DOI: 10.1111/risa.12768

Deterrence and Risk Preferences in Sequential Attacker–Defender Games with Continuous Efforts

Vineet M. Payappalli,[1] Jun Zhuang,[1,*] and Victor Richmond R. Jose[2]

Most attacker–defender games consider players as risk neutral, whereas in reality attackers and defenders may be risk seeking or risk averse. This article studies the impact of players' risk preferences on their equilibrium behavior and its effect on the notion of deterrence. In particular, we study the effects of risk preferences in a single-period, sequential game where a defender has a continuous range of investment levels that could be strategically chosen to potentially deter an attack. This article presents analytic results related to the effect of attacker and defender risk preferences on the optimal defense effort level and their impact on the deterrence level. Numerical illustrations and some discussion of the effect of risk preferences on deterrence and the utility of using such a model are provided, as well as sensitivity analysis of continuous attack investment levels and uncertainty in the defender's beliefs about the attacker's risk preference. A key contribution of this article is the identification of specific scenarios in which the defender using a model that takes into account risk preferences would be better off than a defender using a traditional risk-neutral model. This study provides insights that could be used by policy analysts and decisionmakers involved in investment decisions in security and safety.

KEY WORDS: Attacker–defender games; homeland security; risk aversion; risk-seeking behavior

1. INTRODUCTION

The attacks on the World Trade Center in New York on September 11, 2001 became a pivotal moment in the way we study and understand risks in security and safety. With numerous agencies such as the Office of Domestic Preparedness and the Nuclear Incident Response Team being created after these attacks, the amount of resources that have been allocated to understand and to prepare for these types of risks have grown exponentially. The 2016 U.S. budget for the Department of Homeland Security (DHS) is about \$65 billion in total.[(1)] Such huge investments in the numerous counterterrorism and security efforts being launched every year demand a more careful and rigorous approach to study and understand these risks.

The fundamental question this article investigates is how the notion of risk preferences affects players' equilibrium strategies in a sequential attacker–defender (AD) game and what it implies for the notion of deterrence. In its most general form, "deterrence is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits."[(2)]

The aim of this article is to try to narrow the gap between existing mathematical models of AD games in counterterrorism literature and the extensive literature from behavioral economics and psychology that documents the different attitudes of

[1] Department of Industrial and Systems Engineering, University at Buffalo, The State University of New York, Buffalo, NY, USA.

[2] McDonough School of Business, Georgetown University, Washington, DC, USA.

[*] Address correspondence to Jun Zhuang, Department of Industrial and Systems Engineering, University at Buffalo, The State University of New York, Buffalo, NY 14260-2050, USA; jzhuang@buffalo.edu.

individuals toward risk and uncertainty. This study could be of use to researchers, homeland security practitioners, policymakers, policy analysts, and other government agencies in understanding how players in AD games develop strategies when risk preferences, an important aspect of human behavior and decision making, are introduced in analytical models. This would improve decision making over the large group of existing models, which implicitly assume risk neutrality.

To our knowledge, there is no existing paper that specifically examines the effects of risk preferences on deterrence. The idea of deterrence springs from the advantage that a first-mover may have to significantly affect the actions and choices of a second-mover player (a.k.a., the first-mover advantage). As Hausken(3) mentions, sequential games of this form are useful in enabling analysts to come up with analysis and recommendations that are preemptive (cf. Zhuang and Hausken,(4) Hausken and Zhuang,(5) and Jose and Zhuang(6)). It is also of interest to note that there may be instances in which it is to the advantage of the defender to not always reveal her/his strategy by opting to play in a simultaneous fashion (e.g., see Zhuang and Bier(7)). We believe that this article will serve as a first building block in this research direction.

Specifically, we present analytical results related to the effect of attacker's and defender's risk preferences on the defense effort and their impact on the optimal deterrence level. Numerical illustrations and some discussion of the effect of risk preferences on deterrence and the utility of using such a model are provided, as well as sensitivity analysis of continuous attack investment levels and uncertainty in the defender's beliefs about the attacker's risk preference. A key contribution of this article is the identification of specific scenarios in which the defender using a model that takes into account risk preferences would be better off than a defender using traditional risk-neutral models.

The rest of this article is organized as follows. Section 2 provides a literature review, and Section 3.1 introduces the continuous defense, discrete attack (CDDA) model, which is followed by some analytical results in Section 3.2. Section 3.3 presents numerical illustrations related to the propositions and shows the equilibrium responses of the AD in several interesting scenarios. Also shown in Section 3.3 is the importance of the risk-preference model by comparing the results with a conventional risk-neutral model, and the section provides scenarios in which risk-preference models give better results than risk-neutral models. Section 4 explores the extension where the attacker also has a continuous action space. Section 5 analyzes how the equilibrium is affected if the defender has incomplete information about the attacker's risk preference. Section 6 concludes and presents future research directions. Finally, the Appendix gives calculations and a plot on which a discussion at the end of Section 3.3.1 is based.

2. LITERATURE REVIEW

In the risk analysis literature, numerous studies try to better understand how we deal with risks associated with adaptive/strategic adversaries, where game theory has often been used, with roots dating back to the 1950s. One class of models that has grown in popularity and use are AD games.(8–10) As Cox Jr.(11) mentions, these tools are constantly relied upon when doing risk analysis because of their ability to "reorient current adversarial risk analysis to make it useful" through the development of useful predictive models of causal relationships and improving a defender's decision-making capabilities.

Beyond counterterrorism, AD games have also been applied to other general risk analysis contexts such as cybersecurity(12–14) and war gaming.(15) Hausken and Levitin(16) provide a comprehensive review of AD models from a systems perspective. Developments related to the applications in counterterrorism and corporate competition have supplemented the traditional statistical risk analysis with a new approach called adversarial risk analysis.(17) Hausken(18) applies game theory in probabilistic risk analysis, thereby introducing a behavioral approach in assessing the reliability of systems. In general, the literature has considered adversaries as strategic(19–22) as well as nonstrategic.(23,24)

Decision making under uncertainty has been the object of investigation in various disciplines for decades.(25) Bernoulli's proposal(26) that people maximized expected utility and not expected value was the first step toward introducing risk preferences in decision making. Research on decision making under uncertainty has progressed a long way, with the development of the von Neumann–Morgenstern utility theorem,(27) a better understanding of the willingness to pay for risky investment options, regret theory,(28,29) and prospect theory.(30) Weber and Johnson(25) provide a historical context of these developments in the risk-preference literature. Although most of these developments have found applications primarily in economics and finance, in the broader context, the existence of risk preferences is a universal phenomenon. We attempt to translate some of these developments into the realm of critical national security issues.

We find that in almost all AD games in the literature, players are modeled as risk neutral; i.e., they make decisions that maximize expected payoffs or minimize expected losses.(31) This has conventionally been done following the economic tradition of assuming agents to be perfectly "rational" as well as for modeling convenience.(3) However, extensive empirical and theoretical evidence has shown that risk neutrality may not be realistic or preferred in practice.(26,27,30,32–34)

For example, Stewart *et al.*(35) suggest that policymakers within the U.S. government and its agencies (including the DHS) are risk averse for "low-probability high-consequence events" because of the catastrophic or dire nature of these hazards. This would imply that the U.S. government and its agencies should be treated as risk averse in some AD counterterrorism games. Some studies have found that certain terrorist organizations are also risk averse.(36–38) We also acknowledge that adversaries could be nonrational(39) or display bounded rationality.(40) However, in this article, we focus on rational adversaries who deviate from the traditional norms of risk neutrality. We think that this is a natural starting point in understanding the effect of risk preferences in issues such as deterrence.

In the AD games literature, some authors have recognized the importance of risk preferences. For example, Zhuang and Bier(9) mention that risk aversion and risk-seeking behavior may impact the outcomes when they apply game theory in studying resource allocation for countering terrorism and natural disasters; however, they study risk preferences by incorporating risk parameters only in part of the utility function. Other papers mention the notion of utility functions but often end up using linear utility (i.e., they assume risk neutrality yet use the term "utility" interchangeably with payoffs) or do not fully model utility and risk preferences consistent with the decision and risk analysis literature (e.g., Bell *et al.*(41) and Liu *et al.*(42)).

In the context of sequential games, several papers discuss the notion of risk aversion not necessarily of players, but of strategies. These fall into the broad category of robust game theory where an analyst may want to determine and minimize worst-case scenarios. For example, Yin *et al.*(43) and Qian *et al.*(44) study the notion of risk-averse strategies in a sequential Stackelberg game (which is a game between a leader and a follower competing on quantity(45)), where each player optimizes over a class of possible utility functions.

3. CONTINUOUS DEFENSE DISCRETE ATTACK (CDDA) MODEL

3.1. Model

We consider a two-player sequential game. In the first stage, the defender chooses a continuous level of defense investment $d \in [0, \infty)$ that maximizes her/his expected utility. After observing the defender's level of investment, an attacker in the second stage chooses to either attack (denoted by "A" or $a = A$) or not attack (denoted by "NA" or $a = NA$). If the attacker chooses to attack, his/her success probability P depends on how much the defender invested in defense. This probability success function $P : [0, \infty) \to [0, 1]$ is strictly decreasing in d. To remove trivial cases, we assume that the function P is not equal to 0 or 1 for any $d > 0$.

For each player, we define three parameters. First, the defender and the attacker each values[3] the "target" (the resource that the government tries to defend from terrorist attacks) at v_d and v_a, respectively. In addition, each player has a unit cost for defending (c_d) and attacking (c_a). For the attacker, we assume that $v_a > c_a$ so that the decision whether to attack or not does not become trivial. The utility functions of the defender and the attacker are, respectively, denoted by u_d and u_a. Fig. 1 provides the sequence of steps and Table I summarizes the notation we use in the article.

In this article, we focus on the subgame perfect Nash equilibrium[4] strategy for both players and analyze the impact of incorporating risk preferences in an AD game, focusing on its impact on deterrence.

3.2. Analytical Results

We begin by examining the best response of the attacker using backward induction. Observing the

[3] We assume in our model that players are able to quantify their valuation of targets typically in monetary terms. For example, Shan and Zhuang(46) use the valuation of 47 U.S. urban areas provided by Willis *et al.*(47) to illustrate their model.

[4] An equilibrium found by applying rollback to the extensive form game is referred to as subgame perfect equilibrium.(48)

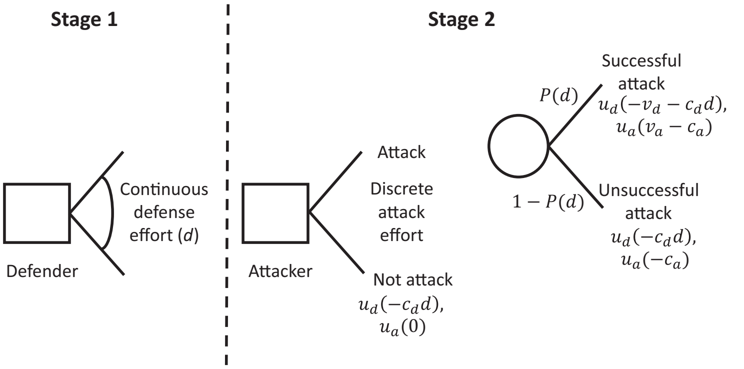

Fig. 1. Sequence of moves in the AD game (CDDA model) with the players' utilities.

Table I. Notation for Decision Variables and Parameters Used in the Article

Decision Variables	a	Attacker's decision ($a \in \{A, NA\}$ in CDDA model) or attacker's effort (attack investment level, $a \geq 0$ in CDCA model)
	$d \geq 0$	Defender's effort (defense investment level)
Functions	$P(d)$ *and* $P(a, d)$	The probability of successful attack
	u_a	Attacker's utility function
	u_d	Defender's utility function
	$U_a(a, d)$	Total expected utility of the attacker
	$U_d(a, d)$	Total expected utility of the defender
	$\hat{a}(d) \equiv \arg\max U_A(a, d)$	Attacker's best response
Parameters	(a^*, d^*)	Equilibrium strategy
	λ	Coeffecient of defender's defense effectiveness
	c_a	Attacker cost for attacking
	c_d	Defender's unit cost of effort
	v_a	Attacker's valuation of the target
	v_d	Defender's valuation of the target

defense level d, the attacker chooses $a \in \{A, NA\}$ that maximizes his expected utility $U_a(a, d)$. Proposition 1 provides an important property about the attacker's best response.

Proposition 1. *The attacker's best response $\hat{a}(d)$ is of a threshold type in d; i.e., there exists a threshold $\bar{d}$ for which the attacker will attack ($\hat{a}(d) = A$) when $0 \leq d < \bar{d}$ and not attack ($\hat{a}(d) = NA$) when $d \geq \bar{d}$.*

Proof. The attacker will maximize his/her expected utility, i.e., his optimization problem is: max $U_a(a, d) = P(d)u_a(v_a - c_a) + (1 - P(d))u_a(-c_a)$. In this case, the attacker will choose $a = A$ if and only if

$$\begin{aligned} & P(d)u_a(v_a - c_a) + (1 - P(d))u_a(-c_a) > u_a(0) \\ \Leftrightarrow \quad & P(d) > \frac{u_a(0) - u_a(-c_a)}{u_a(v_a - c_a) - u_a(-c_a)} \\ \Leftrightarrow \quad & d < P^{-1}\left(\frac{u_a(0) - u_a(-c_a)}{u_a(v_a - c_a) - u_a(-c_a)}\right). \end{aligned} \tag{1}$$

The second inequality holds because $v_a > c_a$ and u_a is nondecreasing in its argument. The third inequality follows from the assumption that P is strictly decreasing in d. (We note that if we instead assume that P is nonincreasing, we can easily replace P^{-1} by the generalized inverse $P^{[-1]}$ and with some work show that the result still holds.) ■

This threshold idea tells us that there exists a level $\bar{d} \in [0, \infty)$ such that the attacker will choose not to attack for any $d \geq \bar{d}$, because the probability of successful attack is too low to provide him/her sufficiently large expected utility for attacking. This threshold $\bar{d}$ is what we will refer to as the *deterrence level*, which is given by:

$$\bar{d} = \begin{cases} 0 & \text{when } r \geq 1 \\ P^{-1}(r) & \text{when } 0 < r < 1 \\ \infty & \text{when } r \leq 0 \end{cases} \tag{2}$$

where $r = \frac{u_a(0) - u_a(-c_a)}{u_a(v_a - c_a) - u_a(-c_a)}$. The conditions $r > 1$ and $r < 0$ are trivial and do not arise for a strictly nondecreasing function u_a. Also, when u_a is a strictly increasing function, there will always be a positive finite $\bar{d}$ as $0 < r < 1$.

First, we note that this quantity is well defined since we assumed that P is strictly decreasing in its argument. Next, we provide an interpretation for this quantity by analyzing the simple case when $u_a(x)$ is linear (i.e., a risk-neutral attacker). For a strictly increasing u_a, the deterrence level in Equation (2) simplifies to $P^{-1}(\frac{c_a}{v_a})$ in the risk-neutral case, which represents the point where the expected gain $P(d)v_a$ equals the cost of attacking c_a.

In the more general setting of nonlinear utility, we study how the deterrence level changes when an attacker is viewed to be *more risk seeking (less risk averse)*. Using Pratt's[32] definition, we say a player with utility function $\hat{u}$ is more risk seeking (less risk averse) than a player with utility function u if there exists an increasing convex function g such that $\hat{u}(x) = g(u(x))$ for all x.

The next proposition provides insights on the deterrence level as we consider the more general setting of risk preferences.

Proposition 2. *The deterrence level $\bar{d}$ is (i) at least as high for a more risk-seeking (less risk-averse) attacker, (ii) nondecreasing in v_a, and (iii) nonincreasing in c_a for a risk-seeking attacker.*

Proof. Since P is decreasing in d, P^{-1} must also be decreasing. Therefore, it is sufficient to study whether $K(u_a, v_a, c_a) := \frac{u_a(0)-u_a(-c_a)}{u_a(v_a-c_a)-u_a(-c_a)}$ is increasing or decreasing. For ease of notation, let $x = -c_a$ and $y = v_a - c_a$. Since we assume that $v_a > c_a > 0$, we have $x < 0 < y$.

(i) Consider two utility functions u_a and $\hat{u}_a$, where $\hat{u}(x) = g(u(x))$ and g is an increasing convex function. By the convexity of g, we know that the marginal utility differential between y and x is greater than the differential between 0 and x, i.e., $\frac{g(u_a(y))-g(u_a(x))}{u_a(y)-u_a(x)} > \frac{g(u_a(0))-g(u_a(x))}{u_a(0)-u_a(x)} \Leftrightarrow \frac{u_a(0)-u_a(x)}{u_a(y)-u_a(x)} > \frac{g(u_a(0))-g(u_a(x))}{g(u_a(y))-g(u_a(x))} \Leftrightarrow K(u_a, v_a, c_a) > K(g(u_a), v_a, c_a)$. Therefore, the deterrence level associated with u_a is lower than the deterrence level associated with $\hat{u}_a$, since P^{-1} is decreasing.

(ii) For $v'_a > v_a$, we note that $u_a(v'_a - c_a) \geq u_a(v_a - c_a)$ for any utility function u_a. Hence, $K(u_a, v'_a, c_a) = \frac{u_a(0)-u_a(-c_a)}{u_a(v'_a-c_a)-u_a(-c_a)} \leq \frac{u_a(0)-u_a(-c_a)}{u_a(v_a-c_a)-u_a(-c_a)} = K(u_a, v_a, c_a)$.

(iii) To prove that $\bar{d}$ is nonincreasing in c_a for a risk-seeking attacker, we need to show that $K(u_a, v_a, c_a)$ is increasing for a convex u_a. We note that

$$\frac{\partial K}{\partial c_a} = \frac{u'_a(-c_a)}{u_a(v_a - c_a) - u_a(-c_a)} - \frac{[u_a(0) - u_a(-c_a)](u'_a(-c_a) - u'_a(v_a - c_a))}{[u_a(v_a - c_a) - u_a(-c_a)]^2},$$

where $u'_a = \frac{\partial u_a}{\partial c_a}$. The first term on the right-hand side is positive because all utility functions are nondecreasing in their arguments. The second term is also positive for a convex u_a because $u'_a(-c_a) - u'_a(v_a - c_a) < 0$; i.e., increasing convex utility functions become steeper. Therefore, for convex u_a, we have $\frac{\partial K}{\partial c_a} \geq 0$. ■

Proposition 2 shows how the deterrence level is affected by changes in the model parameters. In particular, we notice that for a more risk-seeking (less risk-averse) attacker, a defender has to invest more to completely deter an attack. As expected, we also see that as the value of the target to the attacker increases, the deterrence level increases.

Finally, we note that the impact of the attacker's costs c_a is not directly evident in this model, since analytically the effect of c_a on $\bar{d}$ depends on the utility function. Depending on the concavity of the attacker's utility function u_a, we may not necessarily see a monotonic change in the deterrence level. For a risk-seeking attacker, we can show that $\bar{d}$ is nonincreasing in c_a. However, for a risk-averse attacker, this is not guaranteed because the proof of Proposition 2(iii) is not applicable for concave (risk-averse) utility functions.

Next, we consider the defender, who has the benefit of moving first. Her/his defense level choice can be a strategic decision that results in deterrence; however, this choice has to be balanced with the relative value of the target and the cost associated with such defensive investments. Proposition 3 describes the equilibrium strategy of the defender.

Proposition 3. *Let $U_d(d_{int}) := P(d_{int})u_d(-v_d - c_d d_{int}) + (1 - P(d_{int}))u_d(-c_d d_{int})$. The equilibrium strategy of the defender $d^* \in [0, \bar{d}]$ is an interior point (which we denote by d_{int}) if and only if $U_d(d_{int}) > u_d(0)$ and*

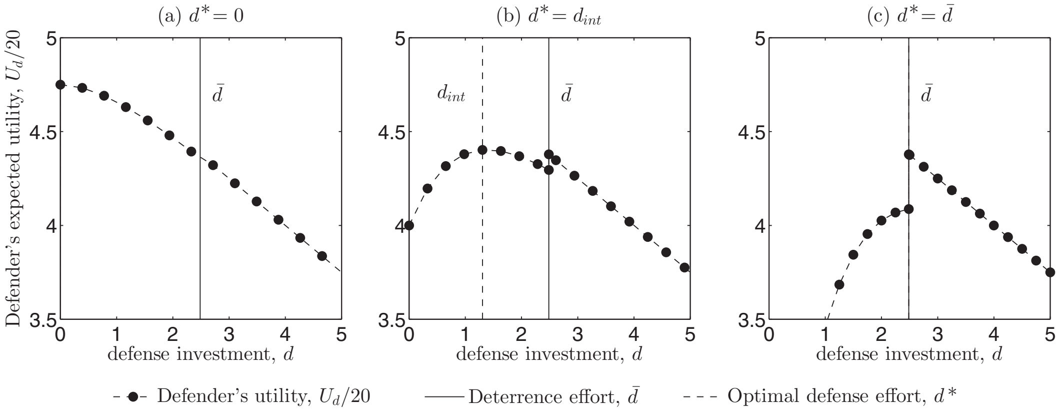

Fig. 2. A set of scenarios showing the three possible types of optimal solutions for the CDDA model. Baseline values: $z_d = z_a = 100$, $v_d = v_a = 60$, $c_d = c_a = 5$, and $\lambda = 1$, where λ is the defense effectiveness coefficient in the exponential success function $P(d) = e^{-\lambda d}$.

$$U_d(d_{int}) > \frac{[u_a(0) - u_a(-c_a)]u_d(-v_d - c_d d)}{u_a(v_a - c_a) - u_a(-c_a)} + \frac{[u_a(v_a - c_a) - u_a(0)]u_d(-c_d d)}{u_a(v_a - c_a) - u_a(-c_a)}.$$

Proof. The defender faces the following optimization problem to maximize her/his expected utility. Plugging in the attacker's best response in Equation (1) to the defender's optimization problem, we have:

$$\max_d U_d(\hat{a}(d), d) = \begin{cases} \left\{ \begin{array}{l} P(d)u_d(-v_d - c_d d) \\ +(1 - P(d))u_d(-c_d d) \end{array} \right\} & \text{if } \hat{a}(d) = A \\ u_d(-c_d d) & \text{if } \hat{a}(d) = NA. \end{cases} \quad (3)$$

The value of d that maximizes the defender's utility will be the equilibrium defender strategy d^*. If we let $d_{int} := \{d : U_d'(d) = 0\}$, then we have

$$d^* = \begin{cases} 0 & \text{when } U_d(0) > max(U_d(\bar{d}), U_d(d_{int})) \\ d_{int} & \left\{ \begin{array}{l} \equiv \text{ interior solution,} \\ \text{when } U_d(d_{int}) > max(U_d(0), U_d(\bar{d})) \end{array} \right. \\ \bar{d} & \left\{ \begin{array}{l} \equiv \text{ deterrence solution,} \\ \text{when } U_d(\bar{d}) > max(U_d(0), U_d(d_{int})). \end{array} \right. \end{cases}$$

The conditions provided in the proposition follow by expanding $U_d(0)$ and $U_d(\bar{d})$. ■

Proposition 3 explains that there are three types of solutions d^* to the defender's problem. Fig. 2 illustrates the three possible scenarios numerically. First, d^* can be 0 when the defender does not invest any amount into defense (Fig. 2(a)). This case happens in the extreme case when v_d is not sufficiently high so that the defender deems the target to be worth protecting or alternatively the probability of successful attack is sufficiently high so that the cost of defense is too high to have any significant impact or savings.

The other extreme case $d^* = \bar{d}$ happens when the cost of defense is relatively cheap such that the defender has sufficient resources to invest in defense (Fig. 2(c)). Even though the defender can reduce the probability of successful attack by investing $d > \bar{d}$, she/he would not choose to do so. The result suggests that the level of investment needs not exceed $\bar{d}$, i.e., there is no need to overinvest in defense.

The case $d^* = d_{int}$ is perhaps the most interesting since this represents the middle ground where the defender neither goes all the way nor does she/he do nothing at all. This interior solution happens when the defender's investment is sufficiently high to minimize the expected disutility while taking into account that she/he needs not spend too much in defending the target. From Proposition 3 and Equation (2), we notice that due to the Boolean nature of the attack, d_{int} is independent of the attacker's utility function u_a, and the deterrence defense level $\bar{d}$ is independent of the defender's utility function u_d. A closed-form solution does not exist for d_{int} and hence for d^* because of the specific way utility functions are defined. More details are provided at the end of Section 3.3.1 and in the Appendix.

3.3. Numerical Illustration

3.3.1. Sensitivity Analyses

To provide some additional insights to this model, we provide a few numerical illustrations that allow us to see in detail how the equilibrium strategies and payoffs depend on the model parameters.

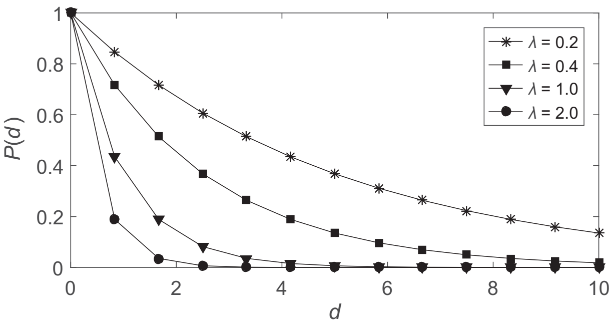

Fig. 3. Probability of successful attack $P(d)$ plotted for different values of defense investment d and defense effectiveness λ. Clearly, a higher value of λ decreases $P(d)$ and vice-versa.

For the purpose of numerical illustration, we assume a few functional forms in this section. In particular, following Bier *et al.,*[49] we assume an exponential success function $P(d)$ given by:

$$P(d) = \exp(-\lambda d),$$

where $\lambda > 0$ is the defense effectiveness coefficient. This function is strictly decreasing in d and is bounded between $(0, 1]$ for $d \in [0, \infty)$ (Fig. 3).

For the players' utility functions, we use power utility functions[50] of the form:

$$u_a(x) = (z_a + x)^{\beta_a} \qquad u_d(x) = (z_d + x)^{\beta_d},$$

where the risk-preference parameters for the AD, β_a and $\beta_d > 0$ are parameters that primarily affect the curvature of the utility function. Finally, the terms z_a and z_d are large positive constants introduced so that $z_a + x$ and $z_d + x$ are always positive and well defined especially when β_a and $\beta_d \in (0, 1)$. In addition, the use of z_a and z_d gives flexibility in the functional form estimation process and could potentially be interpreted as initial wealth (or endowment) if it makes sense in the context being studied. An interesting and useful feature of the power utility function is that it covers the three main categories of risk preferences that we want to investigate. In particular, we are able to cover risk-averse $(0 < \beta < 1)$, risk-neutral $(\beta = 1)$, and risk-seeking $(\beta > 1)$ behaviors.

For sensitivity analyses, we focus on the changes that happen to these three variables: (i) defender's deterrence effort $\bar{d}$, (ii) defender's optimal effort d^*, and (iii) attacker's optimal effort a^*. In particular, we examine these variables as the following seven parameters vary: (i) defender's target valuation v_d, (ii) defender's cost coefficient c_d, (iii) defender's risk-preference parameter β_d, (iv) attacker's target valuation v_a, (v) attacker's cost effectiveness c_a, (vi) attacker's risk-preference parameter β_a, and (vii) defense effectiveness λ. The changes in the equilibrium behavior of the players are captured in the one-way sensitivity plots in Fig. 4 that vary only one parameter at a time while holding all other parameters equal to the baseline case.

The plots in Fig. 4 show several important variables including the two equilibrium solutions d^* and a^*. The baseline values are highlighted by the solid vertical line, while the critical point when the attacker strategy changes is highlighted by the dashed line. In Figs. 4(a) and 4(e), we note that the equilibrium investment of the defender increases, and then stays constant as the target valuation of the defender and attacker, respectively, increases. For the defender, we see that she/he is prompted to invest more to protect the resource as its valuation increases. The case for the attacker (Fig. 4(e)) follows the result provided in Proposition 2(ii), which implies that more effort is required from the defender to deter an attacker as the target valuation increases. This result holds irrespective of the attacker's risk preference.

In analyzing the impact of costs, Fig. 4(b) shows that the defender would invest less when her/his cost increases. This reduced investment may prompt an attacker to attack and the overall expected utility of the defender would then decrease. Hence, a defender may want to later focus her/his attention on mitigating this risk by trying to improve other aspects of defense (e.g., improving the effectiveness of defense λ) when costs are beyond her/his control. On the other hand, when c_a increases, Fig. 4(f) shows that $\bar{d}$ will decrease and approach zero at a point where the attacker is worse off attacking, irrespective of the defender's investment level. To some extent, if governments are able to affect the cost of an attack; e.g., making it more difficult and costly to launch an attack (e.g., increased cost of materials and components for bombs and increased cost for successfully moving resources), the overall defense effort may be significantly reduced.

Related to the risk-preference parameters, Figs. 4(c) and 4(g) provide some interesting results. Here, we see that a more risk-seeking (less risk-averse) defender would defend less although she/he is certain that attack would happen. This is interesting because we would expect that the certainty of the attack makes the defender invest more, but that does not necessarily happen. The reason is that, the defender knows that the high risk-seeking behavior of

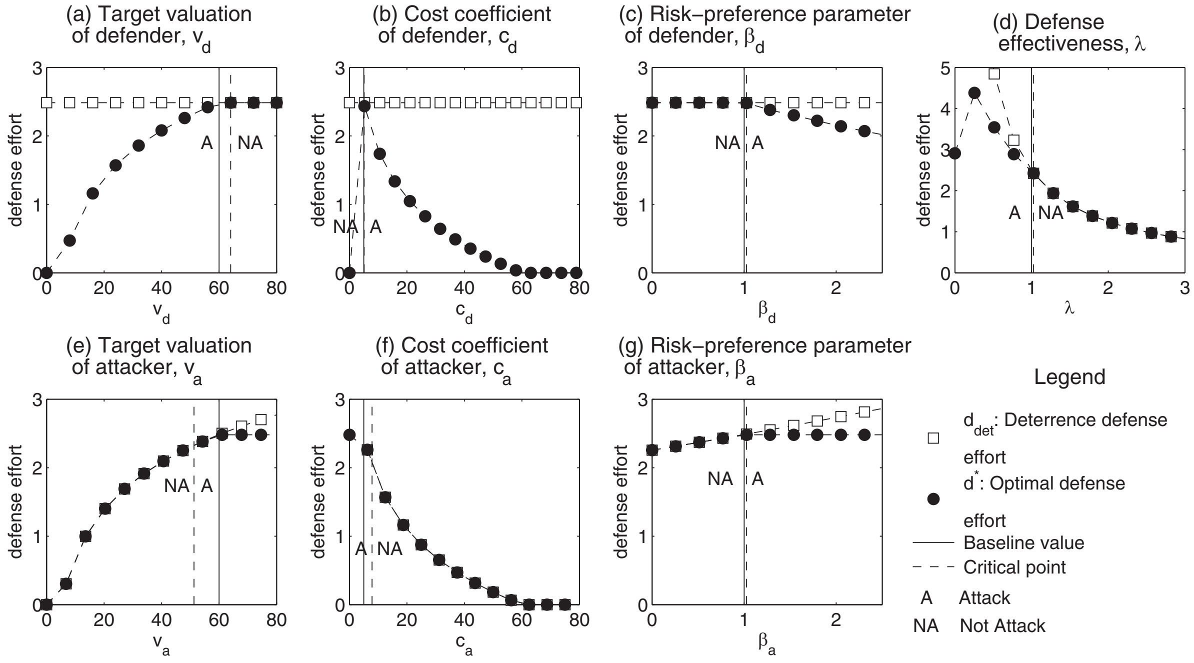

Fig. 4. One-way sensitivity analysis of attacker's equilibrium response (a^*), optimal defense effort (d^*), and deterrence level ($\bar{d}$), with respect to the parameters used in the CDDA model. Regions marked with A and NA refer to the regions for which it is optimal for the attacker to "Attack" and "Not Attack," respectively. Baseline values: $\lambda = 1$, $z_a = z_d = 100$, $v_a = v_d = 60$, $c_a = c_d = 5$, and $\beta_a = \beta_d = 1$.

the attacker makes it very costly for her/his to deter the attack. Hence, the defender "gambles" on the outcome of the attack rather than investing a lot of resources up front. Fig. 4(g) provides an illustration of Proposition 2(i), where $\bar{d}$ increases when facing a more risk-seeking (less risk-averse) attacker.

Finally, Fig. 4(d) focusing on the defense effectiveness parameter λ shows that $\bar{d}$ decreases in λ. This happens because an increase in λ decreases the probability of a successful attack making it more unlikely for an attacker to get a high expected utility from attacking. In terms of the equilibrium level d^*, we see that d^* initially increases, and then eventually decreases. Although the very high success probability of attack at very low values of λ forces the defender not to invest, the increased chance of unsuccessful attacks when λ increases encourages the defender to invest more. However, at higher values of λ, the increase in expected returns from defense is overcome by the significant increase in the cost of investing, leading the defender to invest less. Most of the time, this parameter is beyond the control of both players. If this parameter can be adjusted as well (e.g., by technology investments; see Jose and Zhuang[6]), then this could also be used as a powerful deterrence tool.

It is important to mention here that despite using very simple but reasonable utility functions, it is not possible to derive a closed-form solution for d_{int} and d^*. Hence, we analyzed a few more baseline scenarios to see if the d_{int} follows the same trend as in Fig. 4. The plots are given in the Appendix. It follows from Fig. A1 in the Appendix that due to the highly nonlinear form of the closed-form expression of $\frac{dd_{int}}{d\beta_d}$, it does not follow a specific trend, and hence it cannot be inferred whether d_{int} always follows the same decreasing trend as in Fig. 4. However, in real applications, nonavailability of a closed-form solution of d_{int} does not necessarily hinder the decision-making process of the defender because it may be possible to reasonably estimate the defender's and the attacker's equilibrium responses numerically, or simply use these examples to understand which scenario or realm the problem belongs to.

3.3.2. Model Comparison

We study in this subsection the usefulness of the new model with risk preferences proposed in this article. We define the utility of the model as the difference between the defender's expected damages between the model in Section 3.1 and a model in

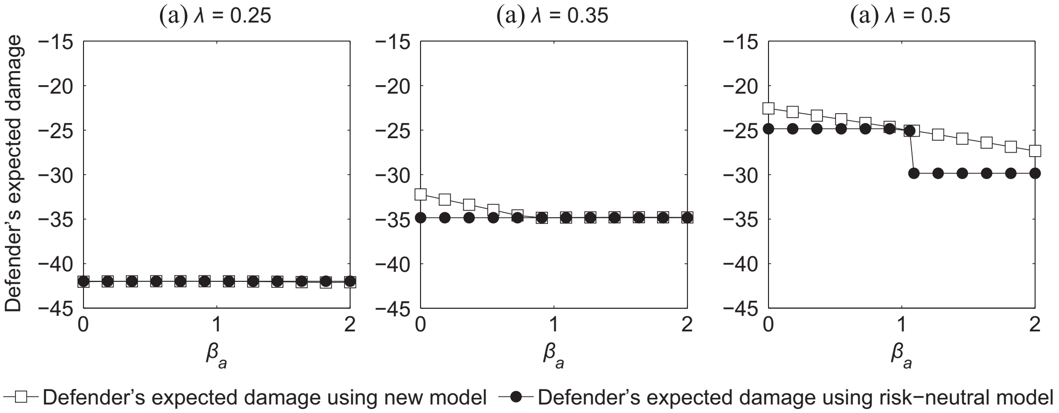

Fig. 5. One-way sensitivity analysis to study the impact of the risk-preference parameter β_a on the difference in expected damage between a CDDA model that takes into account risk preferences (new model) and another that does not (risk-neutral model). Baseline values: $z_a = z_d = 100$, $v_a = v_d = 60$, $c_a = c_d = 5$, and $\beta_d = 1$.

which the defender incorrectly believes that the attacker is risk neutral and acts accordingly. Using the same baseline parameter values as in Section 3.3.1, we perform one-way sensitivity analyses to study the impact of the risk-preference parameter β_a on the utility of the model, as shown in Fig. 5.

We present the baseline case of a risk-neutral defender. The expected damage of the defender is shown in terms of the expected costs, which explains the negative values. For all the values of λ considered here, the difference between the expected values of the two models is zero when $\beta_a = 1$; i.e., the perceived risk-preference level of the attacker is correct.

Fig. 5(a) shows that when the defender's defense effectiveness is low (e.g., $\lambda = 0.25$), the new model's performance is comparable to that of a risk-neutral model, for the range of β_a considered. The difference between the expected damages of the two models is zero because when the defense effectiveness is too low, the certainty of attack and the success rate of attack are high. Hence, the defender is better off by investing d_{int} (an interior solution, which is independent of β_a because of the Boolean nature of the attack).

Fig. 5(b) shows the case when the defense effectiveness is slightly higher (e.g., $\lambda = 0.35$). When $\beta_a < 1$, a defender using a risk-neutral model for the attacker would prepare more for an attack and hence incur higher expected costs of defending than a defender using the new model that correctly considers risk preferences. The difference in expected damage is zero for $\beta_a > 1$ because in such cases the defender is better off by investing d_{int}, which is independent of β_a. Fig. 5(c) shows that for higher values of λ (e.g., $\lambda = 0.5$), when $\beta_a < 1$, the difference is positive because the defender's investment reaches the maximum, $\bar{d}$. When $\beta_a > 1$, the defender using the risk-neutral model for the attacker would defend less than the level required to deter the attack. Hence, attack is certain and the defender's expected damage is higher. On the other hand, the defender using the new model would be able to deter the attack, so her/his expected damage is lower.

We would expect similar results when the defender is risk averse or risk seeking because expected damage is independent of her/his risk preference. From Fig. 5, the new model gives lower expected damage if the true type of the attacker is risk seeking than when he/she is risk averse. Also, the new model does not give considerably less expected damages for very low values of defense effectiveness λ. This happens because when the attack is more likely to be successful, the defender would not try to deter the attack and choose the interior solution, which is independent of β_a. Hence, except in the case when defense effectiveness is very low, the defender is expected to incur losses if she/he uses a risk-neutral model.

This example illustrates by how much our model that correctly considers risk preferences could outperform a risk-neutral model. For example, the sensitivity analysis in Fig. 5 could be used to determine the threshold value of defense effectiveness λ above which the new model performs better than the risk-neutral model against risk-averse as well as

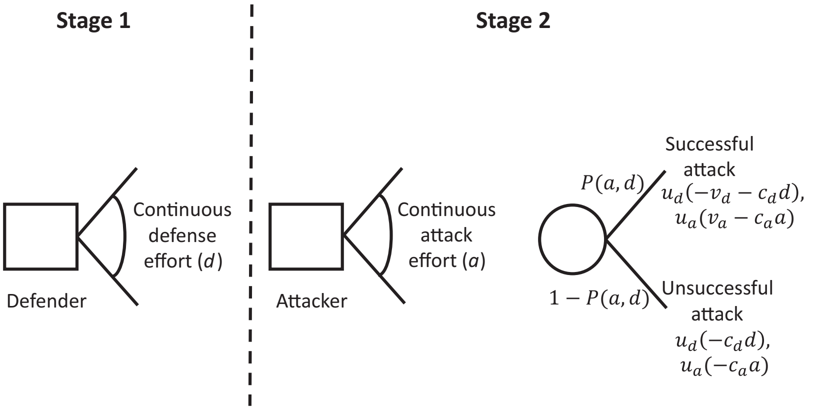

Fig. 6. Sequence of moves in the AD game (CDCA model) with the players' utilities.

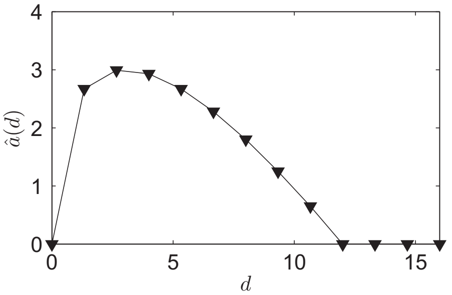

Fig. 7. Attacker's best response $\hat{a}(d)$ as a function of defender's investment d, in the CDCA model. Baseline values: $z_a = z_d = 100$, $v_a = v_d = 60$, $c_a = c_d = 5$, and $\beta_a = \beta_d = 1$.

risk-seeking attackers. For the baseline values considered, when $\lambda = 0.35$ (moderate defense effectiveness) the new model outperforms the risk-neutral model only against a risk-averse attacker, whereas when $\lambda = 0.5$ (high defense effectiveness) the new model outperforms the risk-neutral model against risk-averse and risk-seeking attackers.

These results suggest that users of AD models could value risk preferences less in certain situations but should also be aware of the potential savings/losses that could be incurred in situations where these models yield substantial differences.

4. CONTINUOUS DEFENSE CONTINUOUS ATTACK (CDCA) MODEL

4.1. Model

The model that we present here is an extension of the CDDA model in Section 3. The main difference from the CDDA model is that the attacker is able to choose from a continuous level of attack effort $a \in [0, \infty)$ that maximizes his/her expected utility. The modified game tree is given in Fig. 6. Since it is reasonable to say that the defender's and the attacker's efforts determine whether the attack is successful or not, we need to take this into account when assessing the probability of successful attack. We use the contest success function of the form $P(a, d) = \frac{a}{a+d}$.[51] This function is increasing in a, decreasing in d, and bounded between 0 and 1, $\forall a, d \geq 0$.

By backward induction, we begin by examining the best response of the attacker. Observing the defense level d, the attacker chooses $a \geq 0$ that maximizes his/her expected utility $U_a(a, d)$. His/her optimization problem is: $\max U_a(a, d) = P(a, d)$ $u_a(v_a - c_a a) + (1 - P(a, d))u_a(-c_a a) = \frac{a}{a+d} u_a(v_a - c_a a) + \frac{d}{a+d} u_a(-c_a a)$. The attacker's best response function $\hat{a}(d)$ is obtained using the necessary first-order condition $\frac{\partial}{\partial a} U_a(a, d) = 0$. That is,

$$\hat{a}(d) = \arg\max_a \left(\frac{a}{a+d} u_a(v_a - c_a a) + \frac{d}{a+d} u_a(-c_a a) \right). \tag{4}$$

Hence, the defender's equilibrium investment is $d^* = \arg\max_d U_d(\hat{a}(d), d)$ and the attacker's equilibrium investment is $a^* = \hat{a}(d^*)$. Finding a general analytical solution for $\hat{a}(d)$, a^*, or d^* is not possible, and the following sections discuss how the situation could be analyzed further in such cases.

4.2. Numerical Illustration and Sensitivity Analysis

For the purpose of illustrating insightful scenarios, we use the same functional forms for utility as in Section 3.3. Under power utility $u_a(x) = (z_a + x)^{\beta_a}$,

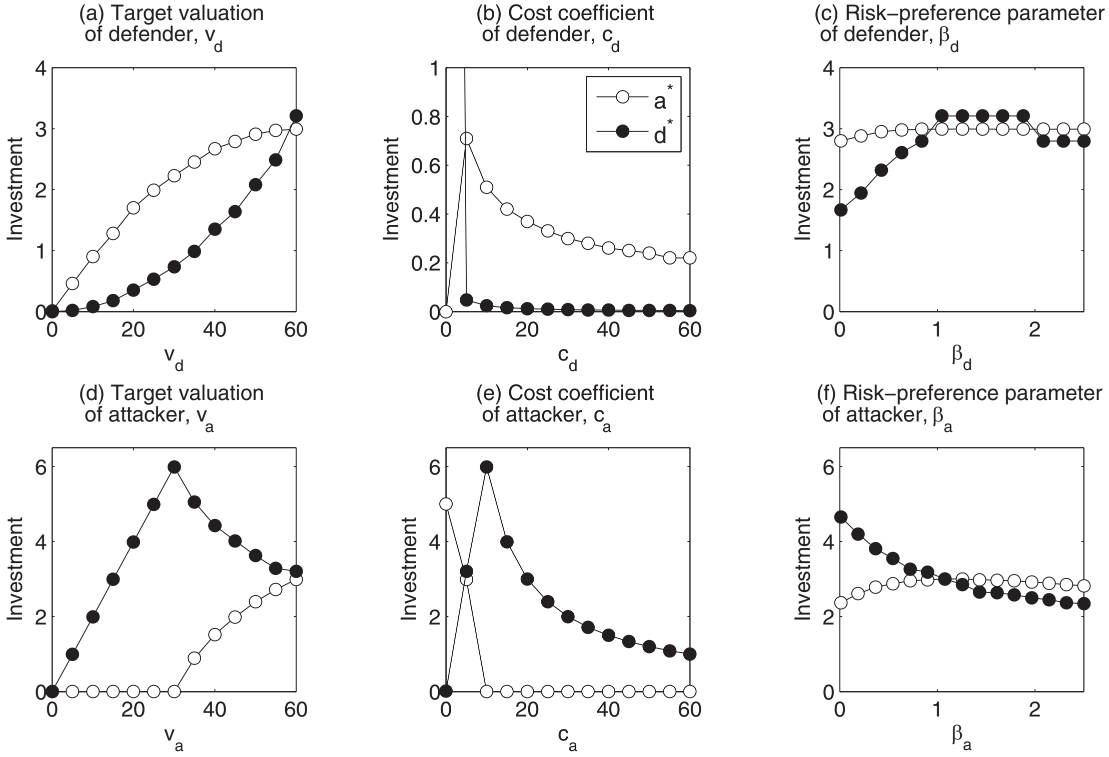

Fig. 8. One-way sensitivity analysis of the equilibrium investments of attacker (a^*) and defender (d^*) with respect to the parameters used in the CDCA model. Baseline values: $z_a = z_d = 100$, $v_a = v_d = 60$, $c_a = c_d = 5$, and $\beta_a = \beta_d = 1$.

Equation (4) becomes:

$$\hat{a}(d) = \arg\max_a \left(\frac{a}{a+d}(z_a + v_a - c_a a)^{\beta_a} \right. \quad (5)$$
$$\left. + \frac{d}{a+d}(z_a - c_a a)^{\beta_a} \right).$$

Closed-form solutions do not exist for $\hat{a}(d), a^*$, and d^* due to the properties of the general power form utility function, as mentioned in Section 3.2. Hence, we study the behavior of $\hat{a}(d)$, a^*, and d^* to observe possible trends and derive insights.

Fig. 7 shows that the best response of the attacker first increases and then decreases in the defender's investment d, and approaches and stays at zero for high values of d.

Fig. 8 illustrates the changes in the equilibrium responses (a^* and d^*) as the parameters $v_a, v_d, c_a, c_d, \beta_a$, and β_d change one at a time, keeping all others at the baseline values. For ease of comparison, we use the same baseline values that are used in the sensitivity analysis of the CDDA model in Section 3.3.1 (Fig. 4).

Due to diminishing marginal expected utility of attacking a defender's valuable target, a^* increases in v_d and then stabilizes (Fig. 8(a)). This behavior is comparable to a^* in Fig. 4(a). However, d^* exponentially increases in v_d in Fig. 8(a) in contrast to the marginally decreasing d^* in Fig. 4(a) due to the possibility of deterrence induced by the Boolean nature of attack in the CDDA model. It is optimal for the defender to increase her/his investment as the attacker's valuation of his/her target (v_a) increases (Fig. 8(d)), and this keeps the attack completely deterred until a particular value of v_a (as observed in Fig. 4(e)). However, the defender is better off by decreasing her/his efforts when v_a increases any further.

Interestingly, both the attacker and the defender invest more at very low values for the cost parameter and invest significantly less when costs are very high (Figs. 8(b) and (e)). In fact, the attacker is deterred completely when the cost of attack is significantly high (Fig. 8(e)). Another interesting observation is that in Fig. 8, a^* in Fig. 8(b) is very similar to d^* in Fig. 8(e). This is surprising because one would not expect so much symmetry in a sequential game.

In addition, the trends of d^* are different in Figs. 8(b) and 8(e), but still similar in Figs. 4(b) and 4(f).

The attacker's response (a^*) to changes in β_d and β_a is similar (Figs. 8(c) and 8(f)). However, deterrence is absent in these cases, which contrasts with the discrete case where a risk-neutral (risk-averse) attacker is deterred against a risk-averse (risk-neutral) defender (Figs. 4(c) and 4(g)).

In summary, the analysis here shows various scenarios in which there could be similarities/dissimilarities between the results from the CDDA and the CDCA models. Solely by extending the attack effort from discrete to continuous, significant variation is observed in the results. Thus, understanding the attacker's decision-making process could be a critical step for the defender in drafting more effective defense strategies. Optimal preemptive defense strategies against an attacker with continuous defense capabilities could be quite different from those against an attacker with discrete attack capabilities.

5. CONTINUOUS DEFENSE CONTINUOUS ATTACK - INCOMPLETE INFORMATION (CDCAII) MODEL

One realistic challenge in modeling risk preferences is determining what level or type of risk attitude to incorporate. In many terrorism and counterterrorism contexts, it is difficult to estimate specific forms of utility or estimate risk-preference parameters. For example, the defender might be uncertain about the attacker's risk attitudes and other parameters. In some contexts, it may be possible to have a rough estimate of players' risk preferences through revealed preferences that can be measured by specific actions taken in the past (e.g., Phillips[36–38]). Other approaches to estimation could be interviewing subject-matter experts.

We model this commonly encountered setting where the defender is uncertain about the attacker's risk preference by extending our model to an incomplete information model in which the players have some beliefs instead of the precise knowledge about their opponent's type. As the second-mover, the attacker has the advantage of observing the defender's actions. It is also very likely for the attacker to be much more informed about the defender than vice versa, because the defender (such as a government entity) is often mandated by transparency laws to divulge a significant amount of information (e.g., defense budget) to the public.

5.1. Model

In this section, we use abbreviations RA, RN, and RS to represent risk-averse, risk-neutral, and risk-seeking behaviors, respectively. In the model considered here, the defender has certain beliefs about the risk preference of the attacker, which is that the attacker could be RA with probability p, RN with probability q, and RS with probability $1 - p - q$. We extend the CDCA model in Section 4 to develop the CDCAII model as follows. The attacker's best response function is $\hat{a}(d) = \arg\max_a U_a(a, d)$. The defender's equilibrium investment is:

$$\begin{aligned} d^* = \arg\max_d (p \cdot U_d(\hat{a}_{RA}(d), a) \\ + q \cdot U_d(\hat{a}_{RN}(d), a) \\ + (1 - p - q) \cdot U_d(\hat{a}_{RS}(d), a)), \end{aligned} \tag{6}$$

where $\hat{a}_{RA}(d)$, $\hat{a}_{RN}(d)$, and $\hat{a}_{RS}(d)$ represent the best responses of a risk-averse, risk-neutral, and risk-seeking attacker as perceived by the defender, respectively. The attacker's equilibrium investment is $a^* = \hat{a}(d^*)$.

5.2. Numerical Illustration and Sensitivity Analysis

Although the defender is uncertain about the attacker's risk preference, the attacker has complete knowledge of the defender's risk preference. Hence, the attacker's best response function in this case is the same as in Fig. 7.

Considering a discrete setting where the defender believes that the attacker is RA, RN, or RS with probabilities p, q, and $1 - p - q$, respectively, the defender's expected utility is calculated as the probability-weighted sum of three utilities (calculated by considering the attacker as RA, RN, and RS), each weighted by the respective probability (p, q, or $1 - p - q$). Using the same functional forms of utility and baseline values as in Sections 3.3 and 4.2, we show in Figs. 9–11 how the equilibrium investment of an RA, RN, and RS defender (d^*), respectively, and that of an attacker (a^*) changes as the defender's beliefs change. In cases where the attacker or defender (or both) is (are) considered not to be RN, the risk preference values are set at 0.5 and 2.0 for RA and RS behavior, respectively. Since a continuous range of risk preference values is not used, discrete step values are obtained for a^* and d^*. In all cases, the defender's investments are identical for all three types of attackers, which makes sense because

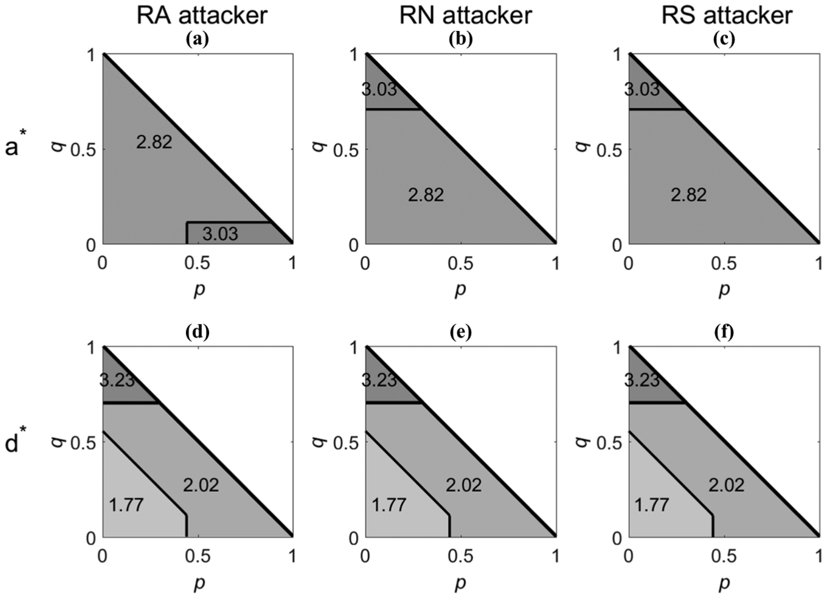

Fig. 9. Sensitivity analysis of equilibrium investments of a risk-averse (RA) defender (d^*) and an attacker (a^*) with respect to the parameters p and q. Baseline values: $v_a = v_d = 60$, $c_a = c_d = 5$, and $\beta_d = 0.5$.

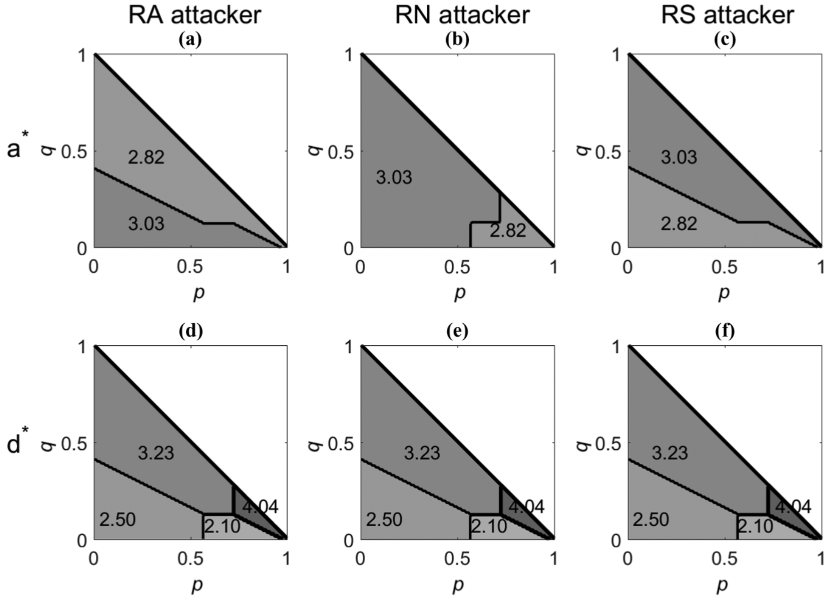

Fig. 10. Sensitivity of equilibrium investment of a risk-neutral (RN) defender (d^*) and an attacker (a^*) with respect to the parameters p and q. Baseline values: $v_a = v_d = 60$, $c_a = c_d = 5$, and $\beta_d = 1$.

the defender does not know the true type of the attacker.

First, an RA defender invests the most when she/he strongly believes that the attacker is RN, and the least when she/he strongly believes that the attacker is RS (Figs. 9(d)–(f)). An RN defender invests the most when she/he strongly believes that the attacker is RA and weakly believes that the attacker is RN; and less when she/he believes that the attacker is RS (Figs. 10(d) –(f)). This is comparable to Fig. 8(f) in which d^* decreases in β_a. An RS defender (Figs. 11(d)–(f)) invests the most when she/he weakly believes that the attacker is RS; except when her/his beliefs of the attacker being RA and RN are high and low, respectively (when she/he invests the least).

When facing an RA defender, the RA and the RN attackers invest the most when the defender's belief about his/her risk preference is accurate (Figs. 9(a) and 9(b)). Against any type of defender,

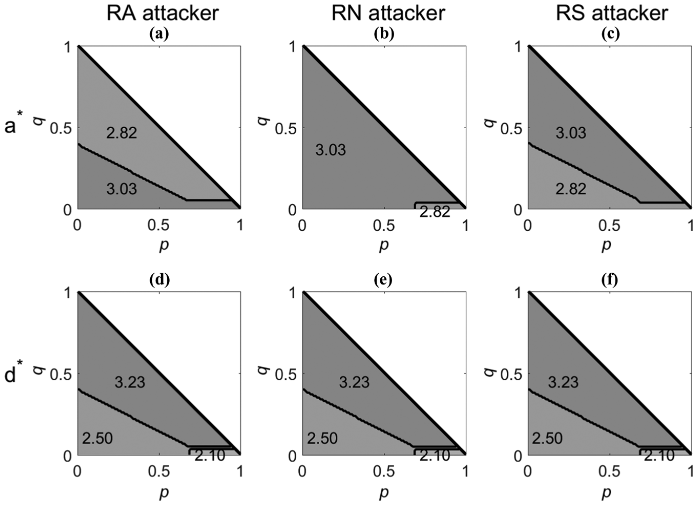

Fig. 11. Sensitivity of equilibrium investment of a risk-seeking (RS) defender (d^*) and an attacker (a^*) with respect to the parameters p and q. Baseline values: $v_a = v_d = 60$, $c_a = c_d = 5$, and $\beta_d = 2$.

an RS attacker invests the most when the defender invests the most (Figs. 9(c) and 9(f), 10(c) and 10(f), and 9(c) and 9(f)). Against an RN defender (Fig. 10), an RA attacker invests less in response to larger investments from the RN defender; however, an RS attacker does the opposite. Also, a^* of an RN attacker is higher for a broader range of p and q than a^* of an RA or an RS attacker, which can be compared to Fig. 8(f) in which a^* is higher when $\beta_a = 1$ than when $\beta_a \neq 1$.

An RN attacker invests less when the defender has a wrong belief about the attacker's risk-preference type, despite the large difference in the possible defense investments (2.10 or 4.04). The attacker's response against an RS defender (Fig. 11) follows a pattern similar to that against an RN defender: An RA attacker invests less in response to larger investments from the RN defender; however, an RS attacker does the opposite.

The illustrated models in Figs. 9–11 highlight the impact of incomplete information about a player's risk-preference types. These are useful in AD games because they can significantly affect the equilibrium responses of the players. The CDCAII model presented here addresses the difficult issue of estimating the level of risk preferences but still provides insights into how results would change based on incorrect belief about the attacker's risk preference type.

6. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this article, we consider a sequential, single-period, single-target AD game, where the defender preemptively invests in defense and the attacker chooses whether to attack or not. Here, the effect of players' risk preferences on the equilibrium behavior of these players is analyzed, focusing on the notion of deterrence, and these results are presented analytically, numerically, and graphically. Numerical illustrations and sensitivity analysis of continuous attack investment levels and uncertainty in the defender's beliefs about the attacker's risk preference are also provided. One key contribution of this article is the identification of specific scenarios in which the defender using our model would be better off than a defender using a risk-neutral model similar to those used in most of the literature.

We find that this incorporation of risk preferences is appealing and that this would certainty strengthen the policymakers' and risk analysts' understanding of models. This incorporates a fundamentally recognized behavioral and economic principle that is often not considered in mathematical models such as AD games for the purpose of convenience. AD game models that incorporate risk preferences provide robustness to a recommendation or an analysis when the recommendation remains the same when parameters are changed. In cases where the solution and equilibrium behavior could significantly vary, it may be useful to inform decisionmakers and risk analysts of such possibilities.

In terms of future research directions, this work opens new questions and areas to be explored. One interesting question is how risk preferences propagate in multiperiod games (e.g., Cole and Kocherlakota[52] and Jose and Zhuang[6]). This puts forward the question of whether changes in deterrence solutions that are due to risk preferences can be sustained in equilibrium for multiperiod games. It would be of interest to understand how solutions may evolve if we also allow intertemporal changes in risk preferences. Another interesting extension would be to understand how risk preferences can also affect the solution in these games when players have multiple objectives. Keeney[53] and Keeney and von Winterfeldt[54] mention that multiple objectives would be a fertile area of research in risk analysis, and we believe that this area could further be enriched by incorporating the notion of risk preferences.

The next step to the model would be to find ways to validate the model and its predictions. This could perhaps be done through behavioral studies or experiments. Thereafter, we expect that incorporating other behavioral theories (e.g., prospect theory or regret theory) into the model could provide additional insights into other specific contexts and applications.

ACKNOWLEDGMENTS

This research was partially supported by the U.S. 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 U.S. 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. We thank the editors and anonymous referees for their helpful comments. The authors assume responsibility for any errors.

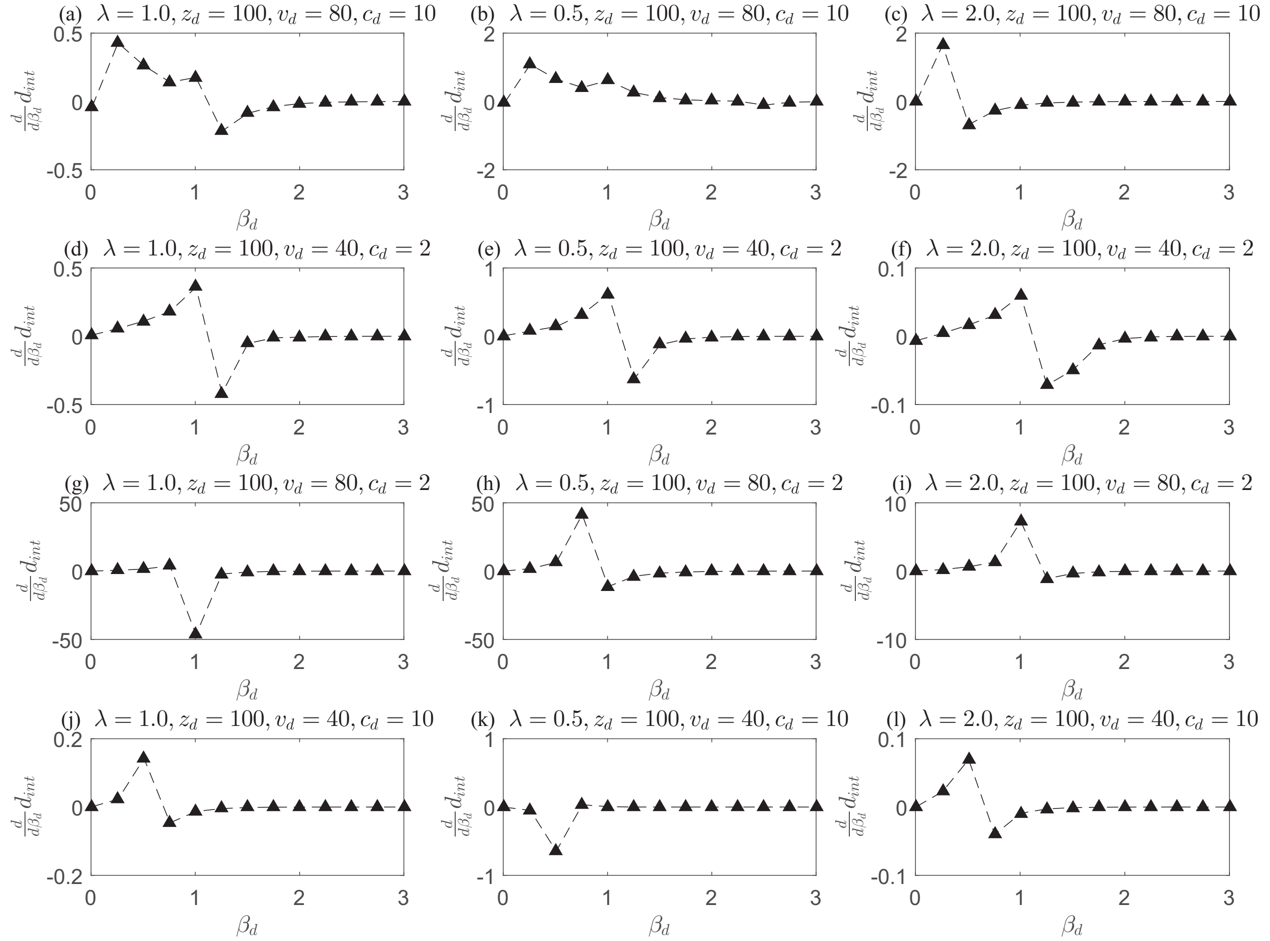

Fig. A1. Plot for slope of d_{int} with respect to β_d.

APPENDIX

We present here the explanation of the concluding paragraph in Section 3.3.1. As it is of interest to analyze the behavior of d_{int} with respect to β_d, we first derive an expression for the slope $\frac{dd_{int}}{d\beta_d}$. Then, we plot the variation of this slope with respect to β_d. If there is a certain type of behavior in d_{int} with respect to β_d, we may be able to say something about this function. For example, if we find a nonmonotonic behavior in certain cases, then we are able to show by contradiction that this function is nonmonotonic. The defender's utility function (when an attack happens) is:

$$U_d(d) = P(d)u_d(z_d - v_d - c_d d) + (1 - P(d))u_d(z_d - c_d d).$$

Assuming functional forms $P(d) = e^{-\lambda d}$ and $u_d(x) = (z_d + x)^{\beta_d}$ as done in Section 3, the utility function is:

$$U_d(d) = e^{-\lambda d}(z_d - v_d - c_d d)^{\beta_d} + (1 - e^{-\lambda d})(z_d - c_d d)^{\beta_d}.$$

By the implicit function theorem, we have:

$$\frac{dd_{int}}{d\beta_d} = -\frac{\partial(U_d(d_{int}))/\partial\beta_d}{\partial(U_d(d_{int}))/\partial d_{int}},$$

where d_{int} is the interior point solution for the defender's investment level. Using our functional forms, we obtain the expression in Equation (A.1) where $G = z_d - v_d - c_d d$ and $H = z_d - c_d d$.

This is an expression for the slope of the interior point solution d_{int} with respect to the defender's risk-preference parameter β_d. Fig. A1 shows the variation in the slope of the interior point solution $\frac{dd_{int}}{d\beta_d}$ with respect to the defender's risk-preference parameter β_d. It is seen that there is no specific trend that the slope follows, which means it cannot be generalized whether the d_{int} increases or decreases with respect to β_d, for all sets of baseline values. This could be due to the high nonlinearity and the nonelementary form of the slope for d_{int} with respect to β_d, even when a simple utility function is used.

$$\frac{dd_{int}}{d\beta_d} = \frac{\begin{array}{c}(c(1-e^{-d\lambda})(H)^{-1+\beta_d} + ce^{-d\lambda}(G)^{-1+\beta_d} + c(1-e^{-d\lambda})(H)^{-1+\beta_d}\beta_d\ln(H)- \\ e^{-d\lambda}(H)^{\beta_d}\lambda\ln(H) + ce^{-d\lambda}(G)^{-1+\beta_d}\beta_d\ln(G) + e^{-d\lambda}(G)^{\beta_d}\lambda\ln(G))\end{array}}{\begin{array}{c}(c^2(1-e^{-d\lambda})(H)^{-2+\beta_d}(-1+\beta_d)\beta_d + c^2e^{-d\lambda}(G)^{-2+\beta_d}(-1+\beta_d)\beta_d- \\ 2ce^{-d\lambda}(H)^{-1+\beta_d}\beta_d\lambda + 2ce^{-d\lambda}(G)^{-1+\beta_d}\beta_d\lambda - e^{-d\lambda}(H)^{\beta_d}\lambda^2 + e^{-d\lambda}(G)^{\beta_d}\lambda^2)\end{array}} \tag{A.1}$$

REFERENCES

1. U.S. Department of Homeland Security. FY 2016 DHS Budget-in-Brief, 2016. Available at: https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf, Accessed on December 26, 2016.
2. George AL, Smoke R. Deterrence in American Foreign Policy: Theory and Practice. New York, NY: Columbia University Press, 1974.
3. Hausken K. Strategic defense and attack of series systems when agents move sequentially. IIE Transactions, 2011; 43(7):483–504.
4. Zhuang J, Hausken K. The timing and deterrence of terrorist attacks due to exogenous dynamics. Journal of the Operational Research Society, 2009; 63(6):726–735.
5. Hausken K, Zhuang J. Governments' and terrorists' defense and attack in a T-period game. Decision Analysis, 2011; 8(1):46–70.
6. Jose VRR, Zhuang J. Technology adoption, accumulation, and competition in multi-period attacker–defender games. Military Operations Research, 2013; 18(2):33–47.
7. Zhuang J, Bier VM. Reasons for secrecy and deception in homeland-security resource allocation. Risk Analysis, 2010; 30(12):1737–1743.
8. Sandler T, Arce DG. Terrorism & game theory. Simulation & Gaming, 2003; 34(3):319–337.
9. Zhuang J, Bier VM. Balancing terrorism and natural disasters—Defensive strategy with endogenous attacker effort. Operations Research, 2007; 55(5):976–991.
10. Sandler T, Siqueira K. Games and terrorism recent developments. Simulation & Gaming, 2009; 40(2):164–192.
11. Cox Jr LAT. Game theory and risk analysis. Risk Analysis, 2009; 29(8):1062–1068.
12. Hamilton SN, Miller WL, Ott A, Saydjari OS. The role of game theory in information warfare. In Proceedings of 4th Information Survivability Workshop (ISW-2001/2002), Vancouver, BC, 2002. Available at: https://www.researchgate.net/publication/243774824_The_Role_of_Game_Theory_in_Information_Warfare.
13. Lye K, Wing JM. Game strategies in network security. International Journal of Information Security, 2005; 4(1–2):71–86.
14. Rao N, Poole S, Ma C, He F, Zhuang J, Yau D. Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. Risk Analysis, 2016; 36(4):694–710.
15. Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q. A survey of game theory as applied to network security. Pp. 1–10 in Proceedings of 43rd Hawaii International Conference on System Sciences (HICSS), Los Alamitos, CA: IEEE, 2010.
16. Hausken K, Levitin G. Review of systems defense and attack models. International Journal of Performability Engineering, 2012; 8(4):355–366.

17. Rios Insua D, Rios J, Banks D. Adversarial risk analysis. Journal of the American Statistical Association, 2009; 104(486):841–854.
18. Hausken K. Probabilistic risk analysis and game theory. Risk Analysis, 2002; 22(1):17–27.
19. Bier VM, Jr LAC, Azaiez MN. Why both game theory and reliability theory are important in defending infrastructure against intelligent attacks. Pp. 1–11 in Bier VM, Azaiez MN (eds). Game Theoretic Risk Analysis of Security Threats. New York: Springer, 2009.
20. Parnell GS, Smith CM, Moxley FI. Intelligent adversary risk analysis: A bioterrorism risk management model. Risk Analysis, 2010; 30(1):32–48.
21. Merrick J, Parnell GS. A comparative analysis of PRA and intelligent adversary methods for counterterrorism risk management. Risk Analysis, 2011; 31(9):1488–1510.
22. Rios Insua D, Rios J. Adversarial risk analysis for counterterrorism modeling. Risk Analysis, 2012; 32(5):894–915.
23. Levitin G, Hausken K. Defence and attack of systems with variable attacker system structure detection probability. Journal of the Operational Research Society, 2010; 61(1):124–133.
24. Shan X, Zhuang J. Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. European Journal of Operational Research, 2013; 228(1):262–272.
25. Weber EU, Johnson EJ. Decisions under uncertainty: Psychological, economic, and neuroeconomic explanations of risk preference. Pp. 127–144 in Glimcher PW, Fehr E, Camerer C, Poldrack RA (eds). Neuroeconomics: Decision Making and the Brain. New York, NY: Elsevier, 2008.
26. Bernoulli D. Exposition of a new theory on the measurement of risk. Econometrica [translation by L Sommer of D Bernoulli, 1738, Specimen theoriae novae de mensura sortis, Papers of the Imperial Academy of Science of Saint Peterburg 5, 175–192]. Econometrica: Journal of the Econometric Society, 1954; 22:23–36.
27. von Neumann J, Morgenstern O. Theory of Games and Economic Behavior. Princeton, NJ: Princeton University Press, 1944.
28. Bell DE. Regret in decision making under uncertainty. Operations Research, 1982; 30(1):961–981.
29. Loomes G, Sugden R. Regret theory: An alternative theory of rational choice under uncertainty. Economic Journal, 1982; 92(368):805–824.
30. Kahneman D, Tversky A. Prospect theory: An analysis of decision under risk. Econometrica, 1979; 47(2):263–292.
31. Bier VM, Oliveros S, Samuelson L. Choosing what to protect: Strategic defensive allocation against an unknown attacker. Journal of Public Economic Theory, 2007; 9(4):563–587.
32. Pratt JW. Risk aversion in the small and in the large. Econometrica, 1964; 32(1/2):122–136.
33. Arrow KJ. Essays in the Theory of Risk-Bearing. Chicago, IL: Markham Publishing Co., 1971.
34. Holt CA, Laury SK. Risk aversion and incentive effects. American Economic Review, 2002; 92(5):1644–1655.
35. Stewart MG, Ellingwood BR, Mueller J. Homeland security: A case study in risk aversion for public decision-making. International Journal of Risk Assessment and Management, 2011; 15(5):367–386.
36. Phillips PJ. Applying modern portfolio theory to the analysis of terrorism. Defence and Peace Economics, 2009; 20(3):193–213.
37. Phillips PJ. The preferred risk habitat of Al-qa'ida terrorists. European Journal of Economics, Finance and Administrative Sciences, 2010; 12(23):21–33.
38. Phillips PJ. The end of Al-qa'ida: Rationality, survivability and risk aversion. International Journal of Economic Sciences, 2013; 2(1):61–81.
39. Pate-Cornell E, Guikema S. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. Military Operations Research, 2002; 7(4):5–20.
40. McLay L, Rothschild C, Guikema S. Robust adversarial risk analysis: A level-k approach. Decision Analysis, 2012; 9(1):41–54.
41. Bell MG, Kanturska U, Schmöcker JD, Fonzone A. Attacker–defender models and road network vulnerability. Philosophical Transactions of the Royal Society Series A, 2008; 366(1872):1893–1906.
42. Liu Y, Comaniciu C, Man H. Modeling misbehavior in ad hoc networks: A game-theoretic approach for intrusion detection. International Journal of Security and Networks, 2011; 1(3/4):243–254.
43. Yin Z, Jain M, Tambe M, Ordónez F. Risk-averse strategies for security games with execution and observational uncertainty. Pp. 758–763 in Proceedings of 25th AAAI Conference on Artificial Intelligence, San Francisco, CA, 2011.
44. Qian Y, Haskell WB, Tambe M. Robust strategy against unknown risk-averse attackers in security games. Pp. 1341–1349 in Proceedings of 14th International Conference on Autonomous Agents and Multiagent Systems, Istanbul, Turkey, 2015.
45. von Stackelberg H. Marktform und gleichgewicht. Vienna, Austria: Julius Springer, 1939.
46. Shan X, Zhuang J. Cost of equity in homeland security resource allocation in the face of a strategic attacker. Risk Analysis, 2013; 33(6):1083–1099.
47. Willis HH, Morral AR, Kelly TK, Medby JJ. Estimating Terrorism Risk. Santa Monica, CA: RAND Corporation, 2006.
48. Dixit A, Skeath S, Reiley D. Games of Strategy. New York, NY: WW Norton & Company, 2015.
49. Bier VM, Haphuriwatt N, Menoyo J, Zimmerman R, Culpen AM. Optimal resource allocation for defense of targets based on differing measures of attractiveness. Risk Analysis, 2008; 28(3):763–770.
50. Fishburn PC, Kochenberger GA. Two-piece von Neumann–Morgenstern utility functions. Decision Sciences, 1979; 10(4):503–518.
51. Skaperdas S. Contest success functions. Economic Theory, 1996; 7(2):283–290.
52. Cole HL, Kocherlakota N. Dynamic games with hidden actions and hidden states. Journal of Economic Theory, 2001; 98(1):114–126.
53. Keeney RL. Modeling values for anti-terrorism analysis. Risk Analysis, 2007; 27(3):585–596.
54. Keeney RL, von Winterfeldt D. A value model for evaluating homeland security decisions. Risk Analysis, 2011; 31(9):1470–1487.