Applying a Bayesian Stackelberg game for securing a chemical plant

Applying a Bayesian Stackelberg Game for Securing a Chemical Plant

Laobing Zhang[a], Genserik Reniers[a,b,c,*]

[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

(*) Author to whom correspondence should be addressed.

tel. (+31)15 27 83749

e-mail: G.L.L.M.E.Reniers@tudelft.nl

Submitted for publication in:

Risk Analysis

Abstract

In this paper, a Stackelberg defender-adversary game for improving chemical plant protection is proposed, considering multiple types of adversaries. The defender moves first (i.e. forming the "game leader"), setting security alert levels at different entrances of the plant and patrolling levels at different zones. The defender does not exactly know which type of adversary she would face, but knows prior probabilities of occurrence of the different types of adversaries. The adversaries move with full observation of the defender's actions (i.e. forming the "game follower"), choosing which target to attack and deciding how to reach to the target as well as by what level of attack effort. In a case study, we implement the model on a refinery facing threats of suicide bombers and environmental activists.

Keywords

Chemical Plant Security, Bayesian Stackelberg game, Terrorism Attack, Environmental Activist

1. INTRODUCTION

After the New York 9/11 terrorist attack, critical infrastructure protection has been an increasingly important topic in the risk analysis society. The process industry is one of the 13 types of critical infrastructures listed by the American government, due to its extreme importance for civil citizens' daily lives as well as its vulnerabilities to malicious attacks.[1] In order to protect chemical plants belonging to the process industries, intelligent interactions between security managers and potential adversaries should be taken into consideration, making security research different from safety research.[2]

Traditional risk assessment techniques have their shortages regarding modelling the intelligent adversaries, and might lead to mis-allocation of the limited security resources.[3, 4] See for instance, the American Petroleum Institute (API) Security Risk Assessment (SRA) standard 780 [5] models the adversaries' attractiveness of attacking the targets in a probabilistic way, without considering that the implementation of counter-measures on targets would reduce the targets' vulnerability as well as their attractiveness. Game theory, however, is good at modelling the strategic interactions among intelligent players. As stated by Cox[6], combining game theory and conventional (probabilistic) risk analysis techniques thus becomes a promising approach for security risk research. Conventional risk analysis techniques (e.g., API SRA standard 780) can provide quantitative inputs for game theory models, while game theory models could process these inputs in an intelligent way, making best use of these data.[6-8]

More specific in process industries protection, there are just a few game theoretic researches that have been published. Feng et al.[9] employed a zero-sum game for analysing resources allocation in a city with multiple chemical facilities. Zhang and Reniers[8] proposed a non-zero-sum, complete information, simultaneous game to improve chemical security by optimally setting the security alert levels (SAL) at different "Typicals". Pavlova and Reniers[10] studied how to form maximal security cooperation with minimal expense in chemical clusters, by employing a two-stage cooperative game. Talarico et al.[11] developed the so-called "MISTRAL" game for improving security of multi-modal

chemical transportation network, and both simultaneous and sequential (however, mixed strategy is not studied) solutions are studied in their work. In the existing researches, simultaneous game studies with complete information are commonly conducted. However, as pointed out by Guikema,[12] the field has moved on from these assumptions. Tambe et al.,[13] Nikoofal and Zhuang,[14, 15] Guikema et al.[16, 17] develop models for modelling the uncertainties of the adversaries. Tambe et al. work successfully at modelling different types of adversaries and deploying several practically useful systems such as the ARMOR,[18] IRIS[19] etc., whereas Nikoofal and Zhuang, Guikema et al. work successfully at modelling the continuous uncertainties of the adversaries' utility functions.

In the present paper, a Bayesian Stackelberg game is developed for chemical plant protection. Section 2 illustrates a simultaneous game-theoretical model for chemical plants protection ("CPP game"), based on the general intrusion detection model in the process industries. Section 3 defines the Bayesian Stackelberg CPP game, which relaxes the simultaneous move and complete information assumptions in the "CPP game". A case study is used to illustrate how the Bayesian Stackelberg CPP game works in reality, in section 4. Conclusions and future research pathways are drawn in the last section.

2. THE CPP GAME

2.1 Physical Security in the Process Industries

Figure 1 shows a general physical intrusion detection and prevention system in the process industries. The different layers of "PERIMETER" divide the plant area into different layers or "ZONEs". In order to intrude higher level zones, a potential intruder has to pass the lower level zones first. A further realistic assumption is that an intruder would never come into the same level of zones twice. For example, if an environmental activist aims to shut down a facility in ZONE 2_2, he would have to pass ZONE 0, perimeter 1, ZONE 1_1, and perimeter 2 (p1 in Figure 1, for instance, is a possible path), and the assumption constraints that he would not step into ZONE 2_1 (e.g., the path p2 in Figure 1) because otherwise he would come twice into level 1 and level 2 of zones. The security

countermeasures at the perimeters (e.g. access control, checkpoint etc.) and the zones (e.g. patrolling, safety barriers etc.) makes the targets in higher zones more secure (i.e. less vulnerable). A "Typical"[19] in the system is defined as the summation of items constituting a security barrier, and thus describes the specific detailed characteristics of a security measure installed at a plant or at a part thereof. For example, at the Main Entrance in Figure 1, there could be some security staffs, barriers, identity recognition system etc., all of which constitute a security barrier, thus the Main Entrance is a "Typical".

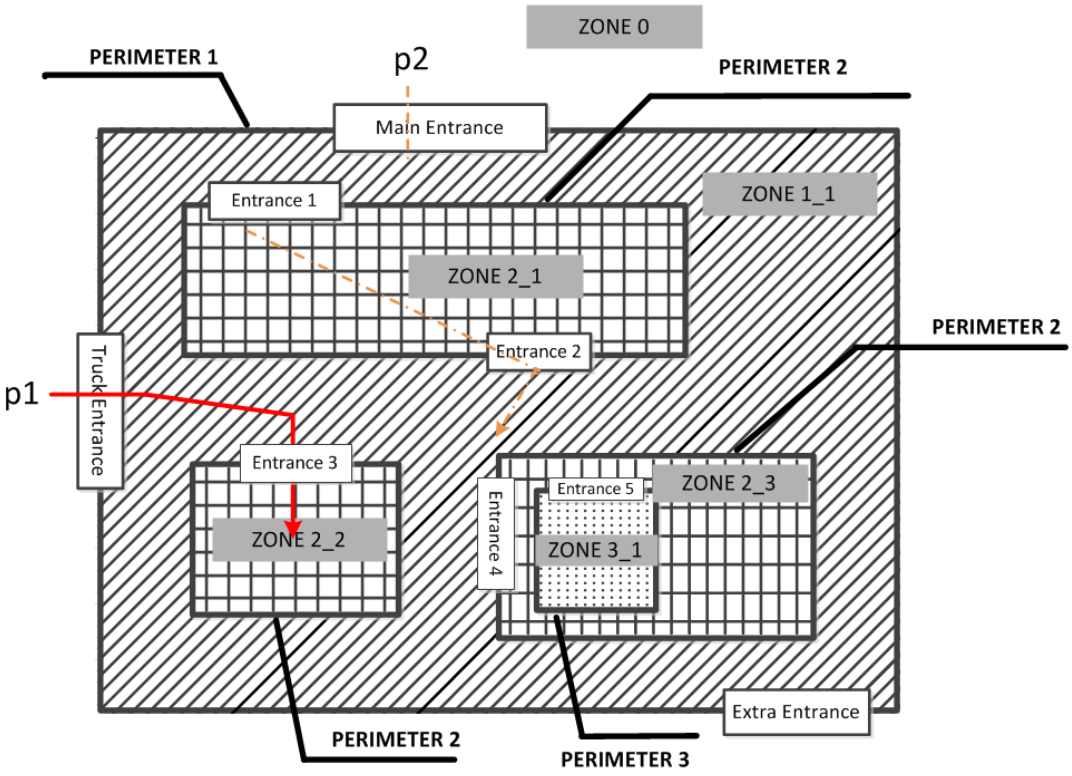


Figure 1. General intrusion preventing in process plants [Source: Zhang and Reniers[8]]

Figure 2 illustrates the potential adversaries' behaviour. The adversaries would, firstly, decide which target to attack, secondly, choose an "easiest way" (the so-called critical path) to reach the target, and thirdly, decide the attack effort level (e.g. armed or not). Note that these steps are not independent, e.g., when the adversaries choose the target, the difficulties of reaching the target is of course a very important factor to be considered. Formula (1) gives the probability of successfully reaching the target.

$$P = \prod_{r=0}^{I} P_r^z \cdot \prod_{r=1}^{I} P_r^p. \quad (1)$$

In which the I denotes the zone level number of the target, for example, in Figure 1, if a target located in ZONE3_1, then we have $I = 3$; P_r^z denotes the probability of successfully passing the zone Level r, while for the last zone (i.e., the attack target locates on this zone), it denotes the probability of successfully from the last perimeter to the target; P_r^p denotes the probability of successfully passing the perimeter r.

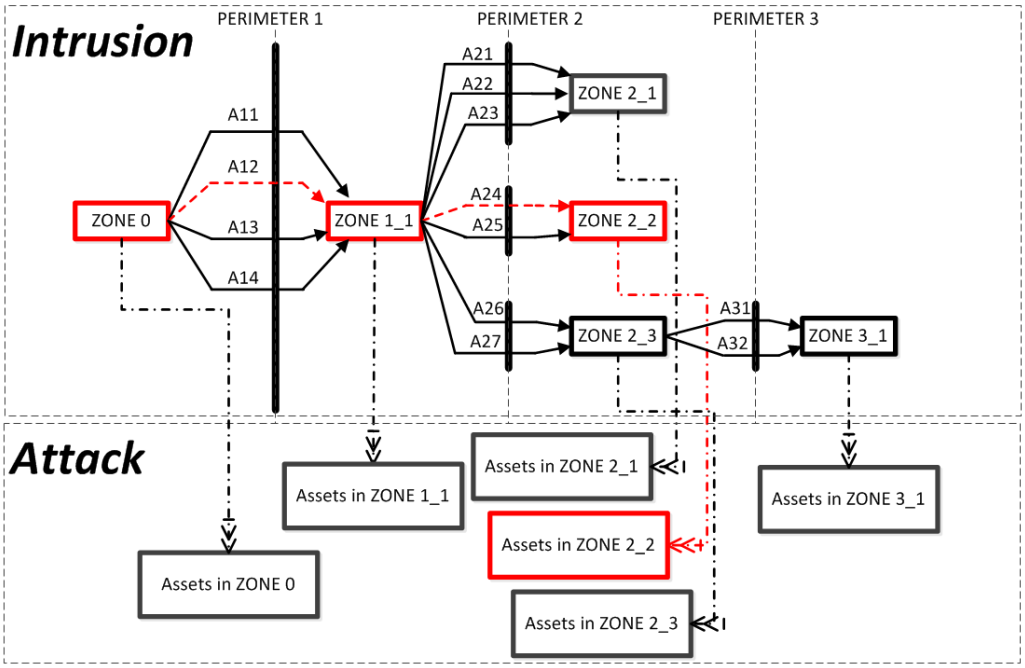


Figure 2. The intrusion and attack procedure [Source: Zhang and Reniers[8]]

2.2 Game-theoretical model for Chemical Plant Protection

The game-theoretical model for chemical process plants protection (CPP game)[8] is played by the security defender and the potential adversary, thus it is a two player game[1]. Players in the CPP game are assumed to be rational and both defender and adversary have complete information of the game. Considering the defence and attack costs, as well as the different value estimation of the targets by the players,[20] the CPP game is not necessarily a zero-sum game.

[1] In the security game domain, the defender is normally denoted as she/her/her, while the attacker is denoted as he/him/his.

The players' strategies can be easily derived from the analysis in section 2.1. The defender's strategies are defined as setting security alert levels (SAL) at different "Typicals", as formulated in formula (2).

$$s^d = z^0 \times \prod_{r=1}^{Q}(A_1^r \times A_2^r \times \ldots \times A_{ent(r)}^r \times z_1^r \times z_2^r \times \ldots \times z_{sub(r)}^r) \quad (2)$$

In which s^d denotes a specific defence decision, also called 'pure strategy' in game-theoretic terminology; z^0 denotes detect level in the ZONE 0 (i.e., the outside zone) of the plant; z_i^r denotes detect level in i^{th} sub zone in zone level r; A_i^r denotes detect level at the i^{th} access of perimeter r; $ent(r)$ denotes number of accesses in perimeter r; $sub(r)$ denotes number of sub zones in zone level r; Q denotes total zone levels in the plant; $\times$ denotes cross product. The definition of the defender's pure strategy indicates that the defender could set different SAL in all the accesses of the perimeters as well as in all the (sub-) zones.

The attacker's strategies are defined as choosing which target to attack and how to reach the target as well as by what attack effort, as formulated in formula (3).

$$s^a = a \times \prod_{r=1}^{I} j_r \times e \quad (3)$$

In which s^a denotes a specific attack action, also called 'pure strategy' in game-theoretic terminology; a denotes the index of the target asset; I denotes the zone level that the target asset located in; j_r denotes the access to pass the perimeter r, and $j_r = 1,2, \ldots, ent(r)$; e denotes attack efforts, $e = 0$ means that the adversary would not execute an attack, i.e., he is deterred. An example of the attacker's pure strategy can be given as that an activist wants to shut-down an facility (with index κ) in ZONE 2_2 in Figure 1, with effort 1 (e.g., unarmed), and he follows the path p1. This example can be formally descript as $s^a = \kappa \times TruckEntr \times Entr3 \times 1$.

Formulas (2) and (3) imply that both players have finite pure strategies, which is the result of the assumptions (i) that the defender has only a finite number of SAL (e.g. 3 or 5 different scenarios or levels[21]) and (ii) that the adversary also has only a finite number of behave efforts (e.g. effort level 1,

level 2 etc.). Define the defender and the attacker's pure strategy sets as $S_d = \{s^d\}$, $S_a = \{s^a\}$ respectively. $n = |S_d|, m = |S_a|$ represent the number of pure strategies of the defender and the attacker respectively. For the sake of clarity, in the following text, s_j^d (s_i^a) represents the j^{th} (i^{th}) pure strategy in the S_d (S_a).

Formulas (4) and (5) define the payoff of the CPP game, for the adversary and the defender respectively.

$$u_a(s_i^a, s_j^d) = \tilde{P}(s_i^a, s_j^d) \cdot \tilde{P}_y(s_i^a) \cdot \tilde{L}(s_i^a) - C_a(s_i^a) \quad (4)$$

$$u_d(s_i^a, s_j^d) = -(P(s_i^a, s_j^d) \cdot P_y(s_i^a) \cdot L(s_i^a) + C_d(s_j^d)) \quad (5)$$

In which u_a denotes the adversary's payoff; u_d denotes the defender's payoff; P ($\tilde{P}$) denotes the probability of successfully reaching the target, which could be calculated by formula (1); P_y ($\tilde{P}_y$) denotes the probability of successfully attacking (e.g. destroying or shutting down) the target after reaching the target; L ($\tilde{L}$) denotes the estimated loss (gain) of the target; from the defender's (the attacker's) perspective respectively. C_a denotes the cost of a certain attack effort; C_d denotes the cost of a certain defence effort. In this paper, only the preventive countermeasures are considered, thus the P_y ($\tilde{P}_y$) and L ($\tilde{L}$) are not influenced by the defender's strategies.

The first component of formula (4) represents the expected gain of the adversary, denoted by the product of probability of reaching the target, probability of attacking the target, and the reward of the target if it is damaged. The second component of formula (4) reflects that the attack costs are considered by the attacker. Formula (5) is defined analogously. By implementing formulas (4) and (5) for each pair of defender and attacker strategies, the payoff matrices of the game would be constructed. In Bayesian games where there are multiple types of attackers, the payoff matrix should be calculated for both the defender the attacker for each type of attackers.

Computing the payoff for the CPP game needs some parameters, they are, the intrusion probabilities P ($\tilde{P}$), the probability that the attack would be executed in condition that the attacker already

reached the target P_y ($\tilde{P}_y$), the estimated consequence of an successful attack L ($\tilde{L}$), and both players' behaviour costs C_d (C_a). In practice, all these parameters should be provided by security experts. However, due to the lack of data as well as theoretic research, some of these parameters are quite difficult to obtain. In the security game community, the contest success function (CSF) is extensively used, for calculating some probabilities in security defence and attack, normally for illustrative purpose.

Following Hausken,[22] Hausken and Zhuang,[23] Talarico et al.[11] etc., the (extended) contest success function (CSF)[24, 25] is employed to compute the P_r^z and P_r^p, as shown in formulas (6) and (7), for illustrative purpose in this article. Combining the CSF and formula (1), the P can be obtained.

$$P_r^z = \frac{e}{e+\alpha_{ri} \cdot z_i^r \cdot t_{ri}/\tau} \quad (6)$$

$$P_r^p = \frac{e}{e+\beta_{rj_r} \cdot A_{j_r}^r} \quad (7)$$

In which e denotes the attack effort, as defined in equation (5); α_{ri} and β_{ij_r} are the constant coefficients of the extended CSF; z_i^r denotes the security alert level in the i^{th} sub-zone of zone level r while $A_{j_r}^r$ denotes the security alert level in access j_r; t_{ri} denotes how much time (in minutes) the adversary stays in the i^{th} sub-zone of zone level r, τ is a configurable coefficient, in this paper, we set it as $\tau = 5$. Note that formula (6) is not a standard CSF, the time t_{ri} is included. However, formula (6) still satisfies the Logit assumption of CSF,[24] i.e. $P_r^z(e, z_i^r) = P_r^z(\lambda e, \lambda z_i^r), \lambda \in R$, which means that when the attacker scales his attack effort and the defender scales her defense level at the same proportion, the successful probability would not change. Figure 3 shows the relationship of the P_r^z and the t_{ri}.

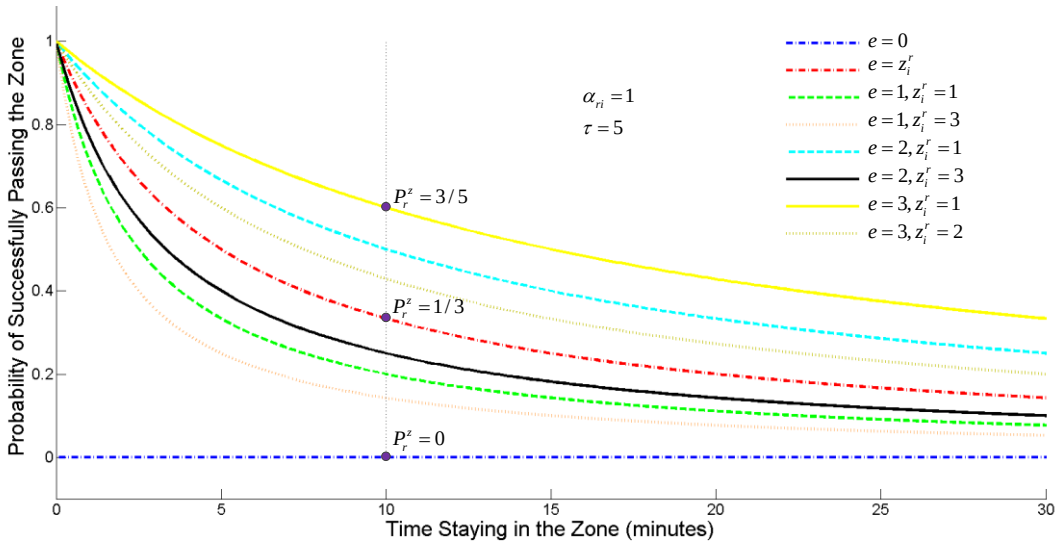


Figure 3. Illustrative probabilities

In Figure 3, the lowest blue line reflects the fact that the probability of passing the zone equals 0 constantly if the attack effort is 0 (i.e. no attack at all). If the adversary attacks, and he is able to pass the zone very quickly (i.e. $t_{ri} \to 0$), then he could be able to successfully pass the zone 100%. However, if it costs the adversary 10 minutes to pass the zone, then in case of an attack effort of 3 and an security alert level of 1 in this zone, the adversary would be able to successfully pass the zone at probability 3/5, as indicated in Figure 3.

2.3 the Nash Equilibrium

In simultaneous CPP game, the Nash Equilibrium (NE)[26] is used to predict the player's actions. A mixed strategy NE $(\bar{x}, \bar{y})$ for the CPP game is defined by formulas (8) and (9).

$$\bar{y} = \underset{y \in Y}{\operatorname{argmax}}\, \bar{x}^T \cdot U_d \cdot y \tag{8}$$

$$\bar{x} = \underset{x \in X}{\operatorname{argmax}}\, x^T \cdot U_a \cdot \bar{y} \tag{9}$$

In which U_d and U_a are the payoff matrices, and their entries at i^{th} row, j^{th} column are defined by formulas (4) and (5) respectively, Y and X are the defender and adversary's mixed strategy space, defined as $Y = \{y \in R^n | y_i \in [0,1], \sum_{i=1}^{n} y_i = 1\}$, $X = \{x \in R^m | x_i \in [0,1], \sum_{i=1}^{m} x_i = 1\}$ respectively.

Note that a pure strategy NE is a special case of the mixed strategy NE (when $\bar{y}_s = 1, \bar{x}_t = 1$, and for any other $j \neq s, i \neq t$, we have $\bar{y}_j = 0, \bar{x}_i = 0$), thus we do not further define a pure strategy NE for the CPP game.

Nash proved that in a finite game (finite players, finite strategy sets), a mixed strategy Nash Equilibrium always exist.[26] For the two players finite game, the Lemke-Howson algorithm[27] can be employed to find the NE.

2.4 the Strategically Zero-Sum Property

Though defenders and attackers always have opposite interests, security games are not necessarily zero-sum games.[28] The payoff definition as shown in formulas (4) and (5) shows the non-zero-sum property of the CPP game from 2 aspects: 1) both players' behaviour costs are considered, and neither player can obtain anything from the other player's behaviour cost; 2) the defender and the attacker might evaluate the same parameters with different values, including both the probabilities (e.g., P and $\tilde{P}$) and the consequences (i.e., L and $\tilde{L}$).

However, if we re-organize the payoff formulas (4) and (5) as:

$$u_a(s_i^a, s_j^d) = \tilde{f}(s_i^a, s_j^d) - C_d(s_j^d) \tag{10}$$

$$u_d(s_i^a, s_j^d) = -f(s_i^a, s_j^d) - C_a(s_i^a) \tag{11}$$

In which:

$$\tilde{f}(s_i^a, s_j^d) = \tilde{P}(s_i^a, s_j^d) \cdot \tilde{P}_y(s_i^a) \cdot \tilde{L}(s_i^a) + C_d(s_j^d) - C_a(s_i^a) \tag{12}$$

$$f(s_i^a, s_j^d) = P(s_i^a, s_j^d) \cdot P_y(s_i^a) \cdot L(s_i^a) + C_d(s_j^d) - C_a(s_i^a) \tag{13}$$

Furthermore, define a zero-sum game $(F, -F)$, which has the same players and strategy sets as the CPP game, while its payoff units are defined by formula (12).

Observation 1. If, in some cases, for all strategy tuples of the CPP game, the condition $\tilde{P} \cdot \tilde{P}_y \cdot \tilde{L} = P \cdot P_y \cdot L$ holds, then $(\bar{x}, \bar{y})$ is a NE of the CPP game if and only if $(\bar{x}, \bar{y})$ is a NE of the game $(F, -F)$.

Proof: Since $\tilde{P} \cdot \tilde{P}_y \cdot \tilde{L} = P \cdot P_y \cdot L$, we directly know that $\tilde{f} = f$. According to the definition of NE,

$$(\bar{x}, \bar{y}) \text{ is a NE of the CPP game} \Leftrightarrow \begin{cases} \bar{x}^T \cdot U_a \cdot \bar{y} \geq x^T \cdot U_a \cdot \bar{y}, \ \forall x \in X \\ \bar{x}^T \cdot U_d \cdot \bar{y} \geq \bar{x}^T \cdot U_d \cdot y, \ \forall y \in Y \end{cases}$$

$$\Leftrightarrow \begin{cases} \bar{x}^T \cdot F \cdot \bar{y} - \bar{x}^T \cdot C_D \cdot \bar{y} \geq x^T \cdot F \cdot \bar{y} - x^T \cdot C_D \cdot \bar{y}, \ \forall x \in X \\ -\bar{x}^T \cdot F \cdot \bar{y} - \bar{x}^T \cdot C_A \cdot \bar{y} \geq -\bar{x}^T \cdot F \cdot y - \bar{x}^T \cdot C_A \cdot y, \ \forall y \in Y \end{cases} \quad (14)$$

In above formulas, C_D and C_A are the behave costs matrix, and their entries at i^{th} row, j^{th} column are the defender's behave cost and the attacker's behave cost respectively, when the attacker plays pure strategy s_i^a and defender plays s_j^d. Since the attacker's strategy would not influence the defender's behave cost, thus C_D has identical rows; analogously, C_A has identical columns. Therefore, we have $\bar{x}^T \cdot C_D \cdot \bar{y} = \sum_{j \in N} C_{dj} \cdot \bar{y}_j = x^T \cdot C_D \cdot \bar{y}$, and $\bar{x}^T \cdot C_A \cdot \bar{y} = \sum_{i \in M} \bar{x}_i \cdot C_{ai} = \bar{x}^T \cdot C_A \cdot y$. Thus formula 14 equals:

$$\begin{cases} \bar{x}^T \cdot F \cdot \bar{y} \geq x^T \cdot F \cdot \bar{y}, \ \forall x \in X \\ -\bar{x}^T \cdot F \cdot \bar{y} \geq -\bar{x}^T \cdot F \cdot y, \ \forall y \in Y \end{cases}$$

$\Leftrightarrow (\bar{x}, \bar{y})$ is a NE of game $(F, -F)$.□

The proof of observation 1 implies that in condition that $\tilde{P} \cdot \tilde{P}_y \cdot \tilde{L} = P \cdot P_y \cdot L$ holds for all strategy tuples, the CPP game is a strategically zero-sum game.[29] In this cases, the analysis of the CPP game becomes easier. For more information of the strategically zero-sum game, interested readers are referred to Moulin and Vial.[29]

Thought the condition of $\tilde{P} \cdot \tilde{P}_y \cdot \tilde{L} = P \cdot P_y \cdot L$ is a strong condition for the CPP game, it might be the case in some situations. For instance, if the defender and the attacker they evaluate the intrusion probabilities, consequences of an attack etc. at the same way, thus we would have $\tilde{P} = P$, $\tilde{P}_y = P_y$, and $\tilde{L} = L$, and then the condition holds definitely. Some published non-zeros-sum security game

models,[CMT REF] which use similar payoff structures as shown in the formulas (4) and (5), are in fact strategically zero-sum games, and can be analysed by analysing an corresponding zero-sum game.

3. BAYESIAN STACKELBERG CPP GAME

3.1 Motivation of Bayesian Stackelberg CPP Game

The CPP game is a simultaneous game with complete information. However, these two assumptions could not hold in reality.

Previous research shows that the public information (e.g. social media, commercial news etc.) gives the security adversaries 80% (some people even think it is 100%) of the necessary information to execute a successful attack.[30] Therefore, it is justifiable to assume that when the attacker moves, he already has complete and perfect information of the game. On the other hand, the defender does not know whether the attacker has perfect information or not, thus she does not know whether she is playing a simultaneous game or a sequential game or even a mixture. Zhuang and Bier[31] prove that when the game follower's best response is a singleton, the game leader could have a "first-mover advantage". Thus in these cases, the (industrial) defender could choose to make the defence plan public, thereby enforcing the adversaries to play a sequential game. Finally, in non-zero-sum[2] simultaneous game, if there is not only one Nash Equilibrium (it is very likely in practical games), then the game becomes unpredictable. Thus we claim that a sequential game is more useful than a simultaneous game in the security domain.

Although it is commonly acceptable to assume that the adversaries have complete information of the security game, the defender faces great uncertainties regarding the potential adversaries. On one hand, the defender does not know which type of adversaries she would face. According to API Standard 780,[5] threats of chemical industries include Criminals, Activists, Terrorists, and Disgruntled personnel. Therefore, when playing the security game, the defender is not sure whether her adversary is a terrorist attacker, or a disgruntled employee, or an environmental activist, and so on.

[2] In zero-sum games, the Nash Equilibrium is interchangeable, thus there is no Equilibrium selection problem.

While different types of threats have various historical record of data, different intent, different motivation, and different capabilities. To this end, different threats could have different strategies, different parameters for calculating payoffs, and different occurrence probabilities. On the other hand, even when the defender knows who would be her adversary (e.g. the defender has efficient intelligence, thus she knows a terrorist organization would attack the plant), it is difficult to estimate the adversary's preferences and private information. For example, how much the adversary values the targets, how much budgets the adversary has, and so on.

Therefore, to relax the above assumptions of the CPP game, making it more realistic and credible, it is necessary to extend the game to a "Bayesian (describes the defender's incomplete information) Stackelberg (describes the sequential move property) CPP game", as described in the following sections.

3.2 Stackelberg CPP Game

In the Stackelberg CPP game, the defender moves first (i.e. forming the game leader), followed by the adversary(i.e. forming the game follower), with full observation (i.e. the follower has perfect information of the game).

For the sake of clarity, define the players' pure strategy index space as $N = \{1,2, \dots, n\}, M = \{1,2, \dots, m\}$, for the defender and the attacker respectively.

A Strong Stackelberg Equilibrium (SSE) (y^*, k^*) for the Stackelberg CPP game is defined by formulas (15) and (16).

$$y^* = \underset{y \in Y}{\operatorname{argmax}}\, U_d(k^*, :) \cdot y \tag{15}$$

$$k^* = \underset{k \in M}{\operatorname{argmax}}\, U_a(k, :) \cdot y \tag{16}$$

In which $U_{player}(i, :)(player = a \text{ or } d)$ represents the i^{th} row of the matrix U_{player}.

Formula (16) reflects the assumption that, observing the defender's strategy y, the adversary would choose the strategy k^* which can maximize his own payoff. Formula (15) reflects the assumption that, the defender knows the adversary's preference, thus she could also work out the formula (16), getting the k^*, based on which she would play the strategy y^* to maximize her own payoff. The defender (i.e. the leader) plays a mixed strategy, therefore the adversary can only observe the distribution of each pure strategy being played by the defender, but he does not know at an exact time, which pure strategy the defender would play.

The MultiLPs algorithm[32, 33] can be employed to compute the SSE for the Stackelberg CPP game.

3.3 Bayesian Simultaneous CPP Game

A Bayesian simultaneous CPP game is a CPP game in which there are multiple adversaries, thus the defender can capture the uncertainties of the different adversaries. The defender only knows the prior occurring probabilities of each types of adversaries. In this paper, we only focus on the uncertainties of the adversaries' types, not on the distributional uncertainties of the adversaries' preferences.

Define $\aleph$ as the set of possible attacker types, for instance, $\aleph = \{terrorist, activist, criminal\}$, and define vector ρ as the prior probability that each type of attackers would occur. Furthermore, for a given type of attackers $l \in \aleph$, denote the corresponding payoff matrix of the defender and the attacker as U_d^l and U_a^l respectively.

In Bayesian games, if the players do not know neither its own type nor the type of the other players, the ex-ante Bayesian Nash Equilibrium (BNE) should be used; if the player knows its own type but not the other players' type, the ex-interim BNE should be used; and if the players know all the players' types, the ex-post BNE should be used. Interested readers are referred to Shoham and Leyton-Brown,[34] Ceppi et al.[35] for more information. In Bayesian CPP game, it is assumed that the defender is unique, while the attackers can be various types, such as terrorist, environment activist, disgruntled employee etc. We assume that the defender knows the prior probabilities of each types

of attackers, while each type of attackers they know who they are. To this end, the ex-interim BNE should be employed to predict the outcome of the Bayesian CPP games.

An ex-interim Bayesian Nash Equilibrium (ex-interim BNE) $(\dot{y}, \dot{x}_1, \dot{x}_2, \dots, \dot{x}_{|\aleph|})$ for the Bayesian Simultaneous CPP game is defined by formulas (17) and (18).

$$\dot{y} = \underset{y \in Y}{\operatorname{argmax}} (\sum_{l \in \aleph} \rho^l \cdot \dot{x}_l^T \cdot U_d^l) \cdot y \tag{17}$$

$$\dot{x}_l = \underset{x_l \in X_l}{\operatorname{argmax}} x_l^T \cdot U_a^l \cdot \dot{y}, l \in |\aleph| \tag{18}$$

The commonly used approach for solving Bayesian game, which firstly reducing the Bayesian game into a complete information normal form game by "Harsanyi Transformation",[36] and secondly working directly on the reduced normal form game, is computing the players ex-ante BNE. The ex-interim BNE as defined by formulas (17) and (18) need new algorithms. Ceppi at el. [35] developed three algorithms for computing ex-interim BNE for 2-player games, namely the B-PNS (based on Support Enumeration), the B-LC (based on Linear Complementarity formulation), and the B-SGC (based on Mixed Integer Linear Programming). In this research, the B-SGC algorithm is employed. Note that all the 3 algorithms can be quite computationally time-consuming, thus before using these algorithms, the dominance checking should be carried out on the game firstly.

3.4 Bayesian Stackelberg CPP Game

A Bayesian Stackelberg CPP game is a Stackelberg CPP game in which there are multiple adversaries (i.e. followers), thus the defender can capture the uncertainties of the different adversaries.

A Bayesian Stackelberg Equilibrium (BSE) $(\tilde{y}, \tilde{k}^1, \tilde{k}^2, \dots, \tilde{k}^{|\aleph|})$ for the Bayesian Stackelberg CPP game is defined by formulas (19) and (20).

$$\tilde{y} = \underset{y \in Y}{\operatorname{argmax}} \sum_{l \in \aleph} \rho^l \cdot U_d^l(\tilde{k}^l, :) \cdot y \tag{19}$$

$$\tilde{k}^l = \underset{k^l \in M^l}{\operatorname{argmax}} U_a^l(k^l, :) \cdot y \tag{20}$$

In which ℵ is the set of adversary types; ρ^l denotes the occurring probability of the l^{th} adversary; $U_d^l(i,:)$ ($U_a^l(i,:)$) represents the i^{th} row of the defender's (adversary's) payoff matrix, when the adversary is the l^{th} type of adversary; $M^l = \{1,2,\dots,m^l\}$, m^l is the number of pure strategies of the l^{th} adversary.

A straightforward approach to compute the BSE is to list all the possible combinations of different types of attackers' best response, and then for each possible combination, the problem can be solved as a linear programming. This approach is a small deviation of the MultiLPs algorithm for solving the complete information Stackelberg game. However, as pointed out by Paruchuri et al.,[37] the computational complexity of this approach will increase exponentially. Paruchuri et al.[37] proposed an efficient algorithm named "Decomposed Optimal Bayesian Stackelberg Solver (DOBSS)" which uses Mixed Integer Linear Programming (MILP) techniques to compute equilibrium for Bayesian Stackelberg games. Table I shows the details of the DOBSS algorithm.

Table I. DOBSS algorithm

Algorithm DOBSS
Input:
The payoff matrix $((U_a^l, U_d^l), \rho^l), l \in \aleph$
Output:
The BSE of the Bayesian Stackelberg CPP Game $(\tilde{y}, \tilde{k}^1, \tilde{k}^2, \dots, \tilde{k}^{\lvert\aleph\rvert})$

$$\tilde{y} = \sum_{i \in M^1} v_{ij}^1 \quad (21)$$

$$\tilde{k}^l = \underset{i \in M^l}{\operatorname{argmax}}\{q_i^l\} \quad (22)$$

Where v_{ij}^l and q^l ($l \in \aleph$) are the optimal solution of the MILP (ω is a large constant number):

$$\max_{q^l, v^l, \gamma^l} \sum_{l \in \aleph} \sum_{i \in M^l} \sum_{j \in N_d} \rho^l \cdot U_d^l(i,j) \cdot v_{ij}^l \quad (23)$$

$$s.t. \sum_{i \in M^l} \sum_{j \in N} v_{ij}^l = 1, \forall l \in \aleph \quad (24)$$

$$\sum_{i \in M^l} v_{ij}^l \leq 1, \forall j \in N, l \in \aleph \quad (25)$$

$$q_i^l \leq \sum_{j \in N} v_{ij}^l \leq 1, \forall i \in M^l, l \in \aleph \quad (26)$$

$$\sum_{i \in M^l} q_i^l = 1, \forall l \in \aleph \quad (27)$$

$$0 \leq \gamma^l - \sum_{j \in N} U_a^l(i,j) \cdot \left(\sum_{h \in M^l} v_{hj}^l\right) \leq \left(1 - q_i^l\right)\omega, \forall i \in M^l, l \in \aleph \quad (28)$$

$$\sum_{i \in M^l} v_{ij}^l = \sum_{i \in M^1} v_{ij}^1, \forall j \in N, l \in \aleph \quad (29)$$

$$v_{ij}^l \in [0,1] \quad (30)$$

$$q_i^l \in \{0,1\} \quad (31)$$

$$\gamma^l \in R \quad (32)$$

In DOBSS, the v_{ij}^l is defined as $v_{ij}^l = q_i^l \cdot y_j$, in which y represents the defender's mixed strategy and q^l is a $(0-1)$ vector whose entries q_i^l indicating whether the pure strategy i is being played by the l^{th} type of attacker or not. Knowing this, the formulas (21), (24), (25), (26), and (30) are easily to be understood by recalling the definition of y and q^l. Formulas (22) and (31) reflect the fact that, observing the leader's (i.e. the defender) committed strategy, the Stackelberg follower (i.e. the adversaries) would play pure strategies maximizing their payoff. Formula (28) further explains this. For any types of the adversary, if the i^{th} pure strategy is played (i.e. $q_i^l = 1$), formula (28) becomes:

$$0 \leq \gamma^l - \sum_{j \in N} U_a^l(i,j) \cdot \left(\sum_{h \in M^l} v_{hj}^l\right) \leq 0 \quad (33)$$

If the i^{th} pure strategy is not played (i.e. $q_i^l = 0$), formula (28) becomes:

$$0 \leq \gamma^l - \sum_{j \in N} U_a^l(i,j) \cdot \left(\sum_{h \in M^l} v_{hj}^l\right) \leq \omega \quad (34)$$

Combine formulas (33) and (34), considering that the ω is a large constant number, we have (in condition of $q_l^l = 1$, and $q_i^l = 0$):

$$\gamma^l = \sum_{j \in N} U_a^l(I,j) \cdot \left(\sum_{h \in M^l} v_{hj}^l\right) \geq \sum_{j \in N} U_a^l(i,j) \cdot \left(\sum_{h \in M^l} v_{hj}^l\right). \quad (35)$$

Since $\sum_{h \in M^l} v_{hj}^l = y_i$, thus formula (35) represents the fact that observing the defender's committed strategy y, the attacker would play the pure strategy (i.e. $q_I^l = 1$) which can maximize his own payoff (i.e. γ^l).

Formula (23), or the cost function of the MILP, represents the fact that the defender can also determine the different types of adversaries' best responses, thus the defender aims at maximizing her expected payoff.

Since the DOBSS works directly on the compact representation of the Bayesian Stackelberg game, some heuristic information can be used to avoid some unnecessary computation, finally resulting on the high performance of this algorithm. Computational experiments carried out in Paruchuri el al.[37] show that DOBSS can solve games with a dozen types of adversaries in a reasonable time (i.e. in hours), while the MultiLPs cannot.

4. CASE STUDY

In this section, a case study is used, to illustrate how the Bayesian Stackelberg CPP game can be used to improve security in the process industry.

4.1 Basic Settings

Figure 4 shows the layout of a typical refinery, which is also an illustrative case used in API,[5] Lee et al.,[38] and Zhang and Reniers.[8]

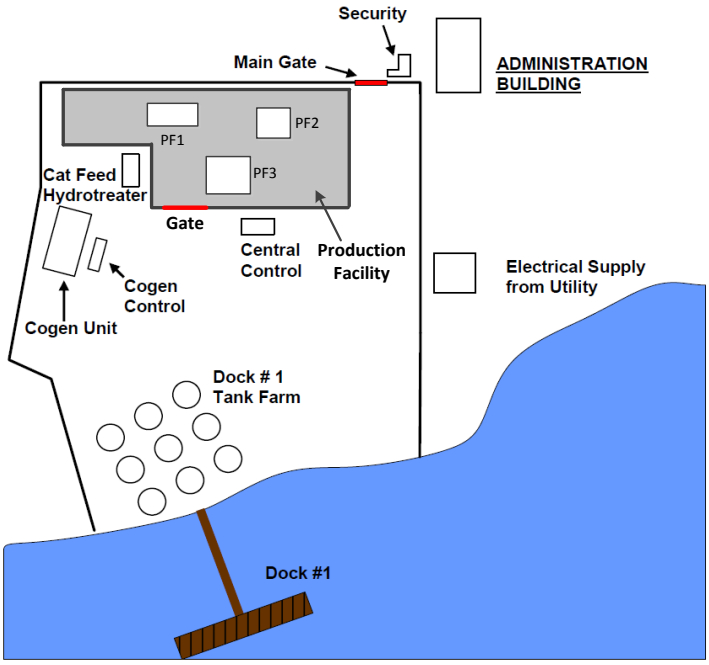
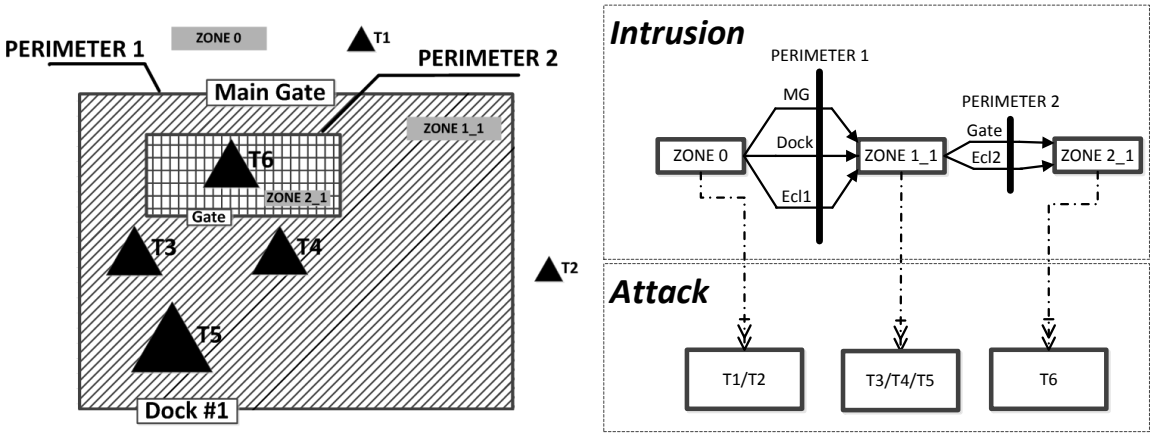


Figure 4. Layout of the plant (PF=Production Facility) [source: Zhang and Reniers[8]]

API[5] concludes that the potential threats for this refinery include terrorists, disgruntled employees, and environmental activists etc. Since the employees have unrestricted access to the whole plant, obviously the intrusion detection system does not work for reducing the threat of the disgruntled employee. In this paper, without loss of generality, we therefore assume that this refinery faces two types of adversaries: the suicide bomber and the environmental activist. Therefore, we have $\aleph = \{suicide\ bomber, environmental\ activist\}$. According to the site specific threat history information given by API, the threat of an environmental activist is stronger than that of a terrorist, and therefore we assume the numbers as $\rho = \{3/7, 4/7\}$.



(a) Abstract Description of the Plant (b) Intrusion and Attack Procedure

Figure 5. Intrusion Detection Model of the Case – description of the plant (left panel (a)) and attacker's viewpoint (right panel (b))

Figure 5 shows the formulated intrusion detection model of the given case study. According to Figure 5, there are 8 "typicals" in the refinery. Furthermore, we have that $Q = 2$, and $sub(1) = sub(2) = 1$, which means both zone level 1 and zone level 2 have only 1 sub zone, $ent(1) = 3$, $ent(2) = 2$, which means that perimeter 1 has 3 accesses and perimeter 2 has 2 accesses, and they are the Main Gate (MG), the Dock #1 (Dock), and the enclose (Ecl1) for the perimeter 1 while the Gate and the enclose (Ecl2) for the perimeter 2. Based on this analysis, a defender's pure strategy can be denoted as $s^d = z^0 \times A^1_{MG} \times A^1_{Dock} \times A^1_{Ecl1} \times z^1_1 \times A^2_{Gate} \times A^2_{Ecl2} \times z^2_1$, and further assume that the defender can set 3 different scenarios or security alert levels at each typical. For instance, a defender strategy $s^d = 3 \times 1 \times 2 \times 1 \times 2 \times 3 \times 2 \times 1$ represents that the defender set the security alert level at ZONE 0 on 3, at the main entrance on 1, at the dock on 2, and so forth.

For illustrating the suicide bomber's pure strategies, noting that there are 2 targets in ZONE 0, thus for attacking targets locating in ZONE 0, there are 2 scenarios; that there are 3 targets in ZONE 1, and there are 3 accesses on perimeter 1, thus for attacking targets locating in ZONE 1, there are $3 \times 3 = 9$ scenarios; while that there are 1 target in ZONE 2, and there are 3 accesses on perimeter 1, 2 accesses on perimeter 2, thus for attacking targets locating in ZONE 2, there are $1 \times 3 \times 2 = 6$ scenarios. Further assuming that the suicide bomber has 3 different attack efforts/levels, thus there are total $3 \times (2 + 9 + 6) = 51$ attacking strategies. Adding the non-attack strategy (e.g., attack

effort equals 0), the suicide bomber has 52 pure strategies. Recalling the definition of the attacker's pure strategy, an instance of the suicide bomber's pure strategy can be $s^a = 2 \times MG \times Gate \times T6$, which means that the he attacks target 6 with effort 2, and he passes perimeter 1 from the main entrance, and passes perimeter 2 from the gate. The environmental activist's pure strategies can be analysed analogously, and we further assume that the environmental activist is not interested in the administration building (T1) and the tank farm (T5), thus he has $3 \times (1 + 6 + 6) + 1 = 40$ pure strategies.

Further numerical settings of this case study, since most of which are referred from Zhang and Reniers,[8] are given in appendix A.

4.2 BSE Equilibrium Analysis

Using the parameters given in section 4.1, the Bayesian Stackelberg Equilibrium (BSE) of the game-theoretical model is shown in Table II.

The BSE indicates that the defender should set the SAL at different "Typicals" as $s^d_{95} = 2 \times 1 \times 2 \times 2 \times 2 \times 1 \times 1 \times 1$ with probability 0.7424, as s^d_{2279} with probability 0.1515, while as s^d_{2282} with probability 0.1061. Observing the defender's committed mixed strategy, if the adversary is an environmental activist, his best response would be playing $s^{ac}_{19} = 2 \times T2$ (that is, attacking the electrical supply station in ZONE 0, by effort 2), while if the adversary is an suicide bomber, his best response would be playing $s^{sb}_{44} = 3 \times Dock \times T5$ (that is, attacking the tank farm, by effort level 3, and passing the perimeter through the Dock #1).

Table II. BSE of the case study using Bayesian Stackelberg CPP Game

Industrial Defender		
Index	Strategy	Probability
s^d_{95}	$2 \times 1 \times 2 \times 2 \times 2 \times 1 \times 1 \times 1$	0.7424
s^d_{2279}	$2 \times 1 \times 2 \times 1 \times 2 \times 1 \times 1 \times 2$	0.1515
s^d_{2282}	$2 \times 1 \times 2 \times 2 \times 2 \times 1 \times 1 \times 2$	0.1061
Environmental Activist		
Index	Strategy	Probability
s^{ac}_{19}	$2 \times T2$	1

Suicide Bomber		
Index	Strategy	Probability
s_{44}^{sb}	$3 \times Dock \times T5$	1

By employing formulas (4) and (5), we can obtain the payoffs of the players on the BSE. If the adversary is an environmental activist, the defender's payoff would be €-261,060.6, the activist's payoff would be €33,000.0; if the adversary is an suicide bomber, the defender's payoff would be €-379,697.0, while the suicide bomber's payoff would be €205,454.5. Therefore, by playing the mixed strategy resulting from the BSE, the defender's expected payoff is €-311,904.8.

The defender's cost on defence is $cost = [215{,}000.0\ 215{,}000.0\ 225{,}000.0]$ by playing each strategies shown in Table II, the expected cost is €216,061.0.

If there is no defence at all (e.g. no perimeter, no patrolling etc.), thus both the environmental activist and the suicide bomber would attack the production facilities, bringing a loss of €1,000,000.0 and €10,000,000.0 to the defender respectively. Therefore, the defender's expected payoff would be €-4,857,100.0.

In a nutshell, if the defender invests about €216,061.0 to protect the plant (i.e. obeying the strategy given in Table II), she would reduce her expected loss from €4,857,100.0 to €311,904.8. The Return on Investment (ROI) is $ROI = (4857100.0 - 311904.8)/216061.0 = 21.0366$.

Some readers might doubt that knowing the adversaries' behaviours, why do we protect the "Typicals" which the adversary would not pass by. For example, the result in Table II shows that neither the environmental activist nor the suicide bomber would intrude to ZONE 2_1 to attack the T6, but the defender still defends the ZONE 2_1 very well (i.e. in s_{2279}^{d} and s_{2282}^{d}, the security level of ZONE 2_1 is 2). Therefore, it seems the investment on defending ZONE 2_1 is inefficient. However, if we set the security alert level (SAL) on the ZONE 2_1 to 1 in the defender's optimal strategies, then the best response of the suicide bomber would change into playing strategy $3 \times MG \times Ecl2 \times T6$ (that is, attacking the production facilities in zone level 2, by effort 3, and passing perimeter 1

through the main gate, pass the perimeter 2 by stepping over the perimeter), although the environmental activist would still play $2 \times T2$. In this case, the defender saves €2,576.0 by reducing the security alert level in ZONE 2_1from 2 to 1, but would suffer a loss of €-383,842.1 (compared to €-311,904.8, it is €71,937.3 more than the loss if the defender plays the Bayesian Stackelberg Equilibrium strategy) if attacked by a suicide bomber. The key reason for this phenomenon is that security research focuses on intentional adversaries, instead of non-intentional adversaries as in the case in safety research. As we mentioned in the beginning of this paper, the intentional adversaries would adjust their behaviour according to the defender's strategies.

4.3 (Inter-)Comparison of different Game Solutions

To show the advantages of the BSE solutions, the ex-interim Bayesian Nash Equilibrium (explained in Section 3.3) for the case study is also calculated, as shown in Table III.

Table III. Ex-interim BNE of the case study

Industrial Defender		
Index	Strategy	Probability
s_{95}^{d}	$2 \times 1 \times 2 \times 2 \times 2 \times 1 \times 1 \times 1$	0.5580
s_{173}^{d}	$2 \times 1 \times 2 \times 1 \times 3 \times 1 \times 1 \times 1$	0.2186
s_{2282}^{d}	$2 \times 1 \times 2 \times 2 \times 2 \times 1 \times 1 \times 2$	0.2234
Environmental Activist		
Index	Strategy	Probability
s_{19}^{ac}	$2 \times T2$	1
Suicide Bomber		
Index	Strategy	Probability
s_{44}^{sb}	$3 \times Dock \times T5$	0.3041
s_{45}^{sb}	$3 \times Ecl1 \times T5$	0.5000
s_{47}^{sb}	$3 \times MG \times Ecl2 \times T6$	0.1959

By playing the ex-interim BNE, the defender's expect payoff is €-323,436.3, which is smaller than the defender's BSE payoff, which is €-311,904.8.

Defender could obtain her BSE payoff only in case that the attackers could be able to observe her strategy perfectly. If this assumption does not hold, or in other words, the attackers plays their ex-interim BNE strategy, then the defender's expected payoff would be:

$$EU = \rho^1 \cdot \dot{x}_1^T \cdot U_d^{terrorist} \cdot \tilde{y} + \rho^2 \cdot \dot{x}_2^T \cdot U_d^{activist} \cdot \tilde{y} = -323{,}925.0$$

It can been seen that if the perfectly observation assumption does not hold, the defender would only get a payoff of €-323,925.0, which is €12,020.2 less than her BSE payoff, and it is also €488.7 less than her ex-interim payoff.

However, if the attackers they do be able to observe the defender's strategies, but the defender does not know this, and plays her ex-interim BNE strategy. In this case, according the definition of ex-interim BNE, any pure strategies in the support[3] of the attackers' ex-interim BNE strategy could be the attackers' best response. Thus the pure strategies listed in Table III, which are, for the suicide bomber, pure strategies s_{44}^{sb}, s_{45}^{sb}, s_{47}^{sb}, for the activist, pure strategy s_{19}^{ac}, are possible best responses for the suicide bomber and the activist respectively. For the defender, her payoff w.r.t. the attackers' different responses can be calculated as:

$$EU_{44\&19} = \rho^1 \cdot U_d^{terrorist}(44,:) \cdot \dot{y} + \rho^2 \cdot U_d^{activist}(19,:) \cdot \dot{y} = -311{,}979.1$$

$$EU_{45\&19} = \rho^1 \cdot U_d^{terrorist}(45,:) \cdot \dot{y} + \rho^2 \cdot U_d^{activist}(19,:) \cdot \dot{y} = -311{,}979.1$$

$$EU_{47\&19} = \rho^1 \cdot U_d^{terrorist}(47,:) \cdot \dot{y} + \rho^2 \cdot U_d^{activist}(19,:) \cdot \dot{y} = -370{,}468.6$$

This results show that being indifferent to play strategies s_{44}^{sb}, s_{45}^{sb}, and s_{47}^{sb}, the suicide bomber could choose to play s_{47}^{sb} to bring huge damages to the defender. In other words, if the attackers are able to observe the defender's strategy, while the defender does not know this and she plays her ex-interim Bayesian Nash Equilibrium, then the defender owns a great risk (her payoff can be as worse as €$-370{,}468.6$).

[3] The support of a mixed strategy x is defined as $S = \{i \in M | x_i > 0\}$. In other words, A pure strategy is in the support of a mixed strategy if that pure strategy is played with positive probability according to the mixed strategy.[39] 101 GT. The Support of Mixed Strategies. Available from: http://gametheory101.com/courses/game-theory-101/support-of-mixed-strategies/.

4.4 Sensitiveness Analysis of ρ

The BSE equilibrium can only be obtained if the defender has the prior probabilities of different types of adversaries. However, in industrial practise, it is difficult to exactly estimate the prior probabilities. Figure 6 shows the defender's payoff and her estimation of ρ.

In Figure 6, we assume that the refinery faces threats as descripted in section 4.1 (i.e. the same ℵ and ρ). However, this is only known by nature, the defender knows the ℵ, but she does not know the exact numbers of ρ. Therefore, the defender has to estimate the ρ. Let's denote her estimation of ρ as $\rho' = [p_{sb}, 1 - p_{sb}]$. The defender then computes her optimal strategies by employing the Bayesian Stackelberg CPP game, using ρ' as input. Let's denote her "optimal" strategy as $\tilde{y}'$ (and by playing this mixed strategy, she thinks that the best responses for the suicide bomber and environmental activist are $\hat{k}^1(\tilde{y}')$ and $\hat{k}^2(\tilde{y}')$ respectively). Subsequently the adversaries observe the defender's strategies, and execute an attack accordingly. Let's denote the suicide bomber's best response to $\tilde{y}'$ as $k^1(\tilde{y}')$, whereas the environmental activist's best response is given by $k^2(\tilde{y}')$ (note that due the mis-estimation of ρ, the adversaries' best responses could be different as the defender's expectation, i.e., $k^1 \neq \hat{k}^1$ and $k^2 \neq \hat{k}^2$). Finally, we substitute the $\tilde{y}'$, the $k^1(\tilde{y}')$, the $k^2(\tilde{y}')$, and the ρ into formulas (4) and (5), to obtain the defender's payoff.

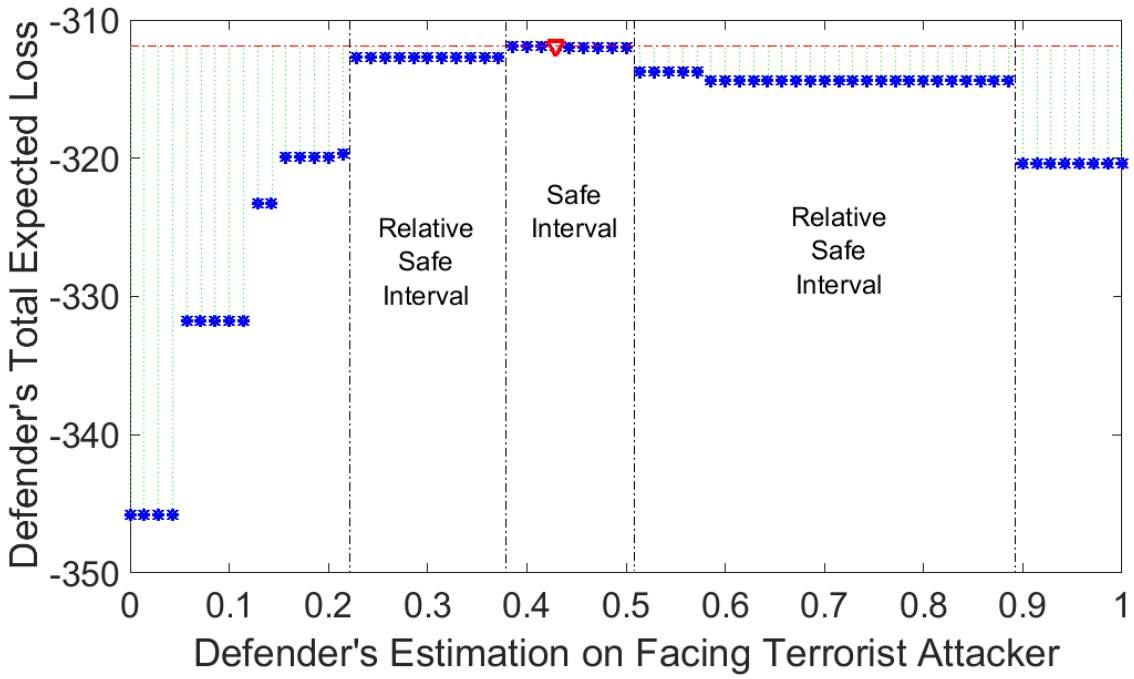


Figure 6. Sensitiveness analysis of ρ

The x-axis in Figure 6 represents the probability of attack by the terrorist p_{sb}, while the y-axis represents the defender's payoff. The blue points (x, y) represents that if the defender estimates that $p_{sb} = x$, then her payoff would be y. The red triangle (and the red line) represents the defender's maximal payoff when the defender's estimation matches the real number (i.e. $p_{sb} = 3/7$).

Sensitivity analysis in Figure 6 shows that the Bayesian Stackelberg CPP game is robust to the defender's estimation of ρ, based on the parameter setting given in section 4.1. The defender has a safe interval $SafItv = [0.37,0.50]$, that is, if her estimation is within the $SafItv$ she would not suffer any extra loss due to the mis-estimation. The defender also has a relative safe interval $RelSafItv = [0.22,0.37] \cup [0.50,0.89]$, if her estimation is within the $RelSafItv$ she would not suffer a huge extra loss.

Figure 6 also shows that, it is better to overestimate the dangerous adversary (i.e. the suicide bomber) than underestimate it. This is due to the fact that dangerous adversaries would cause the highest losses to the plant.

A very representative mis-estimation of the ρ is that the defender thinks she is not facing a terrorist threat (e.g. a suicide bomber), thus $\rho' = [0,1]$. Table IV shows the defender's "optimal" strategies based on her estimation, and the environmental activist's best response.

Table IV. Stackelberg Equilibrium for defender and environmental activist

defender	
Strategy	probability
$1 \times 1 \times 1 \times 1 \times 2 \times 1 \times 1 \times 1$	1.0
activist	
Strategy	probability
$2 \times T2$	1.0

Comparing the results in Table IV and Table III, it is obvious that the defence becomes quite weak if the defender thinks that she only faces an environmental activist threat. Although by reducing the security alert levels at each "Typicals" saves $€216{,}061.0 - €180{,}000.0 = €36{,}061.0$ for the defender, however, if a suicide bomber would attack, the defender would suffer a loss of $€486{,}818.2$, which is much higher than the $€311{,}904.8$ if she effectively estimates the existence of terrorist attacks.

5. CONCLUSION

Adversaries in any setting, also the process industry, are intelligent, and hence it is reasonable to assume that they would collect useful information before they would carry out any attack. Unfortunately, the lack of data w.r.t. adversaries brings huge uncertainties for the security managers. Existing game-theoretical models for security within a chemical plant stay at the primary state assuming simultaneous move of the players and complete information of both players. To this end, the Bayesian Stackelberg CPP game proposed in this article moves forward the state of the art of this domain.

Results of the case study show that the return on security investment could be high. The Bayesian Stackelberg game successfully captured the intelligent interactions between the defender and the adversaries. Moreover, under the settings of the case study, the Bayesian Stackelberg Equilibrium is

also more robust for the defender comparing with the ex-interim Bayesian Nash Equilibrium. Furthermore, the defender's payoff is robust w.r.t her estimation of the prior probabilities of the different adversaries and it is better for the defender to overestimate the dangerous adversaries than to underestimate them.

The proposed model can be further developed with respect to the following aspects: (i) taking into account irrational players. All of the existing researches on using game theory for improving security in the process industry are based on the "rationality assumption". However, human players are not definitely rational, and adversaries are sometimes emotion-oriented; (ii) considering continuous uncertainties of the adversaries' utility functions. However, this kind of uncertainties is quite complicated, and it is in fact a bottleneck of the domain of combination of game theory and security risk analysis.

ACKNOWLEDGEMENTS

This research is supported by the Chinese Scholarship Council (CSC), and partly by the National Nature Science Foundation of China (NSFC) under award numbers 91024030 and 71303252.

Appendix A. Numerical settings of the case study

Most of the information in this appendix are the same as in Zhang and Reniers,[8] the extra information for the environmental activist is added. It is worth noting that all data in this appendix are for illustrative purpose, if the model would be carried out in real plant protection, these information should be provided by security expert teams, such as the API SRA team [5].

Table A.1 provides the various symbols used in Figures 4 and Figure 5 and their meanings, and also offers some background information.

Table A.1 Symbols map between Figure 4 and Figure 5

Symbol in Figure 5	Symbol in Figure 4	Background information
ZONE0	Outdoor Area	
ZONE1_1	Area within Enclosure	
ZONE2_1	Production Facility	
PERIMETER 1	the boundary of the plant	The left/up/right side are enclosures and the down side is the coastline
PERIMETER 2	The boundary of the	

	production facility	
Main Gate	Main gate	
Dock #1	Dock #1	An attacker may intrude from dock #1 as well as from a ship, for example
Gate	The entrance of the production facility	
T1	Administration Building	
T2	Electrical Supply from Utility	
T3	Cogen Unit/ Cogen Control/Cat Feed Hydrotreater	
T4	Central control	
T5	Tank Farm	They are close to each other and they always contain dangerous materials. If one of the tanks belonging to the farm is attacked, then other tanks also have the risks to be destroyed due to domino effects.[40] Therefore, the consequences of this target should be estimated higher than the costs of an individual tank.
T6	Production facilities in production facility area	They are close to each other and they always contain dangerous materials. If one of the tanks belonging to the farm is attacked, then other tanks also have the risks to be destroyed due to domino effects. Therefore, the consequences of this target should be estimated higher than the costs of an individual tank.

Further assuming that the suicide bomber aims at cause maximal damage to the plant, whereas the environmental activists aim to shut down the refinery operations.

Table A.2 gives an indication of the time that is needed to travel from point A to point B in a variety of locations for our illustrative case study.

Table A.2 Cross Zone Time, both from the defender and the attacker's perspective (illustrative figures)

Zone 0 (Time is indicated in minutes)					
To / From	T1	T2	Main Gate	Dock #1	Wall
Anywhere	5	5	5	5	5
ZONE **1_1 (Time is indicated in minutes)**					
To / From	T3	T4	T5	Gate	Wall 2
Main Gate	10	10	15	10	5
Dock #1	6	7	3	10	12

Wall 1	5	5	5	5	5
ZONE **2_1 (Time is indicated in minutes)**					
To / From	T6				
Gate	3				
Wall 2	3				

Table A.3 provides the monetary consequences of the different assets that, if they would be attacked by suicide bomber, would materialize.

Table A.3 Estimated Consequence and Reward Table for the Defender and the Suicide Bomber (illustrative figures)

Asset Index	Consequences (k€)	Reward (k€)
T1	1000	1000
T2	100	100
T3	300	300
T4	800	800
T5	2000	3000
T6	10000	8000

Consequence estimation should, amongst others, take direct economic loss, casualties, business interruption, environment pollution, as well as potential domino effects to other assets into consideration. For example, if an attack on T3 will also cause losses in T5 due to domino effects (L_{35} for example), then when measuring the consequences in T3, L_{35} should also be considered.

Table A.4 provides the monetary consequences of the different assets that, if they would be shut down by environmental activists, would materialize. The activists are aiming at shutting down the plant, instead of killing people or cause environmental problems, thus they would not be interested in the T1 (the office building) and T5 (the tank farm). For the T2, T3, and T4, since these targets are control units of the plant, thus we assume that the values of these targets for the players are the same as in case of a suicide bomber adversary. For the T6, it is the production unit, thus we assume that the activist would cause less damages than the suicide bomber.

Table A.4 Estimated Consequence and Reward Table for the Defender and the Activist (illustrative figures)

Asset Index	Consequences (k€)	Reward (k€)
T1	0	0
T2	100	100
T3	300	300
T4	800	800
T5	0	0
T6	1000	1000

Table A.5 Parameters in each Typical and Assets, both from the defender and the attacker's perspective (illustrative figures)

Typical	Parameter	Values
ZONE 0	α_0	1
ZONE 1_1	α_{1_1}	3
ZONE 2_1	α_{2_1}	6
Main Gate	β_{11}	1
Dock #1	β_{12}	3
Enclosure 1	β_{13}	2
Gate	β_{21}	2
Enclosure 2	β_{22}	3
T1	P_{y1}	0.1
T2	P_{y2}	0.9
T3	P_{y3}	0.7
T4	P_{y4}	0.6
T5	P_{y5}	0.9
T6	P_{y6}	0.99

We assume that while under the same detection level and attack level, ZONE 2_1 is easier to protect than ZONE 1_1 and in its turn, ZONE 1_1 is easier to protect than ZONE 0, due to some practical reasons (size, for example, since the smaller the area, the easier to protect). Under these Assumptions, we have $\alpha_{2\_1} > \alpha_{1\_1} > \alpha_0$. Similarly, we assume that in perimeter 1, the main entrance is the most difficult access to detect intruders, because there are too many people/vehicles coming in/going out from the main entrance. Dock #1 is the most easy access with respect to intruder detection. Under these assumptions, we have $\beta_{12} > \beta_{13} > \beta_{11}$. Analogously, we use identical assumptions for the accesses of perimeter 2. Regarding P_y, T2/T5/T6 are some sensitive assets, so if an attacker is able to reach them and carry out an attack, they are very easily destroyed. T1/T3/T4 are some buildings or some equipment that, even in the event that an attacker executes an attack on them, they are difficult to destroy.

Table A.6 provides the cost for the attacker per level of attack, while Table A.7 gives some figures on the cost of the defender.

Table A.6 Cost of adversarial behaviour level (illustrative figures)

Suicide Bomber		Environmental Activist	
Attack level	**Cost (k€)**	**Behave level**	**Cost (k€)**
1	10	1	6
2	20	2	12
3	40	3	24

Table A.7 Cost of defend Level (illustrative figures)

Typical	Detect level	Cost (k€)		Detect level	Cost (k€)
Detect in ZONE 0	1	40	Detect in ZONE 1_1	1	20
	2	60		2	30
	3	100		3	50
Detect at MG	1	20	Detect at Gate	1	20
	2	30		2	25
	3	50		3	40
Detect at Dock	1	20	Detect in ZONE 2_1	1	20
	2	25		2	30
	3	40		3	50
Detect at Ecl 1	1	20	Detect in Ecl 2	1	10
	2	30		2	20
	3	50		3	40

REFERENCE

[1] Brown G, Carlyle M, Salmerón J, Wood K. Defending critical infrastructure. Interfaces. 2006;36(6):530-44.

[2] Reniers GLL, Cremer K, Buytaert J. 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. J Clean Prod. 2011;19(11):1239-49.

[3] Cox Jr LAT. Some limitations of "Risk= Threat× Vulnerability× Consequence" for risk analysis of terrorist attacks. Risk Anal. 2008;28(6):1749-61.

[4] Cox LAT, Babayev D, Huber W. Some limitations of qualitative risk rating systems. Risk Anal. 2005;25(3):651-62.

[5] Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, (2013).

[6] Cox Jr LAT. Game theory and risk analysis. Risk Anal. 2009;29(8):1062-8.

[7] Bier VM, Azaiez MN. Game theoretic risk analysis of security threats: Springer Science & Business Media; 2008.

[8] Zhang L, Reniers G. A Game-Theoretical Model to Improve Process Plant Protection from Terrorist Attacks. Risk analysis : an official publication of the Society for Risk Analysis. 2016.

[9] Feng Q, Cai H, Chen Z, Zhao X, Chen Y. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. J Loss Prev Process Ind. 2016;43:614-28.

[10] Pavlova Y, Reniers G. A sequential-move game for enhancing safety and security cooperation within chemical clusters. J Hazard Mater. 2011;186(1):401-6.

[11] Talarico L, Reniers G, Sörensen K, Springael J. MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. Reliab Eng Syst Saf. 2015;138:105-14.

[12] Guikema SD. Game theory models of intelligent actors in reliability analysis: An overview of the state of the art. Game theoretic risk analysis of security threats: Springer; 2009. p. 13-31.

[13] Tambe M. Security and game theory: algorithms, deployed systems, lessons learned: Cambridge University Press; 2011.

[14] Nikoofal ME, Zhuang J. Robust allocation of a defensive budget considering an attacker's private information. Risk Anal. 2012;32(5):930-43.

[15] Nikoofal ME, Zhuang J. On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. European Journal of Operational Research. 2015;246(1):320-30.
[16] McLay L, Rothschild C, Guikema S. Robust adversarial risk analysis: A level-k approach. Decision Analysis. 2012;9(1):41-54.
[17] Rothschild C, McLay L, Guikema S. Adversarial risk analysis with incomplete information: A level‐k approach. Risk Anal. 2012;32(7):1219-31.
[18] Pita J, Jain M, Marecki J, Ordóñez F, Portway C, Tambe M, et al., editors. Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport. Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track; 2008: International Foundation for Autonomous Agents and Multiagent Systems.
[19] Tsai J, Kiekintveld C, Ordonez F, Tambe M, Rathi S. IRIS-a tool for strategic security allocation in transportation networks. 2009.
[20] Powell R. Defending against terrorist attacks with limited resources. American Political Science Review. 2007;101(03):527-41.
[21] Reniers G, Van Lerberghe P, Van Gulijk C. Security risk assessment and protection in the chemical and process industry. Process Saf Prog. 2015;34(1):72-83.
[22] Hausken K. Strategic defense and attack for reliability systems. Reliability Engineering & System Safety. 2008;93(11):1740-50.
[23] Hausken K, Zhuang J. The timing and deterrence of terrorist attacks due to exogenous dynamics. Journal of the Operational Research Society. 2012;63(6):726-35.
[24] Skaperdas S. Contest success functions. Economic theory. 1996;7(2):283-90.
[25] Clark DJ, Riis C. Contest success functions: an extension. Economic Theory. 1998;11(1):201-4.
[26] Nash JF. Equilibrium points in n-person games. Proc Nat Acad Sci USA. 1950;36(1):48-9.
[27] Lemke CE, Howson J, Joseph T. Equilibrium points of bimatrix games. Journal of the Society for Industrial and Applied Mathematics. 1964;12(2):413-23.
[28] Bier VM. Choosing what to protect. Risk Anal. 2007;27(3):607-20.
[29] Moulin H, Vial J-P. Strategically zero-sum games: the class of games whose completely mixed equilibria cannot be improved upon. International Journal of Game Theory. 1978;7(3-4):201-21.
[30] (FAS) FoAS. Al qaeda training manual. 2006.
[31] Zhuang J, Bier VM. Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort. Operations Research. 2007;55(5):976-91.
[32] Conitzer V, Sandholm T, editors. Computing the optimal strategy to commit to. Proceedings of the 7th ACM conference on Electronic commerce; 2006: ACM.
[33] Von Stengel B, Zamir S. Leadership with commitment to mixed strategies. 2004.
[34] Shoham Y, Leyton-Brown K. Multiagent systems: Algorithmic, game-theoretic, and logical foundations: Cambridge University Press; 2008.
[35] Ceppi S, Gatti N, Basilico N, editors. Computing Bayes-Nash equilibria through support enumeration methods in Bayesian two-player strategic-form games. Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology-Volume 02; 2009: IEEE Computer Society.
[36] Harsanyi JC. Games with incomplete information played by “Bayesian” players, i–iii: part i. the basic model&. Management science. 2004;50(12_supplement):1804-17.
[37] Paruchuri P, Pearce JP, Marecki J, Tambe M, Ordonez F, Kraus S, editors. Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games. Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems-Volume 2; 2008: International Foundation for Autonomous Agents and Multiagent Systems.
[38] Lee Y, Kim J, Kim J, Kim J, Moon I. Development of a risk assessment program for chemical terrorism. Korean Journal of Chemical Engineering. 2010;27(2):399-408.
[39] 101 GT. The Support of Mixed Strategies. Available from: http://gametheory101.com/courses/game-theory-101/support-of-mixed-strategies/.

[40] Reniers G, Cozzani V. Domino Effects in the Process Industries: Modelling, Prevention and Managing: Elsevier B.V.; 2013. 1-372 p.