Ann Oper Res (2016) 236:255–270
DOI 10.1007/s10479-015-1810-z

Modeling and mitigating the effects of supply chain disruption in a defender–attacker game

Jie Xu · Jun Zhuang · Zigeng Liu

Published online: 18 February 2015

Abstract The outcomes of a defender–attacker game depend on the defender's resources delivered through military supply chains. These are subject to disruptions from various sources, such as natural disasters, social disasters, and terrorism. The attacker and defender are at war; the defender needs resources to defeat the attacker, but those resources may not be available due to a supply chain disruption that occurs exogenously to the game. In this paper, we integrate a defender–attacker game with supply chain risk management, and study the defender's optimal preparation strategy. We provide analytical solutions, conduct numerical analysis, and compare the combined strategy with other protection strategies. Our results indicate that: (a) the defender benefits in a defender–attacker game by utilizing supply chain risk management tools; and (b) the attacker's best response resource allocation would not be deterred by capacity backup protection and/or inventory protection. The feature of this paper is that the defender, being the downstream user of the supply chain, is involved in a strategic contest against the attacker. This model is different than game theory applied to private-sector supply chains because most game theoretic models of private sector supply chains usually explore relationships between suppliers and firms in the same supply chain or between multiple firms competing in the marketplace for customers. Therefore, supply chain risk management for such a military application imposes effects that have not been studied before.

This research was partially supported by the United States Department of Homeland Security (DHS) through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Award Number 2010-ST-061-RE0001. This research was also partially supported by the United States National Science Foundation under Award Numbers 1200899 and 1334930. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the DHS, CREATE, or NSF. We thank guest editors Drs. Katherine Daniell, Alec Morton, and David Rios Insua and two anonymous referees for their helpful comments.

J. Xu · J. Zhuang (✉)
Department of Industrial and Systems Engineering, SUNY at Buffalo, Buffalo, NY 14260, USA
e-mail: jzhuang@buffalo.edu

Z. Liu
Department of Physics and Astronomy, Northwestern University, Evanston, IL 60208, USA

Keywords Supply chain disruption · Defender–attacker game · Pre-disruption protection

1 Introduction

Among crucial elements contributing to military success, military logistics plays a very important role (Kane 2001). Military logistics operations have been used to accommodate a new security environment, change the way logistic functions perform, and revise traditions and organization structures (Simon 2001). The overall military fighting power directly increases in logistics efficiency (Kane 2001). Military logistics and supply chains can defeat an enemy's force without direct engagement (von Clausewitz 2004). As a Chinese saying goes, "supply goes before troops" emphasizes the importance of military supply chains in a defender–attacker game. The military force must have supplies (e.g., food, water, and fuel) to survive or win in the contest (Simon 2001). Such supplies may be subject to disruptions such as natural disasters, social disasters and terrorism. For example, the U.S. military experienced a fuel shortage in Iraq and Afghanistan, which disrupted U.S. efforts to win in the war (National Public Radio 2011).

Risk classification and protection mechanisms have been studied in supply chain risk management. For example, Christopher and Lee (2004) argued that supply chains could be affected by uncertain changes in business strategies. Christopher and Peck (2004) emphasized that it is critical to understand the nature of supply chain risks while building resilient supply chain networks. Chopra and Sodhi (2004) classified supply chain risks into nine categories (capacity risks, delays, disruptions, forecasting risks, intellectual property risks, inventory risks, procurement risks, receivables and system risks) and discussed the corresponding mitigation strategies. Chopra et al. (2007) highlighted the importance of distinguishing between recurrent supply risks and disruptive risks. Hopp et al. (2010) introduced two pre-disruption protection mechanisms, capacity backup (including subtree capacity protection and single-node capacity protection) and inventory protection, to mitigate risks on supply chain networks.

Since the 9/11/2011 attacks, many researchers have studied protection in defender–attacker games (Bier et al. 2005; Sandler and Siqueira 2006; Zhuang and Bier 2007; Insua et al. 2009; Bier and Haphuriwat 2011; Paul and Hariharan 2012). The outcomes of a defender–attacker game are impacted by the defender's resources delivered through military supply chains. Various types of risks (e.g., social disasters, natural disasters, and terrorism) could disrupt military supply chain networks and cause economic losses and casualties. To win the game, players need to understand the characteristics of the game (armed conflict) and be prepared with resources and responding capabilities (Kress 2012). However, to the best of our knowledge, few studies have investigated protection mechanisms on the military supply chain risk management in a defender–attacker game. [An exception is Jin et al. (2010), who simulated the inventory and capacity backup disruption preparation strategies separately with exogenous attacker efforts]. Our paper fills this gap by studying the protection strategies for both capacity backup and inventory against endogenous attacker efforts, providing both analytical and numerical solutions, and comparing different preparation strategies (e.g., having capacity backup or holding inventory). Our paper enriches the literature of both supply chain risk management and defender–attacker games by providing a new modeling framework to study the impact and optimal use of supply chain risk management tools to mitigate the supply chain disruptions.

Unlike traditional (private-sector) supply chain management, the decision maker in military supply chains may have different objectives (e.g., maximizing the payoffs in the contest or minimizing risk during the disruption period), operational environments (e.g., in a war or battle), and decision choices (e.g., recourses allocated in the contest). Thus, the outcomes of military supply chain risk management may differ from that of traditional supply chains. In addition, the strategic interactions between the defender and attacker and the corresponding payoff structure have not been studied in the traditional supply chain management literature. Unlike when the player is involved in a vertical supply–demand relationship and/or a horizontal competition with other manufacturers in a private-sector supply chain, the defender, as the downstream user of the military supply chain, strategically contests with the attacker. Military supply chain risk management imposes effects that have not been studied before, since the attacker collects a stream of payoffs that would not arise in a typical vertical demand–supply relationship or horizontal competition.

The remainder of this paper is organized as follows. Section 2 introduces the model framework and the notation. Section 3 presents the defender's and attacker's optimization problems, derives analytical solutions, and illustrates the attacker's best responses for various protection strategies. Section 4 numerically illustrates the players' equilibrium strategies and payoffs, and provides sensitivity results. Section 5 concludes the paper and provides some future research directions. An Appendix provides proofs.

2 Modeling framework

We consider a game between one attacker and one defender. Common knowledge about the rules of the game is assumed among the players (Dutta 1999). In our defender–attacker game, the defender and the attacker contest and interact strategically with each other considering the exogenous military supply chain disruptions for the defender. During the contesting period, the defender may face supply chain disruptions which would cause a shortage of supplies.[1] For example, the United States had an armed conflict with Iraq and Afghanistan, while the U.S. faced supply shortages due to exogenous supply chain disruptions. We consider a sequential game (Shan and Zhuang 2013; Zhuang et al. 2014) between the defender and the attacker. First, the defender decides what kind of pre-disruption preparation strategies she should take (the combined strategy, capacity backup protection, inventory protection, or no protection). In the above example, the U.S. decides resource allocation and preparation strategies which would be used to contest against opponents in Iraq or Afghanistan. Then, the attacker decides what resources to allocate to contest against the defender. Rebels in Iraq or Afghanistan would allocate resources to contest against the U.S. The defender and the attacker jointly determine their efforts (i.e., the amount of resource allocation) at equilibrium, and their equilibrium payoffs depend on the available resources in the contest, which are subject to exogenous military supply chain disruptions. Figure 1 shows the framework for integrating the defender–attacker game with the (military) supply chain risk management problem. Both the defender and the attacker at war need to relocate resources which may be unavailable due to exogenous disruptions to contest against each other. In particular, we allow the defender to decide the amount of resources allocated in the game and the investment in risk management (capacity backup, inventory, or both) against disruptions. All of these protection mechanisms are realistic. For example, after a disruption occurs, some expendable resources (such as bombs and bullets) are difficult to supply through backup capacity providers in time and need to be stored in inventory, while some perishable resources (such as food and

[1] We acknowledge that resource means all kinds of supplies that would be used to defend/attack against the other adversary; e.g., weapons or armaments.

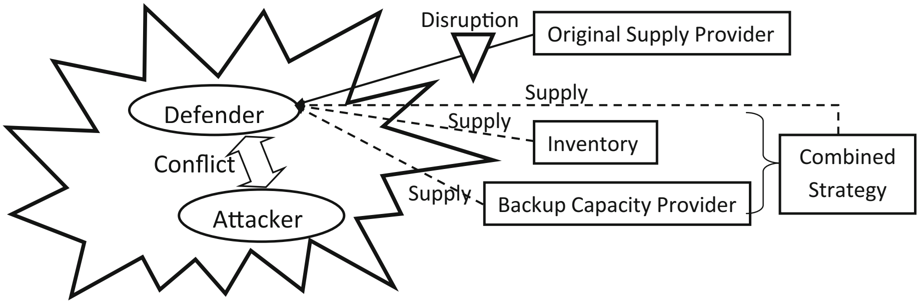

Fig. 1 Research framework: integrating a defender–attacker game with military supply chain risk management

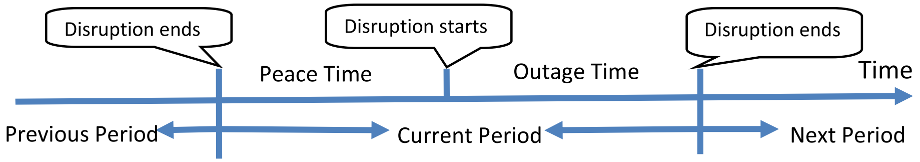

Fig. 2 Periods and timing for peace, outage and disruption

Table 1 Notation used throughout the paper

Characteristics parameters		*Cost parameters*	
x	Peace time (before disruption)	m	Daily revenue per unit of resource
l	Outage time in the disruption	α	Reservation cost of capacity backup
d	Delay time required for capacity backup	β	Daily usage cost of capacity backup
v	Defender's asset valuation	γ_G	Daily resource cost of defender
V	Attacker's asset valuation	γ_T	Daily resource cost of attacker
$f_X(x)$	Probability density function of peace time	h	Holding cost of unit inventory
$f_L(l)$	Probability density function of outage time		
$f_D(d)$	Probability density function of delay time		
Decision variables		*Payoffs*	
r	Daily resource of defender	U_G	Payoff of the government
R	Daily resource of attacker	U_T	Payoff of the attacker
k	Binary variable on capacity backup		
I	Inventory level		

medicines) can not be held in inventory for a long time and need backup capacity. Other resources could use both protection mechanisms.

We acknowledge that, in reality, the supply chain network could be very complex (e.g., different nodes could be supported by different inventories or backup suppliers). However, in this paper, for simplicity, we consider a single generic resource and a single capacity backup provider.

Figure 2 shows the period and timing, consisting of peace time[2] (which starts at the end of the previous-period disruption and ends at the beginning of the current-period disruption) and outage time (which starts from the beginning of the current-period disruption and ends when the disruption influence disappears) for one period. Hence, the length of each period depends on two factors: the peace time and the outage time. Table 1 introduces the notation that is used in this paper, including characteristics parameters, cost parameters, decision variables,

[2] The peace time (x) means time with no disruption or outage.

Table 2 Baseline values for parameters

Parameter	Value	Parameter	Value	Parameter	Value
α	0.02	β	0.05	V	2
v	2	h	0.5	γ_G	0.2
γ_T	0.3	m	0.1	$E[X]$	6
$E[L]$	5	$E[D]$	1		

and payoffs. Table 2 provides baseline values for parameters that are used throughout this paper. Note that the baseline values for parameters are chosen for illustration purposes and may not carry actual meanings. In realistic applications, those parameter values could be estimated based on historical data or expert elicitation. In addition, players' target valuations could be approximated using the expected economic losses or casualties (Shan and Zhuang 2013); unit costs of reservation, usage, and resource could be based on the cost estimations on labor, equipment, supply, and other costs necessary for the corresponding operations; and parameters for probability density functions could be estimated using experiments.

3 Models and analytical results

In this section, we present the defender's and the attacker's optimization problems and provide analytical solutions to the attacker's best response function. In particular, Sect. 3.1 studies the special cases for combined protection, including no protection, capacity backup protection, and inventory protection, respectively; Sect. 3.2 studies combined protection.

We assume that the defender's expected payoff for each day in the contest period is $\frac{rv}{r+R}$ (Skaperdas 1996; Zhuang and Bier 2007), which increases in the defender's daily resource allocation, r, and the defender's asset valuation, v, and decreases in the attacker's daily resource allocation, R. The attacker's expected payoff for each day in the contest period is $\frac{RV}{r+R}$, which increases in the attacker's daily resource allocation, R, and the attacker's asset valuation, V, and decreases in the defender's daily resource allocation, r. During disruptions, the attacker would get the valuation V when the defender does not use capacity backup protection or experiences the delay time. The missing revenue in disruption period m may be different from the revenue in peace time v due to damages during the disruption period. In most cases, the revenue m in the disruption period would be smaller than v in the peace period.

Randomness comes from the length of peace time before disruptions, x, the length of outage time in the disruption, l, and the length of delay time, d. We assume that the lower bound for the outage time in the disruption is larger than the upper bound for the delay time required to provide capacity backup. This is reasonable because the delay time is usually much shorter than the disruption time, and the defender would choose not to use capacity backup protection whenever the delay time is longer than the disruption time. When the defender is indifferent between using and not using disruption protection mechanisms, we assume that the defender will not use them.

3.1 Basic strategies

3.1.1 No protection

Equation (1) provides the defender's optimization problem without protection strategy. There are two components: the expected payoff in contest and the expected loss during disruptions.

$$\max_{r\geq 0} u_G(r) = \underbrace{\left(\frac{r\cdot v}{r+R} - \gamma_G \cdot r\right)\int_x x\cdot f_X(x)\mathrm{d}x}_{\text{expected payoff in contest}} - \underbrace{m\cdot r\cdot \int_l l\cdot f_L(l)\mathrm{d}l}_{\text{expected loss during disruptions}} \tag{1}$$

The attacker decides his resources after observing the defender's decisions. There are two components in the attacker's objective function shown in Eq. (2): the expected payoff in contest and the expected payoff during disruptions.

$$\max_{R\geq 0} u_T(r, R, k, I) = \underbrace{\left(\frac{R\cdot V}{r+R} - \gamma_T \cdot R\right)\int_x x\cdot f_X(x)\mathrm{d}x}_{\text{expected payoff in contest}} + \underbrace{(V-\gamma_T\cdot R)\cdot \int_l l\cdot f_L(l)\mathrm{d}l}_{\text{expected payoff during disruptions}} \tag{2}$$

We consider a one-shot sequential game between the defender and the attacker, where the defender makes the first move. The attacker observes the defender's choices, and then determines his resource. The strategy pair (r^*, R^*) is a Subgame Perfect Nash Equilibrium (Mas-Colell et al. 1995) if and only if $R^* = \hat{R}(r^*)$ and $r^* = \arg\max_r u_T(r, \hat{R}(r))$, where the attacker's best response function $\hat{R}(r) \equiv \arg\max_R u_T(r, R)$ is solved from Eq. (2) as:

$$\hat{R}(r) = \begin{cases} G, & \text{if } r < \frac{V\cdot E[X]}{\gamma_T\cdot[E[X]+E[L]]} \\ 0, & \text{if } r \geq \frac{V\cdot E[X]}{\gamma_T\cdot[E[X]+E[L]]} \end{cases} \tag{3}$$

for $r \geq 0$, where $G \equiv \sqrt{\frac{V\cdot r\cdot E[X]}{\gamma_T\cdot[E[X]+E[L]]}} - r$. (See "Appendix 1" for the proof.)

Equation (3) shows that the attacker's best resource allocation R could be either zero (deterred by a high defender's resource) or positive. Keeping r constant, when R is positive, $R = G$ increases in the attacker's asset valuation V and the expected peace time $E[X]$, and decreases in the attacker's daily resource cost γ_T and the expected outage time $E[L]$. The attacker's best response (resource allocation) without protection strategy is shown in Fig. 4. However, the attacker would win if he uses resources $R > 0$ while the defender does not use any resources $r = 0$.

3.1.2 Capacity backup protection only

Figure 3 shows the period and timing, consisting of peace time, delay time, and outage time. The delay time starts from the beginning of the current-period disruption and ends when the supplies are provided to the defender.

Equation (4) provides the defender's optimization problem when using capacity backup protection only. There are three components: (a) the expected payoff in contest; (b) the expected reservation and usage cost of capacity backup protection; and(c) the expected loss during disruptions. The defender pays the reservation fee at a rate of α per unit of resource during the entire period and the usage fee at a rate of β per unit of resource during the outage time.

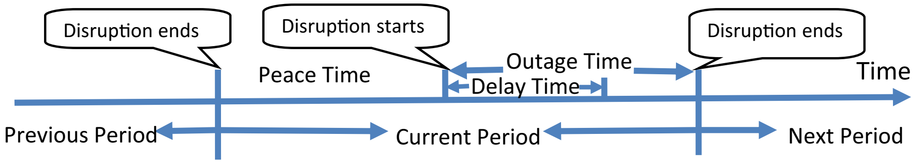

Fig. 3 Periods and timing for peace, delay, outage and disruption

The defender experiences the loss at a rate of m per unit of resource during the period of disruption without backup supplies.

$$
\begin{aligned}
\max_{r\geq 0, k\in\{0,1\}} u_G(r,k,R) = & \underbrace{\left(\frac{r\cdot v}{r+R} - \gamma_G\cdot r\right)\int_x\int_l\left(x+k\cdot\int_d(l-d)f_D(d)\mathrm{d}d\right)f_X(x)f_L(l)\mathrm{d}l\mathrm{d}x}_{\text{expected payoff in contest}} \\
& \underbrace{-\ k\cdot\left[\alpha\cdot r\left(\int_x x\cdot f_X(x)\mathrm{d}x + \int_l l\cdot f_L(l)\mathrm{d}l\right) + \beta\cdot r\int_l\int_d(l-d)f_L(l)f_D(d)\mathrm{d}d\mathrm{d}l\right]}_{\text{expected reservation and usage cost of capacity backup protection}} \\
& \underbrace{-\ m\cdot r\left[\int_d d\cdot f_D(d)\mathrm{d}d\mathrm{d}l + (1-k)\int_l\int_d(l-d)f_L(l)f_D(d)\mathrm{d}d\mathrm{d}l\right]}_{\text{expected loss during disruptions}}
\end{aligned}
\tag{4}
$$

The attacker decides his resources R to allocate after observing the defender's choices. There are two components in the attacker's objective function shown in Eq. (5) below: the expected payoff in contest, and the expected payoff when the defender experiences disruptions.

$$
\begin{aligned}
\max_{R\geq 0} u_T(r,k,R) = & \underbrace{\left(\frac{R\cdot V}{r+R} - \gamma_T\cdot R\right)\int_x\int_l\left(x+k\int_d(l-d)f_D(d)\mathrm{d}d\right)f_X(x)f_L(l)\mathrm{d}l\mathrm{d}x}_{\text{expected payoff in contest}} \\
& \underbrace{+\ (V-\gamma_T\cdot R)\cdot\left[(1-k)\int_l l\cdot f_L(l)\mathrm{d}l + k\left(\int_d d\cdot f_D(d)\mathrm{d}d\mathrm{d}l\right)\right]}_{\text{expected payoff when the defender experiences disruptions}}
\end{aligned}
\tag{5}
$$

As calculated from Eq. (5), the strategy pair (r^*, k^*, R^*) is a Subgame Perfect Nash Equilibrium if and only if $R^* = \hat{R}(r^*, k^*)$ and $(r^*, k^*) = \arg\max_{(r,k)} u_T(r, k, \hat{R}(r, k))$, where the attacker's best response function $\hat{R}(r, k) \equiv \arg\max_R u_T(r, k, R)$ is as follows:

$$
\hat{R}(r,k) = \begin{cases} G_k, & \text{if } r < \frac{V\cdot[E[X]+k(E[L]-E[D])]}{\gamma_T\cdot(E[X]+E[L])} \\ 0, & \text{if } r \geq \frac{V\cdot[E[X]+k(E[L]-E[D])]}{\gamma_T\cdot(E[X]+E[L])} \end{cases}
\tag{6}
$$

for $r \geq 0$ and $k \in \{0, 1\}$, where $G_k \equiv \sqrt{\frac{V\cdot r\cdot[E[X]+k(E[L]-E[D])]}{\gamma_T\cdot(E[X]+E[L])}} - r$. (See "Appendix 1" for the proof).

Equation (6) is a general case of Eq. (3). It shows that the attacker's best resource allocation, R, could be either zero (deterred by a high defender's resource and capacity backup protection) or positive. Keeping r constant, when R is positive, $R = G_k$ is higher when capacity backup protection is used ($k = 1$) than when there is no capacity backup protection ($k = 0$). Keeping r constant, when R is positive, $R = G_k$ increases in the attacker's asset valuation, V, and the expected peace time, $E[X]$, and decreases in the attacker's daily resource cost, γ_T, and the expected delay time, $E[D]$. Similarly, keeping r constant, when the defender uses the capacity backup protection ($k = 1$), the attacker's best resource allocation, R, increases in the expected outage time, $E[L]$; while when the defender does not use the capacity backup protection ($k = 0$), the attacker's best resource allocation, R, decreases in the expected outage time, $E[L]$.

Figure 4 shows the attacker's best response as a function of the defender's daily resource allocation with or without the capacity backup protection. From Fig. 4, we observe that the

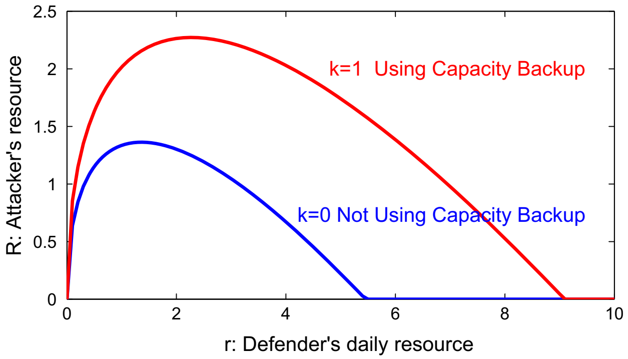

Fig. 4 Attacker's best response as a function of the defender's daily resource allocation when using or not capacity backup protection

attacker's best response resource first increases and then decreases in the defender's daily resource. It is interesting to observe that the attacker would not be deterred by capacity backup protection and would actually use more resources when the defender uses capacity backup protection, in order to remain competitive in the contest.

3.1.3 Inventory protection only

Equation (7) provides the defender's optimization problem using inventory protection only. As with Eq. (4), there are three components: the expected payoff in contest, the expected holding cost of inventory protection, and the expected loss during disruptions. During disruptions, if the defender uses inventory protection, she could use inventory to satisfy the need in the contest. Therefore, during the periods of peace time, x, and time with inventory, I, the defender would defend against the attacker in the contest. If the defender uses r resources per day and has I level of inventory, the defender has $\frac{I}{r}$ days of inventory. By using the inventory mechanism, the defender would need to pay for the holding cost, h. The defender also experiences loss at a rate of m per unit of resource during the period of disruption, l, without inventory.

$$\max_{r\geq 0, I\geq 0} u_G(r, R, I) = \underbrace{\left(\frac{r\cdot v}{r+R} - \gamma_G \cdot r\right)\left[\int_x x\cdot f_X(x)\mathrm{d}x + \int_l \min\left\{\frac{I}{r}, l\right\} f_L(l)\mathrm{d}l\right]}_{\text{expected payoff in contest}}$$
$$- \underbrace{h\cdot\left[I\cdot\int_x x\cdot f_X(x)\mathrm{d}x + \int_l\int_{z=0}^{l}[I-rz]^+ f_L(l)\mathrm{d}z\mathrm{d}l\right]}_{\text{expected holding cost of inventory}} \qquad (7)$$
$$- \underbrace{m\cdot r\cdot\int_l\left[l-\frac{I}{r}\right]^+ f_L(l)\mathrm{d}l}_{\text{expected loss during disruptions}}$$

After observing the defender's choices, the attacker decides his resource level allocated. There are two major components in the attacker's objective function shown in Eq. (8): the expected payoff in contest and the expected payoff when the defender experiences disruptions.

$$
\begin{aligned}
\max_{R\geq 0} u_T(r,R,I) = & \underbrace{\left(\frac{R\cdot V}{r+R}-\gamma_T\cdot R\right)\left[\int_x x\cdot f_X(x)\mathrm{d}x+\int_l \min\left\{\frac{I}{r},l\right\} f_L(l)\mathrm{d}l\right]}_{\text{expected payoff in contest}} \\
& \underbrace{+\ (V-\gamma_T\cdot R)\cdot\int_l\left[l-\frac{I}{r}\right]^+ f_L(l)\mathrm{d}l}_{\text{expected payoff during disruptions}}
\end{aligned}
\tag{8}
$$

The strategy pair (r^*, I^*, R^*) is a Subgame Perfect Nash Equilibrium if and only if: $R^* = \hat{R}(r^*, I^*)$ and $(r^*, I^*) = \arg\max_{(r,I)} u_T(r, I, \hat{R}(r, I))$, where the attacker's best response function $\hat{R}(r, I) \equiv \arg\max_R u_T(r, I, R)$ could be solved from Eq. (8) as:

$$
\hat{R}(r,I)=\begin{cases}
G_I, & \text{if}\, r<\dfrac{V\cdot\left[E[X]+\int_l \min\left\{\frac{I}{r},l\right\}f_L(l)\mathrm{d}l\right]}{\gamma_T\cdot\left[E[X]+\int_l \min\left\{\frac{I}{r},l\right\}f_L(l)\mathrm{d}l+\int_l\left[l-\frac{I}{r}\right]^+ f_L(l)\mathrm{d}l\right]}\\
0, & \text{if}\, r\geq\dfrac{V\cdot\left[E[X]+\int_l \min\left\{\frac{I}{r},l\right\}f_L(l)\mathrm{d}l\right]}{\gamma_T\cdot\left[E[X]+\int_l \min\left\{\frac{I}{r},l\right\}f_L(l)\mathrm{d}l+\int_l\left[l-\frac{I}{r}\right]^+ f_L(l)\mathrm{d}l\right]}
\end{cases}
\tag{9}
$$

for $r \geq 0$ and $I \geq 0$, where $G_I \equiv \sqrt{\dfrac{V\cdot r\cdot\left[E[X]+\int_l \min\left\{\frac{I}{r},l\right\}f_L(l)\mathrm{d}l\right]}{\gamma_T\cdot\left[E[X]+\int_l \min\left\{\frac{I}{r},l\right\}f_L(l)\mathrm{d}l+\int_l\left[l-\frac{I}{r}\right]^+ f_L(l)\mathrm{d}l\right]}} - r$. (See "Appendix 1" for the proof).

Equation (9) shows that the attacker's best resource allocation R could be either zero (deterred by a high level of the defender's resources and inventory protection) or positive. Keeping r constant, when R is positive, $R = G_I$ increases in the attacker's asset valuation, V, and decreases in the attacker's daily resource cost, γ_T. Figure 5 illustrates that the attacker's best response resource first increases in the defender's daily resource, r, and then decreases in r. The attacker's best response resource increases in inventory level, I, in order to remain competitive. This means that the attacker would not be deterred by the inventory protection strategy.

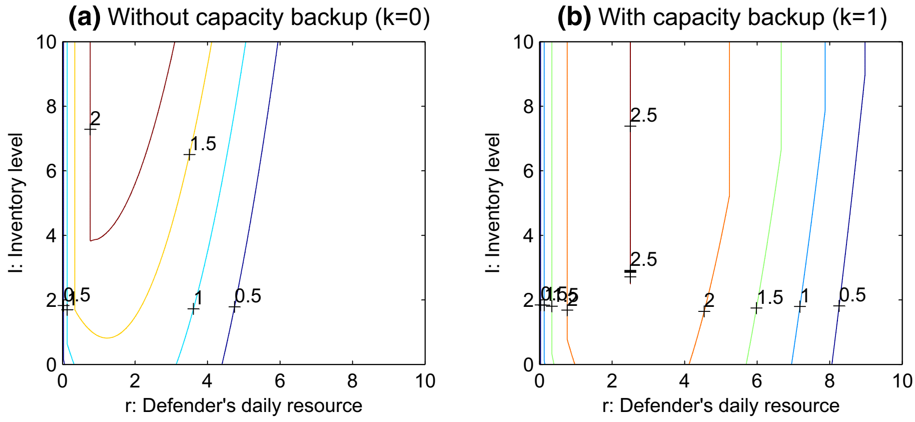

Fig. 5 Contours for the attacker's best response, as a function of the defender's daily resource and inventory level with and without capacity backup protection

3.2 Combining capacity backup protection and inventory protection

Equation (10) provides the defender's optimization problem using the combined strategy. There are four components: the expected payoff in contest, the expected reservation and usage cost of capacity backup protection, the expected holding cost of inventory protection, and the expected loss during disruptions.

$$\begin{aligned}
&\max_{r\geq 0, k\in\{0,1\}, I\geq 0} u_G(r, R, k, I)\\
&= \underbrace{\left(\frac{r\cdot v}{r+R}-\gamma_G\cdot r\right)\int_x\int_l\int_d\left(x+\min\left\{\frac{I}{r},(1-k)l+kd\right\}+k(l-d)\right)f_D(d)f_X(x)f_L(l)\mathrm{d}d\mathrm{d}l\mathrm{d}x}_{\text{expected payoff in contest}}\\
&\quad-\underbrace{k\cdot r\left[\alpha\left(\int_x x\cdot f_X(x)\mathrm{d}x+\int_l l\cdot f_L(l)\mathrm{d}l\right)+\beta\cdot\int_l\int_d(l-d)f_L(l)f_D(d)\mathrm{d}d\mathrm{d}l\right]}_{\text{expected reservation and usage cost of backup}} \qquad (10)\\
&\quad-\underbrace{h\cdot\left[I\cdot\int_x x\cdot f_X(x)\mathrm{d}x+\int_l\int_{z=0}^{l}[I-rz]^+f_L(l)\mathrm{d}z\mathrm{d}l\right]}_{\text{expected holding cost of inventory}}\\
&\quad-\underbrace{m\cdot r\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l}_{\text{expected loss during disruptions}}
\end{aligned}$$

After observing the defender's decisions, the attacker decides to allocate his resources. There are two components in the attacker's objective function shown in Eq. (11): the expected payoff in contest and the expected payoff when the defender experiences disruptions.

$$\begin{aligned}
&\max_{R\geq 0} u_T(r, R, k, I)\\
&= \underbrace{\left(\frac{R\cdot V}{r+R}-\gamma_T\cdot R\right)\int_x\int_l\int_d\left(x+\min\left\{\frac{I}{r},(1-k)l+kd\right\}+k(l-d)\right)f_D(d)f_X(x)f_L(l)\mathrm{d}d\mathrm{d}l\mathrm{d}x}_{\text{expected payoff in contest}} \qquad (11)\\
&\quad+\underbrace{(V-\gamma_T\cdot R)\cdot\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l}_{\text{expected payoff when the defender experiences disruptions}}
\end{aligned}$$

The strategy pair (r^*, k^*, I^*, R^*) is a Subgame Perfect Nash Equilibrium if and only if $R^*=\hat{R}(r^*, k^*, I^*)$ and $(r^*, k^*, I^*)=\arg\max_{(r,k,I)}u_T(r, k, I, \hat{R}(r, k, I))$, where the attacker's best response function $\hat{R}(r, k, I)\equiv\arg\max_R u_T(r, k, I, R)$ could be solved from Eq. (11) as:

$$\begin{aligned}
&\hat{R}(r, k, I)\\
&=\begin{cases}
G_{k,I}, & \text{if } r<\dfrac{V\cdot\left[E[X]+k(E[L]-E[d])+\int_l\int_d\min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}{\gamma_T\left[E[X]+k(E[L]-E[d])+\int_l\int_d\min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l+\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}\\
0, & \text{if } r\geq\dfrac{V\cdot\left[E[X]+k(E[L]-E[d])+\int_l\int_d\min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}{\gamma_T\left[E[X]+k(E[L]-E[d])+\int_l\int_d\min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l+\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}
\end{cases} \qquad (12)
\end{aligned}$$

where $G_{k,I}\equiv\sqrt{\dfrac{V\cdot r\cdot\left[E[X]+k(E[L]-E[d])+\int_l\int_d\min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}{\gamma_T\cdot\left[E[X]+k(E[L]-E[d])+\int_l\int_d\min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l+\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}}-r$ for $r\geq 0$, $k\in\{0, 1\}$ and $I\geq 0$. (See "Appendix 1" for the proof).

Equation (12) shows that the attacker's best resource allocation, R, could be either zero (deterred by the combination of a high level of the defender's resources and capacity backup protection/inventory protection) or positive. When R is positive, $R = G_{k,I}$ is higher when capacity protection is used, $k = 1$, than when there is no capacity protection, $k = 0$. In addition, R increases in the attacker's asset valuation, V, and decreases in the attacker's daily resource cost, γ_T, when R is positive.

Figure 5 shows that the attacker's best response (resource allocation) first increases in the defender's daily resource, and eventually decreases in the defender's daily resource. The attacker's best response (resource allocation) becomes higher when the defender uses capacity backup protection or increases in inventory level, which means that the attacker would not be deterred only by capacity backup protection or inventory protection.

When the defender is more risk averse or when the attacker is more risk seeking, it is more likely that the defender would choose the combined strategy (combination of capacity backup protection and inventory protection) since she could reduce the uncertainty or risk and assure a relatively high revenue.

4 Numerical analysis for equilibrium strategies and payoffs

Considering the uncertainties of each parameter, we conduct extensive numerical analysis to investigate the sensitivity of the parameters on the optimal disruption preparation strategies and the player payoffs.

According to the baseline data, as shown in Table 2, we conduct the following experiments to analyze the numerical sensitivity of the defender's and the attacker's equilibrium strategies and payoffs.

4.1 Combining capacity backup protection and inventory protection

Combining capacity backup protection and inventory protection is the most general case which allows for $I = 0$ and $k = 0$, including capacity backup protection ($I = 0$), inventory protection ($k = 0$), or no protection ($k = I = 0$).

There are four decision variables in combined protection: the defender's daily resource, r, binary variable on capacity backup protection, k, inventory level, I, and the attacker's daily resource, R. Depending on whether these four variables are positive or zero, Table 3 lists all sixteen potential cases. Note that in Table 3 "√" means the case would show or appear in some situations, while "×" means that the case is dominated by other case(s) and would not show.

Table 3 Sixteen cases for combined strategy

Defender resource and inventory	Attacker resource $R > 0$		Attacker resource $R = 0$	
	Backup $k = 1$	No backup $k = 0$	Backup $k = 1$	No backup $k = 0$
$r > 0,\ I > 0$	#1 √	#9 √	#3 √	#11 √
$r > 0,\ I = 0$	#2 √	#10 √	#5 √	#13 √
$r = 0,\ I > 0$	#4 ×	#12 ×	#7 ×	#15 ×
$r = 0,\ I = 0$	#6 ×	#14 ×	#8 ×	#16 √

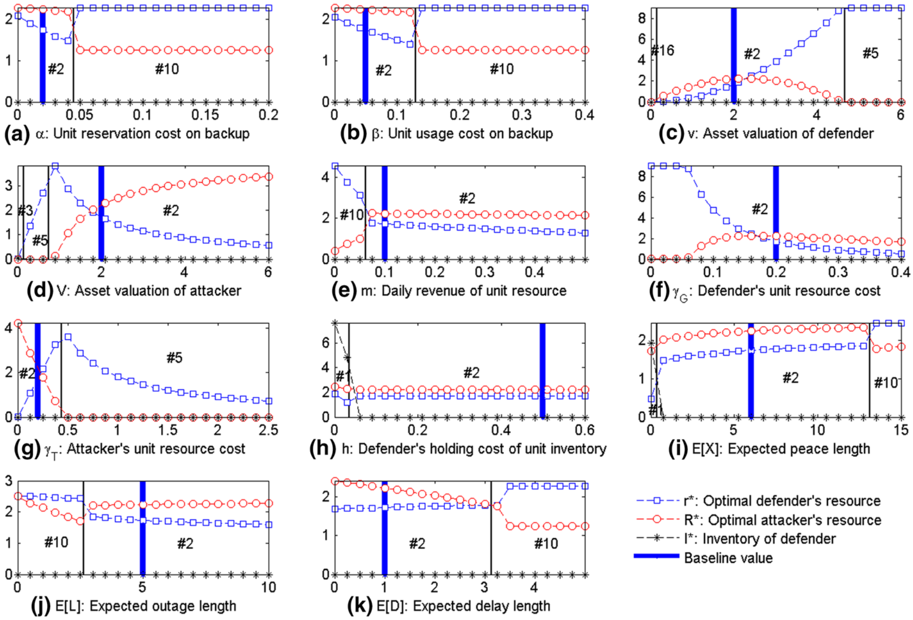

Fig. 6 Optimal player strategies for combined protection with cases defined in Table 3 and baseline values defined in Table 2

Proposition 1 *Under combined protection, six out of sixteen cases, #4, #6, #7, #12, #14 and #15 are dominated, and #8 in Table 3 is weakly dominated.*

See "Appendix 2" for the proof of Proposition 1.

Remark Proposition 1 shows that the defender would use resources ($r > 0$) in eight cases, #1, #2, #3, #5, #9, #10, #11 and #13. However, the defender would not use the resource ($r = 0$) only when the attacker does not use the resource ($R = 0$), or when capacity backup protection and inventory protection are not worthy (#16). In reality, it does not make any sense for the defender to invest in managing the risk of supply chain disruptions if the defender is not willing to exert any resources to win the contest. Therefore, there are nine possible cases: #1, #2, #3, #5, #9, #10, #11, #13 and #16, which illustrate the optimal strategies of defender and the attacker. The defender would not pick cases #4, #7, #8, #12 and #16, while the attacker would not pick cases #6 and #14.

Observation *As seen from Fig. 6, the defender would use combined protection (cases #1 and #3) when (a) the attacker's asset valuation is low; (b) the defender's holding cost is low; or (c) the expected peace time is low.*

4.2 Comparing four protection mechanisms

We compare the expected defender's payoffs under the four protection mechanisms in Fig. 7 using the baseline values shown in Table 2.

Based on the one-way sensitivity analysis in Fig. 7, we find that:

1. The defender benefits in counter-terrorism games by utilizing supply chain risk management tools such as capacity backup or inventory protection, as shown by the gap between

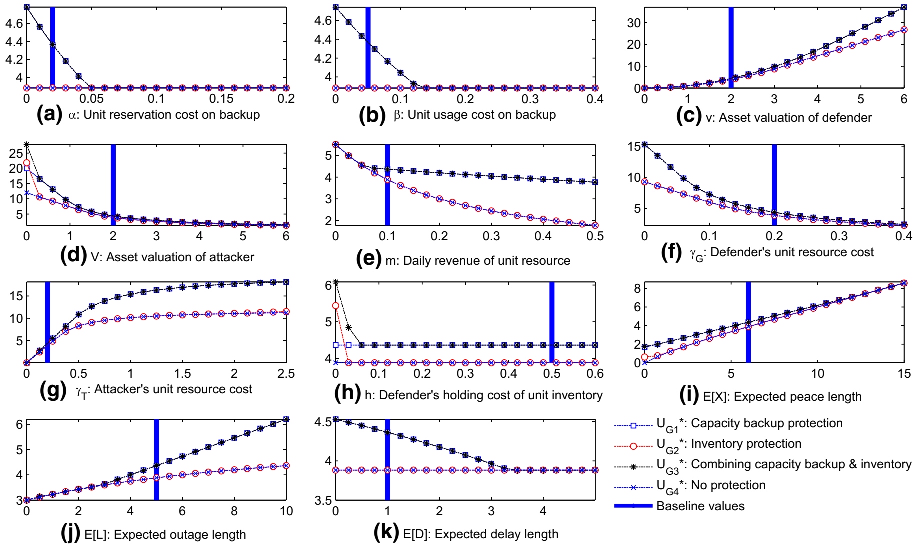

Fig. 7 Comparing defender's payoffs under four protection mechanisms

U^*_{G4} and others. Combined protection always leads to (weakly) higher defender payoffs. This is not surprising because the other two strategies are special cases of the combined strategy.

2. Combined protection is better than capacity backup protection when the attacker's asset valuation, V, the defender's holding cost of unit inventory, h, and the expected peace time, $E[X]$, are low.
3. Combined protection is significantly better than inventory protection, when: (a) the unit reservation cost, α, the unit usage cost of capacity backup, β, the attacker's asset valuation, V, the defender's unit resource cost, γ_G, the holding cost of unit inventory, h, the expected peace length, $E[X]$, and the expected delay length, $E[D]$, are low; and (b) the defender's asset valuation v, daily revenue rate per unit of resource, m, the attacker's unit of resource cost, γ_T, the holding cost of unit inventory, h, and the expected outage length, $E[L]$, are high.
4. Capacity backup protection is significantly better than using inventory protection, when: (a) the unit reservation cost, α, the unit usage cost, β, the defender's unit of resource cost, γ_G, the expected peace length, $E[X]$, and the expected delay length, $E[D]$, are low; (b) the defender's asset valuation v, the daily revenue rate per unit of resource, m, the attacker's unit resource cost, γ_T, the holding cost of unit inventory, h, and the expected outage length, $E[L]$, are high.

5 Conclusions and future research

Defenders' performance may be affected by disruptions to military supply chains. The impact of disruptions could be mitigated by pre-disruption preparation mechanisms. In this paper, we investigate the combined protection mechanism (capacity backup protection and inventory protection), and its impacts on the defender's total expected payoff in a sequential defender–attacker game. We provide a modeling framework to study the impact and optimal use of supply chain risk management tools to mitigate the supply chain disruptions.

Under the combined protection model, the defender's objective is to maximize the total expected payoff by balancing the trade-offs between the protection costs of preparation (e.g., reservation and/or inventory costs) and the disadvantage caused by military supply chain disruptions. We conduct extensive numerical analysis to investigate the optimal protection mechanism. Our results show that the defender does benefit in counter-terrorism games by utilizing supply chain risk management tools such as capacity backup and/or inventory protection, and we document the conditions when such benefit is significant. However, while supply chain risk management tools are beneficial, it is interesting to note that the attacker's best response resource could be higher if the defender uses capacity backup protection and increases in inventory level, which means that the attacker would not be easily deterred by capacity backup protection and/or inventory protection.

Interesting future research directions in this under-studied field of integrating supply chain risk management in a defender–attacker game include: (a) investigating a multi-period inventory protection plan, integrated with a multi-period defender–attacker game (Jose and Zhuang 2013; Wang and Zhuang 2011); (b) extending the single-resource model to a multiple-resource model; (c) considering that both the defender and the attacker could react to disruption by adapting or changing their resource allocations (the defender's daily resource r and the attacker's daily resource R); and (d) extending the single capacity backup model to a more complex model that considers multiple capacity backup providers, and selecting suitable capacity backup supplier(s) from the candidate pool, according to capacity flexibility, cost, and reliability.

Appendices

In this section, we provide proofs for different protection strategies, including capacity backup protection, inventory protection, and combined protection, as well as dominated cases (Proposition 1).

Appendix 1: Proof of best response function for different protections

From the attacker's utility function (Eq. 11), since the attacker's resource allocation R is a continuous variable, we could calculate the optimum of R as a function of the defender's resource allocation, r, decision on using capacity backup, k, and on using inventory, I. In particular, if $R \geq 0$, the first derivative should be zero:

$$\begin{aligned}\frac{dE[u_T]}{dR} &= \left(\frac{V(r+R)-RV}{(r+R)^2} - \gamma_T\right)\left[E[X] + \int_l\int_d \min\left\{\frac{I}{r}, (1-k)l + kd\right\} f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l\right.\\ &\quad \left. + k(E[L]-E[D])\right] - \gamma_T \int_l\int_d \left[(1-k)l + kd - \frac{I}{r}\right]^+ f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l = 0\end{aligned}$$

We solve this equation and get:

$$\begin{aligned}&\hat{R}(r,k,I)\\ &= \begin{cases} G_{k,I}, & \text{if } r < \dfrac{V\cdot\left[E[X]+k(E[L]-E[d])+\int_l\int_d \min\left\{\frac{I}{r},(1-k)l+kd\right\} f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l\right]}{\gamma_T\left[E[X]+k(E[L]-E[d])+\int_l\int_d \min\left\{\frac{I}{r},(1-k)l+kd\right\} f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l+\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+ f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l\right]} \\ 0, & \text{if } r \geq \dfrac{V\cdot\left[E[X]+k(E[L]-E[d])+\int_l\int_d \min\left\{\frac{I}{r},(1-k)l+kd\right\} f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l\right]}{\gamma_T\left[E[X]+k(E[L]-E[d])+\int_l\int_d \min\left\{\frac{I}{r},(1-k)l+kd\right\} f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l+\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+ f_D(d) f_L(l)\mathrm{d}d\mathrm{d}l\right]} \end{cases}\end{aligned}$$

where $G_{k,I} = \sqrt{\frac{V\cdot r\cdot\left[E[X]+k(E[L]-E[d])+\int_l\int_d \min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}{\gamma_T\left[E[X]+k(E[L]-E[d])+\int_l\int_d \min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l+\int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}}$ $- r.$

The second order condition is satisfied, since

$$\frac{d^2E[u_T]}{d^2R} = -\frac{2Vr\left[E[X]+k(E[L]-E[d])+\int_l\int_d \min\left\{\frac{I}{r},(1-k)l+kd\right\}f_D(d)f_L(l)\mathrm{d}d\mathrm{d}l\right]}{(r+R)^3} \leq 0.$$

Best response functions for no protection in Eq. (3), capacity backup protection in Eq. (6), and inventory protection in Eq. (9) are special cases of best response functions for combined protection in Eq. (12) when $I = k = 0$, $I = 0$, and $k = 0$, respectively. Please see above for the proof.

Appendix 2: Proof of dominated cases as shown in Table 3

There are four cases as shown in the following:

1. When $k = 1$ and $r = 0$, from Eq. (10), the payoff function of the defender becomes:

$$\max_{k=1,r=0,I\geq 0} E[u_G(k,r,R,I)] = -\left[h\cdot I\cdot\int_x x\cdot f_X(x)\mathrm{d}x + h\cdot\int_l [I-rl]^+ f_L(l)\mathrm{d}l\right]$$

When $I = 0$, $E[u_G(k,r,R,I)]$ reaches a maximum at 0 due to the first derivative $\frac{dE[u_G]}{dI} \leq 0$. So, for the defender, case #4 is dominated by cases #6 and #8. Similarly, for the defender, case #7 is dominated by cases #6 and #8.

2. When $k = 1$ and $r = 0$, from Eq. (11), the payoff function of the attacker becomes:

$$\max_{R\geq 0} E[u_T(k,r,R,I)] = (V-\gamma_T R)\Bigg(\int_x\int_l\int_d\left(x+min\left\{\frac{I}{r},(1-k)l+kd\right\}+k(l-d)\right) \times f_X(x)f_L(l)f_D(d)\mathrm{d}d\mathrm{d}l\mathrm{d}x + \int_l\int_d\left[kd+(1-k)l-\frac{I}{r}\right]^+ f_L(l)f_D(d)\mathrm{d}d\mathrm{d}l\Bigg)$$

When $R = 0$, $E[u_T(k,r,R,I)]$ reaches a maximum at $V\cdot\left(\int_x x\cdot f_X(x)\mathrm{d}x+\int_l l\cdot f_L(l)\mathrm{d}l\right)$ due to the first derivative $\frac{dE[u_T]}{dR} \leq 0$. Therefore, for the attacker, case #6 is dominated by cases #7 and #8.

3. When $k = 0$ and $r = 0$, Eq. (10) implies:

$$\max_{k=0,r=0,I\geq 0} E[u_G(k,r,R,I)] = -\left[h\cdot I\cdot\int_x x\cdot f_X(x)\mathrm{d}x + h\cdot\int_l\int_{z=0}^{l}[I-rz]^+ f_L(l)\mathrm{d}z\mathrm{d}l\right]$$

When $I = 0$, $E[u_G(k,r,R,I)]$ reaches a maximum at 0 due to the first derivative $\frac{dE[u_G]}{dI} \leq 0$. So, for the defender, case #12 is dominated by cases #15 and #16. Similarly, case #15 is dominated by cases #14 and #16.

4. When $k = 0$ and $r = 0$, from Eq. (11), the payoff function of the attacker becomes:

$$\max_{R\geq 0} E[u_T(r,R,I)] = (V-\gamma_T\cdot R)\cdot\left[\int_x\int_l\left(x+min\left\{\frac{I}{r},l\right\}\right)f_X(x)f_L(l)\mathrm{d}l\mathrm{d}x + \int_l\left[l-\frac{I}{r}\right]^+ f_L(l)\mathrm{d}l\right]$$

When $R = 0$, $E[u_T(r, R, I)]$ reaches a maximum at $\left[\int_x \int_l \left(x + min\left\{\frac{I}{r}, l\right\}\right) f_X(x) f_L(l) \mathrm{d}l\mathrm{d}x + \int_l \left[l - \frac{I}{r}\right]^+ f_L(l)\mathrm{d}l\right] \cdot V$ due to the first derivative $\frac{dE[u_T]}{dR} \leq 0$. Therefore, for the attacker, case #14 is dominated by cases #15 and #16.

In summary, there are nine possible cases: #1, #2, #3, #5, #9, #10, #11, #13 and #16, as shown in Table 3.

References

Bier, V. M., & Haphuriwat, N. (2011). Analytical method to identify the number of containers to inspect at us ports to deter terrorist attacks. *Annals of Operations Research*, *187*(1), 137–158.

Bier, V. M., Nagaraj, A., & Abhichandani, V. (2005). Protection of simple series and parallel systems with components of different values. *Reliability Engineering and System Safety*, *87*(3), 315–323.

Chopra, S., Reinhardt, G., & Mohan, U. (2007). The importance of decoupling recurrent and disruption risks in a supply chain. *Naval Research Logistics*, *54*(5), 544–555.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review*, *46*(1), 53–61.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution and Logistics Management*, *34*(5), 388–396.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, *15*(2), 1–13.

Dutta, P. K. (1999). *Strategies and games: Theory and practice*. Cambridge, MA: MIT Press.

Hopp, J. W., Liu, M., & Liu, Z. (2010). *Protecting supply chain networks against catastrophic failures*. Working paper, Department of Operations and Information Management, Wisconsin School of Business, University of Wisconsin-Madison.

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

Jin, S., Liu, Z., & Zhuang, J. (2010). Monte carlo simulation-based supply chain disruption management for wargames. In *Proceedings of the 2010 winter simulation conference* (pp. 2682–2693).

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

Kane, T. M. (2001). *Military logistics and strategic performance* (Vol. 1). Taylor: Psychology Press.

Kress, M. (2012). Modeling armed conflicts. *Science*, *336*(6083), 865–869.

Mas-Colell, A., Whinston, M. D., & Green, J. R. (1995). *Microeconomic theory*. New York, NY: Oxford University Press.

National Public Radio. (2011). *Among the costs of war: Billions a year in A.C.?* http://www.npr.org/2011/06/25/137414737/among-the-costs-of-war-20b-in-air-conditioning/. Accessed in January, 2015.

Paul, J. A., & Hariharan, G. (2012). Location-allocation planning of stockpiles for effective disaster mitigation. *Annals of Operations Research*, *196*(1), 469–490.

Sandler, T., & Siqueira, K. (2006). Global terrorism: Deterrence versus pre-emption. *Canadian Journal of Economics*, *39*(4), 1370–1387.

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

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

Simon, S. J. (2001). The art of military logistics. *Communications of the ACM*, *44*(6), 62–66.

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

von Clausewitz, C. (2004). *On war*. Boston: Digireads.com Publishing.

Wang, X., & Zhuang, J. (2011). Balancing congestion and security in the presence of strategic applicants with private information. *European Journal of Operational Research*, *212*(1), 100–111.

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

Zhuang, J., Saxton, G. D., & Wu, H. (2014). Publicity vs. impact in nonprofit disclosures and donor preferences: A sequential game with one nonprofit organization and N donors. *Annals of Operations Research*, *221*(1), 469–491.