Kent Academic Repository

Full text document (pdf)

Citation for published version

Wu, Di and Yang, Xiangbin and Peng, Rui and Wu, Shaomin (2020) Risk-attitude-based defense strategy considering proactive strike, preventive strike and imperfect false targets. Reliability Engineering and System Safety, 196 . p. 106778. ISSN 0951-8320.

DOI

https://doi.org/10.1016/j.ress.2019.106778

Link to record in KAR

Document Version

Author's Accepted Manuscript

Risk-attitude-based defense strategy considering proactive strike, preventive strike and imperfect false targets

Di Wu[a], Xiangbin Yan[b], Rui Peng[c*], Shaomin Wu[d]

[a]School of Management, Xi'an Jiaotong University, Xi'an, China

[b]Donlinks School of Economics and Management, University of Science and Technology Beijing, Beijing, China

[c]School of Economics & Management, Beijing University of Technology, Beijing, China

[d]Kent Business School, University of Kent, Canterbury CT2 7FS, United Kingdom

Abstract: This paper analyzes the optimal strategies for the attacker and the defender in an attack–defense game, considering the risk attitudes of both parties. The defender moves first, allocating its limited resources to three different measures: launching a proactive strike or preventive strike, building false targets, and protecting its genuine object. It is assumed that (a) launching a proactive strike has limited effectiveness on its rival and does not expose the genuine object itself, (b) a false target might be correctly identified as false, and (c) launching a preventive strike consumes less resources than a proactive strike and might expose the genuine object. The attacker moves after observing the defender's movements, allocating its limited resources to three measures: protecting its own base from a proactive strike or preventive strike, building false bases, and attacking the defender's genuine object. For each of the defender's given strategies, the attacker chooses the attack strategy that maximizes its cumulative prospect value, which accounts for the players' risk attitudes. Similarly, the defender maximizes its cumulative prospect value by anticipating that the attacker will always choose the strategy combination that maximizes its own cumulative prospect value. Backward induction is used to obtain the optimal defense, attack strategies, and their corresponding cumulative prospect values. Our results show that the introduction of risk attitudes leads the game to a lose-lose situation under some circumstances and benefits one party in other cases.

Keywords: OR in defense; imperfect false target; proactive strike; preventive strike; attack–defense game; cumulative prospect.

[*] Corresponding Author: pengruisubmit@163.com; pengrui1988@bjut.edu.cn.

1. Introduction

The defending of systems against strategic attackers has attracted much research in the last two decades (Levitin & Hausken, 2010; Levitin & Hausken, 2011; Peng, Levitin, Xie, & Ng, 2011). Typical measures used to enhance the system survivability include protecting the system directly, deploying false targets to distract to the attacker, and preventively striking the attacker's base (Gao, Yan, Liu, & Peng, 2019). The attacker, in response, can protect its base against a strike, deploy false bases to distract the defender, and attack the defender's genuine object (Wu, Xiao, & Peng, 2018). In an attack–defense game, the vulnerabilities of the attacker's base and the defender's genuine object are usually characterized by the Tullock model (Tullock, 2001). A common assumption used in existing research is that a preventive strike exposes the genuine object, making the deployment of false targets futile in this scenario. However, in reality, a preventive strike might only expose the genuine object with some probability. For example, imagine that a country at war builds a missile launching center and some false missile launching centers in order to confuse its enemy who has intention to attack the genuine missile launching center to destroy it. When a missile is launched from the genuine missile launching center to preventively strike the attacker's base, the attacker can only confirm which launching center is genuine if it can successfully confirm the origin of the missile. Except for in Wu et al. (2018), another restriction of existing research is that the disinformation action is adopted only by the defender. However, in practice, both parties might use disinformation to distract the opposition. Say, the attacker may also have a genuine missile launching center and some false centers. In Wu et al. (2018), the disinformation measures of both parties are assumed to be perfect, i.e. the opposing party cannot detect the false targets or bases as false. However, in practice, the opponent might be able to confirm that some false targets and bases are false if they acquire information from certain channels, e.g. even if they are similar in appearance, a false target or base usually has a different spectrum structure than the genuine object or base. If the opponent has a spy satellite that successfully takes pictures of the false target or base, and these pictures are then successfully interpreted by experts, then the false target could be confirmed.

In reality, there may be another optional movement for the defender known as proactive strike. A proactive strike will have limited effectiveness on its rival compared with preventive strike, consuming more resources and will not expose the genuine object itself. For instance, the probability of exposing a mobile missile launching station is much smaller than a fixed one. As such, the mobile missile launching station can play the role of a proactive striker. Hausken and Zhuang (2011) analyzed how a government allocates its resources between attacking to downgrade a terrorist's resources and defending against a terrorist attack. In our work, the defender can choose between proactive strike and preventive strike based on cumulative prospective value.

This paper relates to four streams of literature: intentional attack, vulnerability modeling, proactive strike or preventive strike and imperfect false targets. The intentional attack conducted by attackers aims to maximize the system vulnerability. Thus, to minimize its system vulnerability, the defender must take measures such as system element protection and the deployment of false elements. Zhuang and Bier (2007) applied game theory to identify equilibrium strategies for the attacker and defender in a fully endogenous model of resource allocation for countering terrorism. Shere and Cohen (2010) considered a defense allocation problem and employed a max-min method to solve it. Rios and Rios (2012) analyzed intentional attack terrorism through adversarial risk analysis, which deals with decision-making problems that involve intelligent opponents and uncertain outcomes. Hausken and Levitin (2012) conducted a review of the attack–defense game. Zhang and Ramirez-Marquez (2013) considered the protection strategy for critical infrastructures against intentional attacks, constructing a two-stage game model under incomplete information to obtain the optimal strategies. Foraker, Lee and Polak (2016) analyzed the optimal strategy for harbor defense using a min-max algorithm. Zhai, Ye, Peng, and Wang (2017) studied defense and attack strategies for a system with a common bus performance-sharing mechanism that is subject to intentional attacks. Oakes, Mattsson, Näsman, and Glazunov (2018) extended this work and obtained a system-based risk assessment framework for a critical infrastructure.

Many researchers concentrated on the different methods of modeling the vulnerability of objects in the attack–defense game. Traditionally, vulnerability refers to the inability of a system to withstand the effects of a natural or man-made disturbance. In our paper, vulnerability is the probability that the system cannot function under external attacks, i.e., a base's vulnerability after a defender's strike and target's vulnerability after an attacker's attack. Tullock's contest success model is the most commonly used model. For its specific description, see studies such as Bocchetti, Giorgio, Guida, and Pulcini (2009), Peng, Wu, and Zhai (2018), Peng, Zhai, and Levitin (2016) and Peng, Xiao, Guo, and Lin (2019). More recent vulnerability modeling methods include those that have been introduced into the reliability research community from other fields. Trucco, Cagno, Ruggeri, and Grande (2008) built a Bayesian belief network to model the maritime transport system by considering its different actors and their mutual influences. Li, Wang, Song, and Li (2016) analyzed an anti-terrorism issue based on the analytic hierarchy process to identify the key components of the overpass bridge in terrorist attacks, and prioritized a variety of possible attack means with multiple criteria. Jamshidi et al. (2017) found a better assessment method by introducing the innovative concept bid data into the traditional rail failure risk assessment. For a comprehensive review of risk management, see Aven (2016). However, few researchers have considered the risk attitudes of the decision makers in the attack–defense game, which can be incorporated using the cumulative prospect theory (CPT) (Liu, Fan, & Zhang, 2014).

Instead of only passively defending with genuine object protection and false target deployment, the defender can also take the initiative with a proactive strike or preventive strike. Here, the defender tries to destroy the attacker's base before the attacker launches their attack. Hausken and Zhuang (2011) described the basic concepts for an attack–defense game, considering preventive strikes in an infinite time period. Bier and Hausken (2011) presented a novel model capable of distinguishing between the effects of negative incentives and positive incentives for influencing the behavior of intelligent and adaptable adversaries. Hausken (2011c) considered the optimal resource distribution between attack and defense in a duel. Levitin and Hausken (2012) modeled this more precisely and found: (1) if the defender strikes preventively, the attacker's vulnerability depends both on its own protection and on the amount of resources the defender allocated to the strike; and (2) if the attacker survives, the object's vulnerability depends on the amount of resources the attacker then allocates to attacking the object. As for the proactive strike, Sandler and Siqueira (2010) modeled proactive and defensive policies with pseudo contest functions. They found that preemption is usually undersupplied. To the best of our knowledge, no prior paper compares the attack–defense game with both proactive and preventive strike.

Some papers considered the case where the false targets have a certain probability of being detected. Peng, Levitin, Xie, and Ng (2010) and Peng, Levitin, Xie, and Ng (2011) analyzed the optimal distribution of defense resources between protecting the genuine system elements and deploying imperfect false targets in simple series and parallel systems. Levitin and Hausken (2013) considered a question: is it wise to leave some targets unprotected? They introduced the concept of imperfect false targets. Xiao and Peng (2018) offered a comprehensive review of the tradeoff between imperfect false targets, protection and redundancy. However, none of these works incorporated the interaction between false targets and proactive strike or preventive strike.

In contrast to existing studies, this paper considers the use of both proactive strike or preventive strike and false targets. It assumes that a preventive strike can expose the genuine object with some probability. It also assumes that a false target is imperfect (i.e. it has a possibility of being detected). The defender has three different measures: launching a proactive strike or preventive strike, protecting the genuine object, and deploying false targets. The attacker also has three different measures: protecting its genuine base against a proactive strike or preventive strike, deploying false bases, and launching attacks to try to destroy the defender's genuine object. The contest has three potential outcomes: (1) the attacker's genuine base is destroyed by a proactive/preventive strike; (2) the attacker's genuine base survives a proactive/preventive strike and the defender's genuine object survives the attacker's attack; and (3) the attacker's genuine base survives a proactive/preventive strike and successfully destroys the defender's genuine object. To consider the risk attitudes of the defender and attacker, the CPT is used to calculate their cumulative prospect values (Kahneman and Tversky, 1979). Typically, the defender moves first, maximizing its cumulative prospect value by anticipating that the attacker will always choose the strategy combination that maximizes its own cumulative prospect value. The attacker moves after observing the movement of the defender. As far as the risk attitude is concerned, Hausken (2010) considered the risk attitude and found that the risk seeking by all agents is the worst scenario. In our work, similarly, we find that the introduction of risk attitudes will lead to a lose-lose situation when the defender is risk seeking. Hausken (2011a) considered an investment and production game and showed that if one participant has a higher unit cost of production, more fighting will occur. Similarly, Hausken (2011b) proved that high unit cost of safety effort will reduce both productive and safety effort, which finally reduces income. We obtain an opposite conclusion here. Our results perform that the high unit cost decreases the potential loss of both parties and the augment of resource makes both parties suffered.

Our work is specifically motivated by Levitin and Hausken (2012) and Wu et al. (2018). Levitin and Hausken (2012) assumed that a defender distributes its resources between passively defending an object and striking preventively against an attacker seeking to destroy the object. Moreover, if the defender decides to employ protection, it can further choose to build false targets to distract the attacker. Wu et al. (2018) extended the false target strategy to the attacker by assuming that the attacker can build false bases to decrease the vulnerability of its genuine base when the defender chooses to launch a preventive strike. However, neither of these papers considered the case where the false targets can be detected with a certain probability. Moreover, the proactive strike is taken into concern and compared with preventive strike to obtain the optimal defense strategy combination. In addition, they assumed that the objective function of both the defender and attacker is the vulnerability of the genuine object to be defended, which does not reflect the defender and attacker's respective risk attitudes. Differently, this paper introduces the CPT into the defense and attack model so that we can tune the parameters in the cumulative prospect value functions to reflect the different risk attitudes of the defender and attacker.

The major contributions of our paper are as follows:

- We consider the disinformation strategy for both parties, where the false bases and false targets have a certain probability of being detected by their rival.
- We assume that the preventive strike can uncover the genuine object with some probability. Instead, the proactive strike will consume more resources and will not expose the genuine object itself.
- The CPT is combined with the traditional Tullock model to better depict the risk attitudes of the defender and attacker. Both parties in the attack–defense game are concerned not only with the vulnerability of the defender's object, but also in maximizing their respective cumulative prospect values, which consider all possible outcomes.

We believe this to be the first paper that (a) incorporates CPT into an attack–defense game with disinformation strategies for both parties, (b) considers the random exposure of the genuine object by a preventive strike, and (c) compares between proactive strike and preventive strike in an attack–defense game with multiple options.

The rest of this paper is organized as follows. Section 2 describes the model. Section 3 studies the optimal numbers of bases and targets to attack (for the defender and attacker, respectively) for any given number of detected false bases or targets. In section 4, we employ the backward induction method to solve the optimal attack strategies for the attacker for all three possible outcomes. Section 5 analyzes the optimal strategies for the defender, who anticipates the response of the attacker. Section 6 discusses the impact that the exposure probability, detection probabilities and risk parameters have on the optimal strategies. Sensitivity analysis is also performed here, to compare the different strategy combinations under different parameters. Section 7 concludes the paper and discusses several possible directions for future work.

2. The model

Consider a defender who owns a single genuine object subjected to intentional attacks by an attacker. The defender distributes its resources, r, into three different movements: $rx(0 \le x \le 1)$ for a proactive strike with unit strike effort cost c_{pr} (or for a preventive strike with unit strike effort cost c_{ps}, where $c_{pr} > c_{ps}$), $r(1-x)y(0 \le y \le 1)$ for building false targets with unit cost c_{ft}, and $r(1-x)(1-y)$ for protecting the genuine object with unit protection effort cost c_{pt}. The attacker also distributes its resources, R, into three movements: $RX(0 \le X \le 1)$ for protecting its own base from a proactive strike (or a preventive strike) with unit protection effort cost C_{bp}, $R(1-X)Y(0 \le Y \le 1)$ for building false bases with unit cost C_{fb}, and $R(1-X)(1-Y)$ for attacking the genuine object with unit attack effort cost C_{at}. The probability of correctly detecting a false target is denoted by d_{ft}, and the probability of correctly detecting a false base is denoted by D_{fb}. We summarize all notations below.

Notations List

Notations	
C_{bp}	Unit effort cost for base protection
C_{fb}	Unit cost for false base
C_{at}	Unit attack effort cost for genuine object
c_{pr}, c_{ps}	Unit effort cost for proactive strike and preventive strike, respectively
c_{ft}	Unit cost for false target
c_{pt}	Unit effort cost for genuine object protection
R, r	Resources for the attacker and the defender, respectively
x, y	Resource allocation parameters of the defender on strike and false targets, respectively
X, Y	Resource allocation parameters of the attacker on base protection and false bases, respectively
D_{fb}, d_{ft}	Detection probability of false bases and false targets, respectively

d_{ex}	Probability of exposing genuine object by preventive strike
Q_d, Q_a	Number of attacked bases and attacked targets, respectively
k_{fb}, k_{ft}	Number of detected false bases or false targets, respectively
m_{pr}, m_{ps}, m_a	Contest intensity parameters for the genuine base (under proactive strike or preventive strike) and target, respectively
v_b, v_g	The vulnerability of the base and the genuine object, respectively
$p_{fb}(k), p_{ft}(k)$	Probability for detecting k false bases and targets, respectively
x_{ai}, x_{di}	Potential monetary outcomes for the attacker and the defender, respectively
p_i	Probability of each potential outcome
V_a, V_d	Prospect value of the attacker and the defender, respectively
$v(x_k)$	Value of the potential outcome
π_k^+, π_k^-	Decision weight for the value of the potential gain and loss, respectively
g, l, λ	Risk parameters
w^+, w^-	Weighting function for gains and losses, respectively
χ, δ	Weighting function parameters

In a two-period game of perfect information, the defender moves first and the attacker moves only after knowing the resource allocation of the defender. In this game, the CPT is used, and both the defender and the attacker try to maximize their own respective cumulative prospect values by considering different possible outcomes, i.e. the attacker chooses the attack strategy combination that maximizes its cumulative prospect value for any given defense strategy combination, and the defender maximizes its cumulative prospect value by anticipating that the attacker will always choose the strategy combination that maximizes its own cumulative prospect value. It is assumed that the preventive strike uncovers the defender's genuine object with probability d_{ex}.

When the attacker uses false bases, the defender distributes its proactive strike or preventive strike effort evenly into Q_d ($1 \le Q_d \le \lfloor R(1-X)Y/C_{fb} \rfloor + 1 - k_{fb}$) bases to maximize the vulnerability of the genuine base for the case where k_{fb} false bases are detected to be false, i.e. striking Q_d attacked bases evenly at the same time. The vulnerability of the genuine base, given it is a part of the Q_d attacked bases, can be modeled by the contest success function proposed by Tullock (2001):

$$v_b^{\sim} = \begin{cases} \dfrac{\left(rx/Q_d c_{pr}\right)^{m_{pr}}}{\left(RX/C_{bp}\right)^{m_{pr}} + \left(rx/Q_d c_{pr}\right)^{m_{pr}}} & \textit{proactive strike} \\ \dfrac{\left(rx/Q_d c_{ps}\right)^{m_{ps}}}{\left(RX/C_{bp}\right)^{m_{ps}} + \left(rx/Q_d c_{ps}\right)^{m_{ps}}} & \textit{preventive strike} \end{cases}, \tag{1}$$

where m_{pr} and m_{ps} are the contest intensity under proactive strike and preventive strike, $\left(rx/Q_d c_{pr}\right)$ and $\left(rx/Q_d c_{ps}\right)$ is the contest effort the defender takes by spending the corresponding resources on a proactive strike or preventive strike, and $\left(RX/C_{bp}\right)$ is the contest effort of the attacker in base protection. The contest intensity is an exogenous variable that does not rely on the movement of either the attacker or the defender. Following Tullock (2001), the contest intensity commonly derived from the history of warfare, denoting its impact on the vulnerability, where low intensity occurs if neither player can obtain a significant advantage; and high intensity occurs when one party owns significant advantage among the other.

As such, the vulnerability of the base given that k_{fb} false bases are detected is

$$v_b(Q_d, k_{fb}) = \frac{Q_d}{\left\lfloor R(1-X)Y/C_{fb} \right\rfloor + 1 - k_{fb}} \times v_b^{\sim}. \tag{2}$$

The first term on the right side of Eq. (2) illustrates the ratio of the attacked bases to the undetected bases. The defender chooses $Q_d^*(k_{fb}) = \arg\max(v_b(Q_d, k_{fb}))$.

Since the probability of correctly detecting k_{fb} false bases can be obtained by

$$p_{fb}(k_{fb}) = \begin{pmatrix} \left\lfloor \dfrac{R(1-X)Y}{C_{fb}} \right\rfloor \\ k_{fb} \end{pmatrix} D_{fb}^{\,k_{fb}} (1-D_{fb})^{\left\lfloor \frac{R(1-X)Y}{C_{fb}} \right\rfloor - k_{fb}}, \tag{3}$$

the unconditional vulnerability of the base is

$$v_b(Q_d, k_{fb}) = \sum_{k=0}^{\left\lfloor \frac{R(1-X)Y}{C_{fb}} \right\rfloor} p_{fb}(k_{fb}) v_b(Q_d(k_{fb}), k_{fb}). \tag{4}$$

If the attacker's base survives the strike, the attacker will try to destroy the genuine object of the defender. Considering that the genuine object might (or might not) be uncovered by the preventive strike whereas proactive strike will consume more resource but not uncover the genuine object, the vulnerability of the genuine object can be obtained by

$$v_g=\begin{cases}(1-v_b(Q_d^*))\displaystyle\sum_{0}^{\left\lfloor \frac{r(1-x)y}{c_{ft}}\right\rfloor} p_{ft}(k_{ft})v_g(Q_a^*(k_{ft}),k_{ft}) & \textit{proactive strike}\\ (1-v_b(Q_d^*))[d_{ex}\dfrac{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}}{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}+\left(r(1-x)(1-y)/c_{pt}\right)^{m_a}}+ & \\ & \textit{preventive strike}\\ (1-d_{ex})\displaystyle\sum_{0}^{\left\lfloor \frac{r(1-x)y}{c_{ft}}\right\rfloor} p_{ft}(k_{ft})v_g(Q_a^*(k_{ft}),k_{ft})] & \end{cases}, \qquad (5)$$

where $(1-v_b(Q_d^*))$ is the probability that the attacker survives the strike, and $\frac{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}}{\left(R(1-X)(1-Y)/C_{at}\right)^{m_a}+\left(r(1-x)(1-y)/c_{pt}\right)^{m_a}}$ is the destruction probability of the genuine object for the case where it is exposed by the preventive strike. In addition, the probability to detect k_{ft} as false targets can be obtained by

$$p_{ft}(k_{ft})=\binom{\left\lfloor \dfrac{r(1-x)\mathrm{y}}{c_{ft}}\right\rfloor}{k_{ft}} d_{ft}{}^{k_{ft}}(1-d_{ft})^{\left\lfloor \frac{r(1-x)\mathrm{y}}{c_{ft}}\right\rfloor-k_{ft}}, \qquad (6)$$

and

$$v_g(Q_a^*(k_{ft}),k_{ft})=\frac{Q_a^*(k_{ft})}{\left\lfloor r(1-x)y/c_{ft}\right\rfloor+1-k_{ft}}\cdot\frac{\left(R(1-X)(1-Y)/Q_a^*(k_{ft})C_{at}\right)^{m_a}}{\left(R(1-X)(1-Y)/Q_a^*(k_{ft})C_{at}\right)^{m_a}+\left(r(1-x)(1-\mathrm{y})/c_{pt}\right)^{m_a}} \qquad (7)$$

is the vulnerability of the genuine object if k_{ft} false targets are detected, where $Q_a^*(k_{ft})$ is the $Q_a(k_{ft})$ that maximizes $v_g(Q_a(k_{ft}),k_{ft})$ and m_a is the contest intensity.

For any given defender and attacker's resource allocation and a given number of detected false bases, the defender chooses the optimal number of bases to attack to maximize the base destruction probability. In addition, if the attacker survives the strike, for any given defender and attacker's resource allocation and for any number of false targets detected, the attacker chooses the optimal number of targets to attack to maximize the destruction probability of the defender's object. For a given defense strategy combination, the attacker chooses the resource allocation strategy that maximizes its cumulative prospect value by considering all possible outcomes of the contest, including: (1) if its base is destroyed; (2) if its base survives and the genuine target of the defender is not destroyed; and (3) if its base survives and the genuine target of the defender is destroyed. The monetary outcomes of the attacker corresponding to the three possible outcomes of the contest are denoted as x_{a1}, x_{a2} and x_{a3}, respectively. The defender chooses the resource allocation strategy that maximizes its cumulative prospect value by anticipating that the attacker always chooses the strategy combination that maximizes its own cumulative prospect value. Like the attacker, the monetary outcomes of the defender corresponding to the three possible outcomes of the contest are denoted as x_{d1}, x_{d2} and x_{d3}, respectively. The probabilities of the three outcomes of the contest are denoted as p_1, p_2 and p_3, respectively. Thus, the prospect values of the attacker and defender are given by

$$V_a = \sum_{v(x_{ak})\geq 0} v(x_k)\pi_k^+ + \sum_{v(x_{ak})<0} v(x_k)\pi_k^-; \tag{8}$$

$$V_d = \sum_{v(x_{dk})\geq 0} v(x_k)\pi_k^+ + \sum_{v(x_{dk})<0} v(x_k)\pi_k^-, \tag{9}$$

respectively, where $v(x_k)$ is the value of the potential outcome, π_k^+ is the decision weight for the value of the potential gain, and π_k^- is the decision weight for the value of the potential loss. According to Liu et al. (2014) and Wang, Fung, Li, and Pu (2017), $v(x_k)$ can be represented by

$$v(x_k) = \begin{cases} x_k{}^g & x_k > 0, \\ -\lambda(-x_k)^l & otherwise, \end{cases}, \tag{10}$$

where both g and l are exponent parameters and λ is the loss parameter. For $0 < g < 1$, the value function exhibits risk aversion over gains. For $0 < l < 1$, the function exhibits risk seeking over loss. Moreover, the loss-aversion factor, λ, should always be greater than one, since the individuals are essentially more sensitive to losses than gains. The decision weights for the gains and losses can be expressed by

$$\pi_k^+ = w^+(\sum_{j=k}^{n} p_j) - w^+(\sum_{j=k+1}^{n} p_j); \tag{11}$$

$$\pi_k^- = w^-(\sum_{j=1}^{k} p_j) - w^-(\sum_{j=1}^{k-1} p_j), \tag{12}$$

respectively, where w^+ and w^- denote the respective weighting functions for gains and losses. They are represented by

$$w^{+}(p)=\frac{p^{\chi}}{[p^{\chi}+(1-p)^{\chi}]^{1/\chi}}, \tag{13}$$

and

$$w^{-}(p)=\frac{p^{\delta}}{[p^{\delta}+(1-p)^{\delta}]^{1/\delta}}, \tag{14}$$

where both χ and δ are model parameters and can also be estimated through experiments. Note that $w^{+}(p)$ and $w^{-}(p)$ are monotonic and exhibit inverse S-shapes for some specific ranges (Jamshidi et al., 2017).

Through our deduction and model foundation we find that

$$p_1=v_b(Q_d^*), \tag{15}$$

$$p_2=1-v_b(Q_d^*)-v_g\left(X^*,Y^*\right), \tag{16}$$

and

$$p_3=v_g\left(X^*,Y^*\right). \tag{17}$$

In fact, it is reasonable to assume that $x_{a1}<0<x_{a3}$ and $x_{d1}<0<x_{d3}$. However, it is difficult to say whether x_{a2} and x_{d2} are positive or not. We can then rewrite the respective prospect value functions of the attacker and defender as

$$V_a=\begin{cases} x_{a3}{}^{g}\pi_3^{+}-\lambda(-x_{a2})^{l}\pi_2^{-}-\lambda(-x_{a1})^{l}\pi_1^{-}, & x_{a2}<0 \\ x_{a3}{}^{g}\pi_3^{+}-\lambda(-x_{a1})^{l}\pi_1^{-}, & x_{a2}=0, \\ x_{a3}{}^{g}\pi_3^{+}+x_{a2}{}^{g}\pi_2^{+}-\lambda(-x_{a1})^{l}\pi_1^{-}, & x_{a2}>0 \end{cases} \tag{18}$$

$$V_d=\begin{cases} x_{d1}{}^{g}\pi_1^{+}+x_{d2}{}^{g}\pi_2^{+}-\lambda(-x_{d3})^{l}\pi_3^{-}, & x_{d2}>0 \\ x_{d1}{}^{g}\pi_1^{+}-\lambda(-x_{d3})^{l}\pi_3^{-}, & x_{d2}=0. \\ x_{d1}{}^{g}\pi_1^{+}-\lambda(-x_{d2})^{l}\pi_2^{-}-\lambda(-x_{d3})^{l}\pi_3^{-}, & x_{d2}<0 \end{cases} \tag{19}$$

For any given (x,y), the attacker chooses its decision variables $(X^*,Y^*)=\arg\max(V_a)$. The defender chooses $(x^*,y^*)=\arg\max(V_d(X^*,Y^*))$.

We should mention that there is a special case where a preventive strike might not be chosen by the defender, i.e. $x=0$. Here, the attacker does not need to protect its base or use false bases, i.e. $X=0$ and $Y=0$.

3. Optimal Numbers of Bases and Targets to Attack

Since the movements of each party in this multi-period game are common knowledge, we use backward induction to solve the optimal strategies both for the attacker and for the defender. The specific deduction procedure is as follows. First, the defender chooses the optimal number of bases to attack to maximize the vulnerability of the attacker's genuine base under the given combination of x, X, Y and k_{fb}, which gives $Q_d^*(k_{fb}) = \arg\max\left(v_b\left(Q_d, k_{fb}\right)\right)$. Similarly, if the attacker survives the strike, it chooses the optimal number of targets to attack to maximize the vulnerability of the defender's genuine object under the given combination of x, y, X, Y and k_{ft}, which gives $Q_a^*(k_{ft}) = \arg\max\left(v_g\left(Q_a, k_{ft}\right)\right)$. Substituting the optimal $Q_d^*(k_{fb})$ into the V_a in Eq. (8), we find the optimal combination of $\left(X^*, Y^*\right) = \arg\max\left(V_a\right)$ under the given combination of (x, y) with all possible k_{fb} to obtain the optimal attack strategies. Finally, we substitute the optimal $Q_a^*(k_{ft})$ into V_d in Eq. (9) to find the optimal combination of $\left(x^*, y^*\right) = \arg\max\left(V_d\right)$ under the given combination of $\left(X^*, Y^*\right)$ with all possible k_{ft} to obtain the optimal defense strategies. The existence of optimal $Q_d^*(k_{fb})$ and $Q_a^*(k_{ft})$ are shown in Appendix A.

To better illustrate the results of our proposed model, we employ some numerical studies. We use the same parameter settings as those in Wu et al. (2018). Without loss of generality, in the benchmark we assume that the resources of the attacker and defender are equal and all unit costs are the same. The contest intensities are first designed to be the same, but later we will do some sensitivity analysis to study the influences of different parameters. We perform the numerical examples below with the following parameters:

$$r = R = 10, C_{bp} = C_{fb} = C_{at} = c_{ps} = c_{ft} = c_{pt} = 2, c_{pr} = 3, m_{ps} = m_{pr} = m_a = 2, D_{fb} = d_{ft} = d_{ex} = 0.5.$$

First, we analyze the optimal number of bases that the defender should attack. To avoid the tedious calculation, we only consider two different values for each decision parameter here: 0.3 for low resource allocation and 0.7 for high resource allocation. In the calculation of attacked bases, the related decision parameter of the defender is the portion of resources spent on the proactive strike or preventive strike, and the related decision parameters of the attacker are the portions of resources spent on protection and false bases. The implicit assumption here is that the defender can choose either a proactive strike or a preventive strike instead of employing a combination of them. Future work can relax this assumption. There will be eight possible cases, as shown in Fig. 1, for both proactive and preventive strikes.

Specifically, we should note that the optimal number of attacked bases remains the same under these two cases since the difference between unit cost of a proactive strike and a preventive strike is small under benchmark. We further find that when the unit effort cost for a proactive strike increases, the optimal number of attacked bases will decrease.

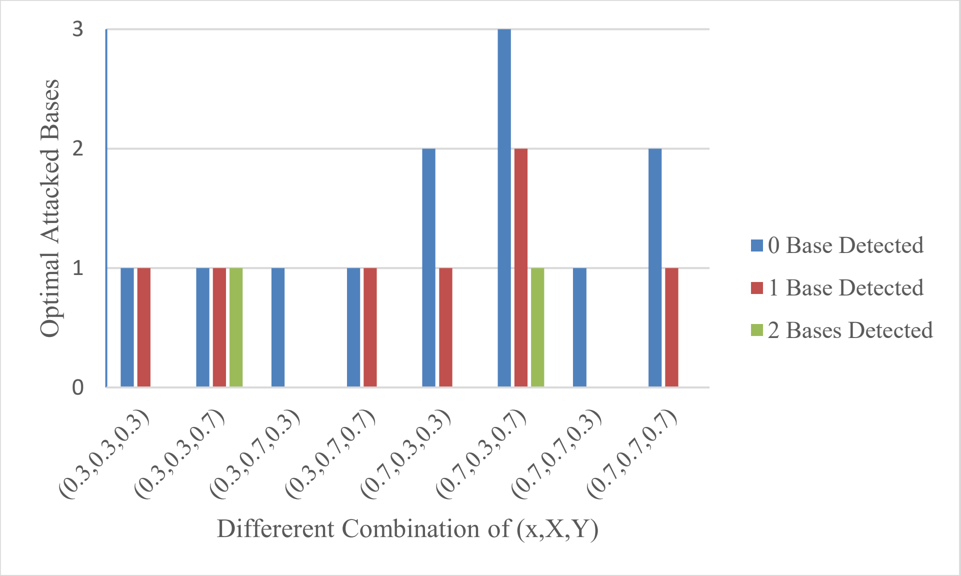

Figure 1. Optimal Attacked Bases under Different Combinations of (x, X, Y)

For each possible number of detected bases, we obtain the optimal number of bases that the defender should attack, as shown in Fig. 1. When the defender spends a large portion of its resources on a strike and the attacker spends a large portion of its resources on false base deployment, $(x, X, Y) = (0.7, 0.3, 0.7)$, the optimal number of attacked bases reaches three if no false bases are detected to be false. In this case, the amount of resources spent on false base deployment is $R(1-X)Y = 4.9$. Given that the unit cost for each false base is 2, the attacker can deploy 2 false bases. Since the defender spends 70% of its resources on a strike, it has enough resources to attack all three bases (one genuine and two false) if no false base is detected to be false. In contrast, when the defender only spends a small portion of its resources on a strike, ($x = 0.3$), it always attacks one base, no matter how many false bases the attacker deploys. This is because a spreading of the resources would lead to a low strike effort on each base, which would make them difficult to destroy.

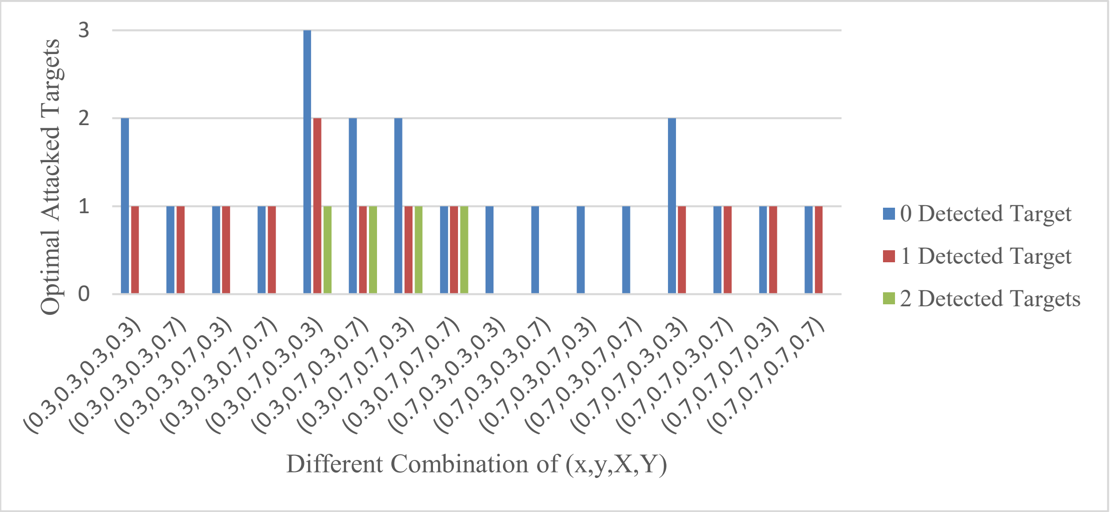

Figure 2 Optimal Number of Attacked Targets under Different Combinations of (x, y, X, Y)

For different combinations of resource allocation and detected false targets, we obtain the optimal number of targets that the attacker should attack, as shown in Fig. 2. Similarly, we find that the optimal number of attacked targets is the same no matter proactive strike or preventive strike is employed due to the same reason discussed above. For case (0.3, 0.7, 0.3, 0.3), where no false targets are detected, the optimal number of attacked targets reaches three. The amount of resources spent on deploying false targets in this case is $r(1-x)y = 4.9$, i.e. two false targets are deployed. The amount of resources the attacker spends on attacking is $R(1-X)(1-Y) = 4.9$, which is almost half of their total resources. Thus, even if no false targets are detected to be false, the attacker has enough resources to attack all three targets: one genuine object and two false targets. When $x = 0.7$, the number of attacked targets is almost always 1 except for when (0.7, 0.7, 0.3, 0.3). In fact, when *x* is big, the amount of resources left for false target deployment is low. When $y = 0.3$, the resources left for false target deployment is $r(1-x)y = 0.9$, which is not enough for even a single false target. Thus, in this case, the attacker should focus only on the genuine object. When $y = 0.7$, the amount of resources left for false target deployment is $r(1-x)y = 2.1$, which is just enough for a single false target. For case (0.7, 0.7, 0.3, 0.3), the amount of resources the attacker spends on attacking is $R(1-X)(1-Y) = 4.9$. Thus, the attacker can afford to attack both the genuine object and the false targets. For cases (0.7,0.7,0.3, 0.7), (0.7, 0.7,0.7,0.3), and (0.7,0.7,0.7,0.7), the amount of resources the attacker spends on attacking are 2.1, 2.1, and 0.9, respectively. For these cases, focusing only on one target gives the attacker a good chance to destroy the defender's object.

4. Optimal Attack Strategy Combination

Having now obtained the optimal numbers of bases and targets to attack, we continue to solve the optimal attack strategy combination using backward induction. For any given (x, y), the attacker chooses its decision variables $\left(X^*, Y^*\right) = \arg\max\left(V_a\right)$, assuming that the optimal numbers of bases and targets will be chosen for each realization of k_{fb} and k_{ft}. Generally, the prospect values are designed by the participant and can be estimated using their previous experiences. However, it is reasonable to assume that $x_{a1} < 0 < x_{a3}$ and $x_{d1} < 0 < x_{d3}$. For illustrative purposes, we examine the following two combinations:

$$x_{d2} = -x_{a2} = 5, x_{d1} = -x_{a1} = 8, x_{a3} = -x_{d3} = 20,$$

and

$$-x_{d2} = x_{a2} = 5, x_{d1} = -x_{a1} = 8, x_{a3} = -x_{d3} = 20.$$

We assume that the detection probabilities of the defender 's false targets and the attacker's false bases are both equal to 0.5. Furthermore, in the benchmark, for the defender, we assume that the probability of exposing the genuine object during a preventive strike is still 0.5. As for the value of risk parameters and weighting function parameters, we assume $g = 0.85, l = 0.85, \lambda = 4.10, \chi = 0.60$ and $\delta = 0.70$. We then conduct sensitivity analysis to analyze the impact of risk preference on the optimal strategies. Consider three different resource allocation strategies for the defender: high (0.8), medium (0.5), and low (0.2), which form nine different cases for different combinations of (x, y). We will analyze the trend of the optimal strategies and the corresponding cumulative prospect values of different parties in the extensions. Here, we just perform an illustrative example to present the procedures of our proposed model. For case $x_{a2} < 0$, the optimal attack strategies for the attacker are shown in Table 1.

Table 1 Optimal Attack Strategies when $x_{a2} < 0$

x	y	V_{a-pr}	V_{a-ps}	X^*	Y^*
0.2	0.2	-9.732	-6.43	0.466	0
0.2	0.5	-3.058	-2.019	0.473	0
0.2	0.8	-3.401	-2.229	0.560	0
0.5	0.2	-12.388	-8.752	0.574	0
0.5	0.5	-10.548	-7.330	0.647	0
0.5	0.8	-7.552	-5.164	0.743	0
0.8	0.2	-11.895	-8.706	0.742	0
0.8	0.5	-10.141	-7.356	0.780	0
0.8	0.8	-7.807	-5.554	0.877	0

From Table 1, we see that no matter what strategy the defender takes, the optimal strategy for the attacker is to spend no resources on false base deployment. Moreover, the optimal attack strategies remain the same no matter a proactive strike or a preventive strike is employed. The only difference for the two cases is that under the former case, the expected prospect value for the attacker is lower since the proactive strike does not expose the genuine object. Additionally, if the defender allocates more resources to a proactive strike or preventive strike then the attacker should allocate more resources to genuine base protection rather than to attacking the defender. This strategy differs from the results found by Wu et al. (2018), who concluded that the attacker in an attack–defense game should spend most of their resources on protection while still spending some resources on false bases. Our paper has a different conclusion because it relaxes a key assumption made in Wu et al. (2018) – that the false bases or false targets cannot be detected – which might not be realistic. Here, since the false bases can be detected, the strategy of false bases becomes less useful. The attacker therefore needs to change its strategy to one of protection. Among all possible prospect values, the prospect value of the attacker is always negative since the success probability and the corresponding reward are small. In the sensitivity analysis, if the reward of destroying the genuine target is greater than a certain threshold, the cumulative prospect value is greater than zero. The attacker can maximize its cumulative prospect value when the defender spends the minority of their resources on a proactive strike or preventive strike and a moderate level of resources on false target deployment. This seems to prove that the defender should spend more of their resources on a proactive strike or preventive strike instead of passive protection. We will further analyze the optimal defense strategies in the next section.

Now we look at case $x_{a2} > 0$ where the attacker obtains a positive prospect value when both the base and the genuine object survive. This situation is more likely when the protection of genuine base is more significant than the destruction of the genuine object. The optimal strategies for this case are shown in Table 2.

Table 2 Optimal Attack Strategies when $x_{a2} > 0$

x	y	V_{a-pr}	V_{a-ps}	X^*	Y^*
0.2	0.2	3.048	1.978	0.812	0
0.2	0.5	3.648	2.368	0.804	0
0.2	0.8	5.283	3.432	0.767	0
0.5	0.2	-4.286	-2.885	0.878	0
0.5	0.5	-3.653	-2.462	0.866	0
0.5	0.8	-2.259	-1.518	0.895	0
0.8	0.2	-9.877	-6.895	1	-
0.8	0.5	-9.877	-6.895	1	-
0.8	0.8	-9.877	-6.895	1	-

The optimal strategies for the attacker are in Table 1 and 2. The attacker now allocates more resources into base protection. This is because the attacker's prospect value is positive if, and only if, its base survives. In particular, when the strike effort is high, the attacker spends all its resources on base protection. In this case, the optimal value of Y does not exist. This is because any value of Y belonging to [0,1] leads to the same situation: all the attacker's resources are spent on base protection, which leaves no resources for either deploying false bases or launching attacks. Note, for all cases considered in Table 2, the attacker does not spend any of their resources on false bases. This implies that, under the given set of parameters, it is more cost effective to spend resources on the direct protection of the genuine base than on the deployment of false bases for distraction. One more interesting point from Fig. 2 is that when the expected prospect value is positive for the attacker, then defender's preventive strike will actually increase its expected prospect value. In contrast, when the expected prospect value is negative for the attacker, then defender's preventive strike will lower its value down. This implies that when the defender spends less in strike, the attacker will benefit. On the other hand, when the defender allocates the majority of its resource in either strike, the attacker will confront with a more severe situation. In section 6, we will show that when the false bases become cheaper, the optimal attack strategies suggest the deployment of false bases.

5. Optimal Defense Strategy Combination

Having solved the optimal attack strategy, we obtain the optimal defense strategy through backward induction. We first consider the case where $x_{d2} > 0$. Here, the optimal defense strategies are obtained if $x = 0.536$ and $y = 0.192$ (for proactive strike) and $x = 0.354$ and $y = 0.127$ (for preventive strike), respectively, and their respective optimal attack strategies are $X = 0.739$ and $Y = 0$ (for proactive strike) and $X = 0.514$ and $Y = 0$ (for preventive strike). The cumulative prospect values of the attacker and defender are $V_a = 7.38$ and $V_d = -12.08$ (for proactive strike) and $V_a = 6.63$ and $V_d = -8.44$ (for preventive strike), respectively. In this benchmark, we can predict the most likely strategies for the defender and attacker as follows. The defender will spend 53.6% (35.4%) of its resources on a proactive strike or preventive strike. The attacker, in response, will spend 73.9% (51.4%) of its resources on base protection and will not waste any resources on building false bases. If, and only if, the genuine base survives the preventive attack, the attacker will spend the remaining of its resources on attacking the defender. The defender will spend 19.2% (12.7%) of its resources on building one false target and will use the remaining of its resources on genuine object protection. The attacker will notice the movement of the defender and will use the remainder of its resources on attacking the two targets equally.

How will the optimal strategies for the defender alter if $x_{d2} < 0$? In this case, the defender prefers to destroy the genuine base over passively defending its genuine object. In reality, this can be seen in scenarios where the attacker is flagitious and has attacked the defender many times before, which makes the defender more determined to destroy the attacker's base. For this case, the optimal defense strategy combination is $x = 0.866$ and $y = 0$ (for proactive strike) and $x = 0.562$ and $y = 0$ (for preventive strike), respectively. In response, the attacker employs the strategy combination of $X = 0.897$ and

$Y = 0$ (for proactive strike) and $X = 0.582$ and $Y = 0$ (for preventive strike). The corresponding cumulative prospect values of the attacker and the defender under this case are $V_a = -7.485$ and $V_d = -14.988$ (for proactive strike) and $V_a = -4.863$ and $V_d = -10.089$ (for preventive strike), respectively.

By comparing these strategies under different assumptions, we have the following findings:

- The defender should allocate most of its resources on a proactive strike or preventive strike, forcing the attacker to spend most of its resources on protection and none of its resources on false base deployment.
- When the attacker is concerned more with its own base survival than with the destruction of the defender's object, the defender will spare more resources on a proactive strike or preventive strike. This forces the attacker to spend more resources on protection and none on building false bases. This agrees with our findings from Section 4: a false base is now less useful than genuine base protection.
- In contrast to the case when $x_{a2} < 0$, when $x_{a2} > 0$ ($x_{d2} < 0$), it becomes more important to destroy the attacker's base. Here, the defender spends more resources on a proactive strike or preventive strike. If the attacker survives the strike, the defender's prospect value is negative, which makes it a lose-lose situation.

If we calculate the social welfare by combining the cumulative prospective values of both parties, we find that it is slightly lower for $x_{a2} < 0$ than for $x_{a2} > 0$. This is because the attacker regards their own base survival as more important than the destruction of the defender's object, which makes its strategy more conservative. The cumulative prospect value of both parties is therefore increased, leading to an increase in social welfare.

6. Influences of Detection Probability, Exposure Probability and Risk Preferences

In the benchmark, we assume that the false targets of the defender and the false bases of the attacker have the same probability of being detected. However, in reality, the defender and attacker might have different levels of camouflage skills, and the surroundings of the false bases and false targets might be different. Thus, the detection probabilities of the two parties might also be different. To study the influence of the detection probabilities on the optimal strategies, we use two probabilities: 0.7 (the high type) and 0.3 (the low type). These probabilities are applicable both to the false target detection and the false base detection, which gives four possible scenarios, as shown in Fig. 3. Due to space constraints, we concentrate on the case where preventive strike is employed and $x_{a2} < 0$. We can further prove that the tendency remains the same as when proactive strike is employed or $x_{a2} > 0$. The optimal strategies and corresponding cumulative prospect values of both parties are shown in Fig. 3.

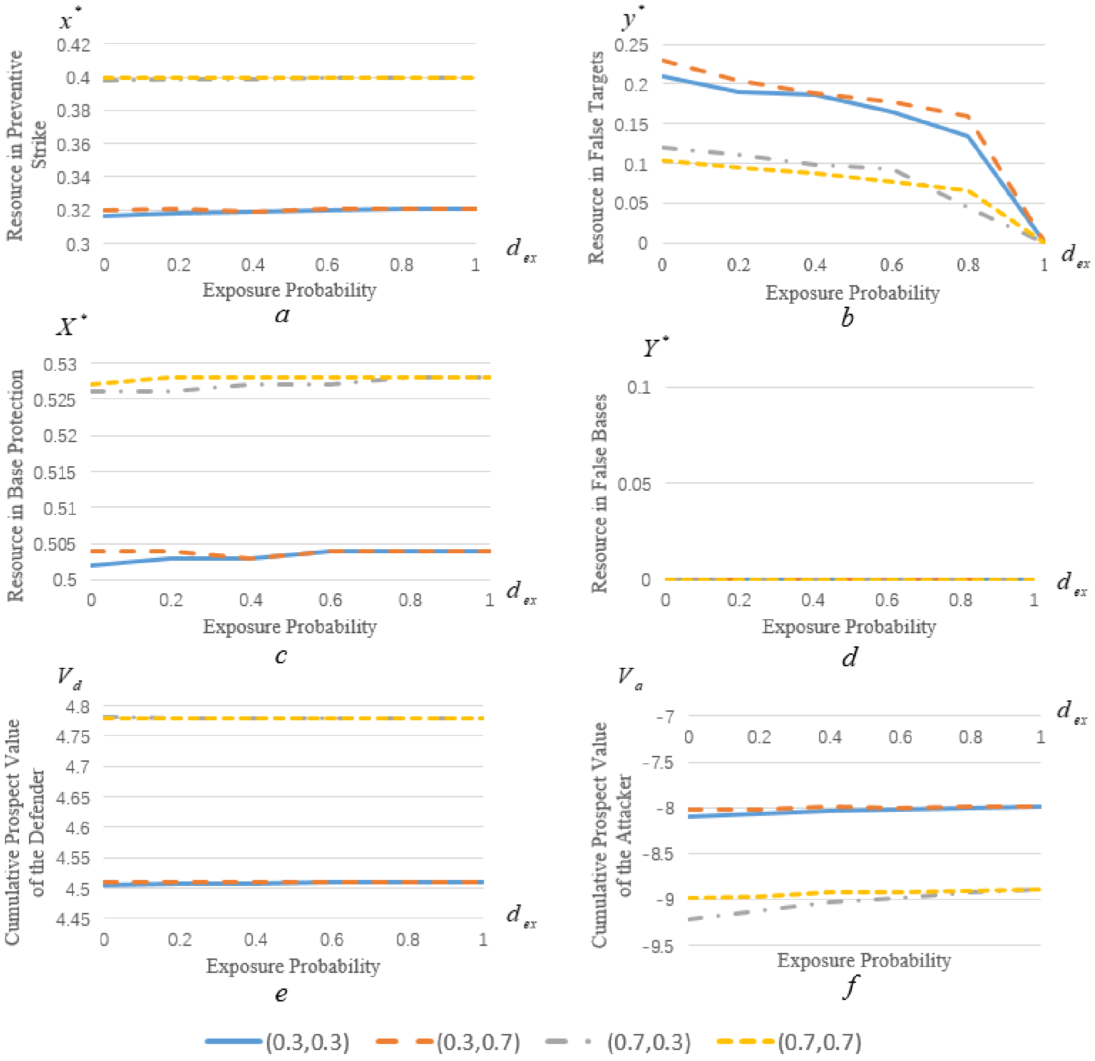

Figure 3 Optimal Strategies and the Corresponding Cumulative Prospect Values under Different Combination of (D_{fb}, d_{ft})

In Fig. 3(a) and 3(b), we can classify the four combinations of detection probabilities into two groups: the defender having a higher D_{fb}, and the defender having a lower D_{fb}. In the former case, the optimal resources spent on a preventive strike and the optimal resources spent on base protection are greater than the latter case. This is because the defender can easily detect the false bases in the former case. It will therefore allocate more resources to a preventive strike on the understanding that it should be easier for it to destroy the attacker. When the defender spends more resources on a preventive strike, the attacker must also spend more resources on base protection. In addition, when the detection probability is 0.3, we find that more false targets are deployed, i.e. it is more effective to deploy false targets when the detection probability is low.

In Fig. 3(e) and 3(f), we find that the cumulative prospect values of both parties depends only on the detection probability of the false bases. In contrast to when the detection probability is lower (0.3), when the detection probability is higher (0.7), the attacker obtains a lower cumulative prospect value and the defender gains a higher cumulative prospect value. In this case, because we are considering the situation where $x_{a2} < 0$ ($x_{d2} > 0$), the prospect value of the defender is positive.

As previously stated, for $0 < g < 1$, the value function exhibits risk aversion over gains, and for $0 < l < 1$, the function exhibits risk seeking over risk losses. In addition, the implicit assumption that the two parties own the same risk preferences has some impacts on the optimal strategies of both parties. In fact, the cumulative prospect value V_a, which the attacker tries to optimize, is influenced by all the risk parameters. Thus, changing the risk parameters of the attacker alters not only the attacker's cumulative prospect value but also its optimal attack strategies. As the defender anticipates the optimal attack strategies when choosing its defense strategies, the optimal defense strategies also change accordingly. Similarly, changes to the defender's risk parameters alter the optimal strategy combination of the defender, which then changes the corresponding optimal attack strategy combination. To analyze the influence of the risk preferences, we now alter the parameters of g, l and λ and analyze the behavior of each party under cases where the participants become more risk averse, risk seeking and more sensitive to losses than gains. The exponent parameters χ and δ can be determined through the experiments in practice (Abdellaoui, Bleichrodt and Paraschiv, 2007, Bleichrodt, 2000), respectively. Sensitivity analysis is therefore unnecessary here. It is easily understood that the risk aversion in the gain domain is negatively associated with g and the risk seeking in the loss domain is negatively associated with l. In this extension, due to space constraints, we still concentrate on the case where

$x_{a2} < 0$. We assume that g and l are equal to 0.9 and 0.8, respectively, and we analyze five different cases, where λ is altered from 3 to 5 in steps of 0.5. We perform the optimal strategies for both parties in Fig. 4 below.

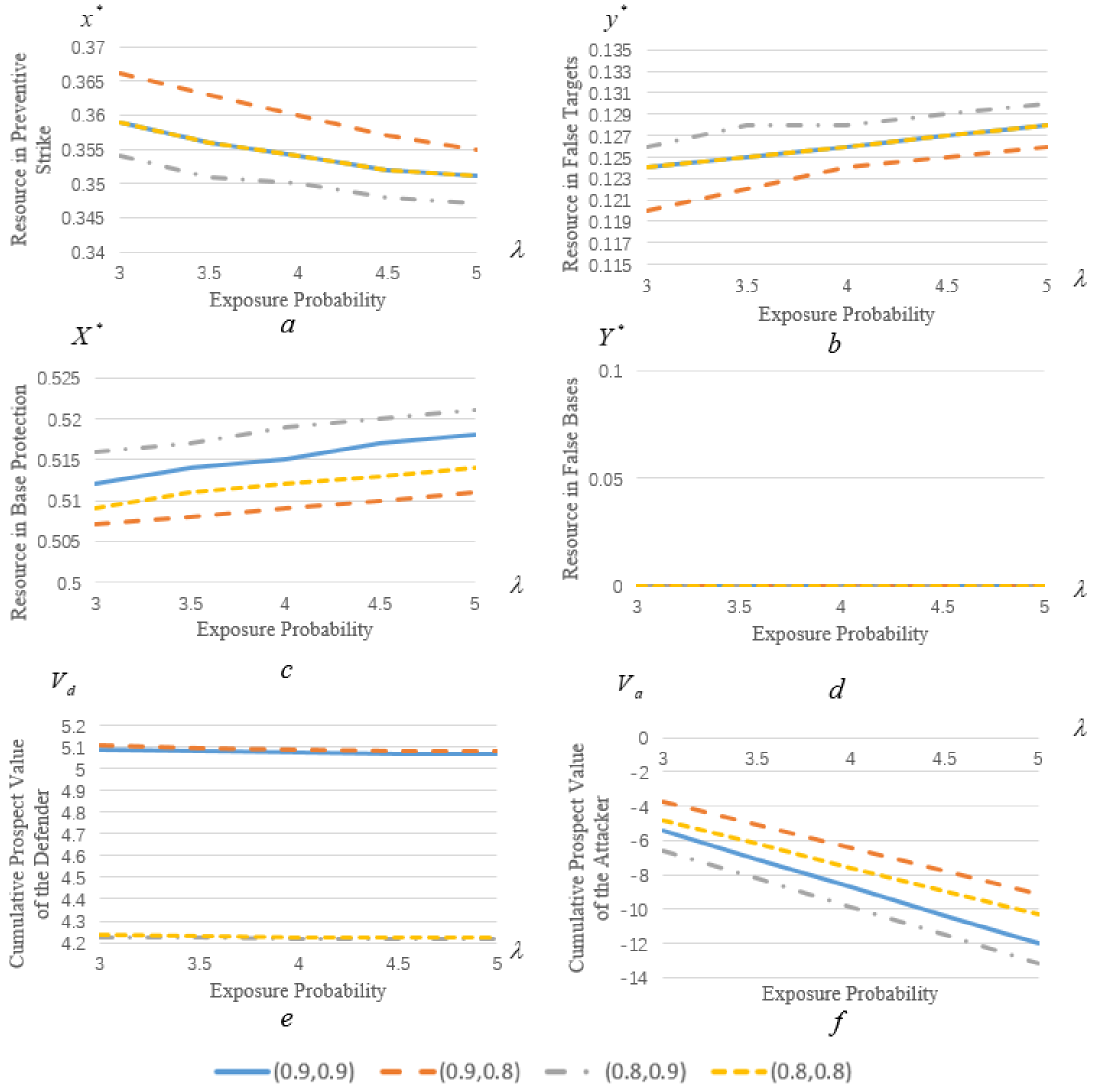

Figure 4 Optimal Strategies and the Corresponding Cumulative Prospect Values under Different Combinations of (g,l)

In Fig. 4(e) and 4(f), the cumulative prospect values of the defender can be divided into two groups: where the defender is more risk seeking in the gain domain than in the benchmark, and where the defender is more risk averse in the gain domain than in the benchmark. When the defender is more risk seeking, the cumulative prospect value is higher. This is because the attacker will spend more resources on base protection, which makes the preventive strike less useful and increases the vulnerability of the defender's object. Knowing this, the defender will move radically in case the attacker survives. The movement of both parties makes this a lose-lose situation. Risk aversion is commonly regarded as a good and safe method to use when making decisions. However, in this paper we prove that in an attack–defense game it is the risk-seeking strategy, not the risk-averse strategy, that might benefit the defender. Similarly the cumulative prospect value of the attacker when $g = 0.8$ and $l = 0.8$ is higher than the other three settings of g and l. This shows that the attacker should be more risk seeking in the loss domain. We also find another interesting phenomenon here: as λ increases, the cumulative prospect value of the defender does not significantly change but the cumulative prospect value of the attacker diminishes rapidly. This is because the case we analyze is $x_{a2} < 0$, which may be disadvantageous to the attacker. In addition, as λ increases, the amount of resources the defender spends on a preventive strike decreases and the amount of resources they spend on false target deployment increases. This consolidates the behavior that, under this case, the defender becomes more risk averse and conservative.

From Fig. 4(c) and 4(d), we can obtain the optimal attack strategies. The false base strategy is not taken by the defender under these given parameters, so we perform some sensitivity analysis to find out the critical values of the parameters that make the false base strategy useful. The base protection strategy becomes more effective as λ increases, which explains the decrease in the prospect value. Since the attacker now spends more resources on base protection, the defender spends more resources on false target deployment and less on a preventive strike, which makes the attacker's base protections less effective. It will therefore be more difficult for the attacker to win the contest, which leads to a lower cumulative prospect value than for other combinations of g and l. By comparing the cumulative prospect values in Fig. 4(e) and 4(f) with those in the benchmark, we further find that the cumulative prospect value becomes smaller, leading to a lose-lose case, if both parties become more risk averse. However, if both parties become more risk seeking, the preventive strike strategy becomes more prevalent and the attacker must stick to protecting their base instead of attacking the genuine object, increasing both parties' welfare and leading to a win-win case. Consequently, in an attack–defense game, risk seeking is sometimes a dominant strategy.

Now we analyze the optimal resources that the attacker should spend on false bases. Note that the strategy of false bases seems functionless, as under all circumstances discussed above, the attacker always chooses not to employ this strategy. This can be easily understood since a key assumption of this paper is that the unit cost of a false base is equal to the unit cost of base protection. If the defender is mighty and spends the majority of its resources on a preventive strike, the attacker must defend its genuine base before attacking the defender. Since the unit costs of protection and false bases are equal, and the false bases might be detected by the defender, the attacker prefers protection over false bases. In contrast, if the defender spends the minority of its resources on a preventive strike, the attacker spends more of its resources on attacking rather than on making false bases. Therefore, under any condition, the false base strategy is always a dominated strategy for the attacker.

We now investigate the situation where the parameters in the benchmark change. We perform sensitivity analysis for the unit cost of protection and the unit cost of false bases, and show the respective results. When the unit cost of base protection is twice as high as the unit cost of a false base, the false base strategy is employed by the attacker. Note that the lower the detection probability, the more resources the attacker will spend on false bases. We perform the optimal attack and defense strategies under three cases to illustrate the function of false bases, with the variation of the detection probability of the false bases ranging from 0.2 to 0.8, as shown in Fig. 5. We ignore the cases where the detection probability is equal to zero or one because here the false base strategy becomes a dominating strategy, which forms a discontinuity point.

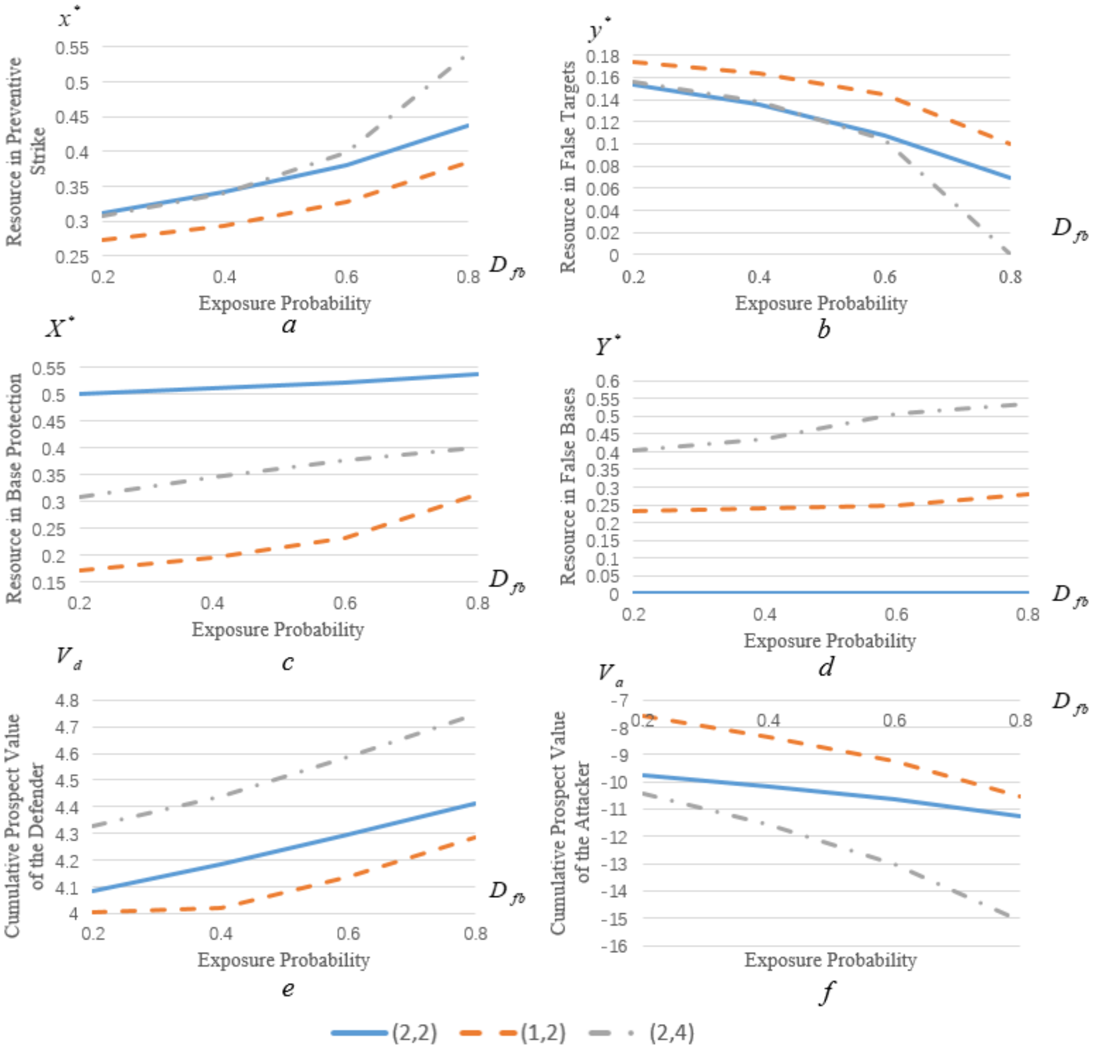

Figure 5 Optimal Strategies and the Corresponding Cumulative Prospect Value under Different Combination of (C_{fb}, C_{bp})

Fig. 5(a) and 5(b) show that an increase in the detection probability of false bases makes the defender spend more resources on a preventive strike and fewer resources on false targets. This is because the genuine base becomes easier to destroy if the false bases can be detected. In addition, when the unit cost for the attacker increases, the defender should be more mighty, and vice versa. Fig. 5(c) and 5(d) show that an increase in the detection probability of false bases makes the attacker spend more resources on base protection and false bases. Interestingly, in Fig. 5(d), both reducing the unit cost of false bases and increasing the unit cost of base protection can push the attacker to spend more resources on false bases, with the latter one being more useful. Since a false base strategy is now a useful and efficient strategy, the attacker spends less resources on base protection. Fig. 5(e) and 5(f) show that the cumulative prospect value of the defender increases with an increase of the detection probability, and the cumulative prospect of the attacker decreases. Moreover, an increase in the unit cost for the attacker increases the cumulative prospect value of the defender and decreases the cumulative prospect value of the attacker. We summarize the major findings and insights by conducting sensitivity analysis:

- It will be more effective to deploy false targets when the detection probability is low. Moreover, the cumulative prospect values of both parties depend only on the detection probability of the false bases.
- A risk-seeking strategy is the dominating strategy for the defender and there is no stable optimal strategy for the attacker. Considered the risk preference of both parties, the false base strategy is always a dominated strategy for the attacker.
- The introduction of detection probability makes the defender more easily to choose preventive strike, forcing and the attacker to concentrate on base protection and false bases instead of fighting back.

7. Conclusions and Future Work

In this paper, we analyze the optimal defense strategy combination for a single object. The defender can choose to protect the genuine object, set up false targets, and employ a proactive strike or preventive strike. Similarly, the attacker can choose to protect its genuine base, set up false bases, and employ an attack after surviving the strike. A preventive strike can expose the defender's own genuine object with some probability while a proactive strike is more expensive but will not expose the genuine object. The false targets and bases are imperfectly camouflaged, i.e. they can be detected with some probability. Using the traditional Tullock model, we employ cumulative prospect theory to consider players' risk attitudes. This provides a better depiction of the behavior of both parties under different risk parameters. Our results show that when the attacker is concerned more with its own base survival than with the destruction of the defender's object, the defender will spare more resources on a strike. This forces the attacker to spend more resources on protection and none on building false bases. In other words, a false base is less useful than genuine base protection in our given case. For theoretical innovation, our proposed model can introduce risk parameters in the traditional attack-defense game, making the modelling of risk preferences for both the attacker and the defender possible. As for practical innovation, our work can provide guidance in locating the optimal strategies for the defender as well as the attacker, considering false targets, proactive strike or preventive strike and respective risk preferences for participants.

This work can be extended in the future. For example, it would be interesting to investigate a more complex system composed of multiple objects, and it would be valuable to investigate the case of multiple attackers. Partially destruction of attacker's base and defender's object may also be an interesting extension to analyze. In this paper, the Tullock model is used to estimate the vulnerability, which is a function of the respective efforts of defender and attacker. In practice, one may need to take into account more complicated factors, such as weather and geographical condition, into determining the vulnerability. The analytical form has its limitation to incorporate too many factors due to mathematic tractability, thus simulation is a good solution is practice (Xiao, Gao and Lee, 2017; Xiao and Gao, 2018). Besides simulation, some other solutions for predicting the vulnerability is through machine learning (Wu and Akbarov, 2011), which is also a promising research to do in the future.

Acknowledgement

The research was supported by the NSFC under grant number 71671016. The last author would like to acknowledge support from Grant No. ES/L011859/1.

References

Abdellaoui, M., Bleichrodt, H., & Paraschiv, C. (2007). Loss aversion under prospect theory: a parameter-free measurement. *Management Science*, 53(10), 1659-1674.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.

Bier, V. M., & Hausken, K. (2011). Endogenizing the sticks and carrots: modeling possible perverse effects of counterterrorism measures. *Annals of Operations Research*, 186(1), 39–59.

Bleichrodt, H. (2000). A parameter-free elicitation of the probability weighting function in medical decision analysis. *Management Science*, 46(11), 1485-1496.

Bocchetti, D., Giorgio, M., Guida, M., & Pulcini, G. (2009). A competing risk model for the reliability of cylinder liners in marine Diesel engines. *Reliability Engineering & System Safety*, 94(8), 1299–1307.

Foraker, J., Lee, S., & Polak, E. (2016). Validation of a strategy for harbor defense based on the use of a min-max algorithm receding horizon control law. *Naval Research Logistics*, 63(3), 247-259.

Gao, K., Yan, X., Liu, X., & Peng, R. (2019). Object defence of a single object with preventive strike of random effect. *Reliability Engineering & System Safety*, 186, 209–219.

Hausken, K. (2010), Risk, production, and conflict when utilities are as if certain, *International Journal of Decision Sciences, Risk and Management*, 2, 3/4, 228-251.

Hausken, K. (2011a), Production, safety, fighting, and risk, *International Journal of Business Continuity and Risk Management*, 2, 4, 324-329.

Hausken, K. (2011b), Production, safety, exchange, and risk, *International Journal of Business Continuity and Risk Management*, 2, 4, 346-350.

Hausken, K. (2011c). Shield versus sword resource distribution in K-round duels. *Central European Journal of Operations Research*, 19(4), 589–603.

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

Hausken, K., & Zhuang, J. (2011). Governments' and Terrorists' Defense and Attack in a T-Period Game. *Decision Analysis*, 8(1), 46–70.

Jamshidi, A., Faghihroohi, S., Hajizadeh, S., Nunez, A., Babuska, R., Dollevoet, R., . . . de Schutter, B. (2017). A Big Data Analysis Approach for Rail Failure Risk Assessment. *Risk Analysis*, 37(8), 1495–1507.

Kahneman, D., & Tversky, A. (1979), Prospect Theory: An Analysis of Decision Under Risk, *Econometrica*, 47, 263-291.

Levitin, G., & Hausken, K. (2010). Resource distribution in multiple attacks against a single target. *Risk Analysis*, 30(8),1231–1239.

Levitin, G., & Hausken, K. (2011). Defense resource distribution between protection and redundancy for constant resource stockpiling pace. *Risk Analysis*, 31(10), 1632–1645.

Levitin, G., & Hausken, K. (2012). Preventive strike vs. false targets in defense strategy. *Reliability Engineering & System Safety*, 96(8), 912–924.

Levitin, G., & Hausken, K. (2013). Is it wise to leave some false targets unprotected? *Reliability Engineering & System Safety*, 112, 176–186.

Li, Y., Wang, T., Song, X., & Li, G. (2016). Optimal resource allocation for anti-terrorism in protecting overpass bridge based on AHP risk assessment model. *KCSE Journal of Civil Engineering*, 20(1), 309–322.

Liu, Y., Fan, Z. P., & Zhang, Y. (2014). Risk decision analysis in emergency response: A method based on cumulative prospect theory. *Computers & Operations Research*, 42(2), 75–82.

Oakes B D, Mattsson L G, Näsman P, & Glazunov A A. (2018). A Systems-Based Risk Assessment Framework for Intentional Electromagnetic Interference (IEMI) on Critical Infrastructures. Risk Analysis, 38(6), 1279-1305.

Peng, R., Levitin, G., Xie, M., & Ng, S. H. (2010). Defending simple series and parallel systems with imperfect false targets. *Reliability Engineering & System Safety*, 95(6), 679–688.

Peng, R., Levitin, G., Xie, M., & Ng, S.H. (2011). Optimal defense of single object with imperfect false targets. *Journal of the Operational Research Society*, 62(1), 134–141.

Peng, R., Wu, D., & Zhai Q. (2018). Defense Resource Allocation Against Sequential Unintentional and Intentional Impacts. *IEEE Transactions on Reliability*, 68(1), 364–374.

Peng, R., Xiao, H., Guo, J., & Lin, C. (2019). Defending a Parallel System against a Strategic Attacker with Redundancy, Protection and Disinformation. *Reliability Engineering & System Safety*, 106651.

Peng, R., Zhai, Q. Q., & Levitin, G. (2016). Defending a single object against an attacker trying to detect a subset of false targets. *Reliability Engineering & System Safety*, 149, 137–147.

Rios, J., & Rios, I. D. (2012). Adversarial risk analysis for counterterrorism modeling. *Risk Analysis*, 32(5), 894–915.

Sandler, T., & Siqueira, K. (2010). Global terrorism: deterrence versus pre-emption. *Canadian Journal of Economics/revue Canadienne Déconomique*, 39(4), 1370-1387.

Shere, K. D., & Cohen, E. A. (2010). A defense allocation problem with development costs. *Naval Research Logistics*, 19(3), 525-537.

Trucco, P., Cagno, E., Ruggeri, F., & Grande, O. (2008). A Bayesian Belief Network modelling of organizational factors in risk analysis: A case study in maritime transportation. *Reliability Engineering & System Safety*, 93(6), 845–856.

Tullock, G. (2001). *Efficient Rent Seeking*. Boston, MA: Springer.

Wang, Z., Fung, R. Y. K., Li, Y. L., & Pu, Y. (2017). An integrated decision-making approach for designing and selecting product concepts based on QFD and cumulative prospect theory. *International Journal of Production Research*, 7, 1–16.

Wu, D., Xiao, H., & Peng, R. (2018). Object defense with preventive strike and false targets. *Reliability*

Engineering & System Safety, 169, 76–80.

Wu, S., & Akbarov, A. (2011). Support vector regression for warranty claim forecasting. *European Journal of Operational Research*, 213(1), 196-204.

Xiao, H., & Gao, S. (2018). Simulation Budget Allocation for Selecting the Top-m Designs with Input Uncertainty. *IEEE Transactions on Automatic Control*, 63(9), 3127-3134.

Xiao, H., Gao, S., & Lee, L. H. (2017). Simulation budget allocation for simultaneously selecting the best and worst subsets. *Automatica*, 84, 117-127.

Xiao, H., & Peng, R. (2018). Trade-Off Between Redundancy, Protection, and Imperfect False Targets in Defending Parallel Systems. In *Recent Advances in Multi-state Systems Reliability* (pp. 227–239). Cham: Springer.

Zhai, Q., Ye, Z. S., Peng, R., & Wang, W. (2017). Defense and attack of performance-sharing common bus systems. *European Journal of Operational Research*, 256(3), 962–975.

Zhang, C., & Ramirez-Marquez, J. E. (2013). Protecting critical infrastructures against intentional attacks: a two-stage game with incomplete information. *IIE Transactions*, 45(3), 244–258.

Zhuang, J., & Bier, V. M. (2007). Balancing Terrorism and Natural Disasters--Defensive Strategy with Endogenous Attacker Effort. *Operations Research*, 55(5), 976–991.

Appendix A. The Existence of the Optimal Solution

To prove the existence of the optimal $Q_d^*(k_{fb})$ and $Q_a^*(k_{ft})$, we need to derive V_d and V_a with respect to Q_d and Q_a. Here we relax the integer assumption in Eq. (2) and Eq. (7):

$$\frac{\partial V_d}{\partial Q_d}=\frac{C_{fb}(-\left(rx/Q_d c_{ps}\right)^{2m_p}+\left(rx/Q_d c_{ps}\right)^{m_p}\left(RX/C_{bp}\right)^{m_p}(m_p-1))}{(\left(rx/Q_d c_{ps}\right)^{m_p}+\left(RX/C_{bp}\right)^{m_p})^2((k_{fb}-1)C_{fb}-R(1-X)Y)}, \tag{A1}$$

When the derivation is equal to zero, we obtain

$$Q_d{}^*=\frac{rx(\left(RX/C_{bp}\right)^{m_p}(m_p-1))^{-1/m_p}}{c_{ps}}. \tag{A2}$$

The second order derivation is

$$\frac{\partial^2 V_d}{\partial^2 Q_d}=\frac{C_{fb}m_p(\left(RX/C_{bp}\right)^{m_p}(m_p-1)\left(rx/Q_d c_{ps}\right)^{2m_p}-\left(rx/Q_d c_{ps}\right)^{m_p}(m_p+1)\left(RX/C_{bp}\right)^{2m_p})}{(\left(rx/Q_d c_{ps}\right)^{m_p}+\left(RX/C_{bp}\right)^{m_p})^3((k_{fb}-1)C_{fb}-R(1-X)Y)Q_d}, \tag{A3}$$

which can be easily proven to be lower than zero. Thus, the existence of the optimal solution is proved.

Similarly, we have

$$\frac{\partial V_a}{\partial Q_a}=\frac{c_{ft}(-\left(R(1-X)(1-Y)/Q_aC_{at}\right)^{m_a}\left(r(1-x)(1-\mathrm{y})/c_{pt}\right)^{m_a}(m_a-1)+\left(R(1-X)(1-Y)/Q_aC_{at}\right)^{2m_a})}{(\left(R(1-X)(1-Y)/Q_aC_{at}\right)^{m_a}+\left(r(1-x)(1-\mathrm{y})/c_{pt}\right)^{m_a})^2((k_{ft}-1)c_{ft}+r(1-x)(1-y))};\text{(A4)}$$

$$Q_a^*=\frac{R(1-X)(1-Y)(\left(r(1-x)(1-y)/c_{pt}\right)^{m_a}(m_a-1))^{-1/m_a}}{C_{at}};\qquad\text{(A5)}$$

$$\begin{aligned}\frac{\partial^2 V_a}{\partial^2 Q_a}=&\frac{m_ac_{ft}(\left(R(1-X)(1-Y)/Q_aC_{at}\right)^{2m_a}\left(r(1-x)(1-\mathrm{y})/c_{pt}\right)^{m_a}(m_a-1))}{(\left(R(1-X)(1-Y)/Q_aC_{at}\right)^{m_a}+\left(r(1-x)(1-y)/c_{pt}\right)^{m_a})^3((k_{ft}-1)c_{ft}+r(1-x)(1-y))}\\&-\frac{m_ac_{ft}\left(R(1-X)(1-Y)/Q_aC_{at}\right)^{m_a}\left(r(1-x)(1-\mathrm{y})/c_{pt}\right)^{2m_a}(m_a+1)}{(\left(R(1-X)(1-Y)/Q_aC_{at}\right)^{m_a}+\left(r(1-x)(1-\mathrm{y})/c_{pt}\right)^{m_a})^3((k_{ft}-1)c_{ft}+r(1-x)(1-y))}.\end{aligned}\qquad\text{(A6)}$$

Since Eq. (A3) and Eq. (A6) are both lower than zero, the existence of the optimal solutions of $Q_d^*(k_{fb})$ and $Q_a^*(k_{ft})$ are proved.