Submitted to *Decision Analysis*
manuscript (Please, provide the mansucript number!)

Two-stage invest-defend game: balancing strategic and operational decisions*

Abdolmajid Yolmeh
Industrial and Systems Engineering Department, Rutgers University, 96 Frelinghuysen Rd, Piscataway, NJ 08854, abdolmajid.yolmeh@rutgers.edu,

Melike Baykal-Gürsoy
Industrial and Systems Engineering Department, CAIT, RUTCOR, Rutgers University, 96 Frelinghuysen Rd, Piscataway, NJ 08854, gursoy@rci.rutgers.edu,

Protecting infrastructures against terrorist attacks involves making both strategic and operational decisions in an organization's hierarchy. Although usually analyzed separately, these decisions influence each other. To study the combined effect of strategic and operational decisions, we present a game-theoretic, two-stage model between a defender and an attacker involving multiple target sites. In the first stage, the defender (attacker) makes a strategic decision of allocating investment resources to target sites in order to improve the defense (attack) capabilities. We consider two cases for investments in the first stage: 1) unconstrained, 2) budget constrained models. The investment allocations for each target site determine its detection probability. In the second stage, the players make operational decisions of which target site to defend or to attack. We distinguish between two types of games that arise in the second stage: Maximal Damage game and Infiltration/Harassment game. We prove that the solution to this game under budget constraints is unique. In fact, when the second stage game is of Infiltration/Harassment type, the invest-defend game has a unique closed-form solution that is very intuitive. The results reveal that an increase in defense investments on a target site decreases the probability of both defending and attacking that target. However, an increase in attack investments increases the probability of both defending and attacking that target. Similarly, an increase in the defender's (attacker's) investment efficiency leads to a decrease (increase) in investments of both the defender and the attacker. Finally, the model is applied to real data to obtain the equilibrium investment and defense strategies. The results from real data demonstrate that the attacker's penalty from a failed attack is an important factor in determining the defender's optimal distribution of investments and defense probabilities. The defender's second stage defense decisions complement the first stage investment decisions. That is, among target sites that receive little or zero investment, the most important one is covered with a relatively high defense probability in the second stage. Moreover, as the attacker's budget increases, the defense investments shift from less important sites to the more important ones.

Key words: terrorism and counter terrorism, infrastructure security games, budget constraint, two-stage game, strategic decision making, sequential game, simultaneous game

1. Introduction

Terrorist attacks are a growing global concern. Every year, thousands of people lose their lives, get injured or kidnapped as a result of such attacks. In 2015, a total of 11,774 terrorist attacks occurred worldwide, resulting in more than 28,300 deaths and more than 35,300 injuries (Bureau of Counterterrorism 2016). Other than physical injuries, the psychological impact of the continued threat of terrorism is also considerable. Such incidents create fear, panic, anxiety and distress in the society. In response, counter-terrorism has received considerable attention from international institutions and national governments. Disastrous events such as the attacks in Madrid, London, Bali, Mumbai and others have placed counter-terrorism high on the political agenda. As a result, many governments reacted by raising their budgets for anti-terrorism spending. However, deterring terrorism is generally expensive and deciding how to allocate resources in order to protect critical infrastructures is a difficult problem. Many factors affect resource allocation, such as target attractiveness, creating a balance between protecting against different types of threats (e.g., biological attacks versus bomb attacks), or equal distribution of federal resources among targets for fairness considerations (Shan and Zhuang 2013a).

Different approaches have been proposed to model strategic interactions in security problems, these methods include system analysis (Paté-Cornell and Guikema 2002), mathematical modeling (Harris 2004) and probabilistic risk analysis methods (Kaplan and Garrick 1981, Paté-Cornell 2002, Paté-Cornell and Guikema 2002, Garrick et al. 2004, Garcia 2005, McGill et al. 2007). However, since the terrorists can also be strategic in their attacks, game theoretic analysis of such attacks yields more realistic results. Therefore, recent studies concentrate on developing game theoretic models to capture terrorism risk and using the solutions of these models in enhancing security measures. Hausken (2002) incorporates a game theoretic dimension into probabilistic risk analysis. Other investigators study such game theoretic models under different system structures (Hausken 2009, 2010), defense measures (Levitin and Hausken 2009, Peng et al. 2010) and attack tactics (Garnaev et al. 2014, Hausken and Levitin 2009, Hausken and Bier 2011). For a review of defense and attack models, see Hausken and Levitin (2012).

Protecting infrastructures against terrorist attacks involves decision making at different levels in an organization's hierarchy: strategic and operational decisions. The strategic decisions are long term decisions with long lasting effects. For example, investment decisions on "hardening" (Bier

* This material is based upon work supported by the National Science Foundation under Grant No.1436288

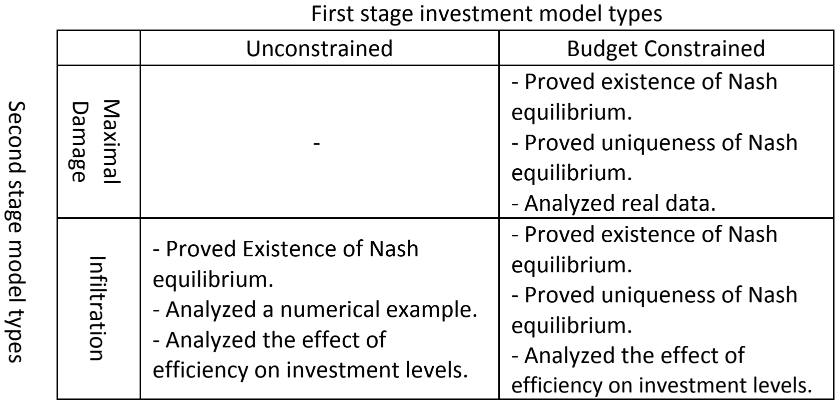
and Abhichandani 2002) the target sites to decrease the success probability of attack is classified as a strategic decision. These decisions include investment on new technologies to enhance security of a site. On the other hand, the operational decisions are short term decisions that relate to the routine day-to-day operations such as patrolling, assigning first responders, and scheduling vehicle checkpoints. Note that the word "strategic" can also be used to describe players. In this context, we will refer to a rational player whose objective is to maximize her/his payoff as a "strategic player".

Most research only focus on either purely strategic decisions (Hausken and Zhuang 2011, Nikoofal and Zhuang 2012) or purely operational decisions (Baykal-Gürsoy et al. 2014, Garnaev et al. 2014, 2015, 2016). Strategic decisions are considered by Nikoofal and Zhuang (2012) who present a game in which a defender makes a strategic decision of allocating resources to harden a set of target sites in order to minimize the maximum damage of an attack. Hausken and Zhuang (2011) analyze a two-stage resource allocation game between a government and a terrorist. In this Stackelberg game, the government moves first and allocates its resources between attacking to downgrade the terrorist's resources and defending against the terrorist attack. Then, the terrorist allocates his resources between attacking and defending options. Other papers study strategic decision of resource assignment to protect targets against attacks (Zhuang and Bier 2007, Shan and Zhuang 2013b, Guan et al. 2017). In the context of making strategic decisions in security, several papers investigate multi-period models in which similar strategic decisions are made throughout multiple periods (Zhuang et al. 2010, Hausken and Zhuang 2011, Jose and Zhuang 2013, Shan and Zhuang 2017). Hence, the primary focus is on the effect of timing of these decisions. Baykal-Gürsoy et al. (2014) consider an infrastructure containing multiple target sites with a single defender and a single attacker. The defender and the attacker make operational decisions of which site to defend and attack, respectively. Each target site has a given "detection probability" of detecting and thwarting an attack, if both players choose the same site. Garnaev et al. (2014) study operational decision of which sites to defend/attack with consideration given to the uncertainty of the attack type. Shan and Zhuang (2014a) analyze the defender's operational decisions such as container screening rate to deter nuclear smuggling. They demonstrate how inspection rates should be modified in the presence of non-credible retaliation threats. There are other articles in the literature that focus on purely operational decisions such as allocating defenders (Garnaev et al. 2016), patrolling (Pita et al. 2008, Shieh et al. 2012, Yolmeh and Baykal-Gürsoy 2018) and scheduling (Tsai et al. 2009).

Even though most researchers study purely strategic or purely operational decision models, these decisions influence each other. For instance, installing a CCTV camera in a certain area might render patrolling that area unnecessary. Or allocations of metal detectors and screening systems to target sites may affect optimal scheduling of patrol units among those targets. Moreover, investing in a new technology to enhance security of a certain target site may reduce its target attractiveness and affect the optimal probability of defending that target. Therefore, considering strategic and operational decisions in the same model would yield a more holistic analysis.

In this paper, we consider both strategic investment decisions and operational defense/attack decisions simultaneously in a comprehensive model and investigate the interaction between these decisions. Specifically, we introduce a two-stage invest-defend game in which, at the first stage, the defender and the attacker make strategic decisions of investing on a set of target sites. This is followed by the second stage game in which the players make operational decisions of which target site to defend or attack. We consider two types of models for investments in the first stage: unconstrained model and budget constrained model. In the unconstrained model, investments are not limited by a fixed budget, however, there is a disutility associated with each investment. We assume that both players are able to make investments to affect the detection probability of specific targets. Although the defender's investments to harden targets have been studied extensively in literature (as reviewed earlier in this section), the attacker's investments to weaken targets have received little attention. However, in reality, attackers also make investments on targets to increase their vulnerability. For example, terrorists tend to follow a planning cycle for their attacks in which they perform extensive surveillance operations to obtain target specific information (United States Army 2010). Some of these operations may take several months to complete and need long term investments to be successful (Smith et al. 2017). Moreover, they may invest in special training programs to attack specific targets. For example, 9/11 terrorists received training in piloting air crafts so that they could use them as weapons to destroy targets that otherwise would have been harder to destroy. At the second stage, the defender and the attacker make operational decisions of which target to defend and attack, respectively. We consider two types of games at the second stage: Maximal Damage game and Infiltration/Harassment game. Maximal Damage game happens when each target has a different value. Infiltration/Harassment game happens when all targets have the same value. Therefore, in the Infiltration/Harassment game, the players cannot differentiate targets except according to their vulnerability to attacks. These game types have been studied in Garnaev et al. (2015, 2014, 2016) and Yolmeh and Baykal-Gürsoy (2017). Different types of players have also been studied in Shan and Zhuang (2014b) and Garnaev et al. (2016). Figure 1 summarizes our results for different first stage investment models and second stage target value models.

Hausken and Levitin (2012) review defense and attack models and propose a three dimensional classification scheme based on the system structure, defense measures and attack tactics. We use this classification method to locate our proposed model along these three dimensions. In our proposed model, there are multiple targets that are not linked in any particular way. Therefore, we



		First stage investment model types	
		Unconstrained	Budget Constrained
Second stage model types	Maximal Damage	-	- Proved existence of Nash equilibrium. - Proved uniqueness of Nash equilibrium. - Analyzed real data.
	Infiltration	- Proved Existence of Nash equilibrium. - Analyzed a numerical example. - Analyzed the effect of efficiency on investment levels.	- Proved existence of Nash equilibrium. - Proved uniqueness of Nash equilibrium. - Analyzed the effect of efficiency on investment levels.

Figure 1 Summary of paper's contributions

can categorize the system as “multiple elements” (option 6). Moreover, in our proposed model, the defender first invests on targets to harden them, then assigns a single first responder to protect them. This can be categorized as multi-level defense (option 5). Similarly, the attacker first invests on targets to make them vulnerable to attack, then chooses a target to attack. This can be categorized as sequential (consecutive) attacks (option 3). To the best of our knowledge, a system with multiple elements, multi-level defense strategy and sequential attacks has not been studied in the literature of defense and attack models. The contribution of this paper is to capture strategic and operational decisions in a comprehensive two-stage game model and study the interaction between these decisions. One of the challenges of combining these decisions is proving the existence and uniqueness of the Nash equilibrium for the overall game model. This requires solving for the Nash equilibrium using backward induction method. Since we are looking for analytic results, finding the Nash equilibrium for the two-stage game involves first developing a closed form solution for the second stage problem to be then used in the first stage game. We present analytical results about the existence and uniqueness of the equilibrium for our proposed game. We then apply our approach to real data. The results of the proposed model can be implemented to determine the optimal defensive resource allocation strategy among target sites.

The remainder of the paper is organized as follows. In section 2, the problem under consideration is described and notations are introduced. In section 3, the two-stage invest-defend game is solved using the backward induction method. In section 4, the proposed approach is applied to the real data from 10 most important urban areas in the US. Main conclusions of the paper and future research suggestions are presented in section 5.

2. Problem Description and Notations

We consider a two-stage invest-defend game between a single defender and a single attacker. We assume that both players are fully rational and they aim to maximize their own payoffs. In the first stage, both the defender (she) and the attacker (he) simultaneously make strategic decisions of investing on targets to change the detection probabilities in their own favor and then in the second stage, they make simultaneous operational decisions of selecting which target to defend and attack, respectively.

Each target has a value of C_i, for $i = 1, 2, \ldots, N$, with N denoting the number of targets. This value could be determined by occupancy levels or any other valuation criterion, e.g., monetary or political value. We assume that the attacker's target valuations are the same as the defender's valuations as in Powell (2007), Golany et al. (2009), Shan and Zhuang (2013a) and Shan and Zhuang (2013b). While we acknowledge that the attacker may value targets differently, using the same target valuations for the attacker results in a game in which the players' payoffs are in opposite direction and this is useful as a worst case analysis. Wang and Bier (2011) use multi-attribute utility functions to model the attacker's preferences.

The second stage game is a matrix game in which players make operational decisions of choosing which target to defend or attack. If the defender defends target i and the attacker attacks $j, j \neq i$, a successful attack on target j will be launched. Therefore, payoff to the defender will be $-C_j$ and the attacker receives a payoff of C_j. However, if both players choose the same target i, the attacker will be detected (and thwarted) with probability d_i. We assume that the attacker suffers a penalty of P in case of a failed attack. Therefore, the defender's payoff is $-(1-d_j)C_j$ and the attacker's payoff is $(1-d_j)C_j - d_jP$. This means that even when both rivals are at the same site, there is a probability that the defender may not be able to detect the attacker. Other studies have modeled detection in different contexts such as deterring smuggling of nuclear weapons carried in containers (Haphuriwat et al. 2011), detecting concealed targets (Levitin 2009), identifying the genuine target among false targets (Levitin and Hausken 2010) and detecting outcome of attacks (Levitin and Hausken 2012b,c).

The objective of each player at the first stage is to maximize his/her own total payoff, which is equal to the sum of payoffs from the first and second stages. If $C_i = C,\ \forall i = 1, \ldots, N$, then the second stage game is called the Infiltration/Harassment game, otherwise it is called the Maximal Damage game.

The parameters of our model are listed as follows:

- N : number of target sites.
- C_i : value of site i. We can, without loss of generality, assume that C_is are sorted in a decreasing order, i.e., $C_1 > C_2 > \ldots > C_N$, in the Maximal Damage game and $C_i = C$, for all $i = 1, 2, \ldots, N$, in the Infiltration/Harassment game.
- P : penalty of an unsuccessful attack for the attacker.
- A : total budget for defensive investments in the budget constrained model.

- B : total budget for attack investments in the budget constrained model.

Decision variables and functions that use these variables are listed as follows:

- α_i (strategic decision of the defender): amount of investment expended on defending site i in the first stage, where $0 \leq \alpha_i < \infty$ for all $i = 1, ..., N$. Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_N)$ represent the defensive investment vector.

- β_i (strategic decision of the attacker): amount of investment expended on attacking site i in the first stage, where $0 \leq \beta_i < \infty$ for all $i = 1, ..., N$. Let $\boldsymbol{\beta} = (\beta_1, \beta_2, ..., \beta_N)$ represent the attack investment vector.

- $d_i(\alpha_i, \beta_i)$: probability of detection at site i in the second stage. Assume that $d_i(\alpha_i, \beta_i)$ is a continuous, strictly increasing and concave function of defensive investments in the first stage, i.e., α_i. Also assume that $d_i(\alpha_i, \beta_i)$ is a continuous, strictly decreasing and convex function of attack investments in the first stage, i.e., β_i.

- $\boldsymbol{x} = (x_1, x_2, \ldots, x_N)$(operational decision vector of the defender): mixed policy of the defender with x_i denoting the probability of defending site i in the second stage, with $0 \leq x_i \leq 1$, for all $i = 1, \ldots, N$, and $\sum_{i=1}^{N} x_i = 1$.

- $\boldsymbol{y} = (y_1, y_2, \ldots, y_N)$(operational decision vector of the attacker): mixed policy of the attacker with y_i denoting the probability of attacking site i in the second stage, with $0 \leq y_i \leq 1$, for all $i = 1, \ldots, N$, and $\sum_{i=1}^{N} y_i = 1$.

- $u_1^d(\boldsymbol{\alpha})$: first stage payoff to the defender in the unconstrained model, which is defined as $u_1^d(\boldsymbol{\alpha}) \equiv -\sum_{i=1}^{N} \alpha_i$.

- $u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$: second stage payoff to the defender, which is given by $u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y}) \equiv -\sum_{i=1}^{N} (C_i(1 - d_i(\alpha_i, \beta_i)x_i)y_i)$ (Baykal-Gürsoy et al. 2014).

- $u_t^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$: total payoff to the defender. In the unconstrained model, the defender's total payoff is given by $u_t^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y}) \equiv u_1^d(\boldsymbol{\alpha}) + u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$. In the budget constrained model, the defender's total payoff is given by $u_t^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y}) \equiv u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$ with the budget constraint $\sum_{i=1}^{N} \alpha_i \leq A$.

- $u_1^a(\boldsymbol{\beta})$: first stage payoff to the attacker in the unconstrained model, which is defined as $u_1^a(\boldsymbol{\beta}) \equiv -\sum_{i=1}^{N} \beta_i$.

- $u_2^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$: second stage payoff to the attacker, which is $u_2^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y}) \equiv \sum_{i=1}^{N} (C_i(1 - d_i(\alpha_i, \beta_i)x_i) - d_i(\alpha_i, \beta_i)x_i P)\, y_i$.

- $u_t^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$: total payoff to the attacker. In the unconstrained model, the attacker's total payoff is given by $u_t^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y}) \equiv u_1^a(\boldsymbol{\beta}) + u_2^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$. In the budget constrained model, the attacker's total payoff is given by $u_t^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y}) \equiv u_2^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y})$ with the budget constraint $\sum_{i=1}^{N} \beta_i \leq B$.

We assume that players make their decisions simultaneously at both stages, in other words, at each stage, the players will not know their opponent's decision before making their own. However, first stage decisions will be revealed to both players at the beginning of the second stage. Due to the long-term nature of strategic decisions, they cannot be reversed. Therefore, it is reasonable to assume that the first stage strategic decisions can be learned through surveillance. For the defender's strategic decisions, this is a reasonable assumption and the attacker can observe the defender's strategic decisions using surveillance. For the attacker's strategic decisions, we assume that the defender is able to learn about the attacker's strategic decisions through espionage.

Definition. A strategy profile $(\boldsymbol{\alpha}^*, \boldsymbol{\beta}^*, \boldsymbol{x}^*, \boldsymbol{y}^*)$ is a *subgame perfect Nash equilibrium* if and only if

$$\boldsymbol{x}^* \equiv \boldsymbol{x}^*(\boldsymbol{\alpha}, \boldsymbol{\beta}) \equiv \arg\max_{\boldsymbol{x}} \left\{ u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}, \boldsymbol{y}^*) \right\}, \tag{1}$$

$$\boldsymbol{y}^* \equiv \boldsymbol{y}^*(\boldsymbol{\alpha}, \boldsymbol{\beta}) \equiv \arg\max_{\boldsymbol{y}} \left\{ u_2^a(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{x}^*, \boldsymbol{y}) \right\}, \tag{2}$$

$$\boldsymbol{\alpha}^* \equiv \arg\max_{\boldsymbol{\alpha}} \left\{ u_t^d(\boldsymbol{\alpha}, \boldsymbol{\beta}^*, \boldsymbol{x}^*(\boldsymbol{\alpha}, \boldsymbol{\beta}^*), \boldsymbol{y}^*(\boldsymbol{\alpha}, \boldsymbol{\beta}^*)) \right\}, \tag{3}$$

$$\boldsymbol{\beta}^* \equiv \arg\max_{\boldsymbol{\beta}} \left\{ u_t^a(\boldsymbol{\alpha}^*, \boldsymbol{\beta}, \boldsymbol{x}^*(\boldsymbol{\alpha}^*, \boldsymbol{\beta}), \boldsymbol{y}^*(\boldsymbol{\alpha}^*, \boldsymbol{\beta})) \right\}. \tag{4}$$

3. Solving the Two-Stage Invest-Defend Game

To solve this game, we use the backward induction method and start from the last stage, i.e., the second stage. The second stage game is solved assuming fixed values for the first stage decisions, $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, and the equilibrium policy of each player in the second stage, $\boldsymbol{x}^*$ and $\boldsymbol{y}^*$ are obtained in terms of $(\boldsymbol{\alpha}, \boldsymbol{\beta})$. The second stage equilibrium, $(\boldsymbol{x}^*, \boldsymbol{y}^*)$, is then used in the first stage game to compute the first stage equilibrium.

3.1. Second stage game

At the second stage game, the first stage decisions, i.e., strategic decisions $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, are assumed to be fixed parameters and the second stage decisions, i.e., operational decisions $(\boldsymbol{x}, \boldsymbol{y})$, are made. The following matrix demonstrates the payoff to both players:

$$\begin{array}{c|cccc}
i \backslash j & 1 & 2 & \cdots & N \\
\hline
1 & -(1-d_1)C_1, (1-d_1)C_1 - d_1 P & -C_2, C_2 & \cdots & -C_N, C_N \\
2 & -C_1, C_1 & -(1-d_2)C_2, (1-d_2)C_2 - d_2 P & \cdots & -C_N, C_N \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
N & -C_1, C_1 & -C_2, C_2 & \cdots & -(1-d_N)C_N, (1-d_N)C_N - d_N P
\end{array}$$

In this matrix, the first element is the payoff to the defender and the second element is the payoff to the attacker. If we assume that $P=0$, then this matrix game turns into a zero-sum game, i.e., $u_2^d(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{x},\boldsymbol{y}) = -u_2^a(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{x},\boldsymbol{y})$. For this zero-sum game, Baykal-Gürsoy et al. (2014) give a unique saddle-point equilibrium. In this section, we extend their result to the case where the attacker suffers a penalty for an unsuccessful attack, i.e., $P>0$.

Theorem 1. *The Nash Equilibrium for the second stage game is given in terms of an index $k\in\{1,\dots,N\}$ such that $\phi_k(\boldsymbol{\alpha},\boldsymbol{\beta}) \le 1 < \phi_{k+1}(\boldsymbol{\alpha},\boldsymbol{\beta})$, where $\phi_i(\boldsymbol{\alpha},\boldsymbol{\beta})$ is defined as $\phi_i(\boldsymbol{\alpha},\boldsymbol{\beta}) = \sum_{j=1}^{i} \frac{C_j - C_i}{d_j(\alpha_j,\beta_j)(C_j+P)}$ for $i \in 1,\dots,N$ and $\phi_{N+1}(\boldsymbol{\alpha},\boldsymbol{\beta}) = \infty$. The strategy of the defender is of threshold type as given below*

$$x_i^* = \begin{cases} \dfrac{\dfrac{1}{d_i(\alpha_i,\beta_i)(C_i+P)}}{\sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j,\beta_j)(C_j+P)}} \left(1 - \sum_{j=1}^{k} \frac{C_j - C_i}{d_j(\alpha_j,\beta_j)(C_j+P)}\right), & i \le k, \\ 0, & i > k. \end{cases} \tag{5}$$

The strategy of the attacker is also of threshold type:

$$y_i^* = \begin{cases} \dfrac{\dfrac{1}{d_i(\alpha_i,\beta_i)C_i}}{\sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j,\beta_j)C_j}}, & i \le k, \\ 0, & i > k, \end{cases} \tag{6}$$

and the equilibrium payoffs are given as:

$$u_2^{d*}(\boldsymbol{\alpha},\boldsymbol{\beta}) \equiv u_2^d(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{x}^*,\boldsymbol{y}^*) = \frac{1 - \sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j,\beta_j)}}{\sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j,\beta_j)C_j}}, \tag{7}$$

$$u_2^{a*}(\boldsymbol{\alpha},\boldsymbol{\beta}) \equiv u_2^a(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{x}^*,\boldsymbol{y}^*) = -\frac{1 - \sum_{j=1}^{k} \dfrac{C_j}{d_j(\alpha_j,\beta_j)(C_j+P)}}{\sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j,\beta_j)(C_j+P)}}. \tag{8}$$

Proof. See Appendix A.1. □

Remark 1. If $C_1 = \cdots = C_N = C$, i.e., the second stage game is of Infiltration/Harassment type, then the Nash Equilibrium requires the use of all target sites, since $\phi_i(\boldsymbol{\alpha},\boldsymbol{\beta}) = 0,\ \forall i = 1,\dots,N$, i.e., $k=N$. In fact, in this case the defense and attack probabilities are proportional to the reciprocal of the detection probability, i.e., $1/d_i(\alpha_i,\beta_i)$ as

$$x_i^* = y_i^* = \frac{\frac{1}{d_i(\alpha_i,\beta_i)}}{M},\ \forall i = 1,\dots,N, \tag{9}$$

and the payoff functions for the defender and the attacker at the second stage are given respectively as

$$u_2^{d*}(\boldsymbol{\alpha},\boldsymbol{\beta}) \equiv u_2^d(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{x}^*,\boldsymbol{y}^*) = -C + \frac{C}{M}, \tag{10}$$

$$u_2^{a*}(\boldsymbol{\alpha},\boldsymbol{\beta}) \equiv u_2^a(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{x}^*,\boldsymbol{y}^*) = C - \frac{C+P}{M}, \tag{11}$$

where $M = \sum_{j=1}^N \dfrac{1}{d_j(\alpha_j,\beta_j)}$.

Corollary 1. *An increase in the attacker's investment on site i, i.e., β_i, leads to an increase in probabilities of both attacking and defending site i. However, an increase in the defender's investment on site i leads to a decrease in probabilities of both attacking and defending site i.*

Proof. By definition, an increase in β_i leads to a decrease in $d_i(\alpha_i,\beta_i)$, implying an increase in $1/d_i(\alpha_i,\beta_i)$, which in turn, increases y_i^* by equation 6, and increases x_i^* by equation 5. Similarly we can prove the effect of increasing α_i on x_i^* and y_i^*. □

Remark 2. The effect of an increase in the defender's investment on site i, seems counter-intuitive at first. However, it can be explained with intuitive arguments. An increase in the defender's investment will lead to a decrease in the attack probability, therefore the defender will decrease her defence probability. In other words, knowing that the attacker is less likely to attack a site leads the defender to defend that site with lower probability. In the extreme situation, if the defender knows that the attacker will never attack site i, then the defender will never defend that site.

3.2. First stage game

Knowing the outcome of the second stage, we can immediately write down the payoff functions at the first stage for both players. We consider two models: unconstrained and budget constrained models. Below we will discuss each model separately.

3.2.1. Unconstrained Model In this model, there are no budget constraints. However, the players incur investment disutility which is considered in the players' respective payoff functions. Hence, the payoff functions are defined as:

$$u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta}) = u_1^d(\boldsymbol{\alpha}) + u_2^{d*}(\boldsymbol{\alpha},\boldsymbol{\beta}) = -\sum_{i=1}^N \alpha_i + \frac{1-\sum_{j=1}^k \dfrac{1}{d_j(\alpha_j,\beta_j)}}{\sum_{j=1}^k \dfrac{1}{d_j(\alpha_j,\beta_j)C_j}}, \tag{12}$$

$$u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta}) = u_1^a(\boldsymbol{\beta}) + u_2^{a*}(\boldsymbol{\alpha},\boldsymbol{\beta}) = -\sum_{i=1}^N \beta_i - \frac{1-\sum_{j=1}^k \dfrac{C_j}{d_j(\alpha_j,\beta_j)(C_j+P)}}{\sum_{j=1}^k \dfrac{1}{d_j(\alpha_j,\beta_j)(C_j+P)}}. \tag{13}$$

In equation 12, the first term, $u_1^d(\boldsymbol{\alpha})$, is the first stage payoff to the defender and corresponds to the investment disutility and the second term, $u_2^{d*}(\boldsymbol{\alpha},\boldsymbol{\beta})$, is the second stage payoff, which is the expected payoff in equilibrium at the second stage game. Similarly, in equation 13, the first and second terms correspond to the attacker's payoff at the first and second stage of the game, respectively. The following lemmas characterize the conditions under which the payoff functions are continuous and concave.

LEMMA 1. *If $P=0$ or if the second stage game is of Infiltration/Harassment type, i.e., $C_1 = \cdots = C_N = C$, then $u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ and $u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})$ are continuous in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$.*

Proof. See Appendix A.2. □

LEMMA 2. *If $P=0$ or if the second stage game is of Infiltration/Harassment type, then $u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ and $u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})$ are strictly concave in each α_i and β_i, respectively.*

Proof. See Appendix A.3. □

LEMMA 3. *If the second stage game is of Infiltration/Harassment type, then $u_d^t(\boldsymbol{\alpha},\boldsymbol{\beta})$ and $u_a^t(\boldsymbol{\alpha},\boldsymbol{\beta})$ are concave in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively.*

Proof. See Appendix A.4. □

The following theorem characterizes the conditions under which there exist a Nash equilibrium for the two-stage invest-defend game.

THEOREM 2. *If the second stage game is of Infiltration/Harassment type, then the overall invest-defend game has a Nash Equilibrium.*

Proof. It is easy to confirm that the strategy spaces for both players are compact and convex (note that investment values are bounded). In Lemma 1 and Lemma 3 we have established that the payoff functions for both players are continuous and concave with respect to their own strategy. Therefore, applying Debreu's existence theorem (see Debreu (1952)), there exist at least one Nash equilibrium. □

REMARK 3. Proving the uniqueness of Nash equilibrium is challenging, however, based on some numerical experiments, we conjecture that it is true.

We now consider the following detection probability function:

$$d_i(\alpha_i,\beta_i) = \frac{e_i^d\alpha_i + L_i}{e_i^d\alpha_i + e_i^a\beta_i + U_i}, \quad 0 \le L_i \le U_i, \quad U_i \neq 0. \tag{14}$$

This function is of the form of a contest success function (Skaperdas 1996). Contest success functions have been used by many researchers to model probability of detecting and thwarting attacks (Levitin 2009, Levitin and Hausken 2009, 2010, Garnaev et al. 2016). In this formula, parameters

$e_i^d > 0$ and $e_i^a > 0$ are investment efficiency factors of site i for the defender and the attacker, respectively. Parameters L_i and U_i are there so that even if both investment efforts are zero, there is a baseline probability of detection that is non-negative and less than or equal to zero. Clearly, $0 \le d_i(\alpha_i, \beta_i) \le 1$. This function satisfies our assumptions for a detection probability function, i.e., it is a continuous, strictly increasing and concave function of defensive investments, α_i, and it is a continuous, strictly decreasing and convex function of attack investments, β_i.

Corollary 2. *If the detection probability function is given in equation 14, and we have* $\frac{(C+P)\frac{e_i^a}{e_i^d}}{\left(N+\frac{C+P}{C}\sum_{j=1}^N \frac{e_j^a}{e_j^d}\right)^2} \ge \frac{L_i}{e_i^d}$ *and* $\frac{(C+P)\frac{e_i^a}{e_i^d}\frac{C+P}{C}}{\left(N+\frac{C+P}{C}\sum_{j=1}^N \frac{e_j^a}{e_j^d}\right)^2} \ge \frac{U_i-L_i}{e_i^a}$*, and the second stage game is of Infiltration/Harassment type, then the first stage game has a unique closed form Nash equilibrium given by:*

$$\alpha_i^* = \frac{(C+P)\frac{e_i^a}{e_i^d}}{\left(N+\frac{C+P}{C}\sum_{j=1}^N \frac{e_j^a}{e_j^d}\right)^2} - \frac{L_i}{e_i^d}, \quad \forall i = 1, \dots, N \tag{15}$$

$$\beta_i^* = \frac{(C+P)\frac{e_i^a}{e_i^d}\frac{C+P}{C}}{\left(N+\frac{C+P}{C}\sum_{j=1}^N \frac{e_j^a}{e_j^d}\right)^2} - \frac{U_i-L_i}{e_i^a}, \quad \forall i = 1, \dots, N \tag{16}$$

and

$$d_i^* \equiv d_i(\alpha_i^*, \beta_i^*) = \frac{e_i^d}{e_i^d + e_i^a\frac{C+P}{C}}, \quad \forall i = 1, \dots, N. \tag{17}$$

Proof. The conditions $\frac{(C+P)\frac{e_i^a}{e_i^d}}{\left(N+\frac{C+P}{C}\sum_{j=1}^N \frac{e_j^a}{e_j^d}\right)^2} \ge \frac{L_i}{e_i^d}$ and $\frac{(C+P)\frac{e_i^a}{e_i^d}\frac{C+P}{C}}{\left(N+\frac{C+P}{C}\sum_{j=1}^N \frac{e_j^a}{e_j^d}\right)^2} \ge \frac{U_i-L_i}{e_i^a}$ ensure that the equilibrium obtained is non-negative. Now, it is easy to check that the provided equilibrium satisfies the first order conditions, and in fact, it is the only solution that can be derived from the first order conditions. □

Corollary 3. *If the detection probability function is given as in equation 14, the second stage game is of Infiltration/Harassment type, $L_i \ll C$, $U_i \ll C$ and $\frac{C+P}{C}\frac{e_i^a}{e_i^d} < N$, then increasing e_i^d decreases both α_i^* and β_i^*. On the other hand, increasing e_i^a increases both α_i^* and β_i^*.*

Proof. Conditions $L_i \ll C$, and $U_i \ll C$ ensure that the solutions in equations 15 and 16 are valid. Now, from these equations, it is easy to take the first derivative with respect to e_i^d and e_i^a and verify the following under the given conditions: $\frac{\partial \alpha_i^*}{\partial e_i^d} \le 0$, $\frac{\partial \beta_i^*}{\partial e_i^d} \le 0$, $\frac{\partial \alpha_i^*}{\partial e_i^a} \ge 0$, and $\frac{\partial \beta_i^*}{\partial e_i^a} \ge 0$. □

Remark 4. Corollary 3 states that if the efficiency factor for the attacker increases, investment levels for both players increase. On the other hand, if the efficiency factor for the defender increases, investment levels for both players decrease. This is an interesting result which is also valid for the budget constrained case (see Corollary 5). If we consider the increase in investment efficiency as discovering a new technology, if a hostile agent, the attacker, obtains this new technology, then we observe a proliferation in security investments. However, if this new technology is obtained by a non-hostile agent, the defender, it leads to a reduction in security investments.

In the next example, we analyze the Nash Equilibrium for the case with two targets.

Example. We consider an example with two targets where the second stage game is of Infiltration/Harassment type, i.e., $C_1 = C_2 = C$, and the detection probability function is given by equation 14. Furthermore, assume that $P = 100, L_1 = L_2 = 0.9, U_1 = U_2 = 1, e_1^d = e_2^d = 1$ and $e_1^a = e_2^a = 1$. Using Corollary 2 we can compute the unique Nash Equilibrium for this example. We further analyze the effect of players' deviations from the Nash equilibrium in their payoff and best response strategies. First, we compute the effects of such deviations on players' total payoff.

The attacker's total payoff is given as:

$$u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta}) = u_1^a(\boldsymbol{\beta}) + u_2^{a*}(\boldsymbol{\alpha},\boldsymbol{\beta}) = -\beta_1 - \beta_2 - \frac{C+P}{\frac{1}{d_1(\alpha_1,\beta_1)} + \frac{1}{d_2(\alpha_2,\beta_2)}} + C. \tag{18}$$

Figure 2a presents the attacker's total payoff as a function of his investment on target 1 when all other decision variables are at their equilibrium level. This figure demonstrates that the attacker's payoff has a well-known inverse U form, that has been identified by many papers in literature (see e.g., Hausken (2006), Hausken et al. (2009), Levitin and Hausken (2012a)). Moreover, Figure 2a shows that the payoff is higher for higher target values and optimal attack investments increase for higher target values.

The defender's total payoff is given as:

$$u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta}) = u_1^d(\boldsymbol{\alpha}) + u_2^{d*}(\boldsymbol{\alpha},\boldsymbol{\beta}) = -\alpha_1 - \alpha_2 + \frac{C}{\frac{1}{d_1(\alpha_1,\beta_1)} + \frac{1}{d_2(\alpha_2,\beta_2)}} - C. \tag{19}$$

Figure 2b illustrates the defender's payoff as a function of her investments on target 1 when all other decision variables are at their equilibrium level. This function is also concave, as was proved in Lemma 2. Moreover for higher target values, the optimum investment value is higher. This is in line with other results in literature, see e.g., Hausken and He (2016).

Attacker's best response: We now compute the attacker's best investment level in target 1 as a function of the defender's investment in target 1. We use the first order condition to obtain the best response:

$$\frac{\partial u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \beta_1} = -1 - (C+P)\frac{\frac{\frac{\partial d_1(\alpha_1,\beta_1)}{\partial \beta_1}}{d_1^2(\alpha_1,\beta_1)}}{\left(\frac{1}{d_1(\alpha_1,\beta_1)} + \frac{1}{d_2(\alpha_2,\beta_2)}\right)^2} = 0, \tag{20}$$

implying

$$\frac{\frac{\frac{\partial d_1(\alpha_1,\beta_1)}{\partial \beta_1}}{d_1^2(\alpha_1,\beta_1)}}{\left(\frac{1}{d_1(\alpha_1,\beta_1)} + \frac{1}{d_2(\alpha_2,\beta_2)}\right)^2} = \frac{-1}{C+P}, \tag{21}$$

to obtain the best response as

$$\beta_1^* = \frac{\sqrt{(C+P)e_1^a(e_1^d\alpha_1+L_1)} - (e_1^d\alpha_1+L_1)(\frac{1}{d_2(\alpha_2,\beta_2)}+1) - (U_1-L_1)}{e_1^a}. \tag{22}$$

Figure 2c depicts the attacker's best response as a function of the defender's investments. Clearly, as defense investments increase, the attacker at first increases attack investments to keep up with the defender, but after a certain point, the attacker starts decreasing his investments, until he is completely deterred from investing.

Defender's best response: We use the first order condition

$$\frac{\partial u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_1} = -1 + C\frac{\frac{\frac{\partial d_1(\alpha_1,\beta_1)}{\partial \alpha_1}}{d_1^2(\alpha_1,\beta_1)}}{\left(\frac{1}{d_1(\alpha_1,\beta_1)}+\frac{1}{d_2(\alpha_2,\beta_2)}\right)^2} = 0, \tag{23}$$

implying

$$\frac{\frac{\frac{\partial d_1(\alpha_1,\beta_1)}{\partial \alpha_1}}{d_1^2(\alpha_1,\beta_1)}}{\left(\frac{1}{d_1(\alpha_1,\beta_1)}+\frac{1}{d_2(\alpha_2,\beta_2)}\right)^2} = \frac{1}{C}, \tag{24}$$

to evaluate the defender's best response function

$$\alpha_1^* = \frac{1}{e_1^d}\left(\frac{\sqrt{Ce_1^d(e_1^a\beta_1+U_1-L_1)} - (e_1^a\beta_1+U_1-L_1)}{\frac{1}{d_2(\alpha_2,\beta_2)}+1}\right) - \frac{L_1}{e_1^d}. \tag{25}$$

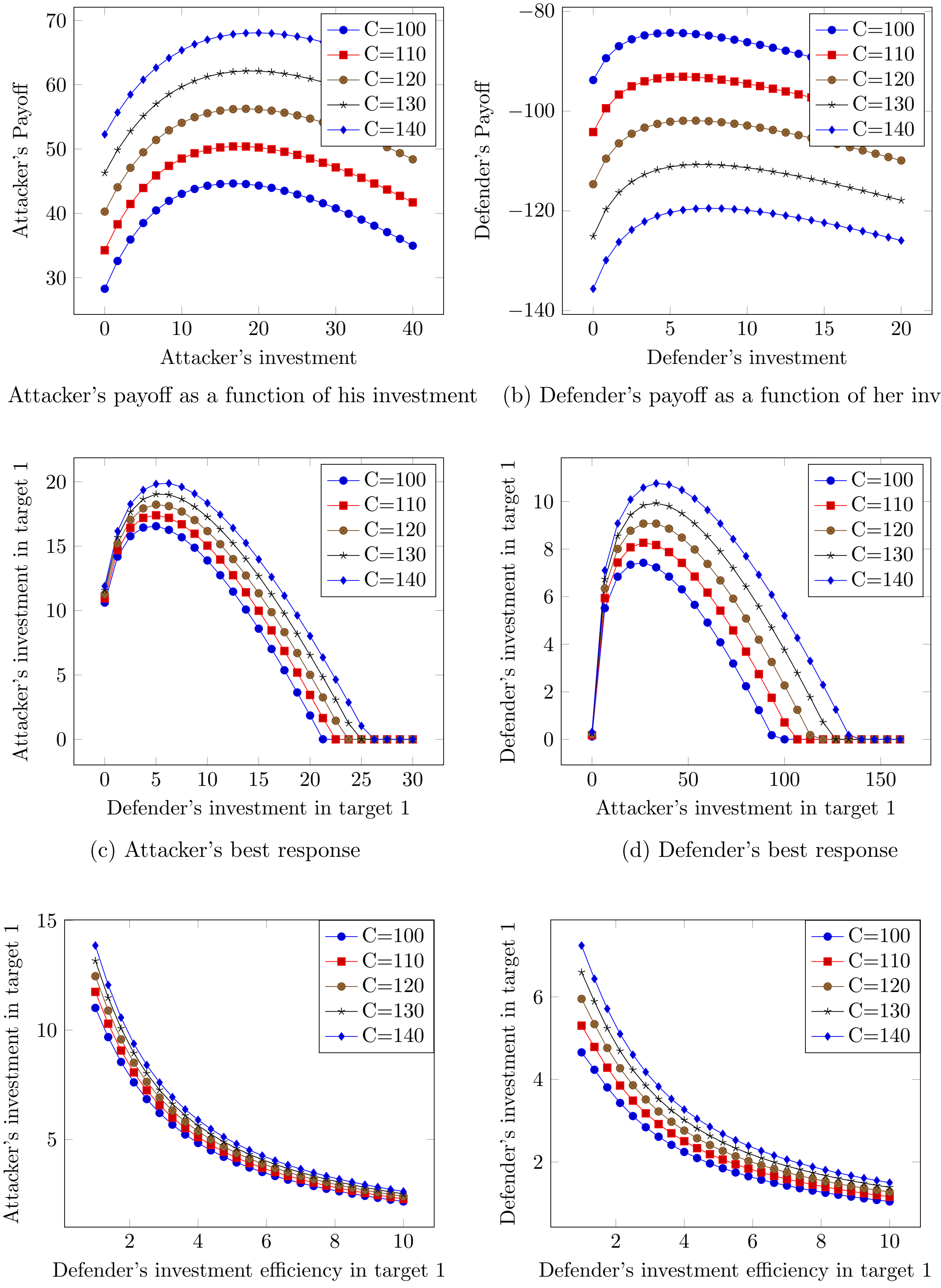
Figure 2d shows the defender's best response as a function of the attacker's investments. As attack investments increase, the defender at first increases defense investments to keep up with the attacker, but after a certain point, the defender starts decreasing her investments, until she is completely deterred from investing. Note that, because the attacker's investment levels do not exceed 20 units (see Figure 2c), in equilibrium, the defender will not be deterred from investing. Another observation is that, the defender's optimum investment level is higher for higher target values. This is in line with other results in literature, see e.g., Hausken and He (2016).

Effect of investment efficiency factors on optimal strategies: We use equations 15 and 16 to compute the Nash equilibrium strategies. Figures 2e and 2f show the effect of the defender's investment efficiency factor on the players' optimal strategies. These figures show that both players' optimal investment levels are decreasing in the defender's efficiency factor.

3.2.2. Budget Constrained Model

In this section, we investigate the budget constrained model in which players do not incur investment disutility, instead they both have a budget limit in the first stage game. Equations 26 and 27 give the player's total payoff functions.

$$u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta}) \equiv u_2^{d*}(\boldsymbol{\alpha},\boldsymbol{\beta}) = \frac{1-\sum_{j=1}^k \frac{1}{d_j(\alpha_j,\beta_j)}}{\sum_{j=1}^k \frac{1}{d_j(\alpha_j,\beta_j)C_j}}, \tag{26}$$



(a) Attacker's payoff as a function of his investment

(b) Defender's payoff as a function of her investment

(c) Attacker's best response

(d) Defender's best response

(e) Effect of the defender's investment efficiency on the attacker's optimal strategy

(f) Effect of the defender's investment efficiency on her optimal strategy

Figure 2 Analysis of the numerical example

$$u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta}) \equiv u_2^{a*}(\boldsymbol{\alpha},\boldsymbol{\beta}) = -\frac{1-\sum_{j=1}^k \dfrac{C_j}{d_j(\alpha_j,\beta_j)(C_j+P)}}{\sum_{j=1}^k \dfrac{1}{d_j(\alpha_j,\beta_j)(C_j+P)}}. \tag{27}$$

The following lemma proves the quasi-concavity of both payoff functions.

Lemma 4. *$u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ and $u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})$ are quasi-concave in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively.*

Proof. See Appendix A.5. □

The following theorem establishes the existence and uniqueness of the Nash equilibrium for the budget constrained invest-defend game.

Theorem 3. *The budget constrained game has a unique Nash Equilibrium $(\boldsymbol{\alpha},\boldsymbol{\beta})$.*

Proof. See Appendix A.6. □

To compute the unique Nash Equilibrium we use the Karush-Kuhn-Tucker (KKT) (Kuhn and Tucker 1951) conditions for both the defender and the attacker. The optimization problem for the defender is given below

$$\max_{\boldsymbol{\alpha}} \quad u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta}) \tag{28}$$

$$\sum_{j=1}^k \alpha_j = A, \tag{29}$$

$$\alpha_j \geq 0, \tag{30}$$

KKT conditions for this optimization problem are

$$\frac{\partial u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_j} = \lambda - \mu_j, \tag{31}$$

$$\sum_{j=1}^k \alpha_j = A, \tag{32}$$

$$\mu_j \alpha_j = 0, \tag{33}$$

$$\mu_j \geq 0, \quad \alpha_j \geq 0. \tag{34}$$

Remark 5. If site i receives investment α_i with $0 < \alpha_i \leq A$, at optimality, we have: $\frac{\partial u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_i} = \lambda$. This implies that if $\alpha_i, \alpha_j > 0$ for $i \neq j$ then: $\frac{\partial u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_i} = \frac{\partial u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_j}$.

The optimization problem for the attacker is as follows:

$$\max_{\boldsymbol{\beta}} \quad u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta}) \tag{35}$$

$$\sum_{j=1}^{k} \beta_j = B, \tag{36}$$

$$\beta_j \geq 0. \tag{37}$$

KKT conditions for this optimization problem are as follows:

$$\frac{\partial u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \beta_j} = \gamma - \pi_j, \tag{38}$$

$$\sum_{j=1}^{k} \beta_j = B, \tag{39}$$

$$\pi_j \beta_j = 0, \tag{40}$$

$$\pi_j \geq 0, \quad \beta_j \geq 0. \tag{41}$$

Remark 6. If site i receives investment β_i with $0 < \beta_i \leq B$, at optimality we have: $\frac{\partial u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \beta_i} = \gamma$. This implies that if $\beta_i, \beta_j > 0$ for $i \neq j$ then: $\frac{\partial u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \beta_i} = \frac{\partial u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \beta_j}$.
Although there is no closed-form equilibrium for the invest-defend game when the second stage game is of the Maximal Damage type, under certain detection probability functions, a closed-form equilibrium exists for the Infiltration/Harassment type second stage game.

Corollary 4. *For the budget constrained game, if the second stage game is of Infiltration/Harassment type, and the detection probability function is given by equation 14, then the first stage game has a unique closed form solution given by:*

$$\beta_i^* = \frac{\frac{e_i^a}{e_i^d}}{\sum_{j=1}^{N} \frac{e_j^a}{e_j^d}} \left(B + \sum_{j=1}^{N} \left(\frac{U_j}{e_j^a} - \frac{L_j}{e_j^a}\right) \right) - \left(\frac{U_i}{e_i^a} - \frac{L_i}{e_i^a}\right), \quad \forall i = 1, \ldots, N, \tag{42}$$

$$\alpha_i^* = \frac{\frac{e_i^a}{e_i^d}}{\sum_{j=1}^{N} \frac{e_j^a}{e_j^d}} \left(A + \sum_{j=1}^{N} \frac{L_j}{e_j^d} \right) - \frac{L_i}{e_i^d}, \quad \forall i = 1, \ldots, N, \tag{43}$$

with:

$$d_i^* = \frac{A + \sum_{j=1}^{N} \frac{L_j}{e_j^d}}{A + \sum_{j=1}^{N} \frac{L_j}{e_j^d} + B + \sum_{j=1}^{N} \left(\frac{U_j}{e_j^a} - \frac{L_j}{e_j^a}\right)}, \quad \forall i = 1, \ldots, N, \tag{44}$$

as long as equations 42 and 43 are non-negative.

Proof. Based on the assumptions, and using the KKT conditions with $\pi_j = \mu_j = 0$ for $j = 1, \ldots, N$, the equations in the corollary are derived. □

Remark 7. In the case that the second stage game is of Infiltration/Harassment type, the equilibrium investment strategy succeeds in making all detection probabilities the same, hence causing the Nash equilibrium defend-attack strategies uniformly distributed over the targets. Thus the equilibrium strategies succeed in achieving the maximum entropy.

Corollary 5. *For the budget constrained game, if the detection probability function is given in equation 14, the second stage game is of Infiltration/Harassment type, i.e., $C_1 = \cdots = C_N = C$, $L_i, U_i \ll A, B$, then increasing e_i^d will decrease both α_i^* and β_i^*. On the other hand, increasing e_i^a will increase both α_i^* and β_i^*.*

Proof. The condition $L_i, U_i \ll A, B$ ensures that the solution in equations 42 and 43 is always valid. From these equations, it is easy to take the first derivatives with respect to e_i^d and e_i^a and verify the following: $\frac{\partial \alpha_i^*}{\partial e_i^d} \leq 0$, $\frac{\partial \beta_i^*}{\partial e_i^d} \leq 0$, $\frac{\partial \alpha_i^*}{\partial e_i^a} \geq 0$, and $\frac{\partial \beta_i^*}{\partial e_i^a} \geq 0$. □

Remark 8. Corollary 5 states that if the investment efficiency factor for the attacker increases, investment levels of both players increase. On the other hand, if the defender's efficiency factor increases investment levels of both players decrease. This is the budget constrained equivalent of Corollary 3.

4. Application to real data

In this section, we apply the budget constrained model to real data from Willis et al. (2005) presented in Table 1. This table provides estimates of the expected annual terrorism losses in the 10 most valuable urban areas of the United States. It also indicates the grant allocation data to these areas. We consider two aspects of the expected damage: monetary value (represented by the expected property loss) and fatality value (represented by the total number of fatalities and injuries). For each of these two aspects, we use the proposed two-stage approach to allocate defense resources among the urban areas. We use the total grant allocation (to all 10 urban areas, i.e., 270 million dollars) as the total available budget for the defender and consider different values for the attacker's budget. Bier et al. (2008) have also used this data set to study the effect of different factors on the optimal allocation of resources. Throughout our experiments, we compare our results with the results obtained by Bier et al. (2008) whenever possible. We assume that the detection probability function is of the form given in equation 14. Unless stated otherwise, we use the following values for the game parameters: $L_i = 0.9, U_i = 1, e_i^d = e_i^a = 1$ for $i = 1, 2, \ldots, N,$ and $B = 0.3A$. Also note that because target valuations are not the same, i.e., $C_1 = \cdots = C_N = C$ does not hold, the second stage game in this section is of Maximal Damage type.

Table 1 Expected damage data for the 10 urban areas with the highest losses

Urban Area	Expected property loss ($million)	Expected Fatalities & Injuries	FY2004 UASI Grant Allocation ($ million)
New York (NY)	413	5350	47
Chicago (CH)	115	1212	34
San Francisco (SF)	57	472	26
Washington DC (WDC)	36	681	29
Los Angeles (LA)	34	402	40
Philadelphia (PHL)	21	199	23
Boston (BSTN)	18	225	19
Houston (HSTN)	11	160	20
Newark (NW)	7.3	74	15
Seattle (STL)	6.7	88	17
Total	719	8863	270

4.1. Analysis based on monetary data

This section presents the results of the two-stage game analysis based on the monetary value of each urban area. Table 2 illustrates the optimal strategies of both players for $P = 400$ and different values for the attacker's budget. It indicates that, for $B = 0.3A$, the defender distributes her investments among the first six most important areas and the level of investment decreases as the value of the area decreases. No investment is allocated to the next important area, i.e., BSTN, however, note that the second stage strategy complements the first stage investment decision by covering BSTN with a relatively high probability. With the exception of this, the second stage defense probabilities also decrease as the value of the area decreases. For the attacker, all of the first stage investments go to BSTN and most of the second stage effort is concentrated in BSTN. This is, roughly speaking, in line with the assumptions of other models, including Bier et al. (2008), that the attacker concentrates his efforts on one area. However the complementary interaction between the first stage and the second stage decisions has not been observed in previous studies. Another interesting observation is that as the attacker's budget increases, decisions at both stages favor more important areas.

Next, we study the effect of the penalty for a failed attack, P, on the optimal first and second stage decisions of both players. Figure 3a shows the effect of P on the defender's optimal investment decisions. As the attacker's penalty of a failed attack increases, the defender distributes her investments to cover more targets. This is due to the fact that as the penalty of a failed attack increases, the attacker is less willing to risk being caught and more willing to attack more vulnerable targets where he is less likely to have an unsuccessful attack. In response, the defender distributes her investments to cover more targets. Another observation is that the investment distribution does not change smoothly as P increases. In other words, the line slopes change at some break points. These break points correspond to a change in the critical index k (in Theorem 1).

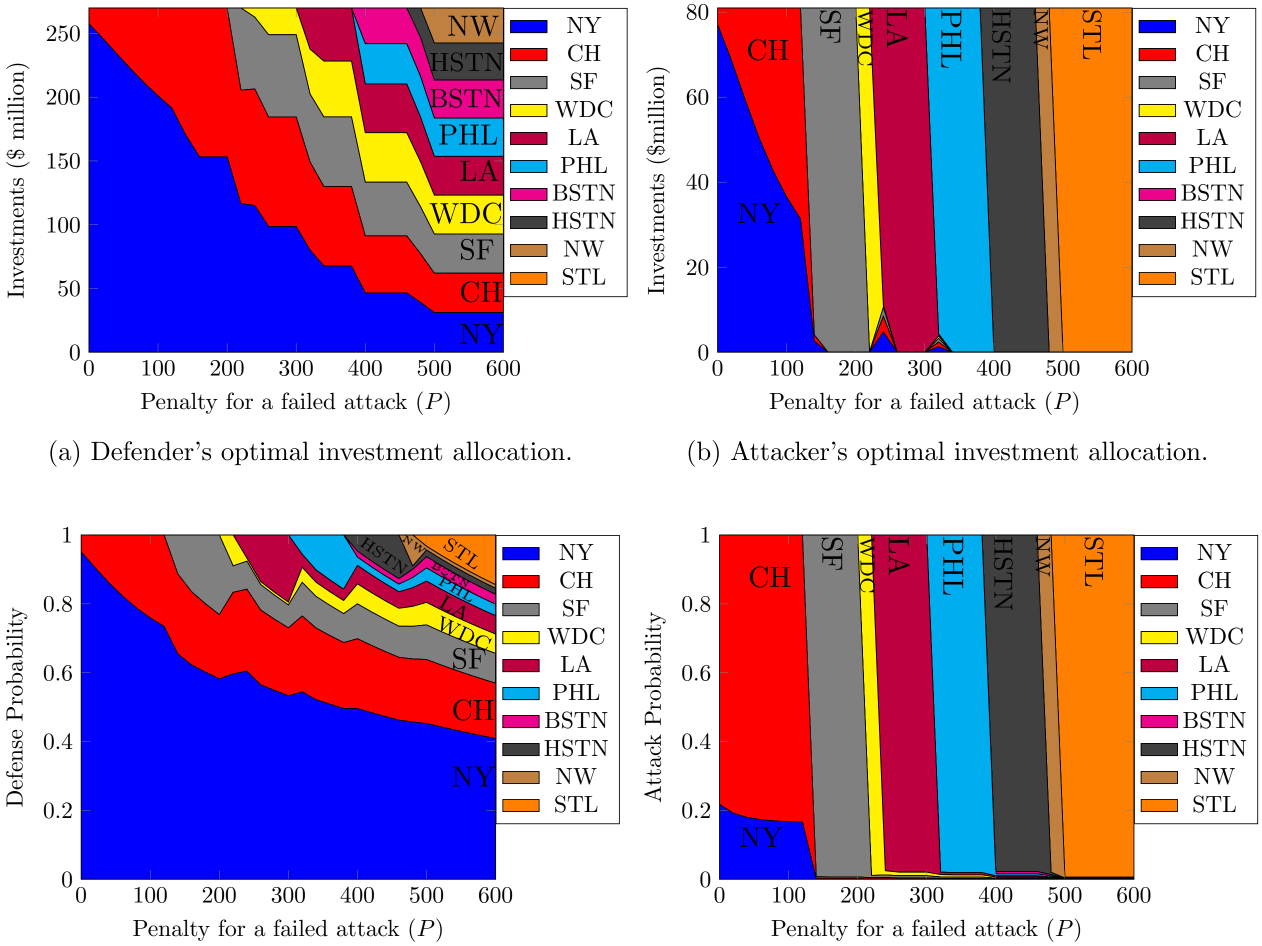
Table 2 Optimal investment and defend/attack strategies for monetary data with $P = 400$

	$B = 0.3A$				$B = 0.6A$				$B = 0.9A$			
	α_i^*	β_i^*	x_i^*	y_i^*	α_i^*	β_i^*	x_i^*	y_i^*	α_i^*	β_i^*	x_i^*	y_i^*
NY	59.82	0.00	0.487	0.000	67.28	0.00	0.483	0.000	97.59	0.00	0.467	0.000
CH	56.01	0.00	0.190	0.002	62.31	0.00	0.184	0.001	85.35	0.00	0.158	0.001
SF	50.16	0.00	0.087	0.003	54.54	0.00	0.080	0.002	64.29	0.00	0.051	0.001
WDC	42.42	0.00	0.043	0.005	43.91	0.00	0.035	0.003	22.78	0.00	0.005	0.002
LA	41.05	0.00	0.038	0.006	41.97	0.00	0.031	0.003	0.00	243.00	0.318	0.995
PHL	20.53	0.00	0.009	0.009	0.00	162.00	0.187	0.990	0.00	0.00	0.000	0.000
BSTN	0.00	81.00	0.145	0.974	0.00	0.00	0.000	0.000	0.00	0.00	0.000	0.000

Each time the critical index k increases, a new target area is added into consideration and to adjust to this change, the line slopes change. Figure 3b illustrates the effect of P on the attacker's optimal investment decisions. The attacker's investments generally concentrate on a single area that is unprotected (in terms of the defender's first stage investments) and has the highest value. Figure 3c shows the defender's second stage defense probability assignments as a function of P. As seen in this figure, the defender's probability assignments are similar to her first stage investment assignments in the sense that more areas get covered as P increases. Moreover, the complementary interaction observed in Table 2, is also visible in Figure 3c. For example, at around $P = 150$, the investments are distributed between two most important areas, i.e., NY and CH. The next most important area, SF, receives no investment in the first stage. However, the second stage defense probability assignment complements the first stage decision by defending SF with a relatively high probability. Another observation is that the defense probability distribution is not monotonic as P increases. In other words, they sometimes increase and sometimes decrease. This is due to changes in the line slopes in Figure 3a. As discussed in this figure, when the critical index k increases, the defender's investment levels for the currently covered targets decrease to accommodate the newly added target area. For some points, these investments reduce with a fairly sharp slope. As a result, and as was proved in Corollary 1, the corresponding defense probabilities increase. When the critical index k does not change and investment levels are fairly stable, based on equation 5, as P increases, the defense probabilities decrease for higher valued targets and increase for lower valued targets. Figure 3d shows the attacker's second stage probabilities as a function of P. The second stage attack probabilities are in line with the first investment decisions. In other words, the second stage probabilities are concentrated on the same target that received majority of the investments in the first stage.

4.2. Analysis based on fatality data

This section presents the results of the two-stage game analysis based on the fatality value of each urban area. We study the effect of the attacker's budget on both players' strategies. This budget



(a) Defender's optimal investment allocation.

(b) Attacker's optimal investment allocation.

(c) Defender's optimal defense policy.

(d) Attacker's optimal attack policy.

Figure 3 Analysis for monetary value data

is represented by a percentage of the defender's budget. Table 3 provides the optimal strategies of both players for $P = 5000$ and different values for the attacker's budget. It shows that, for $B = 0.3A$, the defender distributes her investments among the first six most important areas and the investment level decreases as the value of the area decreases. No investment is allocated to the next important area, i.e., PHL, however, similar to the previous analysis, the second stage strategy complements the first stage investment decision by covering PHL with a relatively high probability. Ignoring this exception, the second stage defense probabilities are also distributed proportional to the value of the area. For the attacker, all of the first stage investments go to PHL and most of the second stage effort is concentrated in PHL. This is, roughly speaking, in line with the assumptions of other models, including Bier et al. (2008), that the attacker concentrates his efforts on one area. Moreover, similar to the results of Bier et al. (2008), different valuations of targets lead to different investment allocations. Similar observations can be made for other values of the attacker's budget.

Table 3 Optimal investment and defend/attack strategies for fatality data with $P = 5000$

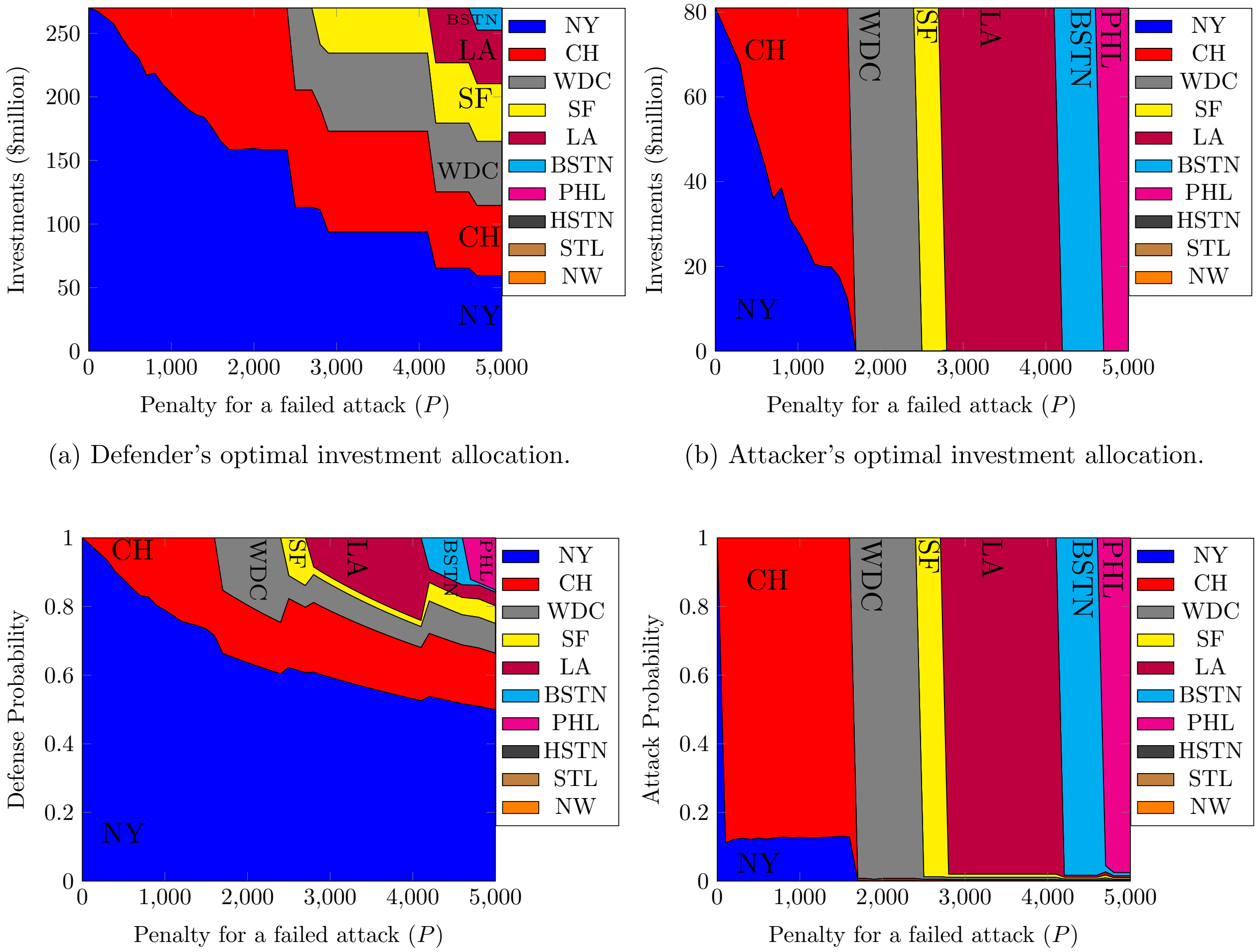
	$B = 0.3A$				$B = 0.6A$				$B = 0.9A$			
	α_i^*	β_i^*	x_i^*	y_i^*	α_i^*	β_i^*	x_i^*	y_i^*	α_i^*	β_i^*	x_i^*	y_i^*
NY	59.37	0.00	0.499	0.000	75.95	13.48	0.574	0.000	158.23	0.00	0.452	0.000
CH	55.13	0.00	0.165	0.002	64.56	11.55	0.185	0.002	111.77	0.00	0.087	0.002
WDC	50.49	0.00	0.087	0.003	53.09	9.60	0.094	0.003	0.00	243	0.461	0.997
SF	45.34	0.00	0.052	0.005	41.49	7.63	0.053	0.005	0.00	0.00	0.00	0.00
LA	42.15	0.00	0.039	0.005	34.91	6.52	0.039	0.006	0.00	0.00	0.00	0.00
BSTN	17.52	0.00	0.007	0.010	0.00	113.23	0.055	0.984	0.00	0.00	0.00	0.00
PHL	0.00	81.00	0.152	0.975	0.00	0.00	0.000	0.000	0.00	0.00	0.00	0.00

Another interesting observation is that as the attacker's budget increases, both first stage and second stage decisions shift towards more important areas.

Next, we study the effect of penalty for a failed attack, P, on the optimal first stage and second stage decisions. Figure 4a shows the effect of P on the defender's optimal investment decisions. As seen in this figure, similar to the case of monetary value analysis, as P increases, the defender distributes the investments to cover more targets. Moreover, in comparison with the case of monetary value analysis, the defender covers fewer areas with investments. Figure 4b shows the effect of P on attacker's optimal investment decisions. According to this figure, attacker's investments generally concentrate on a single unprotected area (in terms of the defender's first stage investments) with the highest value. Figure 4c shows the defender's second stage defense probability assignments as a function of P. As seen in this figure, similar to her first stage investment assignments, more areas get covered as P increases. Moreover, the complementary interaction between the first stage and second stage decisions, as observed in Table 3, is also visible in Figure 4c. This figure also shows that, in comparison with the case of monetary value analysis, the defender covers fewer areas with a positive defense probability. Figure 4d shows the attacker's second stage probabilities as a function of P. According this figure, the second stage attack probabilities are in line with the first stage investment decisions. In other words, the second stage probabilities are concentrated on a single target which is the same target that received majority of the investments in the first stage.

5. Conclusions and future research

In this paper, we introduce two-stage invest-defend games to accommodate both strategic and operational decisions in the same model to respond to more realistic environments. We then prove the existence of Nash equilibria for both unconstrained and budget constrained models and establish its uniqueness for the budget constrained model. We provide closed form solutions for the invest-defend game with the Infiltration/Harassment type second stage for both models. In the



(a) Defender's optimal investment allocation.

(b) Attacker's optimal investment allocation.

(c) Defender's optimal defense policy.

(d) Attacker's optimal attack policy.

Figure 4 Analysis for fatality value data

budget constrained model, the solution of the first stage problem makes all sites indistinguishable through the appropriate investments for defense and attack, hence enforcing a uniform allocation of defense/attack efforts at the second stage. Our results indicate that an increase in defense investments in a target decreases the probability of both defending and attacking that target. However, an increase in attack investments increases the probability of both defending and attacking that target. Our results also demonstrate that an increase in the defender's investment efficiency leads to decrease in investments by both the defender and the attacker. On the contrary, an increase in the attacker's investment efficiency leads to increase in investments by both the defender and the attacker.

When the budget constrained model is applied to real data, the analysis reveals that the attacker's penalty for a failed attack is an important factor in determining the defender's optimal distribution of investments and defense probabilities. In addition, the defender's second stage decisions complement her first stage decisions in the sense that the most important area that receives little or zero investment is covered with a relatively high defense probability in the second stage. Moreover, the Nash strategy prescribes shifting the investments more towards the most important sites as the attacker's budget increases.

This study extends the current security game models by integrating strategic and operational level decisions in a comprehensive model. However, there is still a need to further investigate multi-period invest-defend games with multiple defenders. Another area of interest is the effect of investment transparency vs secrecy on the defense policy.

Appendix A: Proofs of selected theorems and lemmas

A.1. Theorem 1

Proof. To prove this theorem we first establish some lemmas.

LEMMA 5. *The second stage matrix game has a pure Nash Equilibrium if and only if* $(1-d_1)C_1 - d_1P \geq C_2$.

Proof. Suppose we have $(1-d_1)C_1 - d_1P \geq C_2$. It is easy to check that $\mathbf{x} = (1,0,0,...,0)\,, \mathbf{y} = (1,0,0,...,0)$ is a pure Nash Equilibrium strategy pair. This establishes the sufficiency part. We prove the necessity part by contradiction. Suppose that $(1-d_1)C_1 - d_1P < C_2$, and the game has a pure Nash Equilibrium. This pure Nash Equilibrium can not be given by $\mathbf{x} = (1,0,0,...,0)\,, \mathbf{y} = (1,0,0,...,0)$, because at this strategy profile the attacker can strictly increase his payoff by attacking site 2. Moreover, the target for both attack and defend has to be the same, i.e., $x_i = y_i = 1$ for some $i > 1$. However, this implies that $(1-d_i)C_i - d_iP \geq C_1$ which contradicts our assumption of sorted C_is, thus proving the necessity part.

□

Lemma 6 characterizes the conditions under which some strategies of the attacker are dominated by a linear combination of other strategies. This lemma helps us find a critical index to compute the Nash Equilibrium.

LEMMA 6. *If* $\sum_{j=1}^{k} \frac{C_j - C_k}{d_j(C_j+P)} > 1$, *then the attacker's strategies* $l \geq k$ *are strictly dominated by a mixed strategy that is composed of pure strategies* j *for* $1 \leq j < k$, *i.e., there exist* $\lambda_i \geq 0,\ 1 \leq i \leq k-1$ *with* $\sum_{i=1}^{k-1} \lambda_i = 1$ *such that:*

$$\lambda_1 \begin{bmatrix} (1-d_1)C_1 - d_1P \\ C_1 \\ C_1 \\ \vdots \\ C_1 \end{bmatrix} + \lambda_2 \begin{bmatrix} C_2 \\ (1-d_2)C_2 - d_2P \\ C_2 \\ \vdots \\ C_2 \end{bmatrix} + \cdots + \lambda_{k-1} \begin{bmatrix} C_{k-1} \\ \vdots \\ (1-d_{k-1})C_{k-1} - d_{k-1}P \\ \vdots \\ C_{k-1} \end{bmatrix} > \begin{bmatrix} C_l \\ \vdots \\ \vdots \\ (1-d_l)C_l - d_lP \\ \vdots \\ C_l \end{bmatrix}.$$

Proof. The inequality holds for rows $r \geq k$ because C_is are sorted, i.e., $\sum_{j=1}^{k-1} \lambda_j C_j > C_k$ for all $\lambda_i \geq 0, 1 \leq i \leq k-1$ with $\sum_{i=1}^{k-1} \lambda_i = 1$

For rows $r < k$, consider the assumption, $\sum_{j=1}^{k} \frac{C_j - C_k}{d_j(C_j+P)} > 1$. After some algebraic manipulations this inequality can be rewritten as:

$$\frac{(1-d_r)\,C_r - d_r P}{d_r(C_r+P)\sum\limits_{m=1}^{k-1}\frac{1}{d_m(C_m+P)}} + \sum_{j=1, j\neq r}^{k-1} \frac{C_j}{d_j(C_j+P)\sum\limits_{m=1}^{k-1}\frac{1}{d_m(C_m+P)}} > C_k.$$

Setting $\lambda_j = \frac{1}{d_j(C_j+P)\sum\limits_{m=1}^{k-1}\frac{1}{d_m(C_m+P)}}$ gives the result as:

$$\lambda_r\,(1-d_r)\,C_r + \sum_{j=1, j\neq r}^{k-1} \lambda_j C_j > C_k \geq C_l. \quad \square$$

Lemma 7 complements Lemma 6 in characterizing the sites that should be in the mixed Nash Equilibrium.

Lemma 7. *If* $\sum_{j=1}^{k} \frac{C_j - C_k}{d_j(C_j+P)} < 1$, *any strategy profile with* $x_k = 0$ *is not a Nash Equilibrium.*

Proof. By contradiction. Suppose the Nash Equilibrium holds with $x_k = 0$. If $y_k = 0$, consider a critical $k^* \geq k$ such that $\sum_{j=1}^{k^*} \frac{C_j - C_k^*}{d_j(C_j+P)} < 1 < \sum_{j=1}^{k^*+1} \frac{C_j - C_{k^*+1}}{d_j(C_j+P)}$. Using Lemma 5, we can conclude that both players are playing a mixed strategy. Moreover using Lemma 6 we have: $x_j = 0, y_j = 0, \forall j > k^*$. Therefore the attacker is indifferent towards his choices $i = 1, ..., k^*, i \neq k$, in other words:

$$(1-d_1x_1)\,C_1 - d_1x_1P = \cdots = (1-d_{k-1}x_{k-1})\,C_{k-1} - d_{k-1}x_{k-1}P = (1-d_{k+1}x_{k+1})\,C_{k+1} - d_{k+1}x_{k+1}P = \ldots$$
$$= (1-d_{k^*}x_{k^*})\,C_{k^*} - d_{k^*}x_{k^*}P.$$

Solving these equations along with the equation $\sum_{j=1, j\neq k}^{k^*} x_j = 1$ yields:

$$x_{k^*} = \frac{1 - \sum\limits_{j=1, j\neq k}^{k^*} \frac{C_j - C_{k^*}}{d_j(C_j+P)}}{d_{k^*}(C_{k^*}+P)\sum\limits_{j=1, j\neq k}^{k^*}\frac{1}{d_j(C_j+P)}}.$$

Since $\sum_{j=1}^{k^*} \frac{C_j - C_{k^*}}{d_j(C_j+P)} < 1$ and $C_{k^*} \leq C_k$, the following inequality holds:

$$\sum_{j=1, j\neq k}^{k^*} \frac{C_j - C_k}{d_j(C_j+P)} < 1,$$

which could be rewritten as:

$$\sum_{j=1, j\neq k}^{k^*} \frac{C_j - C_{k^*} + (C_{k^*} - C_k)}{d_j(C_j+P)} < 1.$$

This further simplifies to:

$$(C_{k^*} - C_k) < \frac{1 - \sum\limits_{j=1, j\neq k}^{k^*} \frac{C_j - C_{k^*}}{d_j(C_j+P)}}{\sum\limits_{j=1, j\neq k}^{k^*} \frac{1}{d_j(C_j+P)}} = d_{k^*}(C_{k^*}+P)x_{k^*},$$

giving $(1 - d_{k^*}x_{k^*})\,C_{k^*} - d_{k^*}x_{k^*}P < C_k$. Therefore the attacker can strictly improve his payoff by increasing y_k to 1. Hence $y_k = 1$ should hold. Now the defender can strictly increase her payoff by increasing x_k to 1. This is in contradiction with our assumption of $x_k = 0$ being in a Nash Equilibrium. $\square$

We are now aready to prove the theorem. Consider a critical k^* such that $\sum_{j=1}^{k^*} \frac{C_j - C_{k^*}}{d_j(C_j+P)} < 1 < \sum_{j=1}^{k^*+1} \frac{C_j - C_{k^*+1}}{d_j(C_j+P)}$, if $k^* = 1$ then Lemma 5 and Lemma 6 imply that the game has a unique pure strategy Nash Equilibrium. If $k^* \geq 2$, then using Lemma 6 and Lemma 7, the mixed strategy Nash Equilibrium is determined by solving the following systems of equations:

System 1:

$$(1-d_1x_1)C_1 - d_1x_1P = (1-d_2x_2)C_2 - d_2x_2P = ... = (1-d_{k^*}x_{k^*})C_{k^*} - d_{k^*}x_{k^*}P,$$
$$\sum_{j=1}^{k^*} x_j = 1.$$

System 2:

$$-(1-d_1)C_1y_1 - \sum_{j=1, j\neq 1}^{k^*} C_jy_j = -(1-d_2)C_2y_2 - \sum_{j=1, j\neq 2}^{k^*} C_jy_j = ... = -(1-d_{k^*})C_{k^*}y_{k^*} - \sum_{j=1, j\neq k^*}^{k^*} C_jy_j,$$
$$\sum_{j=1}^{k^*} y_i = 1.$$

Both systems have unique solutions. Solving these systems lead to the solution in equations 5 to 8. □

A.2. Lemma 1

Proof. Because the first stage payoffs, $u_1^d(\boldsymbol{\alpha})$ and $u_1^a(\boldsymbol{\beta})$, are linear in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, they are continuous in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. Therefore, in order to prove that the total payoff functions are continuous, we only need to prove that the second stage payoffs are continuous. We first prove that the second stage payoff function for the defender is continuous in both players' strategies. Here is the payoff function:

$$u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \frac{1 - \sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j, \beta_j)}}{\sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j, \beta_j)C_j}}.$$

For a fixed value of k, clearly the payoff function is continuous, therefore we only need to prove that it is also continuous when the value of k changes. If $C_i = C, \ \forall i = 1, \ldots, N$, then $k = N$ always holds and the result follows. We now focus on the case of $P = 0$. The value of k changes only when $\phi_k(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{j=1}^{k-1} \dfrac{C_j - C_k}{d_j(\alpha_j, \beta_j)(C_j)} = 1$ and a small change in either α or β results in $\phi_k(\boldsymbol{\alpha}, \boldsymbol{\beta}) > 1$, hence causing the value of k decreased by one unit. At this point the expected damage is computed using the formula $k' = k - 1$ as the threshold value. We prove that the expected damage under both threshold indices k,or $k-1$, lead to the same value:

$$\left| u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta})|_{k'} - u_2^d(\boldsymbol{\alpha}, \boldsymbol{\beta})|_k \right| = \left| \frac{1 - \sum_{j=1}^{k-1} \dfrac{1}{d_j(\alpha_j, \beta_j)}}{\sum_{j=1}^{k-1} \dfrac{1}{d_j(\alpha_j, \beta_j)C_j}} - \frac{1 - \sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j, \beta_j)}}{\sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j, \beta_j)C_j}} \right|$$
$$= \left| \frac{1}{d_k(\alpha_k, \beta_k)C_k} \frac{1 - \sum_{j=1}^{k-1} \dfrac{C_j - C_k}{d_j(\alpha_j, \beta_j)C_j}}{\sum_{j=1}^{k-1} \dfrac{1}{d_j(\alpha_j, \beta_j)C_j} \sum_{j=1}^{k} \dfrac{1}{d_j(\alpha_j, \beta_j)C_j}} \right| = 0.$$

This establishes continuity of the defender's payoff. Same argument applies when proving the continuity of the attacker's payoff function. □

A.3. Lemma 2

Proof. We have already established the continuity of both payoff functions. In order to prove concavity we show that the second derivative is negative. The first derivative of $u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ is given as:

$$\frac{\partial u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_i} = -1 + \left(\frac{\dfrac{1}{d_i^2(\alpha_i,\beta_i)C_i}\left(1-\sum_{j=1}^{k}\dfrac{C_j-C_i}{d_j(\alpha_j,\beta_j)C_j}\right)}{\left(\sum_{j=1}^{k}\dfrac{1}{d_j(\alpha_j,\beta_j)C_j}\right)^2} \right) \frac{\partial d_i(\alpha_i,\beta_i)}{\partial \alpha_i}.$$

Then the second derivative satisfies:

$$\frac{\partial^2 u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_i^2} = \left(\frac{2}{d_i^3(\alpha_i,\beta_i)C_i} \left(1-\sum_{j=1}^{k}\frac{C_j-C_i}{d_j(\alpha_j,\beta_j)C_j}\right)\right) \frac{\dfrac{1}{d_i(\alpha_i,\beta_i)C_i} - \sum_{j=1}^{k}\dfrac{1}{d_j(\alpha_j,\beta_j)C_j}}{\sum_{j=1}^{k}\dfrac{1}{(d_j(\alpha_j,\beta_j)C_j)^3}} \frac{\partial d_i(\alpha_i,\beta_i)}{\partial \alpha_i}$$

$$+ \frac{\dfrac{1}{d_i^2(\alpha_i,\beta_i)C_i}\left(1-\sum_{j=1}^{k}\dfrac{(C_j-C_i)}{(d_j(\alpha_j,\beta_j)C_j)}\right)}{(\sum_{j=1}^{k}\dfrac{1}{d_j(\alpha_j,\beta_j)C_j})^2} \frac{\partial^2 d_i(\alpha_i,\beta_i)}{\partial \alpha_i^2} < 0.$$

The last inequality is valid because by assumptions either $P=0$ or $C_i=C,\ \forall i=1,\dots,N$, holds. Therefore $u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ is strictly concave in α_is. One can similarly show that $u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})$ is strictly concave in β_is. □

A.4. Lemma 3

Proof. To prove the lemma for $u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$, we first prove that $u_2^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ is concave in $(d_1(\alpha_1,\beta_1), d_2(\alpha_2,\beta_2), ..., d_N(\alpha_N,\beta_N))$. Here is the Hessian matrix for $u_2^d(\boldsymbol{\alpha},\boldsymbol{\beta})$:

$$H = \frac{2C}{\left(\sum_{j=1}^{N}\dfrac{1}{d_j}\right)^3} \begin{bmatrix} \dfrac{\left(\dfrac{1}{d_1}-\sum_{j=1}^{N}\dfrac{1}{d_j}\right)}{d_1^3} & \dfrac{1}{d_1^2 d_2^2} & \cdots & \dfrac{1}{d_1^2 d_N^2} \\ \dfrac{1}{d_2^2 d_1^2} & \dfrac{\left(\dfrac{1}{d_2}-\sum_{j=1}^{N}\dfrac{1}{d_j}\right)}{d_2^3} & \cdots & \dfrac{1}{d_2^2 d_N^2} \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{1}{d_N^2 d_1^2} & \dfrac{1}{d_N^2 d_2^2} & \cdots & \dfrac{\left(\dfrac{1}{d_N}-\sum_{j=1}^{N}\dfrac{1}{d_j}\right)}{d_N^3} \end{bmatrix}.$$

Let H_l be the submatrix of H obtained by taking the upper left hand corner $l \times l$ matrix of H. Furthermore let $|H_l|$, be the lth principal minor of H.

We need to show that the principal minors of H alternate in sign, starting with negative, i.e., $(-1)^l\,|H_l| > 0$ for $l = 1, 2, \dots, N-1$ and $|H| = 0$. Because we are only concerned about the sign of the determinant of H, we can divide (or multiply) rows and columns of H with positive quantities. Therefore, we divide row i by

$\frac{2C}{d_i\left(\sum_{j=1}^N \frac{1}{d_j}\right)^3}$ for $i=1,2,\dots,N$, then we multiply column i by d_i for $i=1,2,\dots,N$. Here is the resulting matrix:

$$H' = \begin{bmatrix} \frac{1}{d_1}\left(\frac{1}{d_1} - \sum_{j=1}^N \frac{1}{d_j}\right) & \frac{1}{d_1 d_2} & \cdots & \frac{1}{d_1 d_N} \\ \frac{1}{d_2 d_1} & \frac{1}{d_2}\left(\frac{1}{d_2} - \sum_{j=1}^N \frac{1}{d_j}\right) & \cdots & \frac{1}{d_2 d_N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{d_N d_1} & \frac{1}{d_N d_2} & \cdots & \frac{1}{d_N}\left(\frac{1}{d_N} - \sum_{j=1}^N \frac{1}{d_j}\right) \end{bmatrix}.$$

H' is a symmetric diagonally dominant matrix because the absolute value of each diagonal element is equal to the sum of the absolute values of all other elements in the same row. Therefore H' is a negative semi-definite matrix. Hence the leading principal minors of H' alternate in sign, starting with negative, i.e., $(-1)^l\,|H'_l| > 0$ for $l=1,2,\dots,N-1$ and $|H'|=0$. Because H' is obtained by multiplying rows and columns of H with positive quantities, H' and H have the same determinant sign, this is also true for the signs of their leading principal minors. Therefore the leading principal minors of H alternate in sign, starting with negative, i.e., $(-1)^l\,|H_l| > 0$ for $l=1,2,\dots,N-1$ and $|H|=0$. Hence $u_2^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ is concave in $(d_1(\alpha_1,\beta_1), d_2(\alpha_2,\beta_2), ..., d_N(\alpha_N,\beta_N))$. It follows that $u_2^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ is concave in $\boldsymbol{\alpha}$, because increasing concave function of a concave function is concave. It then follows that $u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$ is concave in $\boldsymbol{\alpha}$, because the sum of two concave functions is concave. One can similarly prove the lemma for $u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})$. □

A.5. Lemma 4

Proof. To prove this lemma for $u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})$, we prove that all of its upper level sets are convex. Suppose for two points $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha}'$ and some L we have,

$$u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta}) = \frac{1-\sum_{j=1}^k \frac{1}{d_j(\alpha_j,\beta_j)}}{\sum_{j=1}^k \frac{1}{d_j(\alpha_j,\beta_j)C_j}} \geq L, \tag{45}$$

and

$$u_t^d(\boldsymbol{\alpha'},\boldsymbol{\beta}) = \frac{1-\sum_{j=1}^k \frac{1}{d_j(\alpha'_j,\beta_j)}}{\sum_{j=1}^k \frac{1}{d_j(\alpha'_j,\beta_j)C_j}} \geq L, \tag{46}$$

we prove that for all λ with $0\leq\lambda\leq 1$ we have:

$$u_t^d(\lambda\boldsymbol{\alpha} + (1-\lambda)\boldsymbol{\alpha}',\boldsymbol{\beta}) \geq L.$$

To prove this, note that equation 45 implies

$$\sum_{j=1}^k \frac{1+\frac{L}{C_j}}{d_j(\alpha_j,\beta_j)} \leq 1,$$

and equation 46 gives

$$\sum_{j=1}^k \frac{1+\frac{L}{C_j}}{d_j(\alpha'_j,\beta_j)} \leq 1.$$

These two equations provide

$$\sum_{j=1}^{k}(1+\frac{L}{C_j})(\frac{\lambda}{d_j(\alpha_j,\beta_j)}+\frac{1-\lambda}{d_j(\alpha'_j,\beta_j)})\leq 1.$$

Now $u_t^d(\lambda\boldsymbol{\alpha}+(1-\lambda)\boldsymbol{\alpha}',\boldsymbol{\beta})\geq L$ follows from the convexity of $\frac{1}{d_j(\alpha_j,\beta_j)}$ for all j. The proof of quasi-concavity of $u_2^a(\boldsymbol{\alpha},\boldsymbol{\beta})$ follows similarly. □

A.6. Theorem 3

Proof. We fix the critical index k and write down the optimization problem for both players. For the defender, we have the following optimization problem:

$$max \quad u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta}) \tag{47}$$

$$\sum_{j=1}^{k}\alpha_j = A, \tag{48}$$

$$\phi_k(\boldsymbol{\alpha},\boldsymbol{\beta})\leq 1, \tag{49}$$

$$\alpha_j\geq 0, \tag{50}$$

where $\phi_i(\boldsymbol{\alpha},\boldsymbol{\beta})=\sum_{j=1}^{i}\frac{C_j-C_i}{d_j(\alpha_j,\beta_j)(C_j+P)}$ for $i\in\{1,\dots,N\}$ and $\phi_{N+1}(\boldsymbol{\alpha},\boldsymbol{\beta})=\infty$. It is easy to see that constraints 48 and 50 lead to a convex strategy space for the defender. We show that the strategy space characterized by constraint 49 is also convex and therefore the whole strategy space is convex (because intersection of convex sets is convex). Consider two points $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha'}$ with $\phi_k(\boldsymbol{\alpha},\boldsymbol{\beta})\leq 1$, and $\phi_k(\boldsymbol{\alpha'},\boldsymbol{\beta})\leq 1$. We show that any convex combination of $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha'}$ also satisfies constraint 49. Note that $\phi_k(\boldsymbol{\alpha},\boldsymbol{\beta})$ is a convex function of $\boldsymbol{\alpha}$ because it is the sum of convex functions. Hence, $\phi_k(\lambda\boldsymbol{\alpha}+(1-\lambda)\boldsymbol{\alpha'},\boldsymbol{\beta})\leq\lambda\phi_k(\boldsymbol{\alpha},\boldsymbol{\beta})+(1-\lambda)\phi_k(\boldsymbol{\alpha'},\boldsymbol{\beta})\leq 1$. The first inequality follows from the convexity of $\phi_k(\boldsymbol{\alpha},\boldsymbol{\beta})$ and the second inequality is due to the assumptions, $\phi_k(\boldsymbol{\alpha},\boldsymbol{\beta})\leq 1$, and $\phi_k(\boldsymbol{\alpha'},\boldsymbol{\beta})\leq 1$. Therefore, the defender's strategy space is convex. It is easy to check that the strategy space is also compact.

The optimization problem for the attacker is given as follows

$$max \quad u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta}) \tag{51}$$

$$\sum_{j=1}^{k}\beta_j = B, \tag{52}$$

$$\phi_{k+1}(\boldsymbol{\alpha},\boldsymbol{\beta})\geq 1, \tag{53}$$

$$\beta_j\geq 0. \tag{54}$$

The strategy space of the attacker is also convex and compact (the proof is similar to the convexity proof of the defender's strategy space). Therefore the strategy spaces of both players are convex and compact. In

Lemma 4 we establish that the payoff functions for both players are quasi-concave with respect to their own strategy. Moreover, because the critical index k is fixed, the payoff functions are continuous. It also follows that, because $\phi_i(\boldsymbol{\alpha},\boldsymbol{\beta})$ is increasing in i, for each $(\boldsymbol{\alpha},\boldsymbol{\beta})$ there exists an index k such that $(\boldsymbol{\alpha},\boldsymbol{\beta})$ is feasible. Therefore, applying Debreu's existence theorem (see Debreu (1952)) implies that there exist at least one Nash Equilibrium.

To establish uniqueness, we use the index theory approach (see Theorem 7 in Cachon and Netessine (2004)). Because first derivatives are all positive, there is no point with $\frac{\partial u_t^d(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \alpha_i}=0$ and $\frac{\partial u_t^a(\boldsymbol{\alpha},\boldsymbol{\beta})}{\partial \beta_i}=0$ for $i=1,2,...,N$, therefore conditions of this theorem are, vacuously, satisfied. Thus, there exists at most one Nash Equilibrium.

□

References

Baykal-Gürsoy, Melike, Zhe Duan, H Vincent Poor, Andrey Garnaev. 2014. Infrastructure security games. *European Journal of Operational Research* **239**(2) 469–478.

Bier, Vicki M, Vinod Abhichandani. 2002. Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries. *Proceedings of the engineering foundation conference on risk-based decision making in water resources X, Santa Barbara, CA: American Society of Civil Engineers*. 59–76.

Bier, Vicki M, Naraphorn Haphuriwat, Jaime Menoyo, Rae Zimmerman, Alison M Culpen. 2008. Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis* **28**(3) 763–770.

Bureau of Counterterrorism. 2016. National consortium for the study of terrorism and responses to terrorism: Annex of statistical information.

Cachon, Gerard P, Serguei Netessine. 2004. Game theory in supply chain analysis. *Handbook of Quantitative Supply Chain Analysis*. Springer, 13–65.

Debreu, Gerard. 1952. A social equilibrium existence theorem. *Proceedings of the National Academy of Sciences* **38**(10) 886–893. doi:10.1073/pnas.38.10.886.

Garcia, Mary Lynn. 2005. *Vulnerability assessment of physical protection systems*. Butterworth-Heinemann.

Garnaev, Andrey, Melike Baykal-Gürsoy, H Vincent Poor. 2014. Incorporating attack-type uncertainty into network protection. *Information Forensics and Security, IEEE Transactions on* **9**(8) 1278–1287.

Garnaev, Andrey, Melike Baykal-Gursoy, H Vincent Poor. 2015. How to deal with an intelligent adversary. *Computers & Industrial Engineering* **90** 352–360.

Garnaev, Andrey, Melike Baykal-Gursoy, H Vincent Poor. 2016. Security games with unknown adversarial strategies. *IEEE transactions on cybernetics* **46**(10) 2291–2299.

Garrick, B John, James E Hall, Max Kilger, John C McDonald, Tara O'Toole, Peter S Probst, Elizabeth Rindskopf Parker, Robert Rosenthal, Alvin W Trivelpiece, Lee A Van Arsdale, et al. 2004. Confronting the risks of terrorism: making the right decisions. *Reliability Engineering & System Safety* **86**(2) 129–176.

Golany, Boaz, Edward H Kaplan, Abraham Marmur, Uriel G Rothblum. 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.

Guan, Peiqiu, Meilin He, Jun Zhuang, Stephen C Hora. 2017. Modeling a multitarget attacker–defender game with budget constraints. *Decision Analysis* **14**(2) 87–107.

Haphuriwat, Naraphorn, Vicki M Bier, Henry H Willis. 2011. Deterring the smuggling of nuclear weapons in container freight through detection and retaliation. *Decision Analysis* **8**(2) 88–102.

Harris, Bernard. 2004. Mathematical methods in combatting terrorism. *Risk Analysis* **24**(4) 985–988.

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

Hausken, Kjell. 2006. Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy* **25**(6) 629–665.

Hausken, Kjell. 2009. Strategic defense and attack of complex networks. *International Journal of Performability Engineering* **5**(1) 13–30.

Hausken, Kjell. 2010. Defense and attack of complex and dependent systems. *Reliability Engineering & System Safety* **95**(1) 29–42.

Hausken, Kjell, Vicki M Bier. 2011. Defending against multiple different attackers. *European Journal of Operational Research* **211**(2) 370–384.

Hausken, Kjell, Vicki M Bier, Jun Zhuang. 2009. Defending against terrorism, natural disaster, and all hazards. *Game theoretic risk analysis of security threats*. Springer, 65–97.

Hausken, Kjell, Fei He. 2016. On the effectiveness of security countermeasures for critical infrastructures. *Risk Analysis* **36**(4) 711–726.

Hausken, Kjell, G Levitin. 2009. Parallel systems with different types of defence resource expenditure under two sequential attacks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* **223**(1) 71–85.

Hausken, Kjell, Gregory Levitin. 2012. Review of systems defense and attack models. *International Journal of Performability Engineering* **8**(4) 355–366.

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

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

Kaplan, Stanley, B John Garrick. 1981. On the quantitative definition of risk. *Risk analysis* **1**(1) 11–27.

Kuhn, H. W., A. W. Tucker. 1951. Nonlinear programming. *Proceedings of the Second Berkeley Symposium on Mathematical Statistics and Probability*. University of California Press, Berkeley, Calif., 481–492.

Levitin, Gregory. 2009. Optimal distribution of constrained resources in bi-contest detection-impact game. *International Journal of Performability Engineering* **5**(1) 45–54.

Levitin, Gregory, Kjell Hausken. 2009. Intelligence and impact contests in systems with redundancy, false targets, and partial protection. *Reliability Engineering & System Safety* **94**(12) 1927–1941.

Levitin, Gregory, Kjell Hausken. 2010. Defence and attack of systems with variable attacker system structure detection probability. *Journal of the Operational Research Society* **61**(1) 124–133.

Levitin, Gregory, Kjell Hausken. 2012a. Individual versus overarching protection against strategic attacks. *Journal of the Operational Research Society* **63**(7) 969–981.

Levitin, Gregory, Kjell Hausken. 2012b. Parallel systems under two sequential attacks with imperfect detection of the first attack outcome. *Journal of the Operational Research Society* **63**(11) 1545–1555.

Levitin, Gregory, Kjell Hausken. 2012c. Resource distribution in multiple attacks with imperfect detection of the attack outcome. *Risk Analysis* **32**(2) 304–318.

McGill, William L, Bilal M Ayyub, Mark Kaminskiy. 2007. Risk analysis for critical asset protection. *Risk Analysis* **27**(5) 1265–1281.

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

Paté-Cornell, Elisabeth. 2002. Fusion of intelligence information: A bayesian approach. *Risk Analysis* **22**(3) 445–454.

Paté-Cornell, Elisabeth, Seth Guikema. 2002. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Operations Research* **7**(4) 5–23.

Peng, Rui, Gregory Levitin, Min Xie, Szu Hui Ng. 2010. Defending simple series and parallel systems with imperfect false targets. *Reliability Engineering & System Safety* **95**(6) 679–688.

Pita, James, Manish Jain, Janusz Marecki, Fernando Ordóñez, Christopher Portway, Milind Tambe, Craig Western, Praveen Paruchuri, Sarit Kraus. 2008. Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport. *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*. International Foundation for Autonomous Agents and Multiagent Systems, 125–132.

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

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

Shan, Xiaojun, Jun Zhuang. 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.

Shan, Xiaojun, Jun Zhuang. 2014a. Modeling credible retaliation threats in deterring the smuggling of nuclear weapons using partial inspectiona three-stage game. *Decision Analysis* **11**(1) 43–62.

Shan, Xiaojun, Jun Zhuang. 2014b. Subsidizing to disrupt a terrorism supply chaina four-player game. *Journal of the Operational Research Society* **65**(7) 1108–1119.

Shan, Xiaojun, Jun Zhuang. 2017. Modeling cumulative defensive resource allocation against a strategic attacker in a multi-period multi-target sequential game. *Reliability Engineering & System Safety* **In Press**.

Shieh, Eric, Bo An, Rong Yang, Milind Tambe, Craig Baldwin, Joseph DiRenzo, Ben Maule, Garrett Meyer. 2012. Protect: A deployed game theoretic system to protect the ports of the united states. *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*. International Foundation for Autonomous Agents and Multiagent Systems, 13–20.

Skaperdas, Stergios. 1996. Contest success functions. *Economic theory* **7**(2) 283–290.

Smith, Brent L, Paxton Roberts, Kelly R Damphousse. 2017. The terrorists planning cycle. *The Handbook of the Criminology of Terrorism* 62–76.

Tsai, Jason, Christopher Kiekintveld, Fernando Ordonez, Milind Tambe, Shyamsunder Rathi. 2009. Iris-a tool for strategic security allocation in transportation networks. *8th International Joint Conference on Autonomous Agents and Multiagent Systems (Industry Track), May 2009.*.

United States Army, Training & Doctrine Command. 2010. *A military guide to terrorism in the twenty-first century*. Cosimo Incorporated. Appendix A, A1-A6.

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

Willis, Henry H, Andrew R Morral, Terrence K Kelly, Jamison Jo Medby. 2005. *Estimating terrorism risk*. Rand Corporation.

Yolmeh, Abdolmajid, Melike Baykal-Gürsoy. 2017. A robust approach to infrastructure security games. *Computers & Industrial Engineering* **110** 515–526.

Yolmeh, Abdolmajid, Melike Baykal-Gürsoy. 2018. Urban rail patrolling: a game theoretic approach. *Journal of Transportation Security* 1–18.

Zhuang, Jun, Vicki M Bier. 2007. Balancing terrorism and natural disastersdefensive strategy with endogenous attacker effort. *Operations Research* **55**(5) 976–991.

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