Integrating the API SRA methodology and game theory for improving chemical plant protection

Integrating the API SRA methodology and game theory for improving chemical plant protection

Laobing Zhang[a,*], Genserik Reniers[a,b,c] , Bin Chen[d], Xiaogang Qiu[d]

[a] Faculty of Technology, Policy and Management, Safety and Security Science Group (S3G), TU Delft, 2628 BX Delft, The Netherlands.

[b] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), University Antwerp, 2000 Antwerp, Belgium.

[c] CEDON, KULeuven, Campus Brussels, 1000, Brussels, Belgium.

[d] Research Center of Computational Experiments and Parallel System Technology, College of Information System and Management, National University of Defense Technology, Changsha 410073, China.

(*) Author to whom correspondence should be addressed.

tel. (+31)15 27 85695

e-mail: Laobing.zhang@tudelft.nl

Submitted for publication in:

Journal of Loss Prevention in the Process Industries

Abstract

Game theory has been employed in academia to study the improvement of security in chemical plants. Being able to model intelligent interactions between adaptive adversaries and defenders is the main advantage of game theory, while the main criticisms of the usage of game theory is that it is mathematically complicated and that it over-simplifies reality. The ANSI/API standard 780 on Security Risk Assessment for the petroleum and petrochemical industries (abbreviated as the "API SRA methodology"), conversely, provides a systematic approach for obtaining qualitative or semi-quantitative data, and is criticized on its failure at modelling strategic (and intelligent) adversaries. Integration of game theory and the API SRA methodology for improving chemical plant protection is therefore an interesting domain of study. In this paper, the API SRA methodology bridges the gap between "chemical security reality" and "chemical security theory (that is, game theoretic models)", by providing quantitative inputs for game theoretic models and by reflecting on game theoretic results with respect to industrial practice.

Highlights

1) An approach for integrating the API SRA methodology and game theory is proposed;
2) Suggestions for improving the API SRA methodology are given;
3) Discussion and innovative thinking on security games are given.

Keywords

Security risk assessment; ANSI/API standard 780 ; chemical plant protection; game theory

1, INTRODUCTION

Nowadays, the frequency with which terrorist attacks happen, enforce risk analysts to pay ever more attention to such malicious events. Reniers et al. (2011) defined security risks as the risks caused by intentional behaviour, for example, by a terrorist, a disgruntled employee, etc. Safety risks can be defined as risks caused by unintentional events (e.g., natural disasters, industrial accidents etc.). Due to the existence of hazards (e.g., high pressure circumstances, toxic materials, etc.), the process industry could be an attractive target for deliberate attacks. For instance, Orum and Rushing (2008) indicate that a successful attack on the 101 most dangerous chemical facilities in the USA may threaten 1 million people or more.

To better protect process industries, a set of academic researches as well as some industrial standards were published during the last decades. Bajpai and Gupta (2005) proposed that security assessment in chemical sites should consist of threat analysis, vulnerability analysis, countermeasures analysis, and mitigation and emergency response. Other academic publications (e.g., Lee et al., 2010, Argenti et al., 2015) followed Bajpai and Gupta's framework, though improving it and being more concrete on the details of each step. The American Petroleum Institute (API) published its recommended practice 780 in 2013 (API, 2013), namely, the "security risk assessment methodology for the petroleum and petrochemical industries" (the so-called API SRA methodology). The API SRA methodology has been extensively implemented in industrial practise. However, the API SRA methodology as well as the above mentioned chemical security researches are criticized for modelling security adversaries as non-strategic actors (Cox Jr, 2008; Powell, 2007).

Security risk, being "intentionally caused", is different from safety risk, which is "randomly happening". Adversaries in security risks are human beings, and human adversaries may implement their attack adaptively or intelligently (Brown et al., 2006; FAS, 2006). To this end, game theory was introduced into the security domain (Bier and Azaiez, 2008; Cox Jr, 2009; Tambe, 2011). Zhang and Reniers (2016) proposed a chemical plant protection (CPP) game, and later on, Zhang et al. (2017) extended the CPP game to be able to process inputs with distribution-free uncertainties. Feng et al.

(2016) studied a game theoretic approach to optimally allocate security resources in a setting of multiple chemical facilities. Talarico et al. (2015) and Rezazadeh et al. (2017) carried out researches on applying game theory to protect transportation modes of chemical materials. Pavlova and Reniers (2011) studied how to stimulate security investments in chemical clusters, by employing a cooperative game. Game theoretic models are capable to model intelligent interactions between industrial defenders and potential attackers. However, game theoretic models are also seriously criticized for i) their requirements of quantitative inputs, some of which are difficult (or impossible) to obtain; and ii) their strict assumptions, such as the common knowledge assumption, the rational players assumption etc.

This paper therefore aims at illustrating how the API SRA methodology and the game theoretic models can be integrated to improve the protection of chemical facilities. In the remainder of the paper, Section 2 briefly demonstrates the API SRA methodology and the security game methodology, while Section 3 explains how to integrate the API SRA methodology and the security game for improving the protection of chemical plant. A further discussion on the use of security games in industrial plant protection , is given in Section 4. Finally, conclusions are drawn in Section 5.

2, BASELINE MODEL

In this section, the API SRA methodology and the so-called 'security game' are introduced.

2.1, the API SRA Methodology

The American Petroleum Institute (API) published a recommendation on Security Risk Assessment (SRA) for the petroleum and petrochemical industries, in 2004. Later, in 2013, API extended the 2004 version of the SRA methodology without changing its basic idea. In this paper, the API SRA methodology denotes the 2013 version API standard on "Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries" (API, 2013).

2.1.1, the API SRA procedure

Figure 1 in combination with table 1, briefly illustrate the security risk assessment and management procedure of the API SRA methodology. The left-hand side of figure 1 shows the sub-steps of the methodology, while the right-hand side shows the output data of each step. Explanations of the outputs are given in table 1.

In the characterization step, the SRA team roughly scans the given petrochemical plant, and provides a critical assets list CAL as well as asset severity scores AS, according to functions of assets, interconnectivities among assets, and possible consequences. In the threat assessment step, the SRA team decides a threats list TL and threat levels TS that the plant is faced with, based on historical security data (site-specific, national, worldwide) and intelligence. For each asset and threat pair $\{(a,t)|a \in CAL, t \in TL\}$, the asset's attractiveness to the threat $Atr_{(a,t)}$ and possible attack scenarios linking the threat with the asset $Sce_{(a,t)}$ are evaluated. Based on current (situation '1') security countermeasures, vulnerabilities $V^1_{(a,t,s)}$ and consequences $C^1_{(a,t,s)}$ are estimated for each asset, threat, and scenario triad $\{(a,t,s)|a \in CAL, t \in TL, s \in Sce_{(a,t)}\}$. Furthermore, the SRA team calculates the likelihood of an attack from a given threat $t \in TL$ to a given asset $a \in CAL$ as $L^1_{(a,t)} = TS_t \times Atr_{(a,t)}$, and calculates the likelihood of a successful attack from t to a by using scenario $s \in Sce_{(a,t)}$ as $L_{(a,t,s)} = L^1_{(a,t)} \times V^1_{(a,t,s)}$. The risk matrix method is used to calculate a security risk $R^1_{(a,t,s)}$ for each asset, threat, and scenario triad, and in this step, the likelihood of a successful attack $L_{(a,t,s)}$ and the scenario-specific consequence $C^1_{(a,t,s)}$ are used to determine the risk value in the risk matrix. Based on the gaps between the current security risk and the desirable level of risk, scenario-specific countermeasures $CM_{(a,t,s)}$ are proposed by the SRA team, and subsequently all the scenario-specific countermeasures are united into one countermeasure list CML.

The SRA team further re-estimates the vulnerabilities $V^2_{(a,t,s,cm)}$, consequences $C^2_{(a,t,s,cm)}$, and security risks $R^2_{(a,t,s,cm)}$, presuming that a countermeasure $cm \in CML$ is implemented (situation '2'). Based on the recalculation, the risk reduction of each countermeasure ΔR_{cm} can be calculated as the

summation of risk reduced in each asset, threat, and scenario triad, as shown in formula (1). Finally, the proposed countermeasures are ranked according to their potential risk reduction ΔR_{cm} as well as some other practical information (e.g., costs).

$$\Delta R_{cm} = \sum_{a \in CAL} \sum_{t \in TL} \sum_{s \in Sce(a,t)} (R^2_{(a,t,s,cm)} - R^1_{(a,t,s)}). \quad (1)$$

Table 1. Output data of the API SRA methodology

Notation	Definition	Comments*
CAL	Critical assets list	e.g., control centre, gasoline tanks etc. Ref to "assets" column in form 1.
AS	Asset score	Measuring asset severity. Ref to "asset severity ranking" column in form 1.
TL	Threat list	e.g., terrorists, disgruntled employee etc. Ref to "threat" column in form 2.
TS	Threat score	Measuring threat ranking. Ref to "threat ranking" column in form 2.
$At_{(t,a)}$	A given asset's (a) attractiveness to a given threat (t).	$t \in TL, a \in CAL$. Numbers, ref to column 2a1, 2b1 etc. in form 3.
$Sce_{(a,t)}$	A given threat's possible attack scenarios to a given asset.	Ref to "scenario" column in form 4.
$V^1_{(a,t,s)}, C^1_{(a,t,s)}$	Vulnerability '1' and Consequences '1' (in case the attack is successful) of an attack scenario from a given threat to a given asset.	$t \in TL, a \in CAL, s \in Sce_{(a,t)}$. Ref to the "V" and "C1" column in form 4.
$R^1_{(a,t,s)}$	Security risk '1' of a given asset from a given threat by using a given attack scenario.	Ref to the "R1" column in form 4.
$CM_{(a,t,s)}$	Recommended countermeasures to reduce security risk of a given asset from a given threat by using a given attack scenario.	Ref to "proposed countermeasures" column in form 4.
CML	Recommended countermeasure list	$CML = \bigcup_{a,t,s} CM_{(a,t,s)}$.
$V^2_{(a,t,s,cm)}, C^2_{(a,t,s,cm)}$	Vulnerability '2' and Consequences '2' (in case the attack is successful) of an attack scenario from a given threat to a given asset, presuming a suggested countermeasure is implemented.	$cm \in CML$. Ref to "Residual Risk" column in form 5.
$R^2_{(a,t,s,cm)}$	Security risk '2' of a given asset from a given threat by using a given attack scenario, presuming a suggested countermeasure is implemented.	
ΔR_{cm}	Risk reduction by a proposed countermeasure.	Ref to "Risk Reduction" column in form 6.

$PCML$	Countermeasure list with priority ranking	Ref to "overall priority" column in form 6.

* Forms in this column refer to the forms in the API SRA standard document API, 2013. ('1': current state, without any further countermeasures; '2': new state, with new countermeasures).

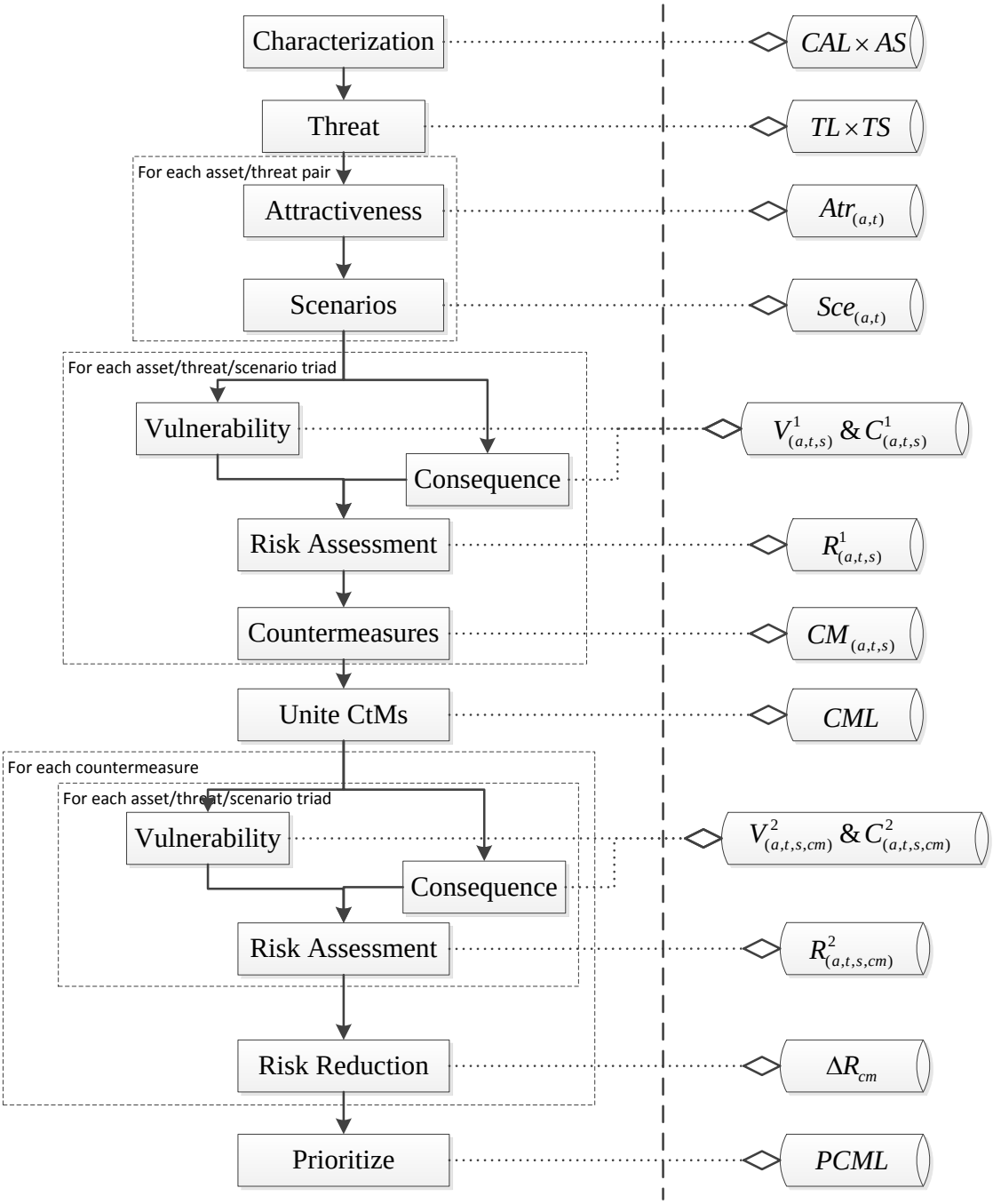

Figure 1. the API SRA Procedure

2.1.2, Comments of the API SRA methodology

The API SRA methodology, since it has been released, has been extensively used in industrial practice and has been much referred to in academic research.

The methodology provides a systematic and practically implementable approach for security risk assessment in the process and petrochemical industries. Besides the procedure and the output data mentioned in the above section, the standard also i) provides clear definitions of terminologies used in the chemical security domain; ii) gives guidance on how to organize an SRA team and what are each members' responsibilities and tasks; and iii) clearly points out what kind of data is required for a successful security risk assessment.

Results of the API SRA methodology is robust (Moore, 2013) due to several reasons: i) it considers multiple types of threats, e.g., from terrorists, disgruntled employees, etc.; ii) it focuses on minimizing the defender's possible maximal (worst-case) losses; and iii) it takes into account the uncertainties during a security risk assessment procedure.

However, the API SRA methodology has several drawbacks. The most commonly mentioned drawback is that it models security adversaries as non-strategic actors. As shown in Figure 1, the SRA team estimates an asset's attractiveness to a threat $Atr_{(a,t)}$ at the very beginning of the procedure, and it is clearly stated in the standard that when estimating the attractiveness, "difficulty of the act, including ease of access and degree of existing security measures (soft target vs hardened target)" should be addressed. Then in the risk re-estimating stage, when a proposed countermeasure $cm \in CML$ is presumed to be implemented, the team only re-estimates the vulnerability and the consequence, without resetting the $Atr_{(a,t)}$ ("retaining the original value for L_1"). This is anti-intuitive. On the one hand, why would the existing countermeasures be able to affect the attractiveness while the new proposed countermeasures cannot do so? On the other hand, if an asset is well protected by the proposed countermeasure, the attractiveness would definitely decrease. Academic research (e.g., Golany et al., 2009) as well as empirical studies (e.g., the Al Qaeda training manual, FAS, 2006) also reveal that human adversaries would plan and implement their attack according to the defender's defence.

The usage of a risk scoring method and a risk matrix can be another drawback of the API SRA methodology. For critiques and possible improvements of risk scoring methods, interested readers are, for instance, referred to Cox (2008), and Baybutt (2016).

2.2, Game Theoretic Risk Analysis of Security Threats

To deal with strategic human adversaries and to give quantitative insights in security management, game theory was introduced into the security domain (Bier and Azaiez, 2008; Cox Jr, 2009; Hall Jr, 2009; Tambe, 2011). In the remainder of the paper, game theoretic models developed for improving security are abbreviated as "security games".

2.2.1, the methodology

Game theory was created to deal with intelligent interactions among multiple strategic actors. A game theoretic model consists of a set of (at least 2) players, strategy sets for each player, and payoffs for each player under each tuple of strategies.

An example can be helpful to explain what is a game theoretic model and how it can be used for security research. Consider a chemical plant with two critical assets $CAL = \{a_1, a_2\}$, and for the sake of simplicity, assume that there is no protective barrier yet and the defender has one guard who can protect one asset. Site-specific data shows that the plant faces a threat from thieves. The defender loses l_1 and l_2 from a successful theft on asset 1 and 2 respectively, while the thief's gain is g_1 and g_2. The thief loses p due to punishment and the defender gains a reward r, if the thief is caught by the defender.

		Defender	
		Protect a_1	Protect a_2
Thief	Steal a_1	$-p, r$	$g_1, -l_1$
	Steal a_2	$g_2, -l_2$	$-p, r$

Figure 2. Illustrative game theoretic model

Modelling the example in a game theoretic approach, there are 2 players, namely the defender and the thief. The defender/thief has two strategies, to protect/steal asset 1 or asset 2. If the defender

protects asset 1 and the thief steals asset 1, the thief would be caught, the defender gets a payoff r and the thief suffers a loss p; if the defender protects asset 1 and the thief steals asset 2, the thief would succeed, the defender suffers a loss l_2 and the thief gains g_2; payoffs for the other 2 strategies tuples can be calculated analogously. Figure 2 shows the game in a normal form.

A game is called a simultaneous game if each player chooses his action without knowledge of the action chosen by the other player. In the example, if the defender does not know which asset the thief will steal and the thief does not know any information of where the guard is, the game is a simultaneous game. A 2-player game is called a sequential game if when one player chooses his action, he already knows the other player's (mixed) strategy. In the example, a more frequent situation is that when the thief decides which asset to steal, he already knows some information about the defender's defence. A mixed strategy is an assignment of a probability for each pure strategy. In the example, the defender's mixed strategy can be to protect asset 1 with a probability x_1, and to protect asset 2 with probability $1 - x_1$.

The classic game theoretic model assumes rational players and common knowledge of the game. A rational player plays a strategy to maximize his/her own payoff. Common knowledge of the game means that all the players know the rules of the game, the payoffs in the game for both himself and others, and that other players also know what he knows. Research during the last decades has paid a lot of attention to relax these 2 assumptions, that is, current research is aimed even more at bounded rational players and incomplete information games (Bayesian games).

A (Bayesian) Nash Equilibrium is commonly used for predicting outcomes of simultaneous games, while for two-player sequential games, the (Bayesian) Stackelberg Equilibrium is extensively employed (Gibbons, 1992).

2.2.2, Criticisms on security games

Security games have been widely studied in academia, and several security game based systems have been deployed in reality (Tambe, 2011). However, criticisms do exist.

Some security game models are criticized as 'magic mathematical games' due to sometimes unrealistic assumptions. Most researchers agree that (human) adversaries would plan and implement attacks adaptively. However, whether adversaries are rational (i.e., aiming at maximizing their payoff) is still a topic under study. Researchers also realize that security risk management involves huge uncertainties such that the 'common knowledge assumption' would not hold. For a more detailed discussion of these criticisms, interested readers are referred to Guikema (2009). In this paper, some insights in these criticisms are provided in the discussion section.

Besides its possible unrealistic assumptions, game theoretic modelling is also criticized for its requirements with respect to of quantitative input. As illustrated in figure 2, parameters p, r, l_1, g_1, l_2, g_2 should be provided in order to analyse the game. In practice, however, it can be quite difficult (almost impossible) to obtain these exact data. Let us take as an example g_1, which denotes the thief's gain from successfully stealing asset 1: it is not possible to know what would be the exact gain for the thief, since it is largely dependable on the thief's perception. In literature, the Chemical Plant Protection game proposed by Zhang and Reniers (2016) requires quantitative data such as the success probabilities and consequences of an attack under any given attack scenarios and any given defence plans, from both the defender and the attacker's point of view. In Feng et al. (2016), the defender needs to know a prior probabilities of occurrence of different types of attackers, and also attackers' estimations of vulnerabilities and consequences under each of the players' strategy pairs. These above mentioned quantitative inputs are very difficult to obtain.

3, SUPPORT SECURITY GAMES WITH THE API SRA METHODOLOGY

Hall Jr (2009) mentions that "If the conditions creating the problems you had to deal with were natural or random, the answer was decision analysis (which looked a lot like what we now call risk analysis). If the conditions creating the problems you had to deal with were the result of deliberate choice, the answer was game theory."

Though game theory is a proper choice for dealing with strategic (human) adversaries, its requirement of quantitative input data limits its applications in industrial security practice. The API SRA methodology is a systematic approach for evaluating security risks in the process industries, and it outputs plenty of data (as shown in table 1). However, the usage of data in the API SRA methodology is incorrect or not sufficient. In this section, an approach to support security games with the output data from the API SRA methodology is therefore proposed.

3.1, Overview

Table 2 describes an approach of constructing/feeding a security game model for chemical plants protection by using outputs from the API SRA methodology. As introduced in the previous section, a game theoretic model consists of players, strategy sets, and payoffs.

The SRA procedure should be conducted by a well-organized risk assessment team (i.e., the SRA team), presuming that the plant is facing some threats (i.e., TL) and each threat has a threat score (i.e., TS) measuring how likely it is that the threat will be true. In a game theoretic setting, the SRA team and the potential adversaries act as 2 players, namely, the defender and the attacker. The attacker may have several different types, and the prior probabilities can be calculated by formula (2), in which p^t denotes the prior probability of attacker type t, and ts^t denotes the threat score of attacker type t. Constructing the game as a defender-attacker game implies that different types of attackers are independent, or, in other words, collusions/conflicts among different types of attackers are not considered. If this is not the case (e.g., a joint attack by terrorists and disgruntled employees), multiple players or multiple stages games should be employed.

$$p^t = \frac{ts^t}{\sum_{l \in TL} ts^l}, t \in TL, ts \in TS. \quad (2)$$

One outcome of the SRA procedure is the recommended countermeasure list CML. The defender's strategy set can be defined as the power set of CML, i.e., $S_d = 2^{CML}$. This definition means that for each countermeasure $cm \in CML$, the defender can decide whether to implement it or not. For instance, if $CML = \{CCTV, Patrol\}$, then $S_d = \{\emptyset, \{CCTV\}, \{Patrol\}, \{CCTV, Patrol\}\}$. The number

of the defender's pure strategies would increase exponentially with this definition. However, on the one hand, some combinations of countermeasures are practically inefficient (e.g., using drones to spy the premises and also having guards on patrol 24/7). On the other hand, due to budget constraints, the defender would only be able to implement limited countermeasures. To this end, the defender's strategy set would not be too large. The modelling of the attacker's strategy is a bit more complicated. First of all, there are multiple types of attackers (e.g., terrorist, activist, etc.), and different types of attackers have different strategy sets. For each type of attacker $t \in TL$, his[a] strategy set can be defined by formula (3), in which S_a^t denotes strategy set for attacker t, (a, s) denotes attacking critical asset $a \in CAL$ by using scenario $s \in Sce_{(a,t)}$. The attacker can also be deterred, without executing an attack.

$$S_a^t = \left\{(a,s)\middle|\forall a \in \text{CAL}, \forall s \in \text{Sce}_{(a,t)}\right\} \cup \{no\ attack\}. \quad (3)$$

Table 2. Mapping the API SRA methodology data to security game terminologies

Game theoretic terminology		The API SRA methodology
Player	Defender	The SRA team
	Attackers	Threats in the threat list TL, e.g., terrorist, activists, etc.
Strategy	Defender strategy set	$S_d = 2^{CML}$.
	Attacker strategy set	$S_a^t = \left\{(a,s)\middle|\forall a \in \text{CAL}, \forall s \in \text{Sce}_{(a,t)}\right\} \cup \{no\ attack\}$.
Payoff*	Defender payoff	$u_d^t(s_d, s_a^t) = \begin{cases} -Cd_{s_d} & s_a^t = no\ attack \\ -V^2_{(a,t,s,cm_{i1\sim ik})} \cdot C^2_{(a,t,s,cm_{i1\sim ik})} - Cd_{s_d} & otherwise \end{cases}$.
	Attacker payoff	$u_a^t(s_d, s_a^t) = \begin{cases} 0 & s_a^t = no\ attack \\ G^t_{(a,s,cm_{i1\sim ik})} - Ca_s & otherwise \end{cases}$.

* If $s_d = \emptyset$, then $Cd_{s_d} = 0$, and $cm_{i1\sim ik} = NULL$.

The API SRA methodology (re-)evaluates scenario-specific vulnerability $V^1_{(a,t,s)}$ ($V^2_{(a,t,s,cm)}$) and consequence $C^1_{(a,t,s)}$ ($C^2_{(a,t,s,cm)}$) (if a countermeasure $cm \in CML$ is presumed to be implemented).

[a] In this paper, attackers/threats are represented by he/him/his, while defenders/managers are represented as she/her/her.

For computing players' payoffs, in case of an attacker type $t \in TL$, assuming that the defender plays a pure strategy $s_d \in S_d$ and the attacker plays a pure strategy $s_a^t \in S_a^t$, there are four possible cases: (i) if $s_d = \emptyset$ and $s_a^t = no\ attack$, it means that the defender does not implement any of the recommended countermeasures, and the attacker does not implement an attack. In this case, both the defender and the attacker have a payoff of 0, i.e., $u_d^t(\emptyset, no\ attack) = u_a^t(\emptyset, no\ attack) = 0$. (ii) if $s_d = \emptyset$ and $s_a^t = (a, s)$, it means that the defender does not implement any of the recommended countermeasures, and the attacker attacks asset a by using scenario s. In this case, the defender's payoff can be defined as the product of the scenario-specific vulnerability $V_{(a,t,s)}^1$ and the scenario-specific consequence $C_{(a,t,s)}^1$, i.e., $u_d^t(\emptyset, (a, s)) = -V_{(a,t,s)}^1 \cdot C_{(a,t,s)}^1$. The attacker's payoff can be defined as $u_a^t(\emptyset, (a, s)) = G_{(a,s)}^t - Ca_s$, where $G_{(a,s)}^t$ denotes attacker t's expected gain from attacking target a by using scenario s, and Ca_s denotes the attack cost of scenario s. (iii) if $s_d = \{cm_{i1}, cm_{i2}, \dots, cm_{ik}\}$ and $s_a^t = no\ attack$, it means that the defender implements several recommended countermeasures while the attacker does not attack. In this case, the defender's payoff is $u_d^t(s_d, no\ attack) = -Cd_{s_d}$ and the attacker's payoff is $u_a^t(s_d, no\ attack) = 0$. (iv) if $s_d = \{cm_{i1}, cm_{i2}, \dots, cm_{ik}\}$ and $s_a^t = (a, s)$, it means that the defender implements several recommended countermeasures and the attacker attacks asset a by using scenario s. In this case, the defender's payoff can be defined as $u_d^t(s_d, (a, s)) = -V_{(a,t,s,cm_{i1\sim ik})}^2 \cdot C_{(a,t,s,cm_{i1\sim ik})}^2 - Cd_{s_d}$ and the attacker's payoff can be defined as $u_a^t(s_d, (a, s)) = G_{(a,s,cm_{i1\sim ik})}^t - Ca_s$.

By constructing a security game based on the output data from the API SRA methodology, the equilibrium for this security game can be calculated. Equilibrium analysis of the constructed security game outputs an equilibrium strategy pair (s) $(\bar{s}_d, \bar{s}_a^t)$ and a corresponding equilibrium payoff (s) $(\bar{u}_d, u_a^t)$.

$\bar{s}_d$ is a bundle of the proposed countermeasures CML (or a $\emptyset$) (see, the definition of S_d in table 2). In the API SRA methodology, the CML is sorted according to a decreasing risk, resulting in a prioritized

countermeasure list $PCML$. To explain and understand the $\bar{s}_d$ in a API SRA methodology approach, the following rule can be used:

$$\forall cm \in CML, if\ cm \in \bar{s}_d, then\ Prt_{cm} = 1;\ if\ cm \notin \bar{s}_d, then\ Prt_{cm} = 2,$$

where Prt_{cm} denotes the priority of countermeasure cm. This rule divides CML into 2 categories, namely, a category with countermeasures which can be implemented and a category with countermeasures which cannot be implemented. When modelling the defender's strategy, her budget constraint is considered, thus the two categories also take into account the defender's budget. The division into categories results from a game theoretic approach, and hence the intelligent interaction between defender and attacker is taken into account.

The attacker's equilibrium strategy $\bar{s}_a^t = (\bar{a}, \bar{s}) \in S_a^t$ denotes that he would attack asset $\bar{a}$ by using scenario $\bar{s}$. Readers may argue that knowing this, why would the defender not enhance countermeasures to protect asset $\bar{a}$ from scenario $\bar{s}$? The answer is simple: security adversaries are intelligent. If the defender changes her equilibrium strategy to protect asset $\bar{a}$ more, the attacker would also change his attack strategy accordingly.

The defender's equilibrium payoff $\bar{u}_d$ reflects the mitigated security risk, and in the API SRA methodology, it is denoted as R^2. The attacker's equilibrium payoff u_a^t reflects the attacker's attack motivation, and in the API SRA methodology, it is named "degree of interest".

It is worth noting that these output analyses are based on a pure strategy setting. In section 4, a discussion on the usage of a mixed strategy for the defender is given. For the attacker, a mixed strategy is alwaysapplicable. A mixed strategy for the attacker can be defined as: $MiS_a^t = \left\{ y \in R^{|S_a^t|} \middle| \sum_{a \in CAL} \sum_{s \in Sce_{(a,t)}} y_{(a,s)} + y_{na} = 1, y_{(a,s)}, y_{na} \geq 0 \right\}$, where $y_{(a,s)}$ (y_{na}) denotes the probability that a pure strategy (a, s) (no attack) would be played. Assuming that $\bar{y}$ is the attacker's mixed equilibrium strategy, the likelihood that the attacker t would attack asset a can be calculated

as: $lk_{(a,t)} = \sum_{s \in Sce_{(a,t)}} \bar{y}_{(a,s)}$, which in the API SRA methodology, it is represented as "attractiveness", as shown in Table 8 in the API SRA document (API, 2013).

Based on the above discussion, figure 3 shows an overview on how to integrate the API SRA methodology and the security game to improve chemical plant protection.

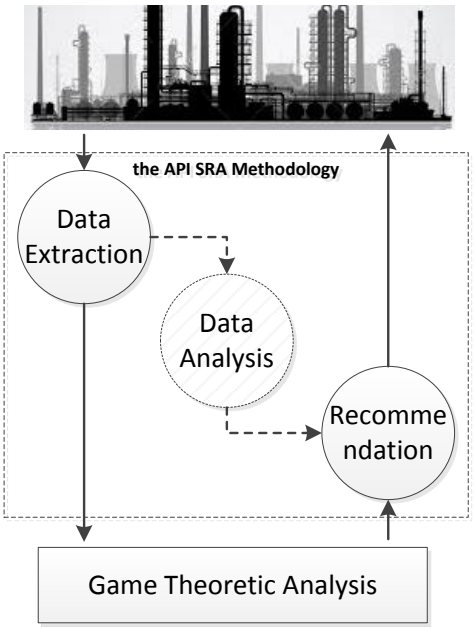

Figure 3. Integration of the API SRA methodology and game theory

3.2, Risk Assessment under a Bundle of Countermeasures

In the payoff definition given in section 3.1, the scenario-specific vulnerability and consequence levels under condition of several countermeasures (i.e., $V^2_{(a,t,s,cm_{i1\sim ik})}$ and $C^2_{(a,t,s,cm_{i1\sim ik})}$) are not clearly described yet. In the API SRA methodology, the SRA team only re-estimates vulnerabilities and consequences presuming that one proposed countermeasure is implemented (see form 6 in the API SRA document (API, 2013)). The game theoretic modelling allows the defender to implement any reasonable bundle of proposed countermeasures, and in these cases, the vulnerability and consequences cannot be obtained directly from the API SRA data.

To address the abovementioned problem, the API SRA team should re-estimate risks under a bundle of countermeasures. It is theoretically necessary for constructing the game theoretic model. Furthermore, synergistic effects of multiple countermeasures should not be under-estimated. An

example of a synergistic effect is the combination of a camera system and having fences. Cameras without fences or fences without cameras are much less efficient than both together.

3.3, Data Assessment from the Adversaries' Viewpoint

A main challenge in assessing and managing security risks in chemical plants is the fact that one is dealing with intelligent adaptive adversaries. To fight with these intelligent attackers, the defender should not only pay attention to her own interests, but also study the attacker's interests. The API SRA methodology implicitly assumes that the attacker's interests are opposite to the ones of the defender, i.e., $G^{t}_{(a,s)} = V^{1}_{(a,t,s)} \cdot C^{1}_{(a,t,s)}$ and $G^{t}_{(a,s,cm_{i1\sim ik})} = V^{2}_{(a,t,s,cm_{i1\sim ik})} \cdot C^{2}_{(a,t,s,cm_{i1\sim ik})}$. However, this is not always the case. Firstly, although there might be positive correlations between the attacker's gain and the defender's loss from an attack, the exact numbers are not necessarily the same. For instance, for an explosion caused by a terrorist, the defender may have casualties, economic loss, environmental pollution etc., while the attacker may find his gain purely from causing fear to people. Generally speaking, the higher loss the defender has, the more fear will be caused in society. But a loss consisting of 1 casualty and 1 million euro economic loss and a loss consisting of zero casualties and 6.8 million euro economic loss may have different effects on public emotion. Nevertheless, from the defender's economic point of view, the loss may be the same (IENM, 2013; Reniers and Van Erp, 2016). Secondly, in some cases, an attacker's gain can be less correlated to the defender's loss. For example, a thief may only earn the device by stealing a computer, while the defender can lose important data from the theft (e.g., company-sensitive information).

It is important to also assess data from the adversaries' viewpoint, since intelligent attackers may represent a high probability to attack targets which could be very safe from an unintentional point of view. However, it is difficult to know the attackers' preferences. The defender may be able to estimate her losses from an oil tank explosion (still uncertainties exist), but how can she know a terrorist attacker's gain from such an explosion? The estimation of probabilities of a successful attack (i.e., vulnerabilities) is even more difficult: under a certain defence plan and an attack scenario, how likely is it that the attack can succeed? On the one hand it is a difficult question itself, on the other hand, a risk-seeking attacker (e.g., a terrorist) and a risk-aversion attacker (e.g., a thief) may have a different

perception. Due to the difficulty of obtaining it, the attackers' data is assumed to be the same as the defender's corresponding data in the API SRA methodology.

Knowing the importance and difficulties of obtaining the attackers' data, some approaches have been proposed (Kiekintveld et al., 2013; Kiekintveld et al., 2011; Nikoofal and Zhuang, 2012, 2015). One approach is to model the attackers' data as distribution-free intervals. That is to say, though it is difficult to estimate the accurate data from the attacker's point of view, it is possible to decide which interval it will be located in. For example, the defender may assume that a terrorist has a reward from a lower bound lb euro to an upper bound ub euro from an oil tank explosion, and the defender does not know the distribution on the interval $[lb, ub]$. Zhang et al. (2017) studied a chemical plant protection game with distribution-free uncertainties on the attacker's data, and their results showed that i) accurately estimating the attacker's data would increase the defender's payoff; ii) increasing the defender's uncertainty on attacker's data would reduce the defender's payoff; iii) if the defender's uncertainty on the attacker's data is large enough, the defender's payoff would be as low as her MiniMax payoff, which means her information of the attacker (the distribution-free interval data) is useless. The third finding in Zhang et al. (2017) explains the reasonability of the API SRA methodology's assumption on the attacker's data, and the first and second findings stimulate researchers to pay more attention to estimate data from the attacker's point of view.

3.4, Scoring Data and Quantitative Data

Game theoretic models need quantitative data, e.g., in table 2, the defender's defence cost Cd, the attacker's cost Ca, the expected risk $-V^2 \cdot C^2$ etc. Though these data are difficult to obtain, the API SRA methodology provides a systematic approach for evaluating them.

The risk scoring method is extensively used in the API SRA standard, to measure the threat level, the attractiveness level, vulnerabilities, consequences etc. For instance, the threat level has a score 1 if there is "no expected attack in the life of the facility's operation", a score 5 if "1 event per year", and a score 2/3/4 if the threat is in between the assessment of "no attack" and "attack every year". The risk scoring method appears to be intuitively correct and is easy to use. However, researchers have

pointed out several drawbacks of the risk scoring method (Cox, 2008), such as being characterized with a low resolution, being inconsistent etc.

A complementary solution is to feed the game theoretic inputs with the API SRA methodology data which are used to decide on the risk score. The prior probabilities can be calculated by using formula (2), with the output of threat rankings. The quantitative vulnerabilities/consequences/attractiveness can be obtained from table 11/table 5/table 8 in the API SRA document. For the convenience of the readers, we show table 11 in the API SRA document in this paper, indexed as table 3 in this paper. For example, if the SRA team estimates a vulnerability level of 2, then according to table 3, the quantitative probability of vulnerability would be $0.2 < V^2 \leq 0.4$. This approach is also studied in Landucci et al. (2017). There is no direct output from the API SRA methodology to obtain the cost of players' behaviours (e.g., Cd, Ca), but it is mentioned that the SRA team shall consider factors such as "the costs of mitigation options". It is worth noting that the quantitative consequence data (table 8 in the API SRA document) contains several factors, i.e., casualties, environmental impacts, economic losses, reputation etc. In this case, a unification approach is needed. Generally, researchers unify different factors into monetary values. Remark that domino effects have an important role in the consequence assessment procedure. However, for the API SRA methodology and for the security game, consequences are just input numbers, and how one obtains this number is not the focus of this paper.

Table 3. Vulnerability scores and corresponding quantitative data (adopted from the API document (API, 2013))

API SRA Methodology			
Vulnerability Level	**Descriptor**	**Conditional Probability of Success**	**Description**
1	Very low	0.0 to 0.2	Indicates that multiple layers of effective security measures to deter, detect, delay, respond to, and recover from the threat exist, and the chance that the adversary would be readily able to succeed at the act is very low.
2	Low	>0.2 to 0.4	Indicates that there are effective security measures in place to deter, detect, delay, respond, and recover; however, at least one weakness exists that a threat would be able to exploit with some effort to evade or defeat the countermeasure.
3	Medium	>0.4 to 0.6	Indicates that although there are some effective security measures in place to deter, detect, delay, respond, and recover, but there is not a complete and effective application of these security strategies and so the asset or the existing countermeasures could still be compromised.
4	High	>0.6 to 0.8	Indicates there are some security measures to deter, detect, delay, respond, and recover, but there is not a complete or effective application of these security strategies and so the adversary could succeed at the act relatively easily.
5	Very high	>0.8 to 1.0	Indicates that there are very ineffective security measures currently in place to deter, detect, delay, respond, and recover, and so the adversary would easily be able to succeed.

Quantitative data derived from risk scores are not always exact numbers, and more often, they are intervals. For instance, a vulnerability level 2 responds to a probability interval from 0.2 to 0.4, and the distribution of the probability on the interval (e.g., $(0.2,0.4]$) remains unknown. Fortunately, developments on robust game theory provide feasible models and algorithms to meet with this challenge (Aghassi and Bertsimas, 2006).

3.5, Simultaneous or Sequential Game?

A game theoretic model is called a simultaneous game if each player chooses his/her strategy without knowing the other players' strategies, otherwise, the game is called a sequential game. The Nash Equilibrium (NE) is used for predicting outcomes of a simultaneous game, while the Stackelberg Equilibrium (SE) is used for 2-player sequential games. A simultaneous security game suffers from several drawbacks. First, a pure strategy NE may not exist. For example, in the illustrative game shown in figure 2, it is reasonable to assume that $g_2, g_1 \geq 0 \geq -p, r \geq 0 \geq -l_1, -l_2$, and in this setting, no pure strategy Nash Equilibrium exists. However, a pure strategy SE always exists, and in the above mentioned setting, the Stackelberg Equilibrium is $(Steal\ a_2, Protect\ a_1)$ if $l_1 \geq l_2$, and it is $(Steal\ a_1, Protect\ a_2)$ if $l_1 < l_2$. Second, NE(s) for a simultaneous security game is (are) based on the "common knowledge" assumption, which is a strong and critical assumption. For instance, common knowledge for the game in figure 2 means that both the defender and the thief know all the

data (i.e., p, r, g_1, g_2, l_1, l_2) from the table, and both know that the other player also knows the table's data, and both know that the other player knows that he himself knows the table, and so forth. In a sequential security game, which is also called defender-attacker model, however, the 'common knowledge' is not necessary. The defender only needs to know data of herself (i.e., r, l_1, l_2) and her estimation of the thief's data (i.e., p, g_1, g_2), while whether the thief knows these data and whether the thief knows that the defender knows these data, are not relevant to the calculation of the SE. For more discussion of this nested thinking, interested readers are referred to Rios and Insua (2012) and Rios Insua et al. (2009)

The API SRA methodology does not pay attention on analysing whether attackers would be able to know the defender's countermeasures (i.e., in game theoretic terminology, strategies). In fact, the API SRA team robustly apply risk management to minimize the plant's maximal potential loss, and in this setting, they do not need the common knowledge assumption (since they even do not estimate the data from the attacker's point of view at all).

However, if the defender would also be able to collect some data from the attacker's point of view, as stated in section 3.3, then in order to make the best use of the available data, the defender would have to distinguish whether she is playing a simultaneous game or a sequential game.

4, DISCUSSION

Research carried out in this paper illustrates how the API SRA methodology and game theory can be complementary to each other for improving chemical plant protection. The API SRA methodology is a systematic approach for obtaining data from a given chemical plant, while game theory is a proper mathematic methodology for analysing these data.

Industrial managers may criticize game theory for its mathematic complexity and its over-simplifications of reality. Game theory, originally developed by mathematicians, can indeed become complicated. However, the industrial SRA team may treat game theoretic models as a black box, and

focus on collecting the correct data and analysing the outputs. Traditional game theoretic research assumes rational players and common knowledge of the game, thus indeed could be considered to be over-simplified. Fortunately, developments on computational game theory have provided models and algorithms for studying games played by bounded rational players and games where 'common knowledge' does not hold. Figure 4 (adopted from Zhang and Reniers (2018)) shows the uncertainty space of the Chemical Plant Protection game (CPP game) (Zhang and Reniers, 2016). The origin point is the CPP game with rational players and common knowledge assumptions. The x-axis represents the attacker's rationality, such as the epsilon-optimal attackers (Pita et al., 2010), quantal response attackers (McKelvey and Palfrey, 1993, 1998; Yang et al., 2012) etc. The y-axis denotes the defender's uncertainty on the attacker's payoffs, such as the discrete uncertainty (Tambe, 2011), Bayesian uncertainty (Kiekintveld et al., 2011), interval uncertainty (Kiekintveld et al., 2013; Nikoofal and Zhuang, 2012, 2015) etc. Each point in the uncertainty space corresponds to a realistic situation and a cluster of models and algorithms. What the industrial manager needs to do is to decide what her current situation is (adversaries and information), and choose the correct model to analyse her data. If the defender cannot decide her adversaries and/or has no information about her adversaries at all, which is mostly the situation now in industrial practise, then she may play her MiniMax strategy as used in the API SRA methodology. If the defender would be able to collect some data about her adversaries, then some advanced models could be used to increase her payoff.

Though the integration of the API SRA methodology and game theory is a promising approach for improving chemical plant protection, some research efforts are still needed.

First, models and algorithms for dealing with combinations of multiple types of uncertainties need to be enhanced. There are abundant studies on dealing with a single type of uncertainty, i.e., points on axis in figure 4. However, in reality, a defender often faces multiple types of uncertainties, e.g., point #1 in figure 4 represents multiple types of attackers and each type of attackers are epsilon optimal players (Pita et al., 2010). Nguyen et al. (2014) proposed a general framework and algorithms to

represent and solve security games with multiple types of uncertainties, however, their work is only applicable to the security games defined in Paruchuri et al. (2008).

Secondly, a mixed strategy is involved in most security game research, and its explanation to security practise needs to be well defined. Traditional game theorists explain mixed strategy as the result of incomplete information (Gibbons, 1992). In his security games, Tambe (2011) explains mixed strategy as that the attacker knows the defender's probabilities of covering each target, but when the attacker attacks, he cannot know which target exactly the defender is covering. Tambe's explanation implies a time difference between the attacker's observation and the attack. For instance, in the game shown in figure 2, in each time slice (e.g., a day), the defender can protect asset 1 at a probability x_1, and protect asset 2 at a probability $1 - x_1$. The attacker may get the x_1, either by an intelligence approach or by long term observation. However, the attacker is assumed not to be able to finish the observation (e.g., to see which asset the defender is protecting) and attack (e.g., execute the attack) in one time slice, otherwise in the illustrative game, the thief would always steal the unprotected asset. This assumption is reasonable since observation and preparation of an attack needs time, and the time slice can be sufficiently short. However, most security equipment (e.g., a bag check machine, a camera etc.) do not support this explanation of mixed strategy, since they are not movable from one point to another point (a pathway or an asset). To this end, security game researchers must be careful on using and explaining mixed strategies.

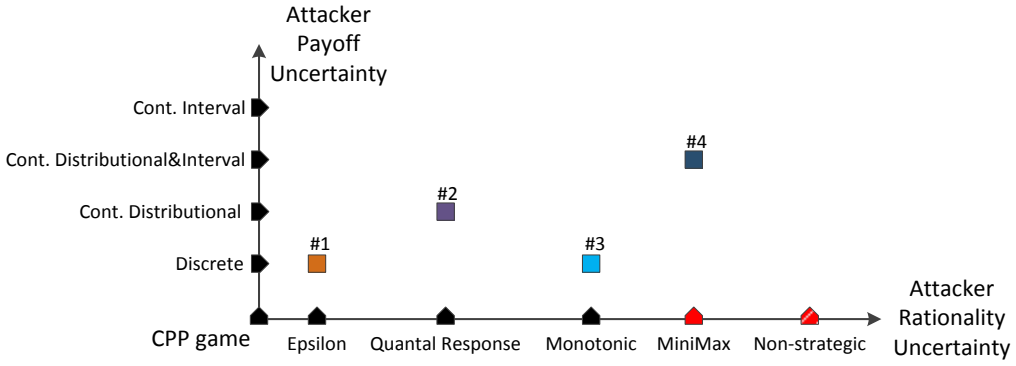

Figure 4 uncertainty space for the CPP game (adopted from Zhang and Reniers (2018))

5, CONCLUSION

Terrorism has been a global concern for decades. Chemical plants, due to their importance to modern society and their special producing conditions, could be attractive targets to terrorists. Aside from the abundant published papers, regulations, standards, physical security in the chemical plants still has a long way to go to improve performance (Khakzad et al., 2017).

In this paper, the possibility of integrating the API SRA methodology with security games to improve chemical plant protection, is explored. The approach elaborated in this innovative paper, is to use the API SRA methodology to extract qualitative/quantitative data from a given chemical plant, whereas to employ the security game to analyse these extracted data. Furthermore, the game theoretic results are interpreted by reflecting them back to the API SRA terminologies.

Besides its advantages on analysing intelligent interactions between the defender and the attackers, game theory can also give guidance to the API SRA methodology for collecting the right data, such as performance of a bundle of countermeasures, attacker's interests, etc.

ACKNOWLEDGEMENTS

This study is supported by China Scholarship Council, and partly by National Key Research & Development (R&D) Plan under Grant No. 2017YFC0803300 and the National Natural Science Foundation of China under Grant Nos. 71673292,61503402.

REFERENCE

Aghassi, M., & Bertsimas, D. (2006). Robust game theory. *Mathematical Programming, 107*(1-2), 231-273.

API. (2013). Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. In A. R. P. 780 (Ed.).

Argenti, F., Landucci, G., Spadoni, G., & Cozzani, V. (2015). The assessment of the attractiveness of process facilities to terrorist attacks. *Safety science, 77*, 169-181. doi: 10.1016/j.ssci.2015.02.013

Bajpai, S., & Gupta, J. (2005). Site security for chemical process industries. *Journal of Loss Prevention in the Process Industries, 18*(4), 301-309.

Baybutt, P. (2016). Designing risk matrices to avoid risk ranking reversal errors. *Process Safety Progress, 35*(1), 41-46.

Bier, V. M., & Azaiez, M. N. (2008). *Game theoretic risk analysis of security threats* (Vol. 128): Springer Science & Business Media.
Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces, 36*(6), 530-544.
Cox Jr, L. A. T. (2008). Some limitations of "Risk= Threat× Vulnerability× Consequence" for risk analysis of terrorist attacks. *Risk Analysis, 28*(6), 1749-1761.
Cox Jr, L. A. T. (2009). Game theory and risk analysis. *Risk Analysis, 29*(8), 1062-1068.
Cox, L. (2008). What's wrong with risk matrices? *Risk Analysis, 28*(2), 497-512.
FAS. (2006). Al qaeda training manual.
Feng, Q., Cai, H., Chen, Z., Zhao, X., & Chen, Y. (2016). Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. *Journal of Loss Prevention in the Process Industries, 43*, 614-628.
Gibbons, R. (1992). *A primer in game theory*: Harvester Wheatsheaf.
Golany, B., Kaplan, E. H., Marmur, A., & Rothblum, U. G. (2009). Nature plays with dice–terrorists do not: Allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research, 192*(1), 198-208.
Guikema, S. D. (2009). Game theory models of intelligent actors in reliability analysis: An overview of the state of the art *Game theoretic risk analysis of security threats* (pp. 13-31): Springer.
Hall Jr, J. R. (2009). The elephant in the room is called game theory. *Risk Analysis, 29*(8), 1061-1061.
IENM. (2013). *Letter of 26 April 2013 to the Parliament*.
Khakzad, N., Martinez, I. S., Kwon, H. M., Stewart, C., Perera, R., & Reniers, G. (2017). Security risk assessment and management in chemical plants: Challenges and new trends. *Process Safety Progress*.
Kiekintveld, C., Islam, T., & Kreinovich, V. (2013). *Security games with interval uncertainty.* Paper presented at the Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems.
Kiekintveld, C., Marecki, J., & Tambe, M. (2011). *Approximation methods for infinite Bayesian Stackelberg games: Modeling distributional payoff uncertainty.* Paper presented at the The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3.
Landucci, G., Argenti, F., Cozzani, V., & Reniers, G. (2017). Assessment of attack likelihood to support security risk assessment studies for chemical facilities. *Process Safety and Environmental Protection*.

Lee, Y., Kim, J., Kim, J., Kim, J., & Moon, I. (2010). Development of a risk assessment program for chemical terrorism. *Korean Journal of Chemical Engineering, 27*(2), 399-408.
McKelvey, R. D., & Palfrey, T. R. (1993). Quantal response equilibria for normal form games.
McKelvey, R. D., & Palfrey, T. R. (1998). Quantal response equilibria for extensive form games. *Experimental economics, 1*(1), 9-41.
Moore, D. A. (2013). Security Risk Assessment Methodology for the petroleum and petrochemical industries. *Journal of Loss Prevention in the Process Industries, 26*(6), 1685-1689.
Nguyen, T. H., Jiang, A. X., & Tambe, M. (2014). *Stop the compartmentalization: Unified robust algorithms for handling uncertainties in security games.* Paper presented at the Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems.
Nikoofal, M. E., & Zhuang, J. (2012). Robust allocation of a defensive budget considering an attacker's private information. *Risk Analysis, 32*(5), 930-943.
Nikoofal, M. E., & Zhuang, J. (2015). On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. *European Journal of Operational Research, 246*(1), 320-330.
Orum, P., & Rushing, R. (2008). Chemical Security 101, What You Don't Have Can't Leak, or Be Blown Up by Terrorists.
Paruchuri, P., Pearce, J. P., Marecki, J., Tambe, M., Ordonez, F., & Kraus, S. (2008). *Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games.* Paper presented at the Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems-Volume 2.
Pavlova, Y., & Reniers, G. (2011). A sequential-move game for enhancing safety and security cooperation within chemical clusters. *Journal of Hazardous Materials, 186*(1), 401-406. doi: 10.1016/j.jhazmat.2010.11.013
Pita, J., Jain, M., Tambe, M., Ordóñez, F., & Kraus, S. (2010). Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition. *Artificial Intelligence, 174*(15), 1142-1171.
Powell, R. (2007). Defending against terrorist attacks with limited resources. *American Political Science Review, 101*(03), 527-541.
Reniers, Cremer, & Buytaert. (2011). Continuously and simultaneously optimizing an organization's safety and security culture and climate: the Improvement Diamond for Excellence Achievement and

Leadership in Safety & Security (IDEAL S&S) model. *Journal of Cleaner Production, 19*(11), 1239-1249. doi: 10.1016/j.jclepro.2011.03.002

Reniers, & Van Erp. (2016). *Operational Safety Economics: A Practical Approach focused on the Chemical and Process Industries*: John Wiley & Sons.

Rezazadeh, A., Zhang, L., Reniers, G., Khakzad, N., & Cozzani, V. (2017). Optimal patrol scheduling of hazardous pipelines using game theory. *Process Safety and Environmental Protection, 109*, 242-256.

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

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

Talarico, L., Reniers, G., Sörensen, K., & Springael, J. (2015). MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. *Reliability Engineering and System Safety, 138*, 105-114. doi: 10.1016/j.ress.2015.01.022

Tambe, M. (2011). *Security and game theory: algorithms, deployed systems, lessons learned*: Cambridge University Press.

Yang, R., Ordonez, F., & Tambe, M. (2012). *Computing optimal strategy against quantal response in security games.* Paper presented at the Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 2.

Zhang, & Reniers. (2016). A Game‐Theoretical Model to Improve Process Plant Protection from Terrorist Attacks. *Risk Analysis, 36*(12), 2285-2297.

Zhang, & Reniers. (2018). Applying game theory for adversarial risk analysis in process plants. In G. Reniers, N. Khakzad & P. van Gelder (Eds.), *Security risk assessment and management in the chemical and process industry*: De Gruyter.

Zhang, Reniers, & Qiu. (2017). Playing Chemical Plant Protection Game with Distribution-free Uncertainties. *Reliability Engineering & System Safety*.