European Journal of Operational Research 228 (2013) 262–272

Contents lists available at SciVerse ScienceDirect

European Journal of Operational Research

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

Innovative Applications of O.R.

Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game

Xiaojun Shan, Jun Zhuang *

University at Buffalo, SUNY, New York, USA

ARTICLE INFO

Article history:
Received 16 March 2011
Accepted 16 January 2013
Available online 29 January 2013

Keywords:
Game theory
Homeland security
Resource allocation
Attacker–defender game
Non-strategic player
Partially strategic player

ABSTRACT

Many models have been developed to study homeland security games between governments (defender) and terrorists (attacker, adversary, enemy), with the limiting assumption of the terrorists being rational or strategic. In this paper, we develop a novel hybrid model in which a centralized government allocates defensive resources among multiple potential targets to minimize total expected loss, in the face of a terrorist being either strategic or non-strategic. The attack probabilities of a strategic terrorist are endogenously determined in the model, while the attack probabilities of a non-strategic terrorist are exogenously provided. We study the robustness of defensive resource allocations by comparing the government's total expected losses when: (a) the government knows the probability that the terrorist is strategic; (b) the government falsely believes that the terrorist is fully strategic, when the terrorist could be non-strategic; and (c) the government falsely believes that the terrorist is fully non-strategic, when the terrorist could be strategic. Besides providing six theorems to highlight the general results, we find that game models are generally preferred to non-game model even when the probability of a non-strategic terrorist is significantly greater than 50%. We conclude that defensive resource allocations based on game-theoretic models would not incur too much additional expected loss and thus more preferred, as compared to non-game-theoretic models.

1. Introduction

Since September 11, 2001, homeland security in the United States has attracted hundreds of billions of dollars in expenditures (Fig. 1). The effectiveness of such large amounts of expenditure is frequently criticized as reflecting "pork-barrel politics", in which funds are directed towards low-risk targets for political reasons (e.g., McLaughlin, 2002; O'Beirne, 2003; de Rugy, 2005). Moreover, even though the DHS has implemented a risk-based method in guiding grant allocations since 2006, risk-related measures are still limited (U.S. Government Accountability Office, 2008).

Operations Research (OR) methods are useful in studying counter-terrorism. For example, Harris (2004) discussed the role of probabilistic risk analysis, randomization, and game theory in defending against terrorist attacks. Brown et al. (2005) developed a two-sided optimization model for pre-localization of defense missile platforms considering adaptive adversaries. Kaplan and Kress (2005) modeled and analyzed the operational effectiveness of suicide-bomber-detector schemes in reducing the casualties caused by suicide-bombing. Brown et al. (2005) developed bi-level and tri-level optimization models to study the defense strategies for critical infrastructures. Lin et al. (2009) built a M/G/1 queue to explore optimal scheduling policies for an antiterrorist surveillance system. Wein (2009) illustrated the close relationship between mathematical modeling and policy recommendations. Baveja and Wein (2009) evaluated and quantified the effectiveness of a two-finger, two-stage biometric strategy for the US-VISIT program using OR methods and Stakelberg game formulations. Jain et al. (2010) developed computer-aided randomized patrol planning systems for airplane transportation security. Recently, Kaplan (2010) employed queueing theory and Markov processes to study how undercover intelligence agents infiltrate and interdict terrorist plots.

One specific area of application of OR methods in homeland security is terrorism risk analysis. Traditional methods of decision and risk analysis do not explicitly take into account the ability of intelligent adversaries to adapt to defenses, and therefore, may overestimate the effectiveness of defensive measures. In contrast, while game theory has been widely applied in counter-terrorism analysis (Azaiez and Bier, 2007; Hausken, 2008; Sandler and Siqueira, 2009; Haphuriwat and Bier, 2011) and other strategic decision-making scenarios (Hausken and Zhuang, 2012), game-theoretic methods have been criticized as attributing excessive levels of knowledge and computational ability to potential terrorists (i.e., assuming players to be fully rational), and

* Corresponding author. Address: University at Buffalo, SUNY, Industrial and Systems Engineering, 317 Bell Hall, Buffalo, NY 14260, USA. Tel.: +1 716 645 4707; fax: +1 716 645 3302.
E-mail address: jzhuang@buffalo.edu (J. Zhuang).

0377-2217/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ejor.2013.01.029

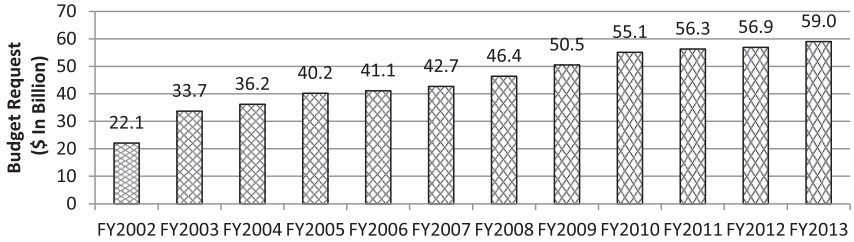

Fig. 1. Annual budget requests for the Department of Homeland Security from Fiscal Year 2002 to 2013. *Source*: U.S. Department of Homeland Security (2012).

frequently recommending insufficient "hedging" (i.e., protecting against only the few most detrimental attack strategies). Similarly, the justification of defending low-risk targets as in "pork-barrel politics" from a game-theoretic perspective may depend critically on the assumption of game theory about terrorist's rationality, since irrational terrorists could attack low-risk targets even when that may not be optimal in a game-theoretic sense. Probably as a result, game theory has been less frequently mentioned in risk analysis in recent years (Hall, 2009).

In fact, game theory, and decision and risk analysis complement each other. Decision and risk analysis can model the probable outcomes of a game and evaluate the payoffs of those outcomes. On the other hand, instead of viewing adversary's decisions as random variables, game-theoretic formulation can help endogenously determine adversary's decisions (Cox, 2009).

One key difference between terrorism and natural disasters is that terrorists are intelligent and adaptive while natural disasters are not. As a result, a certain government's optimal strategies in the face of terrorism may significantly differ from the strategies adopted against natural disasters (Powell, 2007; Zhuang and Bier, 2007; Golany et al., 2009; Levitin and Hausken, 2009). Intelligence plays a key role in informing the government of whether, and how much, the terrorist is strategic (Kress and Szechtman, 2009). In particular, Kaplan et al. (2010) found that when the government's intelligence is poor, it would be easier for strategic insurgents to survive attacks by the government. Overall, decision and risk analysis is useful in devising strategies to deal with natural disasters or non-adaptive threats, while game theory is powerful when coping with terrorism or adaptive threats but usually strongly assumes that the terrorists are fully rational or strategic.

This paper pioneers a novel hybrid approach by integrating the game-theoretic and non-game-theoretic defense allocation models using an adjustable parameter to represent the probability that the terrorist might behave strategically (i.e., will adapt to the observed defense). As a first solid step toward tackling this important problem, we assume that the target government knows the probability of the attacker being strategic and has complete information about the probabilities that each target will be attacked by a non-strategic attacker. Note that the main difference between a strategic and non-strategic attacker lies in their responses to the defender's allocation decision. On the other hand, the main distinction between game-theoretic and non-game-theoretic models is that game-theoretic models take into account the attacker's response to the defender's allocation decision while in non-game-theoretic models, the attacker's decision is exogenously determined and is not a function of the defender's allocation decision. As our results will show in Section 4, game-theoretic models are often preferred to non-game-theoretic models, since game-theoretic models often incur lower expected loss for the defender than non-game-theoretic models.

It is instructive to compare non-adaptive threats such as natural disasters and terrorism. Defensive resource allocations against a strategic attacker has been extensively studied in game theory. In particular, Colonel Blotto games were designed to tackle this type of problem (e.g., Shubik and Weber, 1981; Roberson, 2006). One difference between the game-theoretic portion of our model and traditional Colonel Blotto games is in that our model is sequential while in Colonel Blotto games decisions are made simultaneously. We note that extension of Colonel Blotto games to the realm of sequential, nonzero-sum games has been recently carried out by Powell (2009), which did not consider the scenario that the attacker is partially strategic.

Allowing multiple behavioral types of one player has been pioneered by Kreps et al. (1982). There exist several differences between Kreps et al. (1982) and the current paper. First, Kreps et al. (1982) only allowed the player to take on the alternative type with a very small probability while in the current model the attacker could be non-strategic with any probability between 0 and 1. Second, both behavioral types in the model from Kreps et al. (1982) are fully strategic and play best responses to the other player's moves while in the current model if the attacker is non-strategic, there is no decision to make and thus his moves are not influenced by the defender's decision at all.

The remainder of the paper is structured as follows. Section 2 formulates the model and discusses data sources. Section 3 provides analytic results, an algorithm, and a numerical example, investigating one particular type of non-strategic attack probabilities: evenly distributed to top N valuable targets. Section 4 introduces two types of false beliefs, defines robustness, and conducts both one-way and two-way sensitivity analyses to investigate the robustness of game-theoretic models. Finally, Section 5 provides conclusion and future research directions. Appendix A contains the proofs of the six theorems for this paper, and Appendix B presents illustrations to Theorem 2 and robustness analysis and sensitivity analyses for three other types of non-strategic terrorist as well as identifying the optimal defensive resource allocations for them.

2. Notation, assumptions, and model formulation

2.1. Notation

We use the following notation throughout the paper:

- $q \in [0,1]$ and $1-q$: Probabilities that the terrorist is strategic and non-strategic, respectively.
- n: Number of targets in the system.
- $c_i \geqslant 0$: Government's defensive resource allocation to target i, for $i = 1, 2, \ldots, n$.
- $c \equiv (c_1, c_2, \ldots, c_n)$.
- C: Total budget of the defensive resources. That is,

$$C = \sum_{i=1}^{n} c_i \tag{1}$$

- J: Set of defended targets. That is, $J \equiv \{i: c_i > 0;\ i = 1, 2, \ldots, n\}$
- r: Total probabilities of attacks for both the strategic and non-strategic attacker.
- $h_i(c)$: Endogenously-determined probability that a strategic terrorist will attack target i, for $i = 1, 2, \ldots, n$. We have $h_i(c) \geqslant 0$, and $\sum_{i=1}^{n} h_i(c) = r$.