European Journal of Operational Research 246 (2015) 320–330

Contents lists available at ScienceDirect

European Journal of Operational Research

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

Interfaces with Other Disciplines

On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness

Mohammad E. Nikoofal[a], Jun Zhuang[b,*]

[a] UCP-Católica Lisbon School of Business & Economics, Palma de Cima, Lisbon 1649-023, Portugal
[b] Industrial and Systems Engineering, University at Buffalo, State University of New York, 317 Bell Hall, Buffalo, NY 14260-2050, USA

ARTICLE INFO

Article history:
Received 6 March 2014
Accepted 21 April 2015
Available online 28 April 2015

Keywords:
Defense system
Game Theory
Secrecy
Exposure
Robustness

ABSTRACT

It is commonly accepted in the literature that, when facing with a strategic terrorist, the government can be better off by manipulating the terrorist's target selection with exposing her defense levels and thus moving first. However, the impact of terrorist's private information may significantly affect such government's first-mover advantage, which has not been extensively studied in the literature. To explore the impact of asymmetry in terrorist's attributes between government and terrorist on defense equilibrium, we propose a model in which the government chooses between disclosure (sequential game) and secrecy (simultaneous game) of her defense system. Our analysis shows that the government's first-mover advantage in a sequential game is considerable only when both government and terrorist share relatively similar valuation of targets. In contrast, we interestingly find that the government no longer benefits from the first-mover advantage by exposing her defense levels when the degree of divergence between government and terrorist valuation of targets is high. This is due to the robustness of defense system under secrecy, in the sense that all targets should be defended in equilibrium irrespective of how the terrorist valuation of targets is different to government. We identify two phenomena that lead to this result. First, when the terrorist holds a significantly higher valuation of targets than the government's belief, the government may waste her budget in a sequential game by over-investing on the high-valued targets. Second, when the terrorist holds a significantly lower valuation of targets, the government may incur a higher expected damage in a sequential game because of not defending the low-valued targets. Finally, we believe that this paper provides some novel insights to homeland security resource allocation problems.

1. Introduction

Contrary to facing with natural disasters, where the government discloses her defense investments to the public, understanding when and how defensive investment should be disclosed is a challenging issue for governments facing terrorism attacks. Specifically, when government reveals how the targets are defended, the terrorist may have a better knowledge of the effectiveness of the defensive technologies, which increases the probability of a successful attack (Zhuang & Bier, 2010). Powell (2007a) shows that investing more in defense and disclosing to the public could be a signal to the attacker that the heavily defended targets are more vulnerable and/or valuable, and therefore may increase their probabilities of being attacked. On the other hand, for some targets that are well known to the attackers (e.g., the Sears Tower, the Pentagon, and the Golden Gate Bridge), Shapiro and Siegel (2010) show that the government can be better off by revealing defensive information rather than keeping it secret. Zhuang and Bier (2007) also show that, under complete information, the defender should advertize her defensive investments instead of keeping them secret in order to gain the benefits of first-mover advantages. Note that the above results on the advantages of either exposure or secrecy may not necessarily hold if the terrorist has private information, e.g., about his valuation of targets.

In the homeland security literature, it is commonly assumed that the terrorist behaves strategically in the sense that he responds optimally to the government's defensive actions (Jose & Zhuang, 2013). This assumption, which is usually regarded by modeling a sequential defender-attacker game, may mislead the government to a non-efficient allocation of her limited budget. After the terrorism events on September 11, 2001 there has been a dramatic increase in security at the traditional targets, such as embassies and other government properties. Observing strong security levels may lead to different possible outcomes. First, it could be a signal to the terrorist that these

* Corresponding author. Tel.: +17166454707; fax: (716) 645 3302.
E-mail addresses: mohammad.nikoofal@ucp.pt (M.E. Nikoofal), jzhuang@buffalo.edu (J. Zhuang).

http://dx.doi.org/10.1016/j.ejor.2015.04.043
0377-2217/

heavily defended targets are more vulnerable and/or more valuable, and therefore may increase their probabilities of being attacked. Second, it may stir the terrorist to switch his attack from *hard (firmly defended)* targets to *soft (weakly defended)* targets. Consequently, the defender may succeed only in deterring the attacker from hard targets, while increasing the threat to soft, but not necessarily less valuable targets. Finally, the terrorist may attack heavily defended targets for some reason that may not be anticipated by the government at the time of attack. For example, he may be looking to demonstrate his organization's power, incurring political and psychological threats, or showing how bold he would be in target selection.

Zhuang and Bier (2010) list some possible reasons for secrecy in the homeland security resource allocation problems. As an example, they pose the advantage of secret anthrax sterilization equipment in the U.S. post office. By announcing that information to the public, potential attackers might use private couriers to deliver anthrax. Consequently, the millions of dollars of defense may just stir the attacker to pay the slightly higher shipping fees charged by the private couriers. In contrast, secret sterilization equipment could have been effective against anthrax attacks. Therefore, the first-mover advantage in a sequential game is not always beneficial for the government. Thus, the demanding scenario is to consider the case where the government hides the defense allocations from the terrorist observation. To model such conditions, one can assume that both the terrorist and the government move simultaneously (Berman, Gavious, & Huang, 2011). Note that this does not actually require both players to decide at the same time; they can be viewed as being engaged in a simultaneous game as long as neither party knows the other's decision at the time he makes his own decision (Zhuang & Bier, 2010). The main goal of this paper is then to answer the following research questions:

Research Question 1: What is the impact of asymmetry in terrorist's attributes between government and terrorist on the government's first-mover advantage?

Research Question 2: Under what conditions can the government be better off by keeping secrecy of defense system rather than exposing it? Which feature of secrecy strategy may dominate the first-mover advantage of exposure strategy?

To answer the above questions, we develop a one-shot game between a government and a strategic terrorist. The government defends two targets and chooses between secrecy and exposure of defense system. To study the decisions under secrecy we assume that the government and terrorist play simultaneously; hence we use the Nash equilibrium approach. However, to analyze the game under exposure policy we assume that the game is played sequentially; hence we use the Stackelberg equilibrium approach. Depending on the government's decision, the terrorist may or may not observe the defense allocation, but in any case he chooses his target and the level of attack. To address research question 1, we show that the government's first-mover advantage under exposure is considerable only when both government and terrorist share relatively similar valuations of targets. In contrast, we find that the government no longer benefits from first-mover advantage by exposing her defense level when the degree of divergence between the government's and the terrorist's valuation of targets is high. To answer research question 2, our analysis shows that the defense system under secrecy is robust to the degree of asymmetry between government and terrorist about terrorist valuation of targets, in the sense that all targets should be defended in equilibrium irrespective of how different the terrorist valuation of targets is to the government. This robustness of defense system under secrecy may dominate the first-mover advantage under exposure. We identify two phenomena that lead to this result. First, when the terrorist holds a significantly higher valuation of targets than the government's belief, the government may waste her budget in a sequential game by over-investing (compared to simultaneous game) on the high-valued targets. Moreover, when the terrorist holds a significantly lower valuation of targets, the government may incur higher expected damage in a sequential game because of not defending the low-valued targets.

The remainder of this paper is organized as follows. Section 2 provides some literature review and clarifies the contribution of this paper. Section 3 presents the model framework. Section 4 provides a benchmark and analyzes the game when the defender and attacker share common valuation of targets. Section 5 explores the impact of asymmetric information on defender's strategy and the budget allocation decision. Section 6 compares the robustness of the defense system of a simultaneous game with that in a sequential game. Section 7 presents an illustrative numerical study to support the analytical results. Section 8 summarizes the main results. Finally, Appendix provides the proofs for all propositions.

2. Literature review

Operations research originated from the efforts of military applications during World War II but has been widely resumed with respect to homeland security after September 11, 2001 (Brown, Carlyle, Salmeron, & Wood, 2006; Hu, Homem-de Mello, & Mehrotra, 2011; Kaplan, Kress, & Szechtman, 2010; McLay, Jacobson, & Nikolaev, 2009; Wright, Liberatore, & Nydick, 2006). Among different techniques of operations research, game theory is a popular tool to capture the strategic interactions between the terrorists and the government on resource allocation problems among multiple targets (Cox, 2009; Hall, 2009; Hausken, 2002; Insua, Rios, & Banks, 2009). See Sandler and Siqueira (2009) for a survey of recent advances in the game-theoretic analysis of terrorism. This literature can be divided into two main streams depending on whether the defender reveals or hides her defense plan.

The literature in the first stream assumes that the attacker behaves strategically by optimally responding to the defender's resource allocation. Under this assumption, the defender, as the Stackelberg leader, can strategically manipulate the attacker's response and predict which target will most likely be attacked (Powell, 2007b; Zhuang & Bier, 2007). Within this stream, several studies explore the impact of uncertainty in the attacker's attributes on defense equilibrium (Bier, Haphuriwat, Menoyo, Zimmerman, & Culpen, 2008; Bier, Oliveros, & Samuelson, 2007; Jeneliusa, Westina, & Holmgrenb, 2010; Kardes, 2008; Nikoofal & Zhuang, 2012; Powell, 2007b; Rios & Insua, 2009; Wang & Bier, 2011; Zhang & Ramirez-Marquez, 2012). A number of studies investigate signaling games where the defender updates her belief about the attacker's attributes (Arce & Sandler, 2007; Harvey & Sandler, 1993; Hausken & Zhuang, 2011; Overgaard, 1994; Zhuang, Bier, & Alagoz, 2010). There is also some research that investigates allocating defensive resources facing both strategic threats (e.g., strategic terrorists) and nonstrategic threats (e.g., natural disasters Golany, Kaplan, Marmur, & Rothblum, 2009; Levitin & Hausken, 2009; Powell, 2007b; Zhuang & Bier, 2007 and nonstrategic terrorists Hao, Jin, & Zhuang, 2009; Nikoofal & Gumus, 2015; Shan & Zhuang, 2013b). The only paper in this stream that investigates the impact of the attacker's private information on the robustness of the defender's budget allocation is Nikoofal and Zhuang (2012); however, it fails to compare the robustness of the defense system in a sequential game with that in a simultaneous game, and thus fails to study the tradeoff between secrecy and exposure.

The second stream of research in this literature, which is not as rich as the first stream, studies the case when the defender and the attacker move simultaneously. Zhuang and Bier (2007) and Hausken, Bier, and Zhuang (2008) propose game-theoretical models to study how the defender chooses tradeoffs between investments in protection against natural disaster and terrorism. Rios and Insua (2009) provide a Bayesian decision analysis to analyze the defender's strategy against an intelligent attacker. Dighe, Zhuang, and Bier (2009) show that partial secrecy about defensive allocations (disclosure of the total level of defensive investment, but secrecy about which resources are

defended) can be an optimal strategy for achieving a cost-effective attack deterrence. However, none of these papers study the impact of the attacker's private information on defensive budget allocation.

Bier et al. (2007) compare the equilibrium in sequential and simultaneous games when the attacker's preferences are known by the attacker but not the defender. Their results show that, in equilibrium, the defender is generally better off in the sequential game. Brown and Cox (2011) show that traditional probabilistic risk assessment can lead to poor defensive decisions when the attacker holds private information about his attack probabilities. The authors therefore recommend making robust risk management decisions, which motivates this paper, where the attacker may know something that the defender does not know. Brown, Carlyle, Diehl, Kline, and Wood (2005) and Zhuang and Bier (2011) study whether and how the defender should disclose correct information (truthful disclosure), incorrect information (deception), or no information (secrecy) about her resource allocation. Our paper differs from the above papers mainly because of its focus on characterizing the conditions under which the defender is better off by keeping secrecy, rather than exposing, of her defense system. In particular, the results of this paper contribute to the literature by showing that the secrecy policy may dominate the exposure policy when the attacker's valuation of targets significantly differs from defender's a-priori belief. Moreover, to compare the robustness of defense system under secrecy and exposure strategies, we define distribution-free intervals to more generally capture the defender's uncertainty in the attacker's private information. Note that the above papers apply Harsanyi's transformation (Harsanyi, 1967) to consider different types of the attackers assuming that the defender completely knows the probability distribution of the attacker's attributes.

The model of constant-sum simultaneous defender–attacker game is known as Colonel Blotto games, in which two players simultaneously distribute their fixed amount of resources across n battlefields (Adamo & Matros, 2009; Kovenock & Roberson, 2011; Roberson, 2006; Shubik & Weber, 1981). Within each battlefield, the player that allocates the higher level of the resource wins the battlefield, and each player's payoff is equal to the number of battlefields won. This paper differs from the Colonel Blotto games in at least two aspects. First, our model is not a constant-sum game, and the defender and attacker respectively consider the costs of defense and attack effort in their payoff functions. Second, this paper examines the robustness of the defense when the attacker has private information about his attributes, which has not been studied in the Colonel Blotto game literature.

There is increasing interest to study the dynamic interactions between defender and attacker under asymmetric information, in which either party can update his/her belief about the other's attributes by following the action history (Crawford, 2003; Hausken & Zhuang, 2011; Levitin & Hausken, 2009; Zhuang et al., 2010). For simplicity, this paper does not study dynamic games. However, we acknowledge that comparing secrecy and exposure policies in a dynamic setting is interesting, specifically, when the government or/and terrorist can update their beliefs about each other after each round of the game.

3. Model formulation

We consider a one-shot game in which the defender defends two targets and chooses whether or not to disclose her defense allocation[1]. Let v_i and u_i be the defender's and attacker's valuation of target i, respectively, for $i = 1, 2$. Without loss of generality, we assume that target 1 is more valuable than target 2, i.e., $v_1 \geq v_2$. The defender first decides whether to expose or hide her defense system, and then allocates d_i to target i. Depending on the defender's decisions, the attacker may or may not observe the defense allocation, but in any case he chooses his target i^* and the level of attack, a_{i^*}, where $i \in \{1, 2\}$. For analytical convenience, we assume that the attacker may undertake an attack on, at most, one target. Note that it is also a common assumption in the literature that the terrorist concentrates his attack budget to launch an attack on only one target to incur the highest damage on his selected target (see Bier et al., 2007; Golalikhani & Zhuang, 2011; Golany et al., 2009; Powell, 2007a; 2007b; Zhuang & Bier, 2007 and references therein). Note also that there is another class of constant-sum defender–attacker games, as discussed earlier in Section 2, known as the Colonel Blotto game (Adamo & Matros, 2009; Kovenock & Roberson, 2011; Roberson, 2006; Shubik & Weber, 1981), in which two players distribute their fixed amount of resource across n battlefields. Within each battlefield, the player that allocates the higher level of the resource wins the battlefield, and each player's payoff is equal to the number of battlefields won. Considering a multi-site attack assumption is an important feature of Colonel Blotto games where defender and attacker only consider expected damage, but not the defense or attack levels. However, since our model is not a zero-sum game, and the damage due to an attack follows an exponential function in our model, having a single-site attack assumption is not a hard assumption.

We assume that if the target i is attacked, the expected damage on the target depends on defense level d_i, the effectiveness ratio of an attack[2] $\lambda \geq 0$, and the attacker's effort a_i. Furthermore, the expected damage is decreasing in d_i, but increasing in a_i and λ. Consider an exponential damage function (Bier et al., 2008; Golalikhani & Zhuang, 2011; Nikoofal & Zhuang, 2012; Shan & Zhuang, 2013a) $p(d_i, a_i) = 1 - \exp(-\lambda a_i/d_i)$, where $p(d_i, a_i)$ is the likelihood function of damage. Thus, the expected damage on target i, if attempted by the attacker, is $v_i p(d_i, a_i)$ and $u_i p(d_i, a_i)$, respectively, from the defender's and attacker's perspectives.

The defender's optimization problem has two levels: (i) the outer problem to decide whether to keep secrecy (i.e., $y = S$), or exposure (i.e., $y = E$) of her defense system, and (ii) the inner problem to decide the budget to allocate to each target in order to minimize the summation of the expected damage of attacked target and the total defense costs, given the optimal decision made in the outer problem. The defender's optimization model is therefore as follows:

$$Z = \min_{y\in\{S,E\}} \min_{d_1^y, d_2^y \geq 0} \sum_{i=1}^{2} [v_i p_y(d_i^y, a_i^y) \times \mathrm{I}_{i=i_y^*} + d_i^y] \tag{1}$$

where $\mathrm{I}_{i=i_y^*}$ is the binary indicator that takes 1 if target i is attacked by the attacker under strategy $y \in \{S, E\}$, and 0 otherwise. According to the defender's upper decision, we define $\Delta Z = Z_S - Z_E$ as the defender's first-mover advantage, which is the difference in defender's payoff when she chooses secrecy or exposure of her defense system. Clearly, this difference can be decomposed into two parts: (i) the difference in expected damage due to an attack, which is $\Delta Z_1 = v_{i_S^*}^S \times p_S(d_{i_S^*}^S, a_{i_S^*}^S) - v_{i_E^*}^E \times p_E(d_{i_E^*}^E, a_{i_E^*}^E)$, where i_y^* shows the target that will be attacked if the defender takes strategy $y \in \{S, E\}$; and (ii) the difference in total defense costs, which is $\Delta Z_2 = \sum_{i=1}^{2}(d_i^S - d_i^E)$. Finally, by considering defense cost in defender's optimization problem, we capture the impact of the finite budget constraint (Zhuang & Bier, 2007).

Now, let us study the attacker's optimization problem. While the attacker is strategic, he seeks to select his target and the attack effort together. Specifically, he desires to maximize the total expected damage, subtracting the total attack cost on his target i^*. That is:

$$i_y^* = \arg\max_{i_y} \left\{ \max_{a_i^y \geq 0} \left[u_i p_y\left(d_i^y, a_i^y\right) - a_i^y \right] \right\} \tag{2}$$

[1] For analytical convenience, we consider only two targets, and furthermore, in Sections 6 and 7, we study the N-target case where $N > 2$.

[2] Note that the parameter λ could be used to measure the effectiveness of the budget per unit of investment (Bier et al., 2008), or effectiveness of attack (Nikoofal & Zhuang, 2012); in particular, one unit increment in ratio a_i/d_i increases the probability of damage on target i by $100e^{-\lambda}\%$.

where i_y^* shows the target that will be attacked if defender takes strategy $y \in \{S, E\}$. Similar to the defender's optimization problem, by considering attack budget in the attacker's optimization problem, we capture the impact of finite attack budget constraint (Zhuang & Bier, 2007). Note that we need to take the defender's first decision into account when solving the proposed model. In particular, the Nash equilibrium approach is the way to solve the problem if the game is played simultaneously (i.e., defender decides to keep secrecy, $y = S$); however, if the game is played sequentially (i.e., defender decides to expose, $y = E$), we need to employ the Stackelberg equilibrium approach. Note that in a simultaneous game, the attacker cannot observe the defender's resource allocation and decides on his target and the attack effort at the same time. However, in a sequential game, since the defender exposes her resource allocation, the attacker chooses the target that gives him the maximum payoff. Therefore, the defender can manipulate the attacker's choice of target in a sequential game. For the sake of simplicity in exposition, let us rewrite the defender's objective function (1) as the summation of total budget and the expected damage only on the attacked target. Let $\psi = v^S_{i^*_S} \times p_S(d^S_{i^*_S}, a^S_{i^*_S})$ indicate the expected damage on the attacked target (i^*_S) in a sequential game. Since the defender tries to minimize ψ, her objective function is then $\min_{d_1^E, d_2^E} \psi + \sum_{i=1}^{2} d_i^E$. On the other hand, because the attacker tries to maximize ψ, the defender has to consider additional constraints $v_i p_E(d_i^E, a_i^E) \le \psi$, $\forall i$, which assure that the possible expected damage on target i is less than ψ. Thanks to this observation, we will show that the defender's optimization problem can be rewritten as a *linear programming* model with respect to d_1 and d_2. Furthermore, in order to characterize the defender equilibrium strategy, we then apply the optimality principle of linear programming, which effectively states that when the feasible set is nonempty and bounded, then at least one optimal solution is located at an extreme point (Dantzig, 1951). To summarize, at optimality, the additional constraints $v_i p_E(d_i^E, a_i^E) \le \psi$, $\forall i$ are binding for defended targets, resulting in a tractable model to characterize the defender's equilibrium strategy in a sequential game.

4. Game analysis under equal valuation: a benchmark

To study the impact of uncertainty in the attacker's valuation of targets on defender's decision, as a benchmark, we first investigate the defender's problem when both the defender and attacker share a common valuation of targets (i.e., $u_i = v_i$, $\forall i = 1, 2$). Note that a set of defender's and attacker's strategies is an equilibrium if no player can do better by unilaterally changing his or her strategy. We use the best response correspondences to prove the existence of Nash equilibrium when defender keeps secrecy and the Stackelberg equilibrium when she discloses her defense strategy (Fudenberg & Tirole, 1991). The defender employs the attacker's best response to estimate the attacker's effort. By satisfying the first order condition, i.e., $\frac{\partial[v_i p(d_i, a_i) - a_i]}{\partial a_i} = 0$, the attacker's best response is:

$$a_i^{br} = \begin{cases} 0 & \text{if } d_i \ge \lambda v_i, \text{ for } i = 1, 2 \\ \frac{d_i}{\lambda} \ln\left(\frac{\lambda v_i}{d_i}\right) & \text{Otherwise.} \end{cases} \quad (3)$$

The following proposition presents the defender's equilibrium when both the defender and attacker share a common valuation of targets (note that the proofs for all propositions are presented in Appendix).

Proposition 1. *When the defender and attacker share a common valuation of targets, the following statements are true:*

- *Under secrecy, the optimal allocation is* $d_i^* = \lambda v_i \exp(-\lambda)$ *and Target 1 (i.e., the high-valued target) is attacked;*
- *Under exposure, the optimal allocation depends on* λ*; specifically, if* $\lambda \le 0.5$*, then* $d_i = \lambda v_i$ *and the attacker is deterred; and if* $\lambda > 0.5$*, then* $d_1 = \lambda(v_1 - v_2)$, $d_2 = 0$ *and Target 2 (i.e., the low-valued target) is attacked; and*
- *The defender can never be better off by keeping secrecy of her defense system and her first-mover advantage* ($\Delta Z \ge 0$) *as well as its decomposition is*

$$\Delta Z = \begin{cases} \underbrace{(1 - e^{-\lambda})v_1}_{\Delta Z_1} + \underbrace{\lambda(e^{-\lambda} - 1)(v_1 + v_2)}_{\Delta Z_2} & \text{if } \lambda \le 0.5 \\ \underbrace{(1 - e^{-\lambda})v_1 - v_2}_{\Delta Z_1} + \underbrace{\lambda[(v_1 + v_2)e^{-\lambda} - (v_1 - v_2)]}_{\Delta Z_2} & \text{if } \lambda > 0.5 \end{cases}$$

Remark 1. Proposition 1 indicates that, when both the defender and attacker share a common valuation of targets, the defender can benefit from a *first-mover advantage* by advertizing her defensive investments instead of keeping them secret. The rationale behind this observation is related to the defender's ability to manipulate the attacker's target selection in a sequential game. From Proposition 1, the attacker always attacks the more valuable target (i.e., Target 1) in a simultaneous game. However, in a sequential game, the defender may be better off by shifting her budget away from low-valued to high-valued targets; consequently, the attacker may be deterred, if his attack is not too effective (i.e., $\lambda \le 0.5$), switches attack from high-valued to low-valued targets (i.e., Target 2), or if his attack effort is highly effective (i.e., $\lambda > 0.5$). In the former scenario (i.e., $\lambda \le 0.5$), the defense budget required to deter attack on both targets is not great; therefore the defender can deter an attack on both targets. However, in the latter scenario (i.e., $\lambda > 0.5$), the attack could be more destructive and the defender would need to assign more defense to deter an attack on targets; therefore the defender may have to leave some targets undefended. To describe the rationale behind this observation, note that the high-valued target (Target 1) should be the target that will be protected first by the defender. The more the defender allocates budget to protect Target 1, the less the attacker's payoff will be for it, until the attacker becomes better off by switching to the low-valued target (Target 2). Therefore, the defender should allocate budget to Target 1 in order to equalize the expected damage across both targets. The defense level required to do this is $d_1 = \lambda(v_1 - v_2)$ under which the expected damage is the same if the attack is launched on either targets.

From the last part of Proposition 1, the defender's first-mover advantage, ΔZ, is always positive. However, the two elements of ΔZ are not necessarily positive and may depend on the effectiveness ratio of an attack, λ, and the attacker's decision (see Fig. 1). Recall that ΔZ_1 and ΔZ_2 show the differences in expected damage and total investment in sequential and simultaneous games, respectively. When $\lambda \le 0.5$, the attacker is deterred in a sequential game, but he attacks Target 1 (i.e., the more valuable target) in a simultaneous game. From Fig. 1(a), the defender invests less in the simultaneous game compared to the sequential game (i.e., $\Delta Z_2 < 0$), but in turn, she incurs a damage due to an attack on her more valuable target (i.e., $\Delta Z_1 > 0$). Since the expected damage is greater than the saving from an under-investment decision, the defender is better off in a sequential game. However, when $\lambda > 0.5$, the defender may invest more or less in the simultaneous game compared to the sequential game, which in turn, may lead to less or more expected damage, respectively. To summarize, since what matters is the total loss, the defender is always better off in a sequential game.

Finally, note that both targets are always defended in a simultaneous game; however, in a sequential game, the less valuable target (i.e., Target 2) may be left undefended (when $\lambda > 0.5$). This fundamental difference, between the defense plan in a simultaneous game and that of a sequential game, mainly comes from the fact that the defender loses the first-mover advantage in a simultaneous game. Later, in Section 6, we will show that when the defender suffers from the lack of knowledge about attacker's valuation of targets, all targets should still be defended in equilibrium in a simultaneous game. Such style on budget allocation in a simultaneous game, which is called

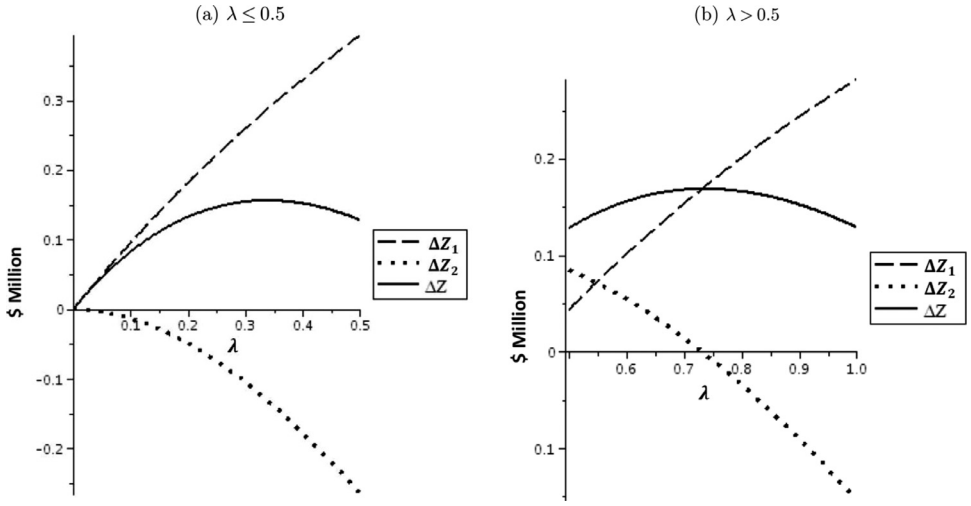

Fig. 1. Decomposition of defender's first-mover advantage under equal valuation scenario ($v_1 = 1$ \$ million, $v_2 = 0.35$ \$ million).

robustness advantage in this paper, would be helpful for the defender when the degree of information asymmetry is high, i.e., when the attacker holds a significantly different valuation of targets from the defender's belief.

5. Game analysis under asymmetric information

We now study the defender's problem under an asymmetric information scenario where the attacker knows the defender's valuation of targets but he holds a different valuation of targets which is privately known only for the attacker. Let $k = \frac{u_i}{v_i}$ show the ratio of the attacker's to defender's valuations of targets[3]. Now, to define asymmetry in the attacker's attribute between the defender and attacker, we assume that they hold different values of k; specifically, let k_a indicate the true value of k, which is privately known by the attacker, and k_d indicate the defender's a-priori beliefs about k. Finally, for analytical convenience, and without loss of generality, we assume that $k_d = 1$, but the attacker may hold any value of $k_a > 0$[4]. By plugging $u_i = k_a v_i$ into the attacker's optimization problem (2), and satisfying the first order condition, the attacker's best response becomes

$$a_i^{br} = \begin{cases} 0 & \text{if } d_i \geq \lambda k_a v_i, \quad \text{for } i = 1,2 \\ \frac{d_i}{\lambda} \ln\left(\frac{\lambda k_a v_i}{d_i}\right) & \text{Otherwise,} \quad \text{for } i = 1,2. \end{cases} \tag{4}$$

The following proposition characterizes the defender's first-mover advantage when the attacker holds private information about his valuation of targets.

Proposition 2. *The defender may be worse off in a sequential game compared to a simultaneous game under asymmetric information. Specifically, the defender loses the first-mover advantage in Regions III, IV, and VII in Fig. 2, where the attacker's valuation of targets significantly differs from the defender's a-priori belief.*

Remark 2. From Proposition 2, verify that the comparison between the defender's loss in sequential and simultaneous games mainly depends on: (i) the degree of information asymmetry between the defender and attacker, and (ii) the effectiveness ratio of an attack, λ. In very simple scenario, when the effectiveness ratio of an attack is low ($\lambda \leq 0.5$), and the attacker holds relatively low valuation of targets (i.e., k_a is low), the defender can easily deter an attack on both targets in a sequential game; hence she can benefit from first-mover advantage. Otherwise, i.e., when the effectiveness ratio of an attack is high and the attacker holds relatively lower valuation of targets than defender (Region IV in Fig. 2), or the attacker holds a significantly higher valuation of targets than defender's belief (Regions III and VII in Fig. 2), the comparison between defender's loss in sequential and simultaneous games mainly depends on the degree of information asymmetry between defender and attacker. The reason for why the defender loses her first-mover advantage in those regions is related to the differences in expected damage (ΔZ_1) and total defense budget (ΔZ_2) under secrecy and exposure presented in Table 1. Using the characterization in Table 1, we now discuss the cases where the defender is better off in a simultaneous game:

- When the attacker holds a significantly higher valuation of targets: note that there are two regions (III and VII) where this condition is satisfied. In both regions, the attacker attacks Target 1 (the more valuable target) in both sequential and simultaneous games. Note that, in a sequential game, the defender manipulates the attacker's target selection and tries to deter an attack by increasing the defense level on Target 1. However, since the attacker holds a significantly higher valuation of targets ($k_a \geq k_{a_1}$ when $0 \leq \lambda \leq 0.5$, and $k_a \geq k_{a_4}$ when $\lambda > 0.5$), the defender fails to achieve her goal and Target 1 is attacked. On the other hand, the defense budget on Target 1 is smaller in a simultaneous game compared to that in a sequential game (see the decomposition of ΔZ in Fig. 3 where $\Delta Z_2 < 0$), which means that the defender incurs higher expected damage in a simultaneous game (see the decomposition of ΔZ in Fig. 3 where $\Delta Z_1 > 0$). Clearly, because the decrease in expected damage in a sequential game due to spending more on defense is less than the saving due to spending less on defense in a simultaneous game, the defender is better off in a simultaneous game. To summarize, when the attacker holds much higher valuations than the defender, the defender (who has very different a-priori belief about attacker's valuation of targets)

[3] We certify that considering constant k for all targets is for the sake of analytical convenience; however, at the same time, it enables us to answer the main research question of the paper exploring whether the government can be better off by keeping secrecy of defense system rather than exposing it.

[4] We would like to note that this setting is a simplified form of modeling a Bayesian game where the defender uses extremely wrong beliefs about the attacker's private information. Specifically, let us assume that attacker has private information about his valuation of targets u_i. Using the structure of a game under asymmetric information, the defender may have only a-priori beliefs about attacker's valuation of targets. Specifically, we assume that, from defender's perspective, the ratio of the attacker's valuation to defender's valuation of targets is $k_\theta = \frac{u_i}{v_i}$, which can be high k_h, medium k_m, or low k_l, with probabilities p_h, p_m, and p_l, respectively, where $p_h + p_m + p_l = 1$. For the sake of simplicity and to extract analytical results, in the paper we only consider a simple setting of the above model where $p_m = 1$. That is to say, from defender's perspective, the ratio of the attacker's valuation to defender's valuation of targets is always k_m. However, the attacker may hold the other two extremes of this ratio (i.e., $k_a = k_h$ or $k_a = k_l$). Finally, for notational convenience, in our model, we define $k_d = k_m$.

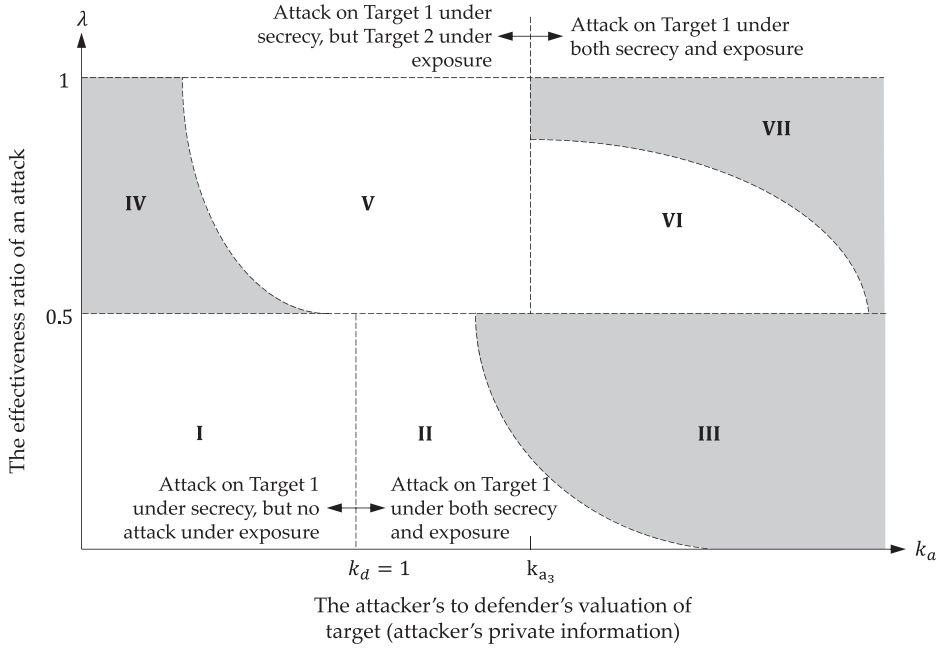

Fig. 2. Defender's equilibrium under asymmetric information.
Note. The defender is better off in a simultaneous game in shaded regions.

Table 1
Comparison of secrecy and exposure under incomplete information.

Condition			Target attacked		Difference in expected damage (ΔZ_1)	Difference in total defense (ΔZ_2)	First-mover advantage (ΔZ)
Region	λ	k_a	Secrecy	Exposure			
I	$\lambda \le 0.5$	$k_a \le 1$	Target 1	No attack	$v_1\left(1-\frac{e^{-\lambda}}{k_a}\right)$	$\lambda(e^{-\lambda}-1)(v_1+v_2)$	Positive
II		$1 < k_a < k_{a_1}$	Target 1	Target 1	$\frac{\left(1-e^{-\lambda}\right)v_1}{k_a}$	$\lambda(e^{-\lambda}-1)(v_1+v_2)$	Positive
III		$k_a \ge k_{a_1}$	Target 1	Target 1	$\frac{\left(1-e^{-\lambda}\right)v_1}{k_a}$	$\lambda(e^{-\lambda}-1)(v_1+v_2)$	Negative
IV	$\lambda > 0.5$	$k_a \le k_{a_2}$	Target 1	Target 2	$v_1\left(1-\frac{e^{-\lambda}}{k_a}\right)-v_2$	$\lambda e^{-\lambda}(v_1+v_2)-\lambda\Delta v$	Negative
V		$k_{a_2} < k_a \le k_{a_3}$	Target 1	Target 2	$v_1\left(1-\frac{e^{-\lambda}}{k_a}\right)-v_2$	$\lambda e^{-\lambda}(v_1+v_2)-\lambda\Delta v$	Positive
VI		$k_{a_3} < k_a \le k_{a_4}$	Target 1	Target 1	$\frac{\Delta v-e^{-\lambda}v_1}{k_a}$	$\lambda e^{-\lambda}(v_1+v_2)-\lambda\Delta v$	Positive
VII		$k_a \ge k_{a_4}$	Target 1	Target 1	$\frac{\Delta v-e^{-\lambda}v_1}{k_a}$	$\lambda e^{-\lambda}(v_1+v_2)-\lambda\Delta v$	Negative

Notes. $\Delta v = v_1 - v_2$; $k_{a_1} = \frac{v_1}{\lambda(v_1+v_2)}$; $k_{a_2} = \frac{v_1}{e^{\lambda}(1-\lambda)\Delta v+\lambda(v_1+v_2)}$; k_{a_3} : the root of $[k_a - \frac{\Delta v}{v_1}\ln k_a - \frac{\Delta v}{v_1}\ln\frac{v_1}{\Delta v} - 1 = 0]$; $k_{a_4} = \frac{\Delta v-e^{-\lambda}v_1}{\lambda(\Delta v-e^{-\lambda}(v_1+v_2))}$.

cannot deter the attack on more valuable target, i.e., Target 1. Under such conditions, the better strategy for the defender could be spending less on defending Target 1 at the ex-ante stage, i.e., before the attack was launched, and therefore, whatever strategy (between secrecy or exposure) that results in less defense level is the better strategy from defender's perspective.

- When the attacker holds a significantly lower valuation of targets: this case is only related to Region IV, where the attacker attacks Target 1 in a simultaneous game, but attacks Taget 2 (the less valuable target) in a sequential game. Note that, in a sequential game, the defender succeeds to deter an attack on Target 1, but she fails to defend the less valuable target (Target 2). Since the attacker holds a significantly lower valuation of targets, the defender could be better off by decreasing the defense on Target 1, but still deter an attack on that. In other words, the defender wastes her budget by over-investing on Target 1 in a simultaneous game. Consequently, the attacker finds the second target undefended and attacks Target 2. On the other hand, in a simultaneous game, the defender invests in each target even more than she does in a sequential game. However, since the attacker attacks Target 1 in a simultaneous game, the extra defense investment is reasonable, which decreases the expected damage on Target 1. Indeed, the expected damage on Target 1 in a simultaneous game is less than that on Target 2 in a sequential game (i.e., $\Delta Z_1 < 0$). To summarize, since the decrease in expected damage is greater than the extra investment in a simultaneous game, the defender is better off in a simultaneous game (see Region IV in Fig. 3).

From the above discussion, being the first-mover may no longer be beneficial when the attacker holds a significantly different valuation of targets. The rationale behind this observation can also be related to the robustness of the budget allocation in a simultaneous game compared to that in a sequential game. Note that, contrary to the defense plan in a simultaneous game, the defender may allocate different levels of budget in a sequential game based on the effectiveness ratio of an attack (see Table 1). Specifically, both targets are defended in a simultaneous game; however, Target 2 may be left undefended in a sequential game when $\lambda > 0.5$. Consequently, the defender may be worse off in a sequential game because of either over-investing on the attacked target, or incurring high expected damage due to not defending the low-valued targets.

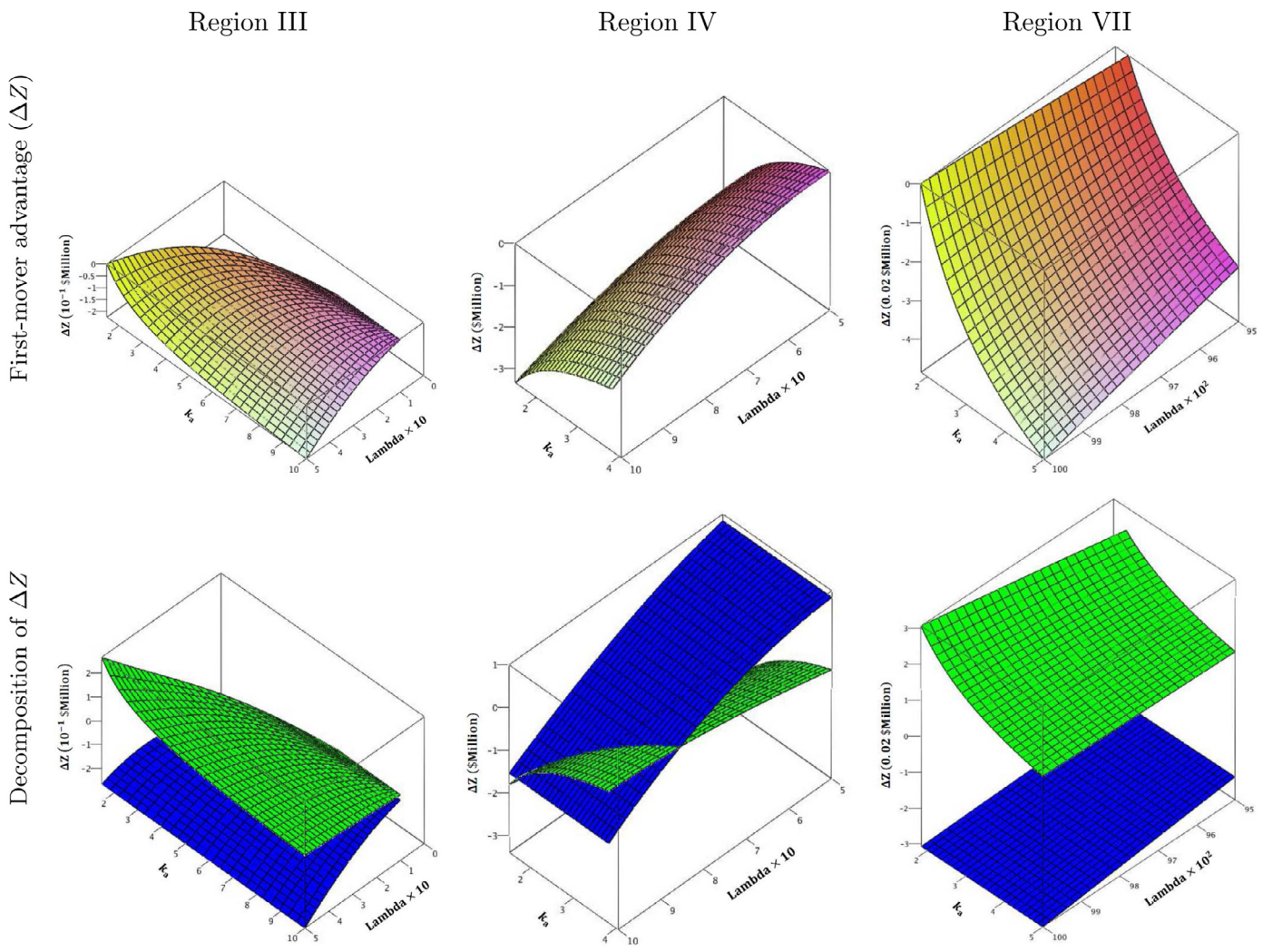

Fig. 3. Decomposition of defender's first-mover advantage under asymmetric information when $\Delta Z < 0$.
Notes. $v_1 = 1$ \$ million, $v_2 = 0.35$ \$ million. The first row shows the first-mover advantage (ΔZ), and the second row explains the decomposition of ΔZ into ΔZ_1 (green/lighter layer) and ΔZ_2 (blue/darker layer). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Below, we extend our results for an N-target case, where $N > 2$. Particularly, in Section 6, we compare the robustness of the budget allocation in a simultaneous game to that in a sequential game, and then in Section 7, we provide an extensive numerical study to support our analytical results presented in Sections 4 and 5.

6. On the robustness of secrecy and exposure

As we discussed in Section 5, when the degree of information asymmetry between defender and attacker is high, the robustness advantage of the defense plan in a simultaneous game dominates the first-mover advantage in a sequential game. In this section, we take a general approach to study the robustness of each policy against the uncertainty in the attacker's valuation of targets. Specifically, we will show that, contrary to the defense plan in a sequential game, the defender uses a comprehensive defense program in a simultaneous game, in which all targets should be defended whether they are high- or low-valued.

Assume that there are N targets, and the attacker's valuation of target i is $\tilde{u}_i$ from the defender's perspective. To capture the defender's uncertainty in the attacker's valuation of targets, we further assume that the defender can define a distribution-free interval for the attacker's target valuation such that $\tilde{u}_i \in [u_i^-, u_i^+]$. We refer to Aghassi and Bertsimas (2006) to find the pros and cons of modeling the uncertainty in distribution-free intervals in game theory[5]. Below, in Proposition 3, we study the impact of uncertainty in defense equilibrium in a simultaneous defender–attacker game.

Proposition 3. *Assume that the defender plays in a simultaneous game (i.e., $y = S$ in optimization problem (1)). Furthermore, let $\tilde{u}_i \in [u_i^-, u_i^+]$. The following statements are then true:*

- *In a simultaneous defender–attacker game, target i is defended in equilibrium for any realization of $\tilde{u}_i$.*
- *The optimal defense budget allocated to target i in equilibrium is increasing in $\tilde{u}_i \in [u_i^-, u_i^+]$ if $v_i \geq \lambda u_i^+$, but decreasing in $\tilde{u}_i \in [u_i^-, u_i^+]$ if $v_i \leq \lambda u_i^-$.*

Remark 3. From Proposition 3, in a simultaneous defender–attacker game, all targets are always defended in equilibrium even if the defender has uncertainty about the attacker's valuation of targets. Recall that, in Section 5, the defender benefits from such a robustness of defense plan under asymmetric information when the attacker holds significantly lower valuation of targets than the defender's

[5] Modeling uncertainty in distribution-free intervals has been widely used in robust optimization (Bertsimas & Sim, 2003; Bertsimas & Thiele, 2006).

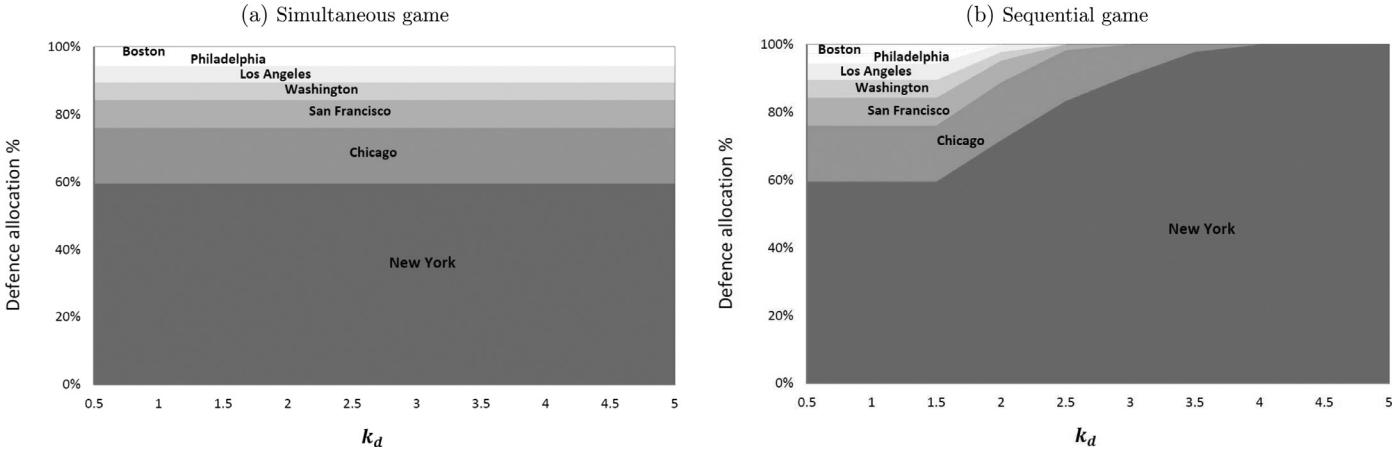

Fig. 4. Optimal defense allocation as a function of k_d for $\lambda = 0.2$.

a-priori belief. This observation indicates a fundamental difference between defender's resource allocation in a simultaneous game and that in a sequential game when the attacker's valuation of targets is unknown by the defender. Specifically, Nikoofal and Zhuang (2012) show that, in a sequential game, the defender is better off by shifting her budget away from low-valued to high-valued targets when the defender's uncertainty in the attacker's valuation of targets increases. Consequently, the attacker switches attack from high-valued to low-valued targets, and, as described in Section 5, it may lead to high damage on undefended targets. Later, in Section 7, we will show that the defender may lose her first-mover advantage in an N-target problem when the attacker's valuation of targets significantly differs from the defender's a-priori belief, which supports our prior results in Section 5.

The second part of the Proposition 3 provides some insights about the robustness of the defense plan in a simultaneous game. Specifically, the defender can find whether the uncertainty in the attacker's valuation of target i may lead to a decrease or increase in the defense budget on target i. This is possible by comparing her valuation of target i with two thresholds that form an interval $[\lambda u_i^-, \lambda u_i^+]$. From Proposition 3, it is not clear whether d_i increases or decreases for any realization of $\tilde{u}_i$ such that $v_i \in [\lambda u_i^-, \lambda u_i^+]$. That being said, when the defender's uncertainty in the attacker's valuation of targets reduces, the defender shortens the interval (by heightening u_i^- and lowering u_i^+); hence it becomes easier to determine whether the uncertainty in the attacker's valuation of target i may result in an increase, when $v_i \geq \lambda u_i^+$, or decrease, when $v_i \leq \lambda u_i^-$, in the defense budget on target i.

7. Numerical study

The characterizations in Proposition 3 give some insights about the robustness of the defense system under secrecy and exposure. In this section, we resort to an illustrative numerical study to support our analytical results presented in Proposition 2. We employ data from Willis, Morral, Kelly, and Medby (2005) which provide estimates of the expected annual terrorism losses to the seven most valuable urban areas of the United States (Table 2). We assume that the expected property loss represents the defender's valuation of the target (Bier et al., 2008; Hao et al., 2009; Hu et al., 2011; Nikoofal & Zhuang, 2012; Shan & Zhuang, 2013a) and that the total defender budget is \$270 million (Willis et al., 2005).

Figs. 4 (a) and 4(b) show the optimal defense allocation as a function of the ratio of the attacker's to defender's valuation of targets in simultaneous and sequential game, respectively. Observe that the

Table 2
Expected property losses for the seven urban areas with the highest losses (\$ million) (Willis et al., 2005).

Urban area	Expected property losses (\$ million)
New York	413
Chicago	115
San Francisco	57
Washington, DC-MD-VA-WV	36
Los Angeles-Long Beach	34
Philadelphia, PA-NJ	21
Boston, MA-NH	18
Total	694

defense equilibrium is quite robust to defender's uncertainty in the attacker's valuation of targets when the defender hides her defense deployment from the attacker's observation, i.e., in a simultaneous game. In particular, the defender uses a more comprehensive defense plan such that she decreases the expected damage of an attack on all targets.

Note that, from Eq. (3), the attacker's effort increases when his valuation of targets increases. Therefore, in a sequential game, the defender would have to harden the defense on New York to make it less desirable for the attacker such that the attacker finds an attack on the second most valuable target, i.e., Chicago, to maximize his payoff. In contrast, while the defense budget is scarce, the defender has to shift the defense from the least valuable targets to harden the most valuable targets. Consequently, the defender uses a more concentrated defense system in which the number of defended targets decreases (see Fig. 4(b) where $k_d \geq 2$ and $\lambda = 0.2$).

Fig. 5 explores the impact of the attacker's private information on the defender's first-mover advantage. In particular, Fig. 5(a) shows the defender's expected loss when the defender knows the magnitude of the attacker's valuation of targets. Specifically, it assumes that both the defender and attacker hold the same valuation of targets, i.e., $k_a = k_d = 1$. As expected, similar to our analytical results in Proposition 1, the defender benefits from the first-mover advantage by exposing her defense deployment when full information is available about attacker's attribute. However, when the attacker's valuation of targets is not observable by the defender and the defender decides based on her prior belief; i.e., $k_d = 1$ (Fig. 5(b)), the defender may or may not be better off in a sequential game. From Fig. 5(b), it is clear that the defender's first-mover advantage is not guaranteed under asymmetric information about attacker's valuation of targets. Specifically, in consistency with our results in Proposition 2, the

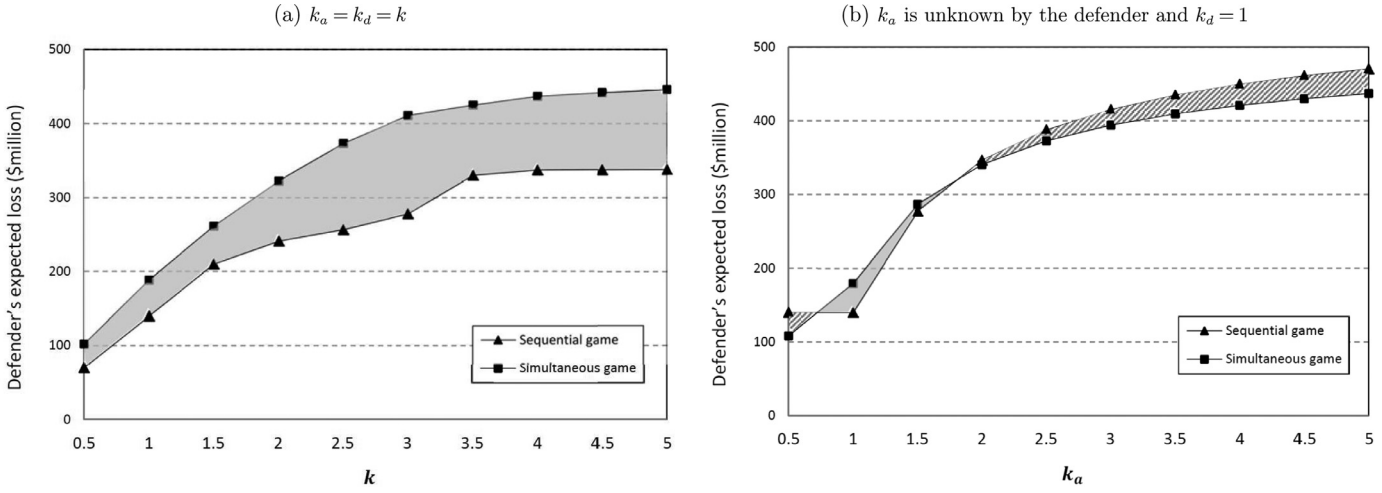

Fig. 5. First-mover advantage under exposure vs. robustness advantage under secrecy.
Notes. The shaded-region indicates the first-mover advantage in sequential game, and the diagonal-region shows the robustness advantage in simultaneous game.

Table 3
Optimal defense allocation ($ million) based on defender's *ex ante* belief $u_i = v_i$.

Urban area	New York	Chicago	San Francisco	Washington	Los Angeles	Philadelphia	Boston	Total
Simultaneous game	67.62	18.83	9.33	5.89	5.56	3.43	2.94	113.6
Sequential game	82.6	23	11.4	7.2	6.8	4.2	3.6	138.8

defender can benefit from the robustness advantage in a simultaneous game when the attacker's valuation of targets is too low ($k_a \leq 0.75$) or too high ($k_a \geq 2$).

Note that Fig. 5(b) shows the defender's *ex-post* expected loss based on her *ex-ante* defense allocation. Table 3 shows the optimal defense allocation based on defender's prior belief when $k_d = 1$ or $u_i = v_i$. It is clear that the defender can benefit from the first-mover advantage when the attacker's valuation of targets matches the defender's prior belief. In contrast, the realized magnitude of the attacker's valuation of targets can be less than (i.e., $k_a < 1$) or more than (i.e., $k_a > 1$) the defender's prior belief. Below, we study each scenario.

- $k_a < 1$: From the attacker's best response function (Eq. 4), an attack on target i is deterred if $d_i \geq \lambda k_a v_i$. When k_a is small, the defender can deter an attack on all targets. Particularly, when $k_a = 0.5$, the adequate budget to deter an attack on all targets is $69.4 million in our example. Indeed, the defender may waste her money by allocating more than this amount, which comes from the defender's uncertainty in the attacker's valuation of targets. From the last column of Table 3, the total budget that the defender allocates to all targets is greater than $69.4 million either in sequential or simultaneous game, which means that the defender may be wasting her money; however, she is better off in a simultaneous game.
- $k_a > 1$: The attacker increases his attack effort when his valuation of target increases (Eq. 4). The defender, therefore, should increase the allocated defense on targets to decrease the expected damage. From Table 3, the defender can be better off in a sequential game since the defensive budget allocated to each target is greater than that in a simultaneous game. However, recall that the defender's expected loss has two terms: (i) the expected damage; and (ii) the total defense costs. When the attacker's valuation of targets is not very high e.g., $1 < k_a < 2$, the defender can still benefit from the first-mover advantage by hardening targets, and consequently, decreasing the total expected damage. In contrast, when the attacker's valuation of targets is too high, e.g., $k_a > 2$, the marginal decrease in expected damage due to hardening the target is less than the increase in defense budget. In other words, the defender can be better off by saving her budget rather than investing on targets to decrease the expected damage. Under this condition, the defender can be better off by decreasing the budget allocated to each target and she should keep secrecy in her defense allocation.

8. Conclusion and future research directions

It is widely discussed in the literature that the government can be better off by exposing her defense deployment against a strategic terrorist. However, observing the high level of security may stir the terrorist to change his attack plan. In this paper, we compare the robustness and effectiveness of the defense equilibrium in a simultaneous game with that in a sequential game under a defender's uncertainty in an attacker's valuation of targets.

Our analysis shows that the government's first-mover advantage is considerable only when both the government and terrorist share a similar valuation of targets. Interestingly, the government can no longer benefit from the first-mover advantage by exposing her defense levels when the degree of asymmetry between the government and terrorist valuation of targets is high. The reason for that comes from the fundamental difference in the defense allocation between secrecy and exposure when the terrorist holds a significantly higher valuation of targets than the government's belief. Specifically, under this condition, the government may waste her budget in a sequential game by over-investing on the high-valued targets. Moreover, when the terrorist holds a significantly lower valuation of targets, the government may incur higher expected damage in a sequential game because of not defending the low-valued targets. We then explore the robustness of the defense equilibrium and show that, contrary to a sequential game, the optimal defense allocation in a simultaneous game is more robust against uncertainty in the attacker's valuation of targets. In particular, under secrecy policy, all targets are always defended in equilibrium even if the defender has uncertainty about the attacker's valuation of targets. It fundamentally differs from the optimal defense system in a sequential game,

in which the defender only defends a subset of most valuable targets when the attacker's valuation of targets increases.

In our model, we consider a one-shot game between the government and terrorist. To the best of our knowledge, the comparison between the efficiency of secrecy and that of exposure has not been studied in a dynamic version of defender–attacker game when terrorist has private information. Thus, one interesting future research direction is to study the efficiency and robustness of defense system in an multiple-period game (Crawford, 2003; Hausken & Zhuang, 2011; Levitin & Hausken, 2009; Zhuang et al., 2010), where the defender could update her belief about the attacker's attributes based on the historical attacker moves.

Acknowledgment

We thank two anonymous referees and the editor of this journal for useful comments. This research was partially supported by the United States Department of Homeland Security (DHS) through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under award number 2010-ST-061-RE0001. This research was also partially supported by the United States National Science Foundation under award numbers 1200899 and 1334930. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the DHS, CREATE, or NSF.

Appendix

Proof of Proposition 1. We first find the optimal budget allocation by solving the inner problem under both secrecy and exposure. We then compare the defender's payoff to find the optimal solution for the outer problem, as well as defender's first-mover advantage. Under secrecy (i.e., $y = S$), the game is played simultaneously; thus, we obtain the best response function of each player by satisfying the first order condition of its own strategy. To extract the defender's optimal strategy, we plug the attacker's best response into the defender's best response. Let us satisfy the optimality condition for the defender's problem by $\frac{\partial[\sum_{i=1}^{2}(v_i p(d_i,a_i)+d_i)]}{\partial d_i}=0$, which gives:

$$\exp\left(\frac{-\lambda a_i}{d_i}\right)=\frac{d_i^2}{\lambda a_i v_i} \tag{5}$$

Plugging the attacker's best response a_i^{br}, expression (3) into (5) gives the optimal defensive budget on target i as $d_i^* = \lambda v_i \exp(-\lambda)$. Therefore, the defender's payoff under secrecy is $Z_S = v_1(1-\exp(-\lambda)) + \lambda(v_1+v_2)\exp(-\lambda)$. Now, under exposure, since the attacker can observe the defender's allocation, he chooses the target that gives him the greater payoff. Since the game is played sequentially, we need to first plug the attacker's best response a_i^{br}, expression (3), into defender's objective function that gives $p(d_i,a_i)=1-\frac{d_i}{\lambda v_i}$. In other words, since the defender tries to minimize the expected damage and attacker wishes to maximize it, we can rewrite the defender's optimization problem as follows:

$$\min_{d_1,d_2}\psi+\sum_{i=1}^{2}d_i \tag{6}$$

$$v_i\left(1-\frac{d_i}{\lambda v_i}\right)\le\psi,\ i=1,2 \tag{7}$$

$$d_1,d_2\ge 0 \tag{8}$$

where ψ shows the expected damage. Note that the above optimization problem is a linear programming problem with respect to d_1 and d_2. Therefore, to characterize the defender equilibrium strategy, we can apply the optimality principle of linear programming, which effectively states that when the feasible set is nonempty and bounded, and then at least one optimal solution is located at an extreme point (Dantzig, 1951). Note that constraint (7) is binding for some of the targets, namely, $i \in I$, so, we have $d_i = \lambda(v_i-\psi), i \in I$, and $d_i = 0, i \notin I$. Replacing these values in Model (6–8) gives a tractable model to characterize the defender's equilibrium strategy. Specifically, one can rewrite the defender's problem as follows:

$$\min_{d_1,d_2}\psi+\textstyle\sum_{i\in I}\lambda(v_i-\psi) \tag{9}$$

$$v_i\le\psi,\ i\notin I \tag{10}$$

$$d_1,d_2\ge 0 \tag{11}$$

Note that the attacker will choose the most valuable target (i.e., target 1), which is also the target that will be protected first by the defender. However, the more the defender allocates budget to protect this target, the less the attacker's payoff will be for it, until the attacker becomes better off by switching to the second most valuable target (i.e., target 2). So, let us start with $I = 1$. The defender payoff function is $\min_{\psi}\lambda v_1+(1-\lambda)\psi$ subject to $v_2 \le \psi$. Clearly, since $\lambda \le 1$, the defender is better off by choosing the least possible value for ψ which is v_2. Thus, if the defender only defends target 1, then $d_1 = \lambda(v_1-v_2)$, $d_2 = 0$, and $Z_E = v_2+\lambda(v_1-v_2)$. Now, if $I = 2$ (i.e., both target are defended), the defender payoff function is $\min_{\psi}\lambda(v_1+v_2)+(1-2\lambda)\psi$. Thus, if $\lambda \le 0.5$, then $\psi = 0$, and otherwise (i.e., $\lambda > 0.5$) $\psi = v_2$. In summary, the optimal solution under exposure policy depends on λ. Specifically, if $\lambda \le 0.5$, $d_i = \lambda v_i$ and $Z_E = \lambda(v_1+v_2)$, and if $\lambda > 0.5$, $d_1 = \lambda(v_1-v_2)$, $d_2 = 0$, and $Z_E = v_2+\lambda(v_1-v_2)$.

We can now compare the defender's payoff under secrecy and exposure to solve for the outer level of defender's problem, y. Clearly, if $\lambda \le 0.5$, $\Delta Z = (1-e^{-\lambda})v_1+(e^{-\lambda}-1)[\lambda(v_1+v_2)]$, which is always positive. Finally, if $\lambda > 0.5$, $\Delta Z = [(1-e^{-\lambda})v_1-v_2]+\lambda[(v_1+v_2)e^{-\lambda}-(v_1-v_2)]$, which is again positive. □

Proof of Proposition 2. Note that, by considering $k_d = 1$, we can conclude that the defender uses the same allocation as that under equal valuation scenarios for both sequential and simultaneous games. However, depending on k_a, the attacker may choose different targets to attack. Therefore, we analyze the attacker's decision and find the defender's payoff under secrecy and exposure below. Under secrecy the likelihood function of damage is $p_S(d_i^S,a_i^S)=1-\frac{1}{k_a\exp(\lambda)}$. Since $v_1 \ge v_2$, it is easy to verify that the attacker always attacks the more valuable target (i.e., target 1). Thus, the defender's *ex-post* loss in a simultaneous game is $Z_S = v_1(1-\frac{\exp(-\lambda)}{k_a})+\lambda(v_1+v_2)\exp(-\lambda)$. The defender loss in a sequential game further depends on the effectiveness ratio of an attack, λ, and the attacker's choice of attack. Specifically, when $\lambda \le 0.5$, the attacker is deterred when $k \le 1$ (so $Z_E = \lambda(v_1+v_2)$), and he attacks the more valuable target when $k > 1$ (so $Z_E = v_1(1-\frac{1}{k_a})+\lambda(v_1+v_2)$). When $\lambda > 0.5$, the attacker can benefit $k_a v_2$ if he attacks target 2, but his payoff if he attacks target 1 further depends on k_a. Specifically, if $k_a \le \frac{\Delta v}{v_1}$, where $\Delta v = v_1 - v_2$, the attacker is deterred from attacking target 1 and is better off by targeting the less valuable target. Otherwise, when $k_a > \frac{\Delta v}{v_1}$, the likelihood function of damage is $p_S(d_i^S,a_i^S)=1-\frac{\Delta v}{k_a v_1}$, and the attacker will attack on target 2 if $\frac{\Delta v}{v_1} < k_a \le \bar{k}_a$ and target 1 if $k_a > \bar{k}_a$, where $\bar{k}_a$ is the root of $k_a-\frac{\Delta v}{v_1}\ln k_a-\frac{\Delta v}{v_1}\ln\frac{v_1}{\Delta v}-1=0$. To sum, when $\lambda > 0.5$, the attacker attacks target 2 if $k_a \le \bar{k}_a$ (so $Z_E = v_2+\lambda\Delta v$), and he attacks target 1 if $k_a > \bar{k}_a$ (so $Z_E = v_1(1-\frac{\Delta v}{k_a v_1})+\lambda\Delta v$). Now, by comparing defender's loss under secrecy and exposure in different settings, it is straightforward to characterize the results in Table 1. □

Proof of Proposition 3. In a simultaneous game, we need to obtain the best response function of each player by satisfying the first order condition of its own strategy. To extract the defender's optimal

strategy, we plug the attacker's best response into the defender's best response. Let us first satisfy the optimality condition for the defender's problem that gives:

$$\exp\left(\frac{-\lambda a_i}{d_i}\right) = \frac{d_i^2}{\lambda a_i v_i} \tag{12}$$

Plugging the attacker's best response $a_i^{br} = \frac{d_i}{\lambda}\ln(\frac{\lambda\tilde{u}_i}{d_i})$ into Eq. (12) gives the optimal defensive budget on target i as $d_i^* = \lambda\tilde{u}_i \exp(\frac{-\lambda\tilde{u}_i}{v_i})$, which is always positive. To prove the second part, we first learn how d_i may change with respect to unknown parameter $\tilde{u}_i$. Verify that $\frac{\partial d_i}{\partial \tilde{u}_i} \geq 0$ when $v_i \geq \lambda\tilde{u}_i$ and $\frac{\partial d_i}{\partial \tilde{u}_i} < 0$, otherwise. Therefore, $\frac{\partial d_i}{\partial \tilde{u}_i} \geq 0$ for $\forall \tilde{u}_i \in [u_i^-, u_i^+]$ if $v_i \geq \lambda u_i^+$, and intuitively, $\frac{\partial d_i}{\partial \tilde{u}_i} < 0$ for $\forall \tilde{u}_i \in [u_i^-, u_i^+]$ if $v_i \leq \lambda u_i^-$. □

References

Adamo, T., & Matros, A. (2009). A Blotto game with incomplete information. *Economics Letters, 105*(1), 100–102.

Aghassi, M., & Bertsimas, D. (2006). Robust game theory. *Mathematical Programming, 107*(1), 231–273.

Arce, D. G., & Sandler, T. (2007). Terrorist signalling and the value of intelligence. *British Journal of Political Science, 37*(04), 573–586.

Berman, O., Gavious, A., & Huang, R. (2011). Location of response facilities: a simultaneous game between state and terrorist. *International Journal of Operational Research, 10*(1), 102–120.

Bertsimas, D., & Sim, M. (2003). Robust discrete optimization and network flows. *Mathematical Programming, 98*(1), 49–71.

Bertsimas, D., & Thiele, A. (2006). A robust optimization approach to inventory theory. *Operations Research, 54*(1), 150–168.

Bier, V. M., Haphuriwat, N., Menoyo, J., Zimmerman, R., & Culpen, A. M. (2008). Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis, 28*(3), 763–770.

Bier, V. M., Oliveros, S., & Samuelson, L. (2007). Choosing what to protect: Strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory, 9*(4), 563–587.

Brown, G., Carlyle, M., Diehl, D., Kline, J., & Wood, K. (2005). A two-sided optimization for theater ballistic missile defense. *Operations Research, 53*(5), 745–763.

Brown, G., Carlyle, M., Salmeron, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces, 36*(6), 530–544.

Brown, G., & Cox, L. A. T. (2011). How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis, 31*(2), 196–204.

Cox, L. A. T. (2009). Game theory and risk analysis. *Risk Analysis, 29*(8), 1062–1068.

Crawford, V. P. (2003). Lying for strategic advantage: Rational and boundedly rational misrepresentation of intentions. *The American Economic Review, 93*(1), 133–149.

Dantzig, G. (1951). Application of the simplex method to a transportation problem. *Activity Analysis of Production and Allocation, 13*, 359–373.

Dighe, N. S., Zhuang, J., & Bier, V. M. (2009). Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker detterrence. *International Journal of Performability Engineering, 5*(1), 31–43.

Fudenberg, D., & Tirole, J. (1991). *Game theory*. MIT Press, Cambridge, Massachusetts.

Golalikhani, M., & Zhuang, J. (2011). Modeling arbitrary layers of continuous-level defenses in facing with strategic attackers. *Risk Analysis, 31*(4), 533–547.

Golany, B., Kaplan, E. H., Marmur, A., & Rothblum, U. G. (2009). Nature plays with dice - terrorists do not: allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research, 192*(1), 198–208.

Hall, J. R. (2009). The elephant in the room is called game theory. *Risk Analysis, 29*(8) 1061.

Hao, M., Jin, S., & Zhuang, J. (2009). Robustness of optimal defensive resource allocations in the face of less fully rational attacker. *Proceedings of the 2009 Industrial Engineering Research Conference* (pp. 886–891).

Harsanyi, J. C. (1967). Games with incomplete information played by "bayesian" players, i-iii part i. the basic model. *Management science, 14*(3), 159–182.

Harvey, E. L., & Sandler, T. (1993). Terrorism and signalling. *European Journal of Political Economy, 9*(3), 383–397.

Hausken, K. (2002). Probabilistic risk analysis and game theory. *Risk Analysis, 22*(1), 17–27.

Hausken, K., Bier, V. M., & Zhuang, J. (2008). Defending against terrorism, natural disaster, and all hazards. In V. M. Bier, & N. Azaiez (Eds.), *Combining reliability and game Theory* (pp. 65–97). New York: Springer.

Hausken, K., & Zhuang, J. (2011). Governments' and terrorists' defense and attack in a t-period game. *Decision Analysis, 8*(1), 46–70.

Hu, J., Homem-de Mello, T., & Mehrotra, S. (2011). Risk-adjusted budget allocation models with application in homeland security. *IIE Transactions, 43*(12), 819–839.

Insua, I. R., Rios, J., & Banks, D. (2009). Adversarial risk analysis. *Journal of the American Statistical Association, 104*(486), 841–854.

Jeneliusa, E., Westina, J., & Holmgrenb, A. J. (2010). Critical infrastructure protection under imperfect attacker perception. *International Journal of Critical Infrastructure Protection, 3*(1), 16–26.

Jose, V. R. R., & Zhuang, J. (2013). Technology adoption, accumulation, and competition in multi-period attacker-defender games. *Military Operations Research, 18*(2), 33–47.

Kaplan, E. H., Kress, M., & Szechtman, R. (2010). Confronting entrenched insurgents. *Operations Research, 58*(2), 329–341.

Kardes, E. (2008). *Discounted robust stochastic games with applications to homeland security and flow control* (Ph.D. thesis). University of Southern California.

Kovenock, D., & Roberson, B. (2011). A Blotto game with multi-dimensional incomplete information. *Economics Letters, 113*(3), 273–275.

Levitin, G., & Hausken, K. (2009). Redundancy vs. protection in defending parallel systems against unintentional and intentional impacts. *IEEE Transactions on Reliability, 58*(4), 679–690.

McLay, L. A., Jacobson, S. H., & Nikolaev, A. G. (2009). A sequential stochastic passenger screening problem for aviation security. *IIE Transactions, 41*(6), 575–591.

Nikoofal, M. E., & Gumus, M. (2015). On the value of terrorist's private information in a government's defensive resource allocation problem. *IIE Transactions, 47*, 1–23.

Nikoofal, M. E., & Zhuang, J. (2012). Robust allocation of a defensive budget considering an attacker's private information. *Risk Analysis, 32*(5), 930–943.

Overgaard, P. B. (1994). The scale of terrorist attacks as a signal of resources. *Journal of Conflict Resolution, 38*(3), 452–478.

Powell, R. (2007a). Allocating defensive resources with private information about vulnerability. *American Political Science Review, 101*(4), 799–809.

Powell, R. (2007b). Defending against terrorist attacks with limited resources. *The American Political Science Review, 101*(3), 527–541.

Rios, J., & Insua, D. R. (2009). Adversarial risk analysis: Applications to basic counterterrorism models. *Algorithmic Decision Theory, Rossi, F. and Tsoukias, A. (eds), Springer Berlin / Heidelberg*, 306–315.

Roberson, B. (2006). The Colonel Blotto game. *Economic Theory, 29*(1), 1–24.

Sandler, T., & Siqueira, K. (2009). Games and terrorism. *Simulation & Gaming, 40*(2), 164–192.

Shan, X., & Zhuang, J. (2013a). Cost of equity in homeland security resource allocation in the face of a strategic attacker. *Risk Analysis, 33*(6), 1083–1099.

Shan, X., & Zhuang, J. (2013b). Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender-attacker game. *European Journal of Operational Research, 228*(1), 262–272.

Shapiro, J. N., & Siegel, D. A. (2010). Is this paper dangerous? Balancing secrecy and openness in counterterrorism. *Security Studies, 19*(1), 66–98.

Shubik, M., & Weber, R. J. (1981). Systems defense games: Colonel Blotto, command and control. *Naval Research Logistics Quarterly, 28*(2), 281–287.

Wang, C., & Bier, V. M. (2011). Target-hardening decisions based on uncertain multiattribute terrorist utility. *Decision Analysis, 8*(4), 286–302.

Willis, H. H., Morral, A. R., Kelly, T. K., & Medby, J. J. (2005). *Estimating Terrorism Risk*. RAND Corporation http://www.rand.org/pubs/monographs/MG388.html.

Wright, P. D., Liberatore, M. J., & Nydick, R. L. (2006). A survey of operations research models and applications in homeland security. *Interfaces, 36*(6), 514–529.

Zhang, C., & Ramirez-Marquez, J. E. (2012). Protecting critical infrastructures against intentional attacks- a two-stage game with incomplete information. *IIE Transactions, 45*(3), 244–258.

Zhuang, J., & Bier, V. M. (2007). Balancing terrorism and natural disasters: Defensive strategy with endogenous attacker effort. *Operations Research, 55*(5), 976–991.

Zhuang, J., & Bier, V. M. (2010). Reasons for secrecy and deception in homeland-security resource allocation. *Risk Analysis, 30*(12), 1737–1743.

Zhuang, J., & Bier, V. M. (2011). Secrecy and deception at equilibrium, with applications to anti-terrorism resource allocation. *Defence and Peace Economics, 22*(1), 43–61.

Zhuang, J., Bier, V. M., & Alagoz, O. (2010). Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research, 203*(2), 409–418.