This item is the archived peer-reviewed author-version of:

A Bayesian network methodology for optimal security management of critical infrastructures

Reference:

Misuri Alessio, Khakzad Nima, Reniers Genserik, Cozzani Valerio.- A Bayesian network methodology for optimal security management of critical infrastructures
Reliability engineering and system safety - ISSN 0951-8320 - 191(2019), p. 1-14
Full text (Publisher's DOI): <https://doi.org/10.1016/J.RESS.2018.03.028>

A Bayesian Network methodology for optimal security management of critical infrastructures

Abstract

Security management of critical infrastructures is a complex task as a great variety of technical and socio-political information is needed to realistically predict the risk of intentional malevolent acts. In the present study, a holistic methodology based on Limited Memory Influence Diagram has been developed for protection of chemical facilities via cost-effective allocation of security measures. Limited memory influence diagram is an extension of Bayesian network intended for decision-making, allowing for efficiently modeling complex systems while accounting for interdependencies and interaction of variables. The probability updating feature of Bayesian Network has been used to investigate the effect of vulnerabilities on perpetrators' preferences when attacking assets. Moreover, the proposed methodology has been shown to be able to compute the optimal defensive strategy given an attack through maximizing the expected utility. Although the application of the methodology has been demonstrated via chemical facilities, it can easily be tailored to a wide variety of critical infrastructures.

Keywords: Critical Infrastructures; Security; Security Management; Limited Memory Influence Diagram; Optimal Resource Allocation;

1) Introduction

Chemical industry usually processes large quantities of hazardous substances, and thus the development of technologies both to avoid dangerous events and to mitigate the consequences of such events has to be considered of primary importance. A chemical accident may lead to the release of toxic or flammable materials which are able to cause a large number of fatalities, catastrophic damages to the properties, and considerable loss of public confidence. For this reason, chemical plants are definitely considered as hazardous facilities.

Before 9/11 terrorist attacks, risk analysis focused mainly on accidental events, which might occur due to human errors, technical failures, or natural events (known as Natech accidents). Since then, however, acts of deliberate actions against chemical facilities have also become of primary concern [1,2]. Various methodologies have been developed to help the management to allocate resources efficiently in the selection of appropriate countermeasures. Initiative guidelines to carry out Security Risk Assessment (SRA) have been provided in [1 - 4]. Subsequently, a number of studies and methodologies have been published: Bajpai and Gupta proposed a semi-quantitative approach for securing oil and gas infrastructures [6] and chemical process industries [7]; a new version of API guidelines was released in 2012 [5]; Srivastava and Gupta proposed stepped-matrices based methodologies for oil and gas facilities [8]; Reniers proposed a methodology based on the combination of rings-of-protection concept and generic practices for securing process industry in Belgium [9]; Argenti et al. proposed a model to assess the attractiveness of assets within a chemical facility from attackers' perspective [10]. A common feature of the majority of these methodologies is that their outcomes are mostly qualitative, or at most semi-quantitative. The most traditional methodologies are usually based on (i) identification of most critical units, (ii) threat assessment, (iii) attractiveness assessment, (iv) vulnerability assessment, (v) calculation of the security risk, and (vi) evaluation of the various risk mitigating options [2-7]. To provide a realistic identification of the criticalities of different assets and understanding the threats the plant may be exposed to, a multitude of different information is required. For example, following API guidelines [4,5] the team appointed to conduct the SRA needs to gather a significant amount of information about the socio-political context, possible actors who might be interested in attempting a deliberate detrimental action against the plant, as well as detailed technical documentation about the layout and the features of the plant. Accordingly, an interdisciplinary and holistic approach to SRA would be required.

In addition, the majority of foregoing methodologies are based on a sequential scoring of the security risk parameters: this means that the mutual influences of parameters on each other cannot be easily accounted for. For example, carrying out a SRA following API guidelines [4,5], the limitations of the linear approach are clear: the attractiveness of a specific target to a given perpetrator is assessed before assessing the vulnerabilities, thus undermining to a large extent the influence of vulnerabilities on targets attractiveness [11].

The necessity to combine different types of information and the need to take into account mutual interactions between parameters require the use of proper models to provide the management with an assessment as realistic as possible. In the present study, Bayesian Network (BN) is used for this purpose due to its flexible and probabilistic framework which allow to consider conditional dependencies among variables of security risk. BN is able to account for new information in belief updating. The BN is extended to a Limited Memory Influence Diagram (LIMID) to identify optimal countermeasures and responses to intentional attacks against a chemical plant. Indeed, Limited Memory Influence Diagram represents a sophistication of Bayesian Network particularly suitable for decision making, and is a versatile tool to merge different types of information, consider complex dependencies, and identify optimal decision alternatives.

While in the safety domain Bayesian Networks are consolidated tools to solve problems with complex interactions, in the field of security only are there a few works available: Argenti et al. [12] proposed a methodology to assess vulnerabilities of chemical clusters considering the conditional failure probabilities of different physical barriers; Van Staalduinen et al. [13] proposed a quantitative risk assessment methodology based on parameters scoring and Bayesian Networks; Paté-Cornell et al. [23, 27] proposed an overarching framework to organize information and assess terrorists' preferences; Rios and Rios Insua [39] proposed a hybrid Bayesian and game-theoretical framework to model attacker-defence games.

A brief description of Bayesian Networks, Influence Diagrams and Limited Memory Influence Diagrams is presented in the next section; since the present study is mainly based on a previous work of Paté-Cornell and Guikema [23, 27], their approach is recapitulated in Section 3. In Section 4, the methodology will be outlined and applied to a case study to describe its features. Conclusions will be presented in Section 5.

2) Bayesian Networks and Influence Diagrams

2.1) Bayesian Network

BN is a flexible tool for knowledge elicitation and reasoning under uncertainty [14]. It is a directed acyclic graph (DAG) which represents relationships among random variables using arcs and nodes. This kind of representation takes advantage of its structure to provide a synthetic and clearly understandable insight of the dependencies among the components of a system. The types of these dependencies are locally defined by assigning marginal and conditional probability tables to nodes. Nodes which do not have children are called leaf nodes. Nodes which do not have parents, are called root nodes. Through the use of d -separation criteria and chain rule, joint probability distribution of a set of random variables $X = \{X_1, X_2, \dots, X_n\}$ can be computed as a multiplication of the probabilities of nodes conditioned on their immediate parents:

$$P(X) = P(X_1, X_2, \dots, X_n) = \prod_{i=1}^n P(X_i | pa(X_i)) \quad (1)$$

where $pa(X_i)$ is the parent set of X_i . For example, considering the set of five random variables and their dependencies represented through the BN depicted in Fig.1, the joint probability distribution can be computed as $P(X_1, X_2, X_3, X_4, X_5) = P(X_1) \cdot P(X_2 | X_1) \cdot P(X_3 | X_1, X_2) \cdot P(X_4 | X_2, X_3) \cdot P(X_5 | X_2)$.

Fig. 1: A Bayesian Network comprising five nodes. X_1 is a root node; X_4 and X_5 are leaf nodes. X_2 and X_3 are intermediate nodes.

BN takes advantage of the Bayes' theorem to conduct belief updating [14], i.e., the computation of posterior probabilities given new information. The set of new information is called evidences E and can be in the form of a set of chance nodes instantiated to one of their possible states:

$$P(X|E) = \frac{P(X) \cdot P(E|X)}{\sum_{X/E} P(X) \cdot P(E|X)} \quad (2)$$

where $P(X|E)$ is the updated joint probability and $\sum_{X/E}(\cdot)$ is the summation over all the values of X except E . Despite the hardness of the problem [15], there exist algorithms for exact and approximate solution which have been implemented in a number of available software: the networks presented in this study have been drawn and computed in software GeNIe [16]. A simple dissertation with further examples of BN can be found in [17].

2.2) Limited Memory Influence Diagrams

Influence Diagrams (IDs) represent a sophistication of BNs to help decision makers to cope with sequential decisions [18]. IDs have the structure of DAGs as BNs, but they comprise two more types of nodes: decision nodes and utility nodes. Decision nodes correspond to the choices available to the decision maker, while utility nodes are variables whose values represent the preferences of the decision maker regarding the outcome. Utility nodes are assigned tables of numerical values for each configuration of their parents. A decision node is usually depicted as square, while a utility node as a diamond.

Two additional assumptions are traditionally required. The first assumption is the regularity of the network [18]: an ID is said to be regular if contains at least one directed path comprising all the decision nodes. This feature denotes a complete topological ordering among the decision variables [19], which means there is a well-defined temporal order to be followed setting decisions. The second assumption is the non-forgetting assumption [18]: previous decisions and observations are known at the moment each decision is made. These two requirements may significantly complicate the network, hindering its application to realistic decision-making problems. By relaxing the two foregoing assumptions, Lauritzen and Nilsson [20] proposed LIMID as an alternative to ID. In a LIMID, the temporal order of decisions is defined by arcs connecting decisions, and information available at the time each decision has to be made is univocally defined by the arcs directing to it. For example, in Fig.2 at the time the decision has to be made, the state of X_2 has to be known.

Fig. 2: A Limited Memory Influence Diagram. Before the Decision can be made, the state of X2 has to be known.

In the context of LIMIDs, each state of a decision node is called a policy, while a sequence of policies identified by more than one decision node is called a strategy. Solving a LIMID usually means finding the optimal policy or strategy, i.e., the one that maximises the expected utility. For example, in Fig.2, for the j -th policy d_j , the expected utility $EU(d_j)$ can be computed as:

$$EU(d_j) = \sum_{X_4} P(X_4|d_j) \cdot U(d_j, X_4) = P(x_{4,1}|d_j)u_{1,j} + P(x_{4,2}|d_j)u_{2,j} + \dots + P(x_{4,m}|d_j)u_{m,j} \quad (3)$$

where $\{x_{4,i}\}$ for $i=1 \dots m$ are the possible states of the variable X_4 . By solving the LIMID, a policy which satisfies Eq. (4) can be identified as the optimal policy d_k :

$$EU(d_k) \geq EU(d_j) \text{ for each } j \neq k \quad (4)$$

The table of values assigned to the Utility node should quantitatively express how much the decision maker would prefer an outcome over another: exhaustive dissertations on this topic can be found in [21, 22].

3) Application of LIMID to Security Risk Assessment

In this section, an application of LIMID to SRA proposed by Paté-Cornell and Guikema [23, 27] is summarized as the starting point of the present study. Paté-Cornell and Guikema [23] applied LIMID to set priorities among terrorism countermeasures for U.S. Homeland Defence. This kind of analysis is particularly suitable for the estimate of risk in complex engineering systems and sets its bases in systems analysis, that is the decomposition of the system of interest in its components to study their interactions. They proposed an overarching model to collect the mass of information needed and to efficiently comprise relationships among them. Their framework is depicted in the form of a LIMID in Fig. 3.

Fig. 3: Overarching LIMID model proposed by Paté-Cornell and Guikema [23].

This representation provides a simplified but still holistic view of the problem of assessing appropriate countermeasures to face terrorist threats. An attack scenario is represented as the combination of possible delivery means, targets and kinds of weapon, while information gathered to deal with it is represented by the “Intelligence Indicators” node. The outcome to the U.S. is depicted as a utility node whose values depend on the type of scenario and the quality of the response.

It is worth noting that this model has been designed to support defenders, and is thus based on the Intelligence’s knowledge about the possible terrorist groups and their preferences among different actions. This issue leads to degrees of subjectivity as in the case of data scarcity, probabilities have to be assessed according to experts’ opinions. The model presented in Fig. 3 is also based on the presumption of terrorist rational behaviour [24], that is, a terrorist group would attempt to maximize the expected utility of their attack. In this regard, the terrorist group evaluates each scenario, intended as the choice of a weapon W_i in [23], with a probability proportional to the expected utility of that scenario. As a result, the conditional probability of each scenario, given a specific perpetrator, can be identified as the ratio of the expected utility of each scenario to the sum of the expected utilities of all scenarios:

$$P_{defender}(W_i|I_{perp}) = \frac{E_{perp}(U_{perp}|W_i, I_{perp})}{\sum_i E_{perp}(U_{perp}|W_i, I_{perp})} \quad (5)$$

where the subscriptions *defender* and *perp* mean that a variable is perceived by the defender or by a generic perpetrator, respectively; $P_{defender}(W_i|I_{perp})$ is the probability estimated by the defender when a perpetrator with an intent to attack of I_{perp} employs weapon W_i ; E_{perp} is the expected utility from the perpetrator’s perspective. To calculate E_{perp} , the defender can use Eq. (6):

$$E_{perp}(U_{perp}|W_i, I_{perp}) = P_{perp}(S|W_i, I_{perp}) \cdot U_{perp}(S|W_i, I_{perp}) + P_{perp}(F|W_i, I_{perp}) \cdot U_{perp}(F|W_i, I_{perp}) \quad (6)$$

where $P_{perp}(S|W_i, I_{perp})$ and $P_{perp}(F|W_i, I_{perp})$ are the defender’s evaluations of how much the perpetrator thinks an attack is successful (i.e. S) or unsuccessful (i.e. F), respectively, $U_{perp}(S|W_i, I_{perp})$ is the utility the perpetrator expects from a successful attack, and $U_{perp}(F|W_i, I_{perp})$ is the utility expected from an unsuccessful attack, again, estimated by the defender. In [23] the utility of an unsuccessful attack is considered zero, so only the first term on the right side of Eq. (6) is reported.

This approach is based on the theory of stochastic behaviours proposed by Luce [24], that is, the choice of one alternative over another does not depend on the presence of other alternatives, but only on the relative weight of the two compared alternatives. In decision theory this is usually called independence of irrelevant alternatives (IIA). Furthermore, as described later by Rubinstein [25], this approach leads to a bounded rationality system: the terrorist in this context is supposed to act as a fully rational agent with a finite set of possible scenarios.

This approach is clearly attractive because allows the defender to give priority to scenarios which both are easiest to implement and have the most convenient outcome to perpetrators. These two pieces of information constitute the expected utility of perpetrator's actions, as presented in Eq. (6). The restriction of terrorist possibilities to a limited and predetermined set of scenarios makes the model feasible, but constitutes a major shortcoming, because it may not be able to completely capture the behaviour of a perpetrator. Indeed, scenarios not considered by the intelligence cannot be taken into account by this model [26]. In other words, this model significantly relies on the value of intelligence and the quality of information that can be processed in the calculations.

Thus, to derive useful results for countermeasures ranking, firstly the defender has to determine the utility from each possible perpetrator's point of view of successful attack carried out following each different strategy. Secondly the defender has to estimate the probability of success, perceived by each perpetrator, and then to compute the expected utility of each scenario according to Eq. (6). After these steps, the probability of each scenario, given a specific perpetrator, is computed according to bounded rationality axioms (i.e. normalization procedure in Eq. (5)). At this point, a ranking of scenarios following perpetrators' preferences has been outlined, and can be used to rank countermeasures querying the LIMID

According to the inherently dynamic nature of terrorism, the adopted approach needs to be dynamic too: the issue of security constitutes a complex phenomenon, not easy to represent with static and conventional methodologies. This is the reason why the influence diagram in Fig.3 has to be seen only as a snapshot of a dynamic counterterrorism approach. Preferences of groups and probabilities of attacks may continuously change and the intelligence indicators need to be updated accordingly. As pointed out by the authors, the presented model has to be used in dynamic and game-theoretic mode [23, 27].

4) The Methodology

4.1) General description of the method

The proposed methodology in the present study is an LIMID from defender's perspective accounting for two decisions. One decision concerns the state-of-the-art of security inside the plant before the security event takes places, while the other describes the possible security responses defenders may take in case of security event. The general formulation of the network is presented in Fig. 4.

Fig. 4: LIMID for optimal security management in critical infrastructures.

The proposed LIMID is composed of thirteen chance nodes, describing uncertainties from defender's perspective. Two sequential decision nodes representing the choices available to the defender to overcome a security event are provided, that is, proactive "Security_Countermeasures" and reactive "Security_Response", whose costs are depicted by two utility nodes, respectively "Countermeasures_Cost" and "Intervention_Cost"; a third utility node to describe the magnitude of the damages given the event "Total_Damages", and a multi-attribute utility node "Total_Utility" to report the sum of the expected utilities have been added to the model.

This model is intended as a general framework for reasoning under uncertainty, and more variables may be taken into account according to the critical infrastructure of interest and the preferences of defender. The model takes into account the possibility that various perpetrators may want to carry out attacks against the considered chemical facility for different reasons. For example, the motivations a disgruntled employee is driven by in causing damage to facility assets may not be the same as of a terrorist. Therefore, the upper part of the model is intended to catch the differences among perpetrators, describing probabilistically their objectives, logistics, and the time they may spend planning the attack. The nodes "Perpetrator", "Logistics", "Objectives_of_Perpetrators", and "Planning" constitute the parents of the "Intelligence_Level_Alert" node. This variable reports the level of alert of an intelligence team which may be either site-specific or provided by authorities, clearly depending on the perpetrator and its attributes. Levels of alert are usually present in the field of security in order to quantify experts' judgment about the severity of the threat. For example, in the Netherlands, the National Coordinator for Security and Counterterrorism (NCTV) periodically releases reports and graphical information about the terrorist threat level in the country [28, 29].

The second level of the model comprises the nodes "Target", "Threat" and "Delivery_Means" which are intended to represent attack features. The possible outcomes of these variables have to be chosen according to the specific application of the methodology as a huge number of factors has to be considered. An essential list of possible threats against defined assets located in chemical facilities has been provided by Reniers et al.

[30]. It is worth noting that these nodes are children of the first decision node “Security_Countermeasures”: this dependency is important, because allows to better depict the preferences of perpetrators. This choice has been made because several game-theoretic approaches describing the behaviour of terrorists as rational decision-makers pointed out that perpetrators may shift their attention to softer targets in reaction of security system strengthening [31, 32].

Assuming that perpetrators are informed about the state-of-the-art of site security countermeasures, they may shift their attention to less protected, more visible, or more vulnerable assets. That means this model is able to outline the effect of vulnerabilities on the relative assets attractiveness. The weight of this influence has to be probabilistically estimated, in order to be put into the model as conditional dependencies linking the “Security_Countermeasures” to the three attack-related chance nodes. This estimate can be conducted adopting a framework analogous to the one presented in Section 3. The methodology proposed in [23, 27] can be used to analyse perpetrators’ preferences among different types of scenarios, given the presence of various types of security countermeasures, and to obtain the conditional probabilities of “Target”, “Threat” and “Delivery_Means”. The above-mentioned feature represents an advantage of this methodology over previous sequential procedures such as [4, 5].

A drawback of this approach is the same as of traditional scenario-based approaches. The model is realized considering a fixed and predetermined set of scenarios for perpetrators and attack features. Thus, it is not able to take into account innovative perpetrators who may be able to plan new strategies, to define new non-traditional targets or to develop novel unpredictable technologies [26]. In order to lessen this shortcoming, the network has to be updated both structurally and parametrically over time. That is, new nodes and states (e.g. a new possible targets) should be added as terrorist groups evolve, and probabilities should be updated as new information becomes available.

The second decision node, “Security_Response”, depicts the responses available to defenders in the case of an attack. It is a temporally-ordered child of the three attack-related nodes, the node “Detection” representing the probability that the attack will be promptly identified, and the previous decision node “Security_Countermeasures”. The meaning of the dotted arcs can be described as a time sequence of events, that is, the response can only be realized after the attack was attempted by perpetrators, and identified by the defender. Probabilities describing the dependence of node “Detection” on the others need to be assessed considering different features of the attack, the countermeasures in place, and the level of alert set by the intelligence.

It seems reasonable that in the case of an impending attack, the personnel will be instructed to pay particular attention to detection procedures. The response node directly affects the outcomes of the attack, depicted as the three consequence nodes “Loss_of_Life”, “Damages_to_plant_and_production” and “Damages_to_Reputation”. It is worth noting that a node “Response_Effectiveness” has been included between the decision and its effects in order to account for the possibility of response ineffectiveness. Furthermore, the consequences have been considered as chance nodes. This choice was made to take into account uncertainty about damages and losses given an attack; however, if the defender prefers to use other tools, for example empirical correlations, chance nodes may be replaced by deterministic nodes.

The utility nodes “Countermeasures_Cost”, “Intervention_Cost” and “Total_Damages” describe respectively the cost of the implementation of countermeasures, the cost of response, and the negative outcome to the company given a security event. It may be useful to convert the monetary values into utility values through the application of utility functions. This way, the preferences of the decision makers can better be outlined while taking into account the effect of constraints such as limited allocable resources for security or risk-tolerance [21, 22]. The node “Total_Utility” is a deterministic node showing the sum of the expected utilities. As previously mentioned, it has been provided to ensure the readability of the results, and although is depicted as a diamond, should not to be confused with a utility node.

The probabilistic dependencies have to be determined by the defender before querying the model. The major part of probabilities has to be estimated directly from experts' judgments, while the preferences of perpetrators among different types of scenarios can be evaluated following the approach reported in Section 3. This procedure can be time-demanding, but offers a relatively easy framework to obtain information about the most probable scenarios the defender may face. Thus, the model is from defender's perspective, but seems reasonable that to understand the best reaction to an attack the defender puts himself in the opponent's shoes before starting the calculations, and evaluates the task from opponent's perspective.

After assessing all probabilities, the model has to be run following a timely-ordered scenario-based approach: setting an evidence on the level of alert of the intelligence, a decision among the security countermeasures is chosen based on available or prospective countermeasures. The probabilities of different types of scenarios are calculated, and the proper response can be defined for each of them. Two kinds of analysis can be conducted from defender's point of view. The first one is the task of finding the best defensive strategy, intended as the collection of two policies maximising the expected utility of the defender given an attack scenario. The second one is finding the best response given an attack, for a fixed security countermeasure. For example, the latter is the case when the defender has already implemented one of the security countermeasures in the first decision before querying this methodology, and cannot modify it.

The task of finding the best defensive strategy, given a specific scenario, is an iterative procedure based on the computation of the highest expected utility obtainable from the combination of countermeasures and responses as depicted in the flowchart in Fig.5. Starting from the top (setting at Level of Alert), a security countermeasure has to be chosen, then the queried scenario has to be set. At this point the first iteration starts: exploring expected utilities obtainable from each possible response decision, and querying the node "Total_Utility" (with the previously fixed security countermeasure), the optimal response can be identified. This optimal response is the one leading to the highest value of expected utility to the defender. This step corresponds to the inner-cycle in Fig.5, i.e., Setting Decision among "Security_Responses" → Evaluate Resulting Expected Utility from "Total_Utility" → Highest among Responses? (if NO) → Setting Decision among "Security_Responses". Once the optimal response has been identified, comparison with other alternatives for each top security countermeasure has to be considered to determine the optimal strategy.

This step corresponds to the outer-cycle in Fig.5, i.e., Decision among "Security_Countermeasures" → ... → Highest among Responses? (if YES) → Highest among Countermeasures? (if NO) → Decision among "Security_Countermeasures". If the security countermeasure cannot be chosen (e.g. in case the defender cannot spend resources on new countermeasures) following the inner-cycle in Fig.5 it is possible to compute the optimal response to each scenario, given the constraint of not modifying the countermeasure.

Fig. 5: Flowchart to query the model.

According to the flowchart, four types of output can be obtained querying the model (i.e. represented as ellipses in Fig.5: (i) the probabilities of each scenario, given a set of security countermeasures, (ii) the probabilities of different perpetrators, given the security countermeasure and the attack scenario, (iii) the best strategy to deal with a particular type of attack scenario, and (iv) the best response, given an attack scenario and considering the presence of constraints (i.e., already implemented security countermeasure) of the first decision node. The reported sequence among decisions reflects the chronological order followed by the events: before the perpetrator decides to get into the plant and carry out an attack, a security countermeasure has already been implemented, and the attack would result in outcomes depending on its features and the quality of security response.

4.2) Application of the methodology to a case study

The illustrative case study in Fig. 6 has been adopted [26] to demonstrate the methodology.

Three targets have been chosen, that is, Offices (i.e. Main Building in Fig.6), Loading Dock, and Storage Tanks. We considered three types of delivery means, as the possibilities the perpetrator has to get into the plant premises to carry out an attack: via Ground, via Air and via Water. This is a simplified assumption, because perpetrator may develop technologies not easy to be taken into account, for example airborne or waterborne

improvised explosive devices (i.e. namely ABIED and WBIED). For the sake of simplicity, only two kinds of threats have been considered, “Bombing” and “Sabotage”. To assess preferences of different threats among different detrimental actions, the model has to be run after the estimate of probabilities from experts. An alternative approach considers evaluation of probabilities as discussed in Section 3.

Fig. 6: Notional Chemical Facility case study [26].

Three different perpetrators have been considered: a terrorist, a disgruntled employee, and an activist. Each perpetrator may have different objectives, so the possibility space of the node “Objectives_of_Perpetrators” comprises two possible states “Symbolism” and “Losses”: it seems reasonable that an intentional attack against the facility may be carried out with the intent of either causing damage to the assets (“Losses”) or gaining the attention of media (“Symbolism”). For the node “Logistics”, three states were considered to denote terrorists supported by an organization (“Background”), a small group (“Small_Group”), or an individual (“Individual”). Another feature of perpetrators considered by the model is the time spent planning the attack: this may result in better informed or better equipped perpetrators and is considered in the node “Planning” with its three states “Long_Term”, “Short_Term”, “Improvisation”.

The probabilistic dependencies of perpetrator-related nodes on the node “Perpetrator” has to be assessed by experts. The intelligence node is assigned five possible levels of alert (“Low”, “Guarded”, “Elevated”, “High”, “Severe”), which are conditionally dependent on the perpetrator of interest and its characteristics. The intelligence node is a parent node of the security countermeasures decision node. This means that information about threats and possible attacks has to be provided by intelligence to assess the severity of the security issue at the moment the decision has to be made.

We consider five decisions available to the defender: “No_Additional_Countermeasures”, “Fence”, “Fire_Barriers”, “CCTV”, “Patrol”. It is worth noting that they have different effects on perpetrator’s choice of targets, means, and threats, and also on consequences resulting from an attack (i.e., denoted by arcs connecting “Security_Countermeasures” to the others). For example, the presence of a patrol may shift the preferences of perpetrators, carrying out an attack via water instead of ground. Fire barriers are also

considered as they can lessen the effects of a hypothetical attack against the facility. To take into account the cost of different countermeasures, hypothetical values were assigned and converted into utility values through a utility function [21]:

$$U(y_i) = 1 - \frac{y_i - y_{max}}{y_{max}} \quad (7)$$

where $y_{max} = 0.5$ M\$ is the available budget and y_i is the cost of the i-th countermeasure. Table 1 reports the selected costs and their correspondent utility values for the first decision node.

Table 1: Security Countermeasures with their costs and utilities

Decision	Cost [M\$]	U (Decision, $y_{max}=0.5M\$$)
No_Additional_Countermeasures	0	2
Fence	2	-2
Fire_Barriers	1.5	-1
CCTV	1	0
Patrol	0.6	0.8

We adopted the same strategy to define costs and preferences among possible responses. The outcomes of a decision node have to be mutually exclusive, but common security responses do not generally comply with this criterion. For example, emergency shut down (ESD) and evacuation plan in the case of harmful events are likely to be adopted together. As such, the proposed responses are organized in severity orders. The possible reactions of the defender to an attack, and their respective costs and utilities are reported in Table 2. Also in this case, a spendable budget of 0.5M\$ has been considered.

Table 2: Security Responses and their costs and utilities.

Decision	Cost [M\$]	U (Decision, $y_{max}=0.5M\$$)
Do_Nothing	0	2
ESD (Emergency Shut Down)	1	0
ESD + Evacuation Plan	2	-2
ESD + Evacuation Plan + Alert Authorities	3	-3
ESD + Evacuation Plan + Alert Authorities + Evacuation of Neighbouring Residential Area	3.5	-5

In order to determine the utility values of the “Total_Damage”, the influence of each of the three consequence nodes has been estimated and then combined together to obtain the total loss. The influence of each variable has been determined as follows:

- Damages to the plant and production: the amount of the plant’s structural and economic damages has been discretized in three probabilistic outcomes; this is a simplified assumption, but helps to have a handy estimation of economic losses. We considered “Short_Period_Damages” if the production stops for a short time and with little or no physical damages to assets, “Medium_Period_Damages” if the production stops for a significant amount of time and the plant structures report severe but repairable damages, and “Long_Period_Damages” if the production stops for an amount of time which can heavily affects the business of the plant, and the assets are heavily damaged and not fixable. Illustrative values assigned to each situation are listed in Table 3.

Table 3: Monetary quantification of the outcomes of the variable "Damages_to_plant_and_production".

Damages_to_plant_and_production	Monetary Loss [M\$]
Short_Period_Damages	1
Medium_Period_Damages	10
Long_Period_Damages	100

To estimate values in Table 3, a number of methodologies have been proposed: for example, regarding business interruption, American Petroleum Institute suggests a calculation based on the number of production hours lost [33]; Arunraj et al. proposed to consider also material wastage and material recycling costs [34] while a more recent approach has been proposed by Hashemi et al. based on business interruption insurance [35].

- Loss of Life: the possibility space of this node was discretized in four states according to the number of losses given an attack. 3.5M\$ has been considered as the mean value of statistical life (VSL), and due to the fact that the discretization procedure divides the possibility space into intervals, to each of them has been attached the value corresponding to the upper bound. This choice can arbitrarily vary according to the preferences of the decision maker. For a broader discussion about the meaning of VSL one can refer to Viscusi et al [36]. Outcomes of this node with their monetary quantification are reported in Table 4. The value attached to the interval "More_than_10" corresponds to the monetary value of a long period damage to the plant.

Table 4: Monetary quantification of the outcomes of the variable "Loss_of_Life".

Loss_of_Life outcome	Monetary Loss [M\$]
No_Injuries	0
From_1_to_5_deaths	17.5
From_6_to_10_deaths	35
More_than_10_deaths	100

- Damages_to_Reputation: three states have been considered for this variable, "None", "Low", "High". This node is important because one of the results of an attack may be the loss of reputation of the facility although there is no accepted definition or common agreement in the literature about how to assign a pecuniary value to it. An estimation based on the facility share price volatility has been proposed by Way et al. [37], while Hashemi et al. proposed a scenario-based procedure [35]. In order to keep the model simple, we model reputational losses by applying a multiplicative factor to the monetary losses given by the other two kinds of consequences. Multiplying factors F_{DR} are reported in Table 5.

Table 5: Multiplying factors associated to outcomes of the variable "Damages_to_Reputation".

Damages_to_Reputation	Multiplying Factor F_{DR}
None	1.00
Low	1.25
High	1.50

According to the above-mentioned assumptions and the adopted monetary quantities, total monetary losses $y_{i,TD}$ were computed according to Eq. (8):

$$y_{i,TD} = F_{DR} \cdot ([M\$]_{Loss_of_Life} + [M\$]_{Damages_to_plant_and_production}) \quad (8)$$

Utility values for the “Total_Damage” node have been computed converting each $y_{i,TD}$ through Eq. (7) with a risk tolerance $y_{max} = 1$ M\$. Table 6 partly reports the utility table of the node “Total_Damage”.

Table 6: Part of utility values computed for the node “Total_Damage”.

Loss_of_Life	Damages_to_plant_and_production	Res_Symbolism	Monetary Loss [M\$] $y_{i,TD}$ from Eq.(8)	U (Outcomes, $y_{max}=1M\$$)
No_injuries	Short_Period_Damages	None	1	1
No_injuries	Long_Period_Damages	High	150	-148
From_1_to_5_deaths	Short_Period_Damages	None	18.5	-16.5
From_1_to_5_deaths	Long_Period_Damages	High	176.25	-174.25
From_6_to_10_deaths	Short_Period_Damages	None	36	-34
From_6_to_10_deaths	Long_Period_Damages	High	202.5	-200.5
More_than_10_deaths	Short_Period_Damages	None	101	-99
More_than_10_deaths	Long_Period_Damages	High	300	-298

After the complete definition of the problem, the calculation procedure was performed using GeNIe [16].

The first feature of the model is to depict how perpetrators’ preferences about possible scenarios may vary according to the implementation of the countermeasures. It was assumed that if perpetrators wanted to carry out an attack before the implementation of the security system, they will not renounce after. Thus, results obtained through the next procedure can be seen as probabilities given an imminent attack. Due to the relations between scenario-feature nodes (i.e., “Target” is the parent of both “Threat” and “Delivery_Means”), after making a decision among security countermeasures, probabilities of different targets will be updated. Setting evidence at “Target”, the software computes the probabilities of different delivery means given the target, and finally computes the probabilities of different threats given the two previous features. Results can be organized in form of trees: for example, attack-features probabilities for “No_Additional_Countermeasures” and for “Fence” are depicted in Figs.7 and 8, respectively.

TARGET	DELIVERY	THREAT	
Storage Tanks P=0.434	Via Air P=0.19	Bombing P=0.58	Scenario 1
		Sabotage P=0.42	Scenario 2
	Via Ground P=0.67	Bombing P=0.46	Scenario 3
		Sabotage P=0.54	Scenario 4
	Via Water P=0.14	Bombing P=0.50	Scenario 5
		Sabotage P=0.50	Scenario 6
Loading Dock P=0.233	Via Air P=0.16	Bombing P=0.47	Scenario 7
		Sabotage P=0.53	Scenario 8
	Via Ground P=0.47	Bombing P=0.36	Scenario 9
		Sabotage P=0.64	Scenario 10
	Via Water P=0.37	Bombing P=0.39	Scenario 11
		Sabotage P=0.61	Scenario 12
Offices P=0.333	Via Air P=0.13	Bombing P=0.53	Scenario 13
		Sabotage P=0.47	Scenario 14
	Via Ground P=0.72	Bombing P=0.42	Scenario 15
		Sabotage P=0.58	Scenario 16
	Via Water P=0.15	Bombing P=0.47	Scenario 17
		Sabotage P=0.53	Scenario 18

Fig. 7: Probabilities of attack attributes, given the decision "No_Additional_Countermeasures"

TARGET	DELIVERY	THREAT	
Storage Tanks P=0.233	Via Air P=0.24	Bombing P=0.51	Scenario 1
		Sabotage P=0.49	Scenario 2
	Via Ground P=0.58	Bombing P=0.37	Scenario 3
		Sabotage P=0.63	Scenario 4
	Via Water P=0.18	Bombing P=0.44	Scenario 5
		Sabotage P=0.56	Scenario 6
Loading Dock P=0.334	Via Air P=0.174	Bombing P=0.40	Scenario 7
		Sabotage P=0.60	Scenario 8
	Via Ground P=0.474	Bombing P=0.29	Scenario 9
		Sabotage P=0.71	Scenario 10
	Via Water P=0.352	Bombing P=0.33	Scenario 11
		Sabotage P=0.67	Scenario 12
Offices P=0.433	Via Air P=0.18	Bombing P=0.46	Scenario 13
		Sabotage P=0.54	Scenario 14
	Via Ground P=0.65	Bombing P=0.34	Scenario 15
		Sabotage P=0.66	Scenario 16
	Via Water P=0.17	Bombing P=0.40	Scenario 17
		Sabotage P=0.60	Scenario 18

Fig. 8: Probabilities of attack attributes, given the decision "Fence".

The trees have to be read from left to right. For example, focusing on the uppermost branch of Fig.7, the following probabilities can be calculated:

$$P(\text{Target} = \text{Storage_Tanks} \mid \text{Secur_Count} = \text{No_Add_Count}) = 0.434$$

$$P(\text{Del_means} = \text{Via_Air} \mid \text{Secur_Count} = \text{No_Add_Count}, \text{Target} = \text{Storage_Tanks}) = 0.19$$

$$P(\text{Threat} = \text{Bombing} \mid \text{Secur_Count} = \text{No_Add_Count}, \text{Target} = \text{Storage_Tanks}, \text{Del_means} = \text{Via_Air}) = 0.58$$

Accordingly, the joint probability of the scenario presented in the uppermost branch (i.e., a bombing attack carried out via Air, against the storage tanks area) can be calculated as:

$$P(\text{Bombing, via Air, Storage tanks}) = 0.58 * 0.19 * 0.434 = 0.0478$$

Resulting probabilities obtained for each scenario, from both trees are reported in Fig. 9, in the form of bar chart. Scenarios are labelled with numbers from 1 to 18, starting from the uppermost branch of each tree.

Fig. 9: Attack scenarios' probabilities for "No_Additional_Countermeasures" (in black) and "Fence" (in white).

According to Fig.9, the three most likely scenarios for "No_Additional_Countermeasures" are:

1. $P(\text{Scenario 4}) = P(\text{Sabotage, Via Ground, Storage Tanks}) = 0.157$
2. $P(\text{Scenario 16}) = P(\text{Sabotage, Via Ground, Offices}) = 0.1391$
3. $P(\text{Scenario 3}) = P(\text{Bombing, Via Ground, Storage Tanks}) = 0.1338$

According to Fig. 9, the three most likely scenarios for "Fence" are:

1. $P(\text{Scenario 16}) = P(\text{Sabotage, Via Ground, Offices}) = 0.1858$
2. $P(\text{Scenario 10}) = P(\text{Sabotage, Via Ground, Loading Dock}) = 0.1124$
3. $P(\text{Scenario 15}) = P(\text{Bombing, Via Ground, Offices}) = 0.0957$

It is worth remarking that probabilities of different attributes associated to an attack vary according to the implemented security countermeasure, implying the shift of perpetrator's preferences to other targets, means, or threats. As previously mentioned, attack scenarios allowed by this model do not include the possibility that an attack will not be attempted. According to the present model, an attack will be carried out

despite the countermeasures in place although the attack's consequences can be mitigated via appropriate responses. Thus, the results calculated through the trees in Figs. 7 and 8 reflect the conditional probabilities given an attack. As a result, some scenarios may have even higher probabilities in the presence of a "Fence" than "No_Additional_Countermeasures" due to the fact that the presence of a security countermeasure may shift the attention of perpetrators to softer targets (easier targets) than harder targets.

For example, the probability of *Scenario "16" = (Sabotage, Via Ground, Offices)* in case of having "Fence", compared to "No_Additional_Countermeasures", grows from 0.1391 to 0.1858 because with the implementation of "Fence" the offices may be considered as softer targets than the other targets and thus more attractive in perpetrators' mind [31, 32]. On the contrary, probabilities of attacks against hard targets such as the storage tanks, decrease after the implementation of "Fence". For example, due to the strengthening of the security system, the probability of *Scenario "4" = (Sabotage, Via Ground, Storage Tanks)* decreases from 0.157 to 0.0851.

The second possible outcome derived from this model is the probabilistic outlining of various kinds of perpetrator, among the allowed ones, given an implemented security countermeasure, an attack scenario, and a level of alert of the intelligence. The dependence of perpetrator's features on the resulting detrimental action is clear as different perpetrators may have different objectives, capabilities or logic. The dependence on the intelligence level of alert implies that the intelligence may have assigned various levels of awareness to each perpetrator, so a specific scenario is more likely to be carried out by some perpetrators than the others.

Fig. 10 depicts a section of the model with results obtained for sabotage of the storage tanks, conducted via ground, in presence of existing fences to protect the perimeter of the plant. The scenario was set according to an elevated level of alert provided by the intelligence. As can be seen, if this scenario occurs, the most probable perpetrator would be a disgruntled employee, the most probable motivation would be related to symbolism, and the most probable types of logistic and planning would be individual and short-term, respectively.

Fig. 10: Part of the model depicting probabilities of perpetrators, given a defined scenario. The scenario elements (evidence) are denoted by bold font.

The third feature of the developed model is its capability of ranking strategies to deal with attack scenarios. Theoretically, to compute the rankings of strategies, the combinatorial computation of each possible pairing of decisions among the decision nodes "Security_Countermeasures" and "Security_Response" would be required; however, GeNIe computes directly the expected utility of each strategy, and stores the values inside

the decision nodes. Thanks to this modelling feature, only setting the scenario of interest would suffice. Expected utilities obtained considering a bombing attack via air against the loading dock are presented in Table 7.

Table 7: Expected utilities for each strategy E (Security countermeasure, Security response), given a bombing attack via air against the loading dock.

E (Security countermeasure, Security Response)	Security Countermeasure				
Security Response	No Additional Count	Fence	Fire Barriers	CCTV	Patrol
Do Nothing	-73.100	-77.100	-58.390	-75.100	-74.300
ESD	-66.026	-70.026	-59.836	-68.026	-67.226
ESD + Evacuation Plan	-69.188	-57.227	-47.691	-69.210	-59.088
ESD + Evacuation Plan + Authorities	-65.368	-69.368	-51.408	-67.368	-66.568
ESD + Evacuation Plan + Authorities + Evacuation Residential Area	-61.212	-69.524	-50.619	-67.524	-66.724

According to Table 7, the optimal strategy is the one which maximises the expected utility, i.e., to implement fire barriers and, if the above-mentioned attack takes place, to actuate the emergency shut down and to evacuate the plant. It is worth noting that Table 7 provides also results for the task of response-only optimization, that is, when the modification of the security countermeasures is not possible. This is the case, for example, when the defender has already implemented a CCTV and seeks an optimal response to an attack scenario without implementing new countermeasures.

Values in bold in Table 7 represent the optimal response for each column of fixed initial countermeasure. For example, in case of the same attack scenario, if CCTV is in place (4th column in Table 7), the optimal response would be the fourth security response, i.e., to activate the ESD, to actuate the evacuation of the personnel, and to ask for authorities' intervention. Furthermore, in case the defender has already decided not to implement additional countermeasure (1st column in Table 7), the fifth security response would be optimal in which the evacuation of the neighbouring residential area would be required in addition to the previous ones. According to the assigned utilities, the obtained expected utilities are always negative: this feature is logical, because the defender can only try to minimize the damages in case of an attack with appropriate countermeasures, and proper response, accounting also for the cost of decisions.

4.3) Discussion and future directions

The presented methodology constitutes a simple representation of the issue of cost-effective resources allocation of security measures to critical infrastructures. As previously mentioned, the developed LIMID should be considered as a static representation of the issue, and thus should constantly be updated. As other scenario-based methodologies, the presented model can only account for a predefined set of perpetrators and attack scenarios. However, the model would be able to deal efficiently with innovative perpetrators and unforeseen scenarios if were updated on a regular basis in accordance with the evolution of terrorist groups and availability of new intelligence information.

For a more realistic modelling and prediction, the behaviour of the perpetrators should be taken into account in assessing scenarios' probabilities following the approach based on Luce [24] and Rubinstein [25], as reported in Section 3. However, from one hand, the exhaustive calculation of all possibilities may be very time demanding for a wide variety of attacks' and perpetrators' features, and from the other hand, the results based on the assumption of fully rational perpetrators may be oversimplifying.

An interesting extension of the developed LIMID can be a two-sided model proposed in [23, 27] as depicted in Fig. 11.

Fig. 11: Two-sided LIMID model [23, 27].

This model is intended to provide a continuously updatable framework to represent terrorist's behaviour and preferences and to react properly, following a dynamic and game-analytic approach. The LIMID on the left panel depicts the attack task from perpetrator's perspective (assessed by U.S. Intelligence). It is used to outline different attack opportunities from terrorist's point of view, following the approach presented in Section 3, assuming that they would act to maximize their expected utility [23]. The LIMID on the right panel is from U.S. Defence's perspective and is intended to provide a framework for ranking the best responses, given the information gathered from the left LIMID. Future works may be dedicated to the development of this kind of approach in the context of chemical security.

Another possible advancement, with respect to Fig.11, could be the application of a defence-attack-defence sequence as proposed in [38, 39] via combining LIMID and game theory, assuming rational attackers and defenders.

The defence-attack-defence model provides a framework to outline a sequential model where (i) the defender allocates defensive resources (node D1 in Fig. 12), (ii) making an observation of such defensive measures the attacker makes his move (node A in Fig. 12), trying to achieve the best result, and (iii) the defender can make an additional decision (node D2 in Fig. 12) to recover. This approach is similar to the model developed in the present study, because it is able to present the shift of attacker's preferences, given the defensive resource chosen by the defender.

Fig. 12: The defence-attack-defence model [39].

As can be seen from Fig.12, this representation contains the strong assumption of common knowledge. In other words, both the defender and the attacker share the same information and perspective, and their only uncertainty is the success level of the attack, i.e., the chance node S . It has also been proposed to relax the assumption of common knowledge, and represent the same problem through two LIMIDs, one from attacker's perspective and the other from defenders' [39], similar to the one in Fig. 11.

The above-mentioned two presented developments and the model presented in the present study are all based on the assumption that perpetrators will be fully rational in making decisions, that is, they would make decisions to maximize their expected utility. This assumption, however, may not be realistic [40]. Aside from attempting to relax the assumption of rationality, perpetrators should be classified in different categories according to their attitudes. Caplan proposes a classification of terrorists into three subsets, namely sympathizers, actives and suicidal [41]; each of them has different responses to incentives, different self-interest, and different expectations, and so groups belonging to each subset may rank scenarios according to specific criteria. Thus, it is clear that assuming a common rational behaviour may be misleading. Future works should be dedicated to research how values systems, beyond the simplifying assumption of rationality, can be efficiently accounted for in a LIMID framework.

5) Conclusions

The discipline of critical infrastructures security is relatively young, and its importance is growing due to the increasing significance of threats of various perpetrators. Chemical facilities' managements need to be aided by tools to decide which can be the best approach to such kind of dynamic and complex issue.

In the present paper, a novel methodology for optimal security management of critical infrastructures with a particular emphasis on chemical plants has been outlined. The proposed model constitutes a flexible framework based on limited memory influence diagram to incorporate different variables and information in order to develop an effective strategy against intentional attacks.

The model is intended to support decision makers in the task of finding the best strategy to tackle security events, mitigating catastrophic outcomes. Different countermeasures can be implemented, and different responses can be followed, while the expected utility theory can be used to identify optimal strategies. The model is also able to account for the effect of countermeasures' implementation on shifting the perpetrators' preference from one target to another. This feature is a great achievement since the most conventional methodologies do not account for such a shift due to perpetrators' knowledge about the weaknesses of the security system.

The LIMID can be used to obtain four outputs. It can be queried to obtain (i) information about perpetrators' preferences given the security system, (ii) information about perpetrators given a scenario, (iii) the optimal strategy, and (iv) the optimal response to deal with an attack.

The input data required to fulfil the conditional probabilities of the model are mainly assessed by experts according to their experience, exposing the methodology to degrees of subjectivity.

The developed model is neither intended as a complete work nor as an axiomatic framework: the methodology was presented as a developable structure, which can be modified flexibly according to preferences of the user. Future works may focus on the improvement of the model via game theory.

References

- [1] Baybutt P., Reddy V., 2003, Strategies for protecting process plants against terrorism, sabotage and other criminal acts. *Homeland Defence Journal*, 2,1.
- [2] Bajpai S., Gupta J.P., 2005, Site security for chemical process industries. *Journal of Loss Prevention in the Process Industries*, 18:301-309.
- [3] CCPS (Centre for Chemical Process Safety), 2003, Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers. Wiley, New York, 13:978-0816908776.
- [4] API (American Petroleum Institute), 2003, API RP-70: Security for Offshore Oil and Natural Gas Operations.
- [5] API (American Petroleum Institute), 2012, API RP-780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries.
- [6] Bajpai S., Gupta J.P., 2007, Securing oil and gas infrastructure. *Journal of Petroleum Science and Engineering*, 55: 174-186.
- [7] Bajpai S., Gupta J.P., 2007, Terror proofing chemical process industries. *Process Safety and Environmental Protection*, Tran IChemE, Part B, 85 (B6): 559-565.
- [8] Srivastava A., Gupta J.P., 2010, New methodologies for security risk assessment of oil and gas industry. *Process Safety and Environmental Protection*, 88:407-412.
- [9] Reniers G., Van Lerberghe P., Van Gulijk C., Security Risk Assessment and Protection in the Chemical and Process Industry. *Process Safety Progress*, 2015. 34, 1:72-83.
- [10] 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.
- [11] Khakzad N., Reniers G., van Gelder P., 2017, A multi-criteria decision making approach to security assessment of hazardous facilities, *Journal of Loss Prevention in the Process Industries*.
- [12] Argenti F., Landucci G., Reniers G., 2016, Probabilistic vulnerability assessment of chemical plants subjected to external acts of inference. *Chemical Engineering Transactions*, 48:691-696.
- [13] Van Staalduinen M.A., Khan F., Gadag V., Reniers G., 2017, Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructures. *Reliability Engineering and System Safety*, 157:23-34.
- [14] Pearl J., 1988, Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann, San Francisco, CA.
- [15] Cooper G. F., 1987, Probabilistic Inference Using Belief Networks is NP-Hard, Technical Report, KSL-87-27, Medical Computer Science Group, Stanford University.
- [16] GeNIe Modeler, BayesFusion, LCC, <http://www.bayesfusion.com/>

- [17] Charniak E., 1991, Bayesian Networks without Tears. AAAI, AI Magazine, 12, 4: 50-63.
- [18] Shachter R. D., 1986, Evaluating Influence Diagrams. Operations Research, 34:871-882.
- [19] Cabañas R., Antonucci A., Cano A., Gómez-Olmedo M., Evaluating interval-valued influence diagrams. International Journal of Approximate Reasoning, 2017. 80:393-411.
- [20] Lauritzen S. L., Nilsson D., 2001, Representing and Solving Decision Problems with Limited Information. Management Science 47, 9: 1235-1251.
- [21] Blank L., 1980, Statistical Procedures for Engineering, Management and Science. McGraw Hill, New York.
- [22] Gilboa I., 2009, Theory of Decision under Uncertainty. Cambridge University Press, New York.
- [23] Paté-Cornell E., Guikema S., 2002, Probabilistic Modelling of Terrorist Threats: A systems Analysis Approach to Setting Priorities Among Countermeasures. Military Operations Research, Vol.7, No. 4.
- [24] Luce R.D., 1959, Individual Choice Behavior: A Theoretical Analysis. New York, John Wiley.
- [25] Rubinstein A., 1998, Modeling Bounded Rationality, MIT Press, Cambridge, Mass.
- [26] McGill W. L., Ayyub B. M., Kaminskiy M., 2007, Risk Analysis for Critical Asset Protection. Risk Analysis, vol.27, 5:1265-1281.
- [27] Paté-Cornell E., Garber R., Guikema S., Kucik P., 2008, Games and Risk Analysis, Three Examples of Single and Alternate Moves, in: Bier V. M., Azaiez M. N., 2009, Game Theoretic Risk Analysis of Security Threats, Springer.
- [28] National Coordinator for Security and Counterterrorism, April 2017, Terrorist Threat Assessment for the Netherlands 44. A summarized PDF version of the bulletin can be found at: [https://english.nctv.nl/binaries/Dutch%20Threat%20Assessment%20for%20the%20Netherlands%20\(44\)%20April%202017_tcm32-254514.pdf](https://english.nctv.nl/binaries/Dutch%20Threat%20Assessment%20for%20the%20Netherlands%20(44)%20April%202017_tcm32-254514.pdf)
- [29] National Coordinator for Security and Counterterrorism, April 2017, Terrorist Threat Assessment for the Netherlands (DTN) 44. An infographic can be found at [https://english.nctv.nl/binaries/20170331%20DTN%20\(2\)_tcm32-255188.pdf](https://english.nctv.nl/binaries/20170331%20DTN%20(2)_tcm32-255188.pdf)
- [30] Reniers G., Herdewel D., Wybo J.L., 2013, A Threat Assessment Review Planning (TARP) decision flowchart for complex industrial areas, Journal of Loss Prevention in the Process Industries 26: 1662-1669.
- [31] Sandler T., Lapan H. E., 1988, The calculus of dissent: An analysis of terrorists' choice of targets. Synthese, 76:245-261.
- [32] Bier V.M., Nagaraj A., Abhichandani V., 2005, Protection of simple series and parallel systems with components of different values. Reliability Engineering and System Safety, 87:313-323.
- [33] API (American Petroleum Institute), 2008, API RP-581: Risk-based Inspection Technology.
- [34] Arunraj N.S., Maiti J., 2009, A methodology for overall consequence modelling in chemical industry, Journal of Hazardous Materials, 169: 556-574.
- [35] Hashemi S.J., Ahmed S., Khan F., 2015, Probabilistic Modeling of Business Interruption and Reputational Losses for Process Facilities, AIChE, Process Safety Progress, vol.34, 4: 373- 382.
- [36] Viscusi K. W., Aldy E. J., 2003, The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World, The Journal of Risk and Uncertainty, vol. 27, 1:5-76.
- [37] Way B., Khan F., Veitch B., 2013, Is reputational risk quantifiable?, The International Conference on Marine Safety and Environment (IMSE 2013), Kuala Lumpur, Malaysia.

- [38] Insua Rios I., Rios J., Banks D., 2009, Adversarial Risk Analysis, Journal of the American Statistical Association, vol. 104, 486: 841-854.
- [39] Rios J., Rios Insua D., 2012, Adversarial Risk Analysis for Counterterrorism Modeling, Risk Analysis, vol.32, 5: 894-915.
- [40] Bhashyam S. S., Montibeller G., 2016, In the Opponent's Shoes: Increasing the Behavioral Validity of Attackers' Judgments in Counterterrorism Models, Risk Analysis, vol. 36, 4: 666-680.
- [41] Caplan B., 2006, Terrorism: The relevance of the rational choice model, Public Choice, 128(1): 91-107.