Reliability Engineering and System Safety 136 (2015) 35–46

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

# Target-oriented utility theory for modeling the deterrent effects of counterterrorism

Vicki M. Bier [a,*], Fuat Kosanoglu [b]

[a] Department of Industrial Engineering, University of Wisconsin-Madison, 1513 University Avenue, Room 3270A, Madison, WI 53706, USA
[b] Department of Industrial Engineering, University of Wisconsin-Madison, 1513 University Avenue, Room 3237, Madison, WI 53706, USA

ARTICLE INFO

*Article history:*
Received 12 July 2013
Received in revised form
3 November 2014
Accepted 8 November 2014
Available online 21 November 2014

*Keywords:*
Decision analysis
Utility theory
Risk analysis
Reliability

ABSTRACT

Optimal resource allocation in security has been a significant challenge for critical infrastructure protection. Numerous studies use game theory as the method of choice, because of the fact that an attacker can often observe the defender's investment in security and adapt his choice of strategies accordingly. However, most of these models do not explicitly consider deterrence, with the result that they may lead to wasted resources if less investment would be sufficient to deter an attack. In this paper, we assume that the defender is uncertain about the level of defensive investment that would deter an attack, and use the target-oriented utility to optimize the level of defensive investment, taking into account the probability of deterrence.

## 1. Introduction

Resource allocation in security has been extensively studied by many authors after the terrorist attacks on September 11, 2001. Numerous studies use game theory as the method of choice, because of the fact that an attacker can observe the defender's investment in security and adapt to his choice of strategies. For example, Bier et al. [1] has argued that defending a target against determined adversaries is more difficult than against an opportunistic attacker. Thus, the optimal defensive allocation should take into account the attacker's strategy and capabilities.

Investment in defense aims to reduce vulnerability by hardening a system, minimizing the consequences of an attack, and/or deterring a possible attack. Bier and Abhichandani [1] suggest a model for optimal resource allocation in series and parallel systems, assuming that the attacker wishes to maximize the probability of success for an attack on the system, and the defender tries to minimize the probability of system failure. The extension of this work by Bier et al. [2] assumes that the attacker wishes to maximize the expected damage from an attack, while the defender's objective is to minimize the expected loss, taking into account not only system functionality, but also the inherent values of the components. In this model, the attacker may still launch an attack even if he cannot disable the entire system, due to the inherent values of components (so, for example, disabling a single component in a parallel system can be worthwhile even though it won't lead to system failure).

Levitin has extensively studied security models. Most of his work assumes a static threat, and uses reliability theory rather than game theory [3–7]. However, the following works illustrate his use of game theory to model optimum resource allocation in security. Levitin and Hausken [8] compare the effectiveness of redundancy versus component hardening. In this study, the authors analyze a two-stage minmax reliability game where the defender moves first by investing in protection; the attacker can then observe the system protections, and choose the best attack strategy. In a later study, Hausken and Levitin [9] present a game-theoretic optimization model in which two fully strategic agents (an attacker and a defender) both have perfect knowledge about the system and the available actions. The system consists of series and parallel subsystems, and each component consists of elements in parallel. The defender can physically separate the system components, in order to apply different protection strategies to them; conversely, the attacker can attack different combinations of components using different attack strategies. The defender objective is to minimize expected damage, while the attacker maximizes expected damage, both subject to a budget constraint. In more recent work, Hausken and Levitin [10–12] assume that the defender can deploy false targets that the attacker cannot easily distinguish from the true targets. Both the defender and the attacker are assumed to be fully strategic, and both are assumed to have complete knowledge about the system structure and the available actions, but only the defender is assumed to know which targets are false.

In some situations (such as computer networks, aviation security, etc.), the level and effectiveness of defensive investment may depend on the actions of other defenders. Kunreuther and Heal [13] examine an interdependent-security (IDS) model in which any agent in the

* Corresponding author. Tel.: +1 608 262 2064; fax: +1 608 262 8454.
*E-mail address:* bier@engr.wisc.edu (V.M. Bier).

http://dx.doi.org/10.1016/j.ress.2014.11.006

group suffers a loss $L$ in case of a successful attack. A loss can occur either if an agent doesn't invest in protection of its own asset, or due to contamination by other agents that didn't invest in security; for example, even an airline that screens all incoming baggage could be affected by a bomb transferred from another airline that didn't screen baggage. In this model, each agent has perfect information about the risks and costs of security investment, and decides whether to invest in security. Heal and Kunreuther [14] propose a general model that encompasses three different types of IDS problems. In the first type, an agent may still suffer a loss due to contamination from other agents even if he invests in security (partial protection with negative externalities). In the second type of IDS problem, if an agent invests in security, he will not be vulnerable to contamination by other agents (complete protection with negative externalities). For the third type of IDS problem, agents that invest in security may create positive externalities for other agents. In this model, for each type of problem, each agent makes its own decision regarding investment in security. If an agent invests in security, he may avoid direct loss with certainty, yet may be harmed by other agents that don't invest in security.

Note that most of these models do not explicitly consider deterrence, with the result that they may lead to wasted resources if less investment would be sufficient to deter an attack. In practice, though, one objective of investment in defense is often to deter a possible attack. Miller [15] discusses the circumstances under which deterrence strategies are likely to be most or least effective. McGill [16] discusses possible methods to deter an attack, including reducing the perceived level of loss resulting from a successful attack, decreasing the success probability of an attack by investing in defense, or increasing the perceived likelihood of retaliation after an attempted attack.

Sandler and Arce [17] present a model to demonstrate deterrence when a terrorist group can attack either a business site or a tourist site. In this model, both sites wish to minimize the cost of deterring an attack plus the expected loss from an attack, while the attacker tries to maximize his payoff from launching an attack. Deterrence in this case involves deflecting the attack to another target. Arce et al. [18] study a model where an attacker can use either a conventional attack or suicide tactics, while a defender invests in protection of multiple targets. When the attacker's effort exceeds the defender's effort, the attacker wins, and vice versa. Arce et al. find that, at equilibrium, the attacker may be deterred with positive probability, and if not will choose to attack at most one target.

In some cases, the defender and the attacker may have different valuation for the same targets. Powell [19] proposed a model in which the attacker and the defender have different valuations for the targets, which results a sequential nonzero-sum "Blotto" game. He shows that there exists a unique resource allocation strategy that minimizes the defender's loss and maximizes the attacker's payoff. In particular, the defender allocates resources to minimize the attacker's maximum payoff, and in best response the attacker attacks the target that minimizes the defender's payoff. Moreover, the defender is always successful in deterring attacks on the target that is more valuable to the defender.

However, Hausken [20] has a model in which the second mover (the attacker) can never be deterred from attacking the target that is more valuable to the defender in a sequential game, as long as the defender has fixed resources. This is because, unlike in [19], Hausken allows for variable attacker effort in response to the observed defenses. He also shows that the attacker can be deterred from attacking the target is more valuable to the defender, when the defender has an unconstrained budget, as long as the unit cost of defense is less than half of the unit cost of attack.

Bier et al. [21] study a strategic model in which a defender allocates his resources to defense, and an attacker chooses a location to attack. The defender is assumed to be uncertain about the attacker's preferences, while the attacker can perfectly observe the defender's investment in security. The attacker seeks to maximize his payoff from launching an attack, and the defender seeks to minimize the damage of an attack. In this model, defensive investment in one component may increase the probability of an attack on another component. Thus, the defender may optimally leave some components undefended, sometimes preferring higher vulnerability at a particular component (even if lower vulnerability could be achieved at no cost) for strategic purposes. When the attacker has an "outside option" other than attacking, it is possible for defensive investment to deter an attack in this model, by reducing the success probability of an attack. In an application of this model, Bier et al. [22] quantify the attractiveness of various targets, and explore how the optimal budget allocation depends on the cost effectiveness of defensive investment.

Hausken and Zhuang [23] develop a model in which the defender moves first and the attacker moves second in each of multiple time periods. The attacker and the defender are myopic, in the sense of considering payoffs in only one time period when choosing their strategies for that period. Since parameter values may change through time (e.g., due to technological changes), the attacker and the defender will in general use different strategies in each time period. Hausken and Zhuang indicate that when the attacker's valuation of the target is not sufficiently large, the attacker will not attack at all even if there is no investment in defense, and will instead carry over the unused attack resources to the next period. Moreover, even if the attacker's valuation of the target would have been large enough to justify an attack on an undefended target, the attacker may still be deterred by additional investment in defense if the defender's valuation of the target is sufficiently large to justify suitable investment.

Azaiez and Bier [24] assume that the defender wishes to deter an attack by maximizing the cost of an attack to the attacker. The authors assume that the defender's investment in security increases the level of effort required for the attacker to attain a given probability of success. However, Azaiez and Bier do not explicitly consider the level of attack cost at which an attacker would be deterred, leading to possible overinvestment in security.

Another recent paper proposes a model to determine how many containers would need to be inspected in order to deter smuggling attempts [25]. The model assumes that a sufficiently high probability of being caught may deter an attacker from smuggling weapons of mass destruction into US ports. The defender moves first by choosing an inspection level to minimize the inspection cost plus the expected loss (both the expected damage and the cost of any resulting retaliation) from a weapon being successfully smuggled into the US, while the attacker wishes to find the best response to the defender's policy in order to maximize his expected reward. In an extension of this work, Haphuriwat et al. [26] suggest a model to identify the required percentage of containers to inspect in order to deter one or more nuclear weapons from being smuggled in to the US in shipping containers.

Bordley and Kirkwood [27] propose a new target-oriented utility approach that can be applied to the problem of deterrence in security. Target-oriented utility theory assumes that the decision maker wishes to minimize the probability of failing to achieve an uncertain target. In this paper, we assume that the defender is uncertain about the level of investment that would be sufficient to achieve deterrence. The defender objective is then to maximize the expected value of deterrence (the probability of deterring an attack, times the expected loss if an attack occurs), minus the defensive cost. For additional studies, Hausken and Levitin [28] classify some recent studies of defense and attack models.

Section 2 of this paper presents a basic model for a single-component system assuming that the probability of deterrence is a function of the level investment in security. Section 3 presents a revised model, taking into account the fact that investment in