of investment required to deter attacks (to include defense of both resources), or make it so costly to deter attacks that the defenders no longer find it worthwhile to do so. Thus, centralizing defensive allocations allows a centralized defender to achieve a lower expected loss than the expected sum of losses to the decentralized defenders. (Interestingly, in the decentralized case, mixed defenses are never strictly preferred, as discussed in Appendix B.)

Note, however, that in practice, decentralized decision-making could be better in cases where the decision maker itself is the target of attack, since a successful attack could have a destabilizing effect on the decision-making process [10] — *e.g.*, if attacks on the defender's communication and control capabilities disrupt the ability of a centralized defender to control the defenses of geographically dispersed resources. In addition, centralized decision making may be more costly in practice (because of possible transaction costs to achieve coordination), or suffer from lack of detailed information about the resources on the part of the centralized decision maker (information asymmetry). Our model does not take these considerations into account.

The model indicates that partial defense is especially likely to lead to attack deterrence when the cost of attacking is high. This suggests that making attacks more costly may be one important component of a cost-effective security strategy.

One illustrative application of this model is to the case of onboard air marshals. If the information about which planes have air marshals is kept secret but the number of air marshals is known (at least approximately),[3] then having air marshals on only some planes can result in attack deterrence. By contrast, if the presence of air marshals on any given plane were made public, then one would need to have air marshals on all planes (or none, if too costly), as those planes without air marshals would become targets of attack. The importance of secrecy was highlighted by the Federal Law Enforcement Officers Association when the cover of air marshals was allegedly in danger due to the rigid dress code enforced by the Federal Air Marshal Service [11]. This in principle could present a significant risk, since it increases the chance that terrorists could identify the air marshals, overpower them, and hijack a plane [9].

Similarly, U.S. Customs and Border Protection (CBP) [16] considers prevention of terrorists and terrorist weapons entering the US to be its top priority, but also realizes the potential tradeoffs between security and efficiency. The Container Security Initiative attempts to address these tradeoffs by proposing inspection of high-risk containers at foreign ports [17]. If 100% inspection is infeasible or undesirable due to cost considerations, models such as ours could potentially be used to help assess the percentage of containers that must be inspected to achieve attack deterrence.

4. Directions for further work

Decision makers facing the dilemma of whether to invest in security may not necessarily follow the recommendations of traditional game-theoretic models. Traditionally, much research has focused on identifying (Nash) equilibriums under the assumption of rationality. Unfortunately, these equilibriums do not always predict people's choices in actual decisions. Behavioral game theory ([7]; [5]) provides a means to weaken the rationality assumptions of traditional game theory, and extend game theory to include psychological aspects. Experiments could therefore be used to test the behavior of decision makers faced with defensive choices similar to those in this paper, in order to explore the possible effects of phenomena such as "probability neglect" [15], individual differences in risk attitude [13], coordination [8], learning [12], and reputation building [6].

In our model, the attacker can be deterred by partial defense only if the details of the defensive allocations to the various targets are not disclosed. We hypothesize that this type of defensive strategy is especially likely to be desirable when the defender's resources are roughly equally attractive to the attacker. By contrast, if the defender owns one attractive resource and one or more resources of little or no interest to the attacker, the optimal defensive strategy may be more likely to involve leaving the low-valued resources undefended and disclosing the defensive allocations, since the attacker may be unlikely to attack the lower-valued resources even if they are not defended. Further research to clarify the situations under which deterrence can be achieved by partial defense (*e.g.*, with larger numbers of assets of unequal values) would be desirable. It would also be interesting to explore what happens to our results when defenses are imperfect (*i.e.,* when defenses do

---

[3] Information sufficient to generate a reasonably good estimate of the number of air marshals can be found on the internet with only a quick search (*e.g.*, "a Federal Air Marshal flies 181 days per year, flies 15 days per month, spends 900 hours in an aircraft per year, spends five hours in an aircraft per day…" "We have hundreds of Assistant Federal Security Directors for Law Enforcement stationed directly at airports across the country. There are also Federal Air Marshals attached to each of the fifty-six FBI Joint Terrorism Task Forces nationally;" http://www.tsa.gov/lawenforcement/people/index.shtm). In fact, this information may well have been disclosed precisely for its deterrent effect. Potential attackers would presumably be able to gain even more information about the number of air marshals if they spend more effort.

not reduce the success probability of attacks to zero), and when the attacker knows the level of defensive investment (*i.e.*, number of targets defended) only imperfectly.

Moreover, in this paper, we focus exclusively on discrete investments (*e.g.*, air marshals, since it is not possible to put a fraction of an air marshal on each plane). We anticipate that the same phenomenon will occur for continuous rather than discrete investments, if the success probability of an attack is a non-convex function of the level of defensive investment. For example, this might occur if low levels of security investment are relatively ineffective, and some minimum level of investment is needed in order to have highly cost-effective defenses (creating a region in which the success probability of an attack is a concave function of the defensive investment). This again should be confirmed.

Secrecy about defensive investments could also be desirable for other reasons, of course. For example, the attacker may be unsure about the values of the defender's resources, and attempt to infer the values of those resources to the defender by observing her levels of defensive investment. In this case, disclosing a high level of investment in a valuable target could make that target more attractive to the attacker, rather than deterring an attack. Yet another reason for secrecy about defensive investments could be if highly defended targets are inherently more prestigious to attackers. A more complete understanding of the conditions under which secrecy can be desirable would help to integrate these various considerations into a single model.

Therefore, to increase the realism and flexibility of the model, it would be interesting to introduce models with defender deception, defender learning, and attacker learning. Until now, we have assumed that all players have complete information about the game. However, the possibility of defender deception (rather than just secrecy) about the level of defenses would allow us to model cases in which the attacker is unsure about the defender's resource values, and attempts to infer the value of each resource to the defender by observing the defensive allocations. In this case, there could be incentives for deception on the part of the defenders. For example, deception could allow the defender to shift attacks to well-defended resources with low vulnerability, or to prevent attacks on high-value resources by making low-value resources appear more attractive to the attacker. Learning could help the defender better understand the attractiveness of various resources to the attacker, and conversely, help the attacker better plan and execute attacks against defender resources. In particular, in a repeated-game context, attacker learning could eventually reduce or even eliminate the benefits of defender deception.

Finally, combined effects of learning and reputation building could be studied analytically in a dynamic model, in which interactions occur repeatedly over time. Such a model might be applicable in cases where the defensive investments are flexible (*i.e.*, where the fixed cost of defense is relatively small), so that defensive investments can be modified from one period to another at a modest cost.

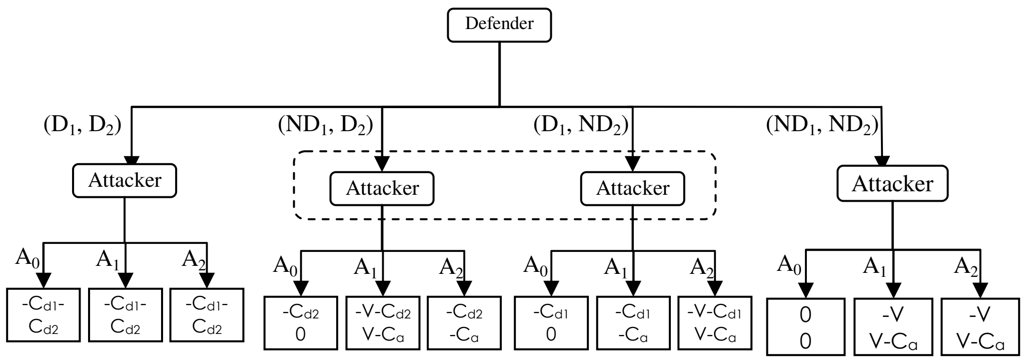

Figure 1: Game in extensive form for a centralized defender

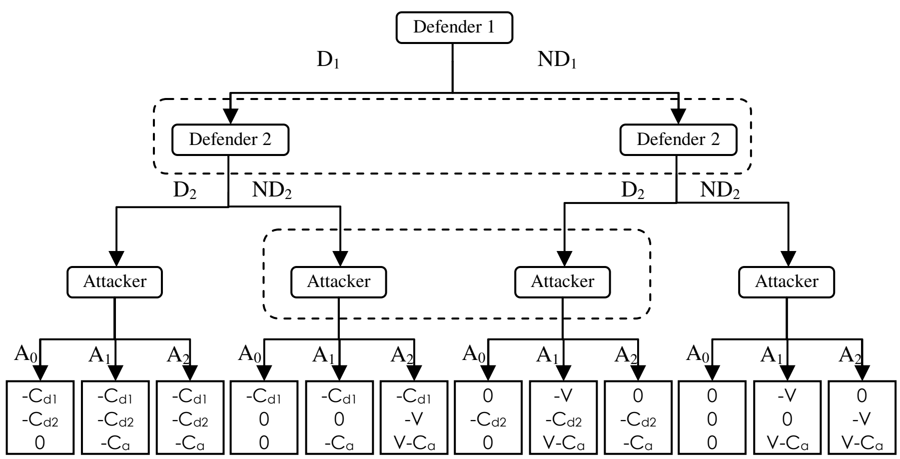

Figure 2: Game in extensive form for two decentralized defenders

Table 1: Equilibrium strategies and payoffs for the centralized case

Parameter Values		Attacker		Defender	
		Strategy	Payoff	Strategy	Payoff
$0.5V < C_a < V$ and $C_{d1} > C_{d2}$		$t_1 A_1 + (1- t_1) A_0$, where $t_1 = (C_{d1} - C_{d2}) /2V$	0	$r (D_1, ND_2)+(1-r) (ND_1, D_2)$, where $r = 1 - C_a/V$	$- C_{d1}$
$0.5V < C_a < V$ and $C_{d1} = C_{d2}$		A_0	0	$r (D_1, ND_2)+(1-r) (ND_1, D_2)$, where $1 - C_a/V \leq r \leq C_a/V$	$- C_{d1}$
$0.5V=C_a$ and $C_{d1} > C_{d2}$	Equilibrium 1	$t_1 A_1 + (1- t_1) A_0$, where $t_1 = (C_{d1} - C_{d2})/2V$	0	$r (D_1, ND_2)+(1-r) (ND_1, D_2)$, where $r = 1 - C_a/V$	$- C_{d1}$
	Equilibrium 2	$t_1 A_1 + t_2 A_2 + (1- t_1- t_2) A_0$, where $t_1 + t_2 < 1$; $t_1, t_2>0$; and $t_1 - t_2 = (C_{d1}-C_{d2})/V$	0	$r (D_1, ND_2)+(1-r) (ND_1, D_2)$, where $r = 0.5$	$- C_{d1} + t_2 (- V)$
$0.5V= C_a$ and $C_{d1}= C_{d2}$	Equilibrium 1	A_0	0	$r (D_1, ND_2)+(1-r) (ND_1, D_2)$, where $1 - C_a/V \leq r \leq C_a/V$	$- C_{d1}$
	Equilibrium 2	$t_1 A_1 + t_2 A_2 + (1- t_1- t_2) A_0$, where $t_1 + t_2 < 1$; $t_1, t_2>0$; and $t_1 - t_2 = (C_{d1}-C_{d2})/V$	0	$r (D_1, ND_2)+(1-r) (ND_1, D_2)$, where $r = 0.5$	$- C_{d1} + t_2(- V)$
$C_a < 0.5V$ and $V < C_{d1} + C_{d2}$		$0.5 A_1 + 0.5 A_2$	$V - C_a$	(ND_1, ND_2)	$- V$
$C_a< 0.5V$ and $V = C_{d1} + C_{d2}$	Equilibrium 1	$0.5 A_1 + 0.5 A_2$	$V - C_a$	(ND_1, ND_2)	$- V$
	Equilibrium 2	A_0	0	(D_1, D_2)	$- C_{d1} - C_{d2}$
$C_a < 0.5V$ and $V > C_{d1} + C_{d2}$		A_0	0	(D_1, D_2)	$- C_{d1} - C_{d2}$

Table 2: Equilibrium strategies and payoffs for the decentralized case

Parameter Values		Attacker		Defender 1		Defender 2	
		Strategy	Payoff	Strategy	Payoff	Strategy	Payoff
$C_{d2} \leq C_{d1} < 0.5V$		A_0	0	D_1	$- C_{d1}$	D_2	$- C_{d2}$
$C_{d2} \leq 0.5V \leq C_{d1}$	Equilibrium 1	A_0	0	D_1	$- C_{d1}$	D_2	$- C_{d2}$
	Equilibrium 2	$0.5 A_1 + 0.5 A_2$	$V - C_a$	ND_1	$- 0.5V$	ND_2	$- 0.5V$
$0.5V < C_{d2} \leq C_{d1}$		$0.5 A_1 + 0.5 A_2$	$V - C_a$	ND_1	$- 0.5V$	ND_2	$- 0.5V$

Appendix A: Calculating Equilibrium Payoffs of the Centralized Model

In order to calculate the equilibrium strategy and payoffs, we consider cases in which both, none, and one of the resources are defended.

A.1: Both resources are defended

When both resources are defended, the attacker's optimal strategy is A_0, as this is the only strategy that gives a non-negative payoff. Then the defender payoff is $- C_{d1} - C_{d2}$, and the attacker payoff is 0.

A.2: None of the resources are defended

When none of the resources are defended, then the attacker's optimal strategy is any mixture of strategies A_1 and A_2. The defender payoff is - V, and the attacker payoff is $V - C_a$.

A.3 One of the resources is defended

Note that the defender cannot choose pure strategy (D_1, ND_2) or (ND_1, D_2) at any equilibrium. For example, if the defender chooses (D_1, ND_2) with certainty, the attacker's best response is to choose A_2, in which case the defender would like to switch to strategy (ND_1, D_2), and so on. Therefore, we must consider mixed strategies.

Let r and (1 - r) be the probabilities that the defender chooses strategies (D_1, ND_2) and (ND_1, D_2), respectively, where $0<r<1$. Let t_1, t_2, and $(1- t_1 - t_2)$ be the probabilities that the attacker chooses strategies A_1, A_2, and A_0, respectively, where $0 \le t_1, t_2 \le t_1 + t_2 \le 1$. At any possible equilibrium, (r^*, t_1^*, t_2^*), the following two conditions must be satisfied:

First, the defender is indifferent between choosing (D_1, ND_2) and (ND_1, D_2) given t_1^* and t_2^*; *i.e.*, -

$$C_{d1} + t_2^* (- V) = - C_{d2} + t_1^*(- V) \quad (1)$$

Second, given r^*, the attacker payoffs of choosing pure strategies A_0, A_1, and A_2 are 0, $- C_a + (1 - r^*) V$, and $- C_a + r^*V$, respectively. Thus, there are in principle seven possible attacker strategies: pure strategies A_0, A_1, and A_2; mixing between A_0 and A_1; mixing between A_0 and A_2; mixing between A_1 and A_2; and mixing among all of A_0, A_1, and A_2.

We now consider each of these in turn:

- In order for pure strategy A_0 to be an equilibrium ($t_1^* = t_2^* = 0$), we must have
  $\max \{- C_a + (1 - r^*) V, - C_a + r^*V\} \le 0$
  or in other words $C_a/V \le r^* \le 1 - C_a/V$. According to (1), we also require $C_{d1} = C_{d2}$.
- In order for pure strategy A_1 to be an equilibrium ($t_1^* = 1$; $t_2^* = 0$), we must have
  $\max \{0, - C_a + r^*V\} \le - C_a + (1 - r^*) V$ .According to (1), this can be true only when $C_{d1} = C_{d2}+V$, which contradicts our assumption that $C_{d1} < V$.
- In order for pure strategy A_2 to be an equilibrium ($t_1^* = 0$; $t_2^* = 1$), we must have
  $\max \{0, - C_a + (1 - r^*) V\} \le - C_a + r^*V$
  According to (1), this can be true only when $C_{d2} = C_{d1}+V$, which contradicts our assumption that $C_{d2} < V$.
- In order for mixing between A_0 and A_1 to be an equilibrium ($0< t_1^* <1$; $t_2^* = 0$), we must have
  $$- C_a + r^*V \le 0 = - C_a + (1 - r^*) V \quad (2)$$
  According to (1) and (2), we then get $t_1^*= (C_{d1}-C_{d2})/V$, $r^* = 1 - C_a/V$, and $C_a \ge 0.5V$.
- In order for mixing between A_0 and A_2 to be an equilibrium ($t_1^* = 0$; $0< t_2^* <1$), we must have
  $- C_a + (1 - r^*) V \le 0 = - C_a + r^*V$
  According to (1), this can be true only when $t_2^*= (C_{d2} - C_{d1})/V \le 0$, since we have assumed that $C_{d2} \le C_{d1}$. Hence, we have a contradiction.
- In order for mixing between A_1 and A_2 to be an equilibrium ($t_1^*+ t_2^* = 1$; $t_1^*, t_2^*>0$), we must have $0 \le - C_a + r^*V = - C_a + (1 - r^*) V$ (3)
  According to (1) and (3), we then have $r^* = 0.5$, $t_1^* = 0.5 + (C_{d1} - C_{d2})/2V$, $t_2^* = 1 - t_1^*$, and $C_a \ge 0.5V$.
- In order for mixing among all of A_0, A_1, and A_2 to be an equilibrium ($t_1^* + t_2^* < 1$; $t_1^*, t_2^*>0$), we must have
  $$- C_a + r^*V = - C_a + (1 - r^*) V = 0 \quad (4)$$
  This can be true only when $C_a = 0.5$ V. In that case, we have $r^* = 0.5$, and $t_1^*- t_2^* = (C_{d1}-C_{d2})/V$.

A.4: Equilibrium Payoffs

Comparing the (expected) defender payoffs of the three possible defender actions (defending both resources, defending neither resource, and defending only one resource), the equilibriums are as follows:

- If $C_a = 0.5V$, and $C_{d1} > C_{d2}$, then there are two equilibria. In the first equilibrium, the defender chooses (D_1, ND_2) with probability $r = (1 - C_a/V)$, and (ND_1, D_2) with probability $(1 - r)$; the attacker chooses A_1 and A_0 with probabilities $t_1 = (C_{d1} - C_{d2})/2V$ and $1 - t_1$, respectively. The expected defender payoff equals $- C_{d1}$, and the expected attacker payoff equals 0. In the second equilibrium, the defender chooses (D_1, ND_2) with probability $r = 0.5$, and (ND_1, D_2) with probability $(1 - r)$; the attacker can choose A_1, A_2, and A_0 with probabilities given by t_1, t_2, and $1 - t_1 - t_2$, respectively, for any t_1, t_2 such that $t_1 + t_2 < 1$; $t_1, t_2 > 0$; and $t_1 - t_2 = (C_{d1}-C_{d2})/V$. In this case, the expected attacker and defender payoffs equal 0 and $- C_{d1} + t_2 (- V)$, respectively.
- If $C_a = 0.5V$ and $C_{d1} = C_{d2}$, then there are two equilibria. In the first equilibrium, defender chooses (D_1, ND_2) with probability r, and (ND_1, D_2) with probability $(1 - r)$, for any $(1 - C_a/V) \leq r \leq C_a/V$; the attacker chooses A_0. The expected attacker and defender payoffs in this equilibrium equal 0 and $- C_{d1}$, respectively. In the second equilibrium, the defender chooses (D_1, ND_2) with probability $r = 0.5$, and (ND_1, D_2) with probability $(1 - r)$; the attacker can choose A_1, A_2, and A_0 with probabilities t_1, t_2, and $1 - t_1 - t_2$, respectively, for any t_1, t_2 such that $t_1 + t_2 < 1$; $t_1, t_2>0$; and $t_1 - t_2 = (C_{d1}-C_{d2})/V$. In this case, the expected attacker and defender payoffs equal 0 and $- C_{d1} + t_2 (- V)$, respectively.
- If $0.5V < C_a < V$ and $C_{d1} > C_{d2}$, then the defender optimal strategy is to choose (D_1, ND_2) with probability given by $r = (1 - C_a/V)$, and (ND_1, D_2) with probability $(1 - r)$. At this equilibrium, the attacker chooses A_1 and A_0 with probabilities $t_1 = (C_{d1} - C_{d2})/2V$ and $1 - t_1$, respectively. The expected defender payoff equals $- C_{d1}$, and the expected attacker payoff equals 0.
- If $0.5V < C_a < V$ and $C_{d1} = C_{d2}$, then the defender equilibrium strategy is to choose (D_1, ND_2) with probability r, and (ND_1, D_2) with probability $(1 - r)$, for any r such that $(1 - C_a/V) \leq r \leq C_a/V$. At this equilibrium, the attacker chooses A_0. The expected attacker and defender payoffs in this case equal 0 and $- C_{d1}$, respectively.
- If $C_a < 0.5V$ and $V < C_{d1} + C_{d2}$, then the defender's optimal strategy is to choose the strategy (ND_1, ND_2). At this equilibrium, the attacker is assumed to choose A_1 and A_2 with probabilities $t_1 = 0.5$ and $1 - t_1$, respectively. The defender payoff equals $- V$; and the attacker payoff equals $V - C_a$.
- If $C_a < 0.5V$ and $V = C_{d1} + C_{d2}$, then there are two equilibria that involve use of pure strategies by the defender: In the first equilibrium, the defender chooses the strategy (ND_1, ND_2); the attacker chooses A_1 and A_2 with probabilities $t_1 = 0.5$ and $1-t_1$, respectively; the defender payoff equals $- V$, and the attacker payoff equals $V - C_a$. In the second equilibrium, the defender chooses the strategy (D_1, D_2); the attacker chooses A_0; the defender payoff equals $- C_{d1} - C_{d2} = - V$; and the attacker payoff equals 0. Since the defender payoff is the same in both equilibria, there is no reason to expect one strategy to be preferred to the other; moreover, the defender could in principle randomize between (D_1, D_2) and (ND_1, ND_2).
- If $C_a < 0.5V$ and $V > C_{d1} + C_{d2}$, then the defender's optimal strategy is to choose the strategy (D_1, D_2); the attacker chooses A_0; the defender payoff equals $- C_{d1} - C_{d2}$; and the attacker payoff equals 0.

The equilibrium payoffs and strategies are summarized in Table 1.

Appendix B: Calculating Equilibrium Payoffs of the Decentralized Model

In order to calculate the equilibrium strategy and payoffs, we consider three possible pure strategies (both, none, and one of the resources are defended). However, we also have to consider mixed strategies in this case. In particular, one defender could choose to defend while the other chooses a mixed strategy; one defender could choose not to defend while the other chooses a mixed strategy; or both defenders could choose mixed strategies.

B.1: Both defenders choose to defend

When both defenders choose to defend, the attacker's optimal strategy is A_0, as it is the only strategy that gives a non-negative payoff. Then the payoffs of defenders 1 and 2 are $-C_{d1}$ and $-C_{d2}$, respectively, and the attacker payoff is 0.

B.2: Neither defender chooses to defend

When neither defender chooses to defend, then any mixture of strategies A_1 and A_2 is optimal for the attacker. For simplicity, we assume that the attacker will attack each resource with probability 0.5. Therefore, both defenders have an expected payoff of $-0.5V$, and the attacker payoff equals $V - C_a$.

B.3: Only one defender chooses to defend

Note that there cannot be a pure-strategy equilibrium in which only one defender chooses to defend. For example, if defender 1 chooses strategy D_1 and defender 2 chooses strategy ND_2, then the attacker's best response is to choose A_2, in which case defender 2 would prefer to switch to D_2, and so on.

B.4: One defender chooses to defend and the other chooses a mixed strategy

In order to use a mixed strategy, the defender must be indifferent between defending and not defending. That implies in particular that the expected payoffs of the two defenders in this case must equal the payoffs when the defenders choose strategies D_1 and D_2, respectively (or in other words, $-C_{d1}$ and $-C_{d2}$), no matter what the attacker response is. This suggests that for each mixed-strategy equilibrium (if one exists), there would also exist a pure-strategy equilibrium in which the defender payoffs are (weakly) larger. Note also that the attacker will know which action of the mixed strategy is played (because we assume that the attacker knows the total number of defended targets), which makes the mixed strategy less interesting. Since in practice implementing a mixed strategy is likely to be more difficult than implementing a pure strategy, without generating any benefit, we do not expect that a defender would choose a mixed strategy in this case, and therefore do not further consider the possibility of mixed strategy in cases where the defenders could choose strategies D_1 and D_2 in equilibrium.

B.5: One defender chooses not to defend and the other chooses a mixed strategy

By similar logic to the above, there is no need to consider this case further, since it cannot outperform the candidate equilibrium in which the defenders choose strategies ND_1 and ND_2, respectively.

B.6: Both defenders choose a mixed strategy

Again, in order to use mixed strategies, both defenders must be indifferent between defending and not defending. This implies in particular that the expected payoffs of the defenders in this case must equal the payoffs when they choose strategies D_1 and D_2, respectively, or in other words, $-C_{d1}$ and $-C_{d2}$. Thus, there is no need to consider this case further, since it cannot outperform the case when the defenders choose strategies D_1 and D_2.

B.7: Equilibrium Payoffs

Comparing the defender payoffs discussed in Sections B.1 and B.2, the equilibrium defender options are as follows:

- If $0.5V < C_{d2} \leq C_{d1}$, then the equilibrium strategies for defenders 1 and 2 are ND_1 and ND_2, respectively. At this equilibrium, the attacker is assumed to choose either A_1 or A_2 with a probability of 0.5. The expected payoff equals $-0.5V$ for each defender, and the attacker receives a payoff of $V - C_a$, as discussed in Section B.2.
- If $C_{d2} \leq C_{d1} < 0.5V$, then the equilibrium strategies for defenders 1 and 2 are D_1 and D_2, respectively. At this equilibrium, the attacker chooses A_0. The expected defender payoffs equal $-C_{d1}$ and $-C_{d2}$, respectively, and the attacker receives a payoff of 0.
- If $C_{d2} \leq 0.5V \leq C_{d1}$, then there are two equilibria. In the first equilibrium, defenders 1 and 2 choose D_1 and D_2, respectively; the attacker chooses A_0; the payoffs of defenders 1 and 2 are given by $-C_{d1}$ and $-C_{d2}$, respectively; and the attacker receives a payoff of 0. In the second

equilibrium, defenders 1 and 2 choose ND_1 and ND_2, respectively; the attacker chooses either A_1 or A_2 (with an assumed probability of 0.5); the payoff is - 0.5V for each defender; and the attacker receives a payoff of V - C_a. Since defender 1 prefers the second equilibrium, while defender 2 prefers the first equilibrium, there is no clear reason to expect any particular equilibrium to be realized, especially since the two defenders are assumed to make decisions in a decentralized manner. However, some coordination mechanism might make it possible to achieve the socially optimal equilibrium.

The equilibrium payoffs and strategies are summarized in Table 2.

References

[1] Sandler T., Arce D., *Terrorism and game theory*, Simulation and Gaming, Vol. 34, No. 3, pp. 319-337, 2003.

[2] Ayres I., Levitt S., *Measuring the positive externalities from unobservable victim precaution: An empirical analysis of Lojack*, The Quarterly Journal of Economics, Vol. 113, No. 1, pp. 43-77, 1998.

[3] Bier V. M., *Game-theoretic and reliability methods in counter-terrorism and security*, Mathematical and Statistical Methods in Reliability (A. Wilson, N. Limnios, S. Keller-McNulty, and Y. Armijo, editors), Series on Quality, Reliability and Engineering Statistics, World Scientific, Singapore, pp. 17-28, 2005.

[4] Bier V. M., Oliveros S., Samuelson L., *Choosing what to protect: Strategic defensive allocation against an unknown attacker*, Journal of Public Economic Theory, Vol. 9, No. 4, pp. 563-587, 2007.

[5] Camerer C. Behavioral Game Theory: Experiments in Strategic Interactions, Princeton University Press, Princeton, NJ, 2003.

[6] Camerer C., Ho T., Chong J., *Behavioral game theory: Thinking, learning and teaching*, in Essays in Honor of Werner Guth, Steffen Huck (editor), Palgrave Press, 2005.

[7] Crawford V., *Theory and experiment in the analysis of strategic interactions*, Advances in Economics and Econometrics: Theory and Applications, Seventh World Congress, Vol. 1, Cambridge University Press, Cambridge, UK, 1997.

[8] Farrell J., Rabin M., *Cheaptalk*, Journal of Economic Perspectives, Vol. 10, No. 3, pp. 103-118, 1996.

[9] Frank T., *Cover blown, but air marshal still flies*, USA Today, June 1, 2006.

[10] Frey B., Luechinger S., *Decentralization as a disincentive for terror*, European Journal of Political Economy, Vol. 20, No. 2, pp. 509-515, 2004.

[11] Hudson A., *Air marshals—secrecy ruined by dress code*, The Washington Times, July 9, 2004.

[12] Hopkins E. *Two competing models of how people learn in games*, Econometrica, Vol. 70, No. 6, pp. 2141-2166, 2002.

[13] Keeney R., Raiffa H., Decisions with Multiple Objectives: Preferences and Value Trade-Offs, Cambridge University Press, New York, NY, 1993.

[14] Major J., *Advanced techniques for modeling terrorism risk*, Journal of Risk Finance, Vol. 4, No. 1, pp 15-24, 2002.

[15] Sunstein C., *Terrorism and probability neglect*, The Journal of Risk and Uncertainty, Vol. 26, No. 2-3, pp. 121-136, 2003.

[16] U.S. Customs and Border Protection, *Keeping cargo safe: Container Security Initiative (CSI)*, accessed on January 15, 2008, at: http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/

[17] U.S. Customs and Border Protection, *Securing U.S. Ports*, accessed on January 15, 2008, at: http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/port_security/securing_us_ports.xml

[18] Woo G., *Quantitative terrorism risk assessment*, The Journal of Risk Finance, Vol. 4, No. 1, pp. 7-14, 2002.

[19] Zhuang J., Bier V. M. *Balancing terrorism and natural disasters—Defensive strategy with endogenous attacker effort*, Operations Research, Vol. 55, No. 5, pp. 976-991, 2007.

[20] Zhuang J., Bier V. M. *Secrecy and deception at Equilibrium with Applications to Anti-Terrorism Resource Allocation*, Economics and Politics, under review, 2008.

Nikhil S. Dighe has a B.E. in Mechanical Engineering from Maharaja Sayajirao University, Baroda, India and a M.S. in Industrial and Systems Engineering, University of Florida, Gainesville and a M.S. in Industrial Engineering, University of Wisconsin-Madison.

Jun Zhuang is an assistant professor of the Department of Industrial and Systems Engineering at the University at Buffalo, The State University of New York. Jun has a B.S. in Industrial Engineering from Southeast University, China, a M.S. in Agricultural Economics from University of Kentucky, and a M.S. and a Ph.D. in Industrial Engineering from the University of Wisconsin-Madison. His current research interests include the application of Operations Research, Decision and Risk Analysis, Stochastic Dynamic Programming, Game Theory and their applications on Homeland Security, Computer Network Security, Transportation, and Supply Chain Management.

Vicki Bier is a Professor in the Department of Industrial and Systems Engineering and the Department of Engineering Physics at the University of Wisconsin-Madison, where she directs the Center for Human Performance and Risk Analysis. She has a B.S. in Mathematical Sciences from Stanford University, and a Ph.D. in Operations Research from the Massachusetts Institute of Technology. Prior to joining the University of Wisconsin, she worked as a consultant for Pickard, Lowe, and Garrick, Inc., and for Arthur D. Little, Inc. Professor Bier specializes in Decision and Risk Analysis. Her current research, which is supported by the Department of Homeland Security, involves the application of game theory to homeland security and critical infrastructure protection.