Applying game theory for securing oil and gas pipelines against terrorism

Reference:
Rezazadeh Amirali, Talarico Luca, Reniers Genserik, Cozzani Valerio, Zhang Laobing.- Applying game theory for securing oil and gas pipelines against terrorism
Reliability engineering and system safety - ISSN 0951-8320 - 191(2019), p. 1-19
Full text (Publisher's DOI): https://doi.org/10.1016/J.RESS.2018.04.021
To cite this reference: https://hdl.handle.net/10067/1626250151162165141

Applying game theory for securing oil and gas pipelines against terrorism

Amirali Rezazadeh[a,b], **Luca Talarico**[c], **Genserik Reniers**[b,d,e], **Valerio Cozzani** [a], **Laobing Zhang**[b]

a: LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, via Terracini n.28, 40131 Bologna, Italy

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

c: Faculty of Applied Economics, Research Groups ANT/OR, University of Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium

d: CEDON, KULeuven, Campus Brussels, 1000, Brussels, Belgium

e: Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000, Antwerp, Belgium.

Abstract

Security-related risks of oil and gas pipelines are assessed in this paper using the technique of game theory in combination with a security risk assessment approach. A Socio-political index is defined and embedded in an innovative and comprehensive assessment method, considering the effects of social, economic and political elements on pipeline attractiveness and vulnerability. After having analysed the security threats, security measures, aimed at increasing the security level of a pipeline system, are assessed by using a game-theory model. The pipeline segments which are the most probable to be attacked are determined. In addition, having assessed the possible outcomes of attacks to each segment, the security of different segments of specific pipeline routes can be further improved. Our approach can efficiently allocate limited security resources to decrease the security risk along a pipeline route. It should be noted that although this study focuses on oil and gas pipelines, the proposed methodology could be easily adapted to other pipeline systems.

1. Introduction

Since 9/11, the security domain has attracted the attention of the scientific community and it has canalized the efforts by the private industry as well as by public institutions and organizations to make the world more secure. Before the spread of the terrorist threat on a worldwide scale, the focus in the oil and gas industry was mainly on safety-related efforts to prevent safety-related accidents.

Security-related accidents are however different from safety-related accidents, since the former are intentional acts, while the latter are triggered by random and unintentional human errors and/or technical failures. For this reason, the procedure to evaluate security-related risks includes some distinctive elements, although some aspects of an approach suitable for assessing safety related risks are also shared.

In the security domain, the most critical infrastructures should be ranked as structures with the highest priority to be protected. According to the Department of Homeland Security (2003) and The White House (2000), critical infrastructures represent "…systems and (physical or virtual) assets so vital to a nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety…". Bearing this in mind, chemical and oil & gas industries certainly are exposed to high levels of security risk.

In fact, chemical facilities represent attractive targets for malicious acts, since hazardous substances are generally stored and/or handled in these locations. Consequently, the US Department of Homeland Security (DHS 2007) released in April 2007 a risk-based performance standard for security of chemical facilities located in the United States. According to this standard, the security risk is obtained combining three primary factors: attractiveness, vulnerability and consequences.

Another sector, which faces high security risk, is the transportation industry, especially if hazardous materials are the object of the movements such as in the transportation of oil and gas products via pipeline. In general, the products transported through pipeline are vital for any nations' economy as they represent raw materials for energy production and essential supplies for many industries.

Up to now, terrorist groups have demonstrated the capability to perform attacks in both oil & gas facilities and transportation systems. Many successful attacks on pipeline systems have been reported in recent years (e.g. see (Reniers et al. 2010), and (RAND 2016)). As a result, along with chemical infrastructures, oil and gas pipeline networks should be included in a cluster of infrastructures, which are potentially exposed, to high security threats. In this field, CCPS (2008) published guidelines for chemical transportation safety, security and risk management.

Looking deeper into security threats, intentional acts can be categorized into four categories, based on the purpose of the attack: vandalism, sabotage, terrorism, and cyber-attack. Similarly, according to CCPS (2003), the source of threat can be categorized as foreign government, disgruntled employee or contractor, criminal, violent activist and terrorist (for political, religious and environmental reasons). Moreover, security incidents can originate from insiders, from outsiders and insiders working as colluders with outsiders.

Since terrorist activities have risen in recent years, particularly in Europe targeting chemical facilities (see e.g. two terrorist attacks in France in June and July 2015), and following repetitive terrorist attacks on pipeline systems in different countries as reported by (RAND 2016), in this paper we focus on terrorist threats on oil & gas pipelines originating from outsiders.

In this paper, we develop a practical security risk assessment method to analyse and predict possible terrorist threats. In addition, it is a useful method to allocate limited security resources to protect critical route segments as much as possible.

A method, often recommended for security risk assessment, is game theory. After all, this is one of the reasons why game theory was developed. Game theory originally came from mathematics and economic science but nowadays it has also been widely used in the security domain. In game theory, or in its advanced forms, Adversarial Risk Analysis (ARA), there are two decision makers with mutually opposing interests. Through game theory it is possible to model decision variables for different players (i.e., the strategy sets associated with players that may include which targets to attack, under what conditions, when, and how) and also to include chance or consequence variables. It means that we can see both players, one being a terrorist and the other one a defender, in one model with their possible or preferable options and probable outcomes for each strategy. In this way, assuming that each player aims at maximizing his own payoff, it is feasible to find the optimal solution for both players.

A significant advantage of game theory is related to the fact that vulnerability and consequences are usually functions of the allocation decisions made by the players, and not linked to exogenous numbers or random variables such as for instance in safety-related risk assessments. These aspects significantly influence the capability of a game theoretic model for risk assessment to support much more predictive decision making and to guarantee a more effective resource allocation. For more details about the game theory concept, the reader is referred to (Peters 2015), while for some game-theoretical applications in security we refer e.g. to (Tambe 2012), to (Bier and Azaiez 2009) and (Reniers and Pavlova 2013).

In this study, we will consider social, economic and political conditions, which are typical of a geographical region as determining parameters for a terrorist threat able to worsen or increase the attractiveness and/or the vulnerability of a pipeline segment crossing that specific area. For this purpose, a Socio-political Index is used in our assessment method to consider the security risk in each area. Furthermore, we approximated the payoffs for players in this game in a monetary scale, and all associated costs have been estimated by consulting security experts.

To the best of our knowledge, up to the present, an application of game theory to the security of a pipeline system is new. Wadhawan and Neuman (2016) used a game-theoretical approach to model cyber and physical attack for oil stealing from pipeline system. Also Islam, Nix, and Kantarcioglu (2012) developed a game theory model to enhance monitoring of Wireless Sensor Network to increase security against pipeline oil stealing. Rezazadeh et al. (2017) built a game theoretical model to generate optimal patrolling routes on pipeline system. In this paper, game theory is adopted for the security assessment of a pipeline system with a particular focus on terrorism acts to oil and gas pipelines. The novelty of this work is developing a game theoretic model for pipeline terrorism attacks based on a credible risk assessment.

An innovative security game model for oil & gas pipelines, which we called the **P**ipeline **S**ecurity **G**ame (**PSG**) is introduced in Section 2. Section 3 is devoted to model a pipeline network in a suitable way to be analysed by the proposed PSG. An evaluation of the utility functions as well as possible payoffs for each player are presented in Section 4. This section also discusses and evaluates the concepts of attractiveness, likelihood, consequences and probability of a successful attack. Section 5 explains the methodology of solving the PSG, which has two approaches. In Section 6, an illustrative application of the PSG is described. The results of the illustrative case study are presented and discussed separately for these two approaches in section 7. Section 8 concludes this paper and gives some suggestions for future researches. All the details of the calculations can be found in the appendix.

In order to reduce ambiguity, in the following the defender is considered as a female and the attacker as a male so that in the remainder of the paper, the pronoun "he" will be used for an attacker and "she" for a defender.

2. Pipeline Security Game (PSG)

2.1. Preliminaries of PSG

Before introducing the **P**ipeline **S**ecurity **G**ame (**PSG**) used for risk assessment/management within gas & oil pipeline some of the main assumptions and its main features are described. In general, when building a security game, the first step is to determine whether the game is simultaneous or sequential. Other focus points are represented by the completeness of information for both players (attacker and defender), which are assumed to be rational decision makers.

According to a released Al Qaeda's training manual, at least 80% of information about their enemy (which in our case is the defender of the pipeline) can be obtained by just using openly public resources and without resorting to any illegal means (FAS 2006). Moreover, since we will focus on one type of adversary only, which is the terrorist, also the defender can have a significant amount of information on the characteristics and the capabilities of her adversaries. Consequently, it can be a realistic assumption to consider players to be fully informed in the PSG game.

On the other hand, recent terrorist attacks have shown that these groups choose their target wisely to achieve the highest results. Defenders are usually represented by a security department trying to analyse their actions carefully. Based on these facts, in the PSG, both players are assumed entirely rational.

For these reasons, the Pipeline Security Game (PSG) was developed as a simultaneous-move game with perfect and complete information. The game is a two-players non-zero sum game, and we assume that both players are rational, and the rationality is common knowledge. Other Game Theory models, in which decision-making is under the assumption of human-bound rationality, are not considered. For more details on modelling the rationality of players, readers are referred to the PROTECT project to schedule the patrolling in the port of Boston by the Unites States Coast Guard (Bo An et al. 2012).

It is evident that these assumptions simplify the PSG, but they can be seen as the first step to find out how much the technique of game theory can help in security-related risk assessment/management for a pipeline system.

2.2. Players of PSG

As mentioned before, the PSG is modelled as a two-players non-zero-sum game, with the two players being a defender and an attacker.

The defender is assumed being a security manager who is making decisions on the infrastructure to be protected and on which level and types of security measures to be adopted based on a certain security budget. The attacker is assumed to be any terroristic group or individual planning to attack a pipeline system with different purposes, such as for instance the disruption of critical supply of material/energy for the industry or for urban usage, the release of hazardous substances and explosions that might harm neighbouring populations or the environment (see e.g. (Talarico et al. 2015)). As mentioned in the Introduction, in this paper the focus is mainly on the terrorist security threat and not to sabotage/vandalism acts or cyber-attacks.

3. Modelling a pipeline network for the PSG model

To assess the risk of a terrorist attack on specific pipeline segments, it is necessary to evaluate the vulnerability and the attractiveness of a possible target for an attacker. In this paper, in order to allow the PSG to explicitly identify suitable strategies, aimed at increasing the overall level of security, the whole pipeline network has been divided into small and homogeneous segments. In fact, a pipeline system can be a quite extended transportation network crossing several countries and sometimes passing through remote and/or not easily accessible areas (such as deserts). Therefore, a segmentation of the overall pipeline network is useful to better identify the vulnerability and the attractiveness of each section located in a particular area. Dividing a pipeline into homogeneous segments will allow the use of specific parameters associated with each segment. This approach is well explained in Reniers and Dullaert (2011). In the procedure proposed in this paper, parameters are classified in location-related as well as infrastructure-related parameters as follows:

(a) Location-related parameters: these parameters influence the possibly lethal consequences of a terrorist-related pipeline transport accident.

(b) Infrastructure-related parameters: these parameters affect the possibly lethal consequences in addition to the likelihood of a terrorist related pipeline transport accident.

These parameters might depend on a series of factors as shown in Table 1 (see (Reniers and Dullaert 2011) for more details). The Second factor, which is the "flow rate" of fluid in a pipeline, is added to original procedure.

Table 1: Location-related & Infrastructure related parameters considered to assess the attractiveness of each segment

Location related parameters
1. Population density (expressed in terms of land-use) 1a. Residential area 1b. Industrial area 1c. Agricultural area 1d. Other function
Infrastructure related parameters
2. Flowrate (Maximum release inventory)
3. Depth of pipeline
4. Wall thickness of pipeline
5. Diameter of pipeline (a new segment starts when the nominal diameter changes)
6. Presence of crossings (evaluated considering 50m on both sides of the pipeline) 5a. Roads: the presence of a road in the vicinity of a pipeline increases the likelihood of Roadwork; 5b. Other pipelines (e.g. high-pressure pipelines): the presence of another pipeline increases the likelihood of domino effects; 5c. Railroads: the presence of railroads increases the likelihood of vibrations; 5d. Navigable waterways: the presence of inland waterways increases the likelihood of pipeline fracture (for example due to anchor throwing).
7. Presence of wind turbines (if a pipeline part is present within a distance equal to the length of the turbine mast (+/- 400m) this part of the pipeline is considered a separate segment)

It should be noted that the location of a pipeline might influence both the likelihood of an accident and its consequences. For instance, the presence of human activity near a pipeline increases the likelihood of a pipeline fracture as well as the impact of a possible accident. This is why agricultural cultivation has often been considered as a relevant location-related parameter for segmentation purposes.

4. Strategy set for each player

4.1. Defender

The defender's strategies consist of a set of countermeasures, which can be implemented on a pipeline system to reduce the likelihood of being attacked and/or to mitigate the consequences of an attack.

Sd_n = the n^{th} defender strategy, (which means the n^{th} set of countermeasures)

A countermeasure can be based on a single managerial or physical measure aimed at reducing the likelihood and/or the consequences of an attack. In some cases, a defence strategy might be made by a combination of single countermeasures such as fences and closed-circuit television.

To each countermeasure, two relative numbers are associated: the performance score(ps) which measures its effectiveness, and its cost (c).

In Table 2 several countermeasures with their abbreviations are presented.

Table 2: Set of defensive countermeasures

Goal: Reducing Likelihood Countermeasures	
Group	**Description**
Traditional Countermeasures*	Lighting
	Fences
	Access Control ID
	Integrated electronic access control
	Ground Patrol
	Aerial Patrol
Advanced Countermeasures*	Open-Air Intrusion Detection Sensors
	Not Open-Air Sensor
	Remote Sensing Systems
	Drones Unmanned Aerial Vehicle
Recent Technologies*	Distributed acoustic sensing
	Thermal infrared Sensor
	Other ground sensors
Goal: Reducing Consequences Countermeasures	
Other Countermeasures	Trained Personnel
	Isolation Valve and ESD
	Non-flammable supports
	Procedures and emergency response plans
	Non-flammable valves and gaskets
	PMS or monitoring system

The groups of countermeasures marked with an asterisk in Table 2 are categorized according to a framework proposed by Talarico et al. (2015).

For every countermeasure, in Table 2, security experts should determine a performance score (abbreviated as ps), and based on the characteristics of the associated measure. The value of ps might range from 1 to 100 and indicates the effectiveness of that measure for detecting and preventing any malicious act. In other words, a countermeasure with a ps of 1 is completely ineffective, and a countermeasure with a ps of 100 has the highest effectiveness.

Usually, some countermeasures are combined in a countermeasure set to increase their overall efficiency in a cost-effective way. The performance score associated with these sets is estimated together with security experts and has a range between 1 and 100 with a similar meaning.

The cost of a countermeasure set (being a simple countermeasure or a combination of countermeasures) should be determined as C_d. This indicator C_d represents the expenses that the defender should pay for implementing the particular countermeasure set. As stated before all costs in this paper have been determined after some consultations with risk experts.

In general, all security departments employ a variety of countermeasures to mitigate possible consequences of an attack. The differences between those solutions mainly rely in their effectiveness. As a result, those countermeasures should present different Performance Scores. For instance, two separate companies can both have an emergency response plan as well as safety and security policies in place, nevertheless the completeness of the plans and procedures may be different. In addition, even if both companies employ trained personnel, the type of training and/or the experience of the security staff might significantly vary from firm to firm, therefore resulting in different levels of effectiveness. To show the defender strategies which might be available for every pipeline segment, a table can be drawn in which the rows indicate different defender strategies and the columns represent the countermeasures involved by that specific defensive strategy as well as the associated performance score and cost.

In Table 3, an example of defensive strategies for a specific segment is shown. In this case, three possible options were considered for the defender.

Table 3, Example of strategies available for a pipeline segment

	Defender strategies	Countermeasure	ps	C_d
1	$\boldsymbol{Sd_1}$	Fences + Open-Air Intrusion Detection Sensors	90	€ 2,700,000
2	$\boldsymbol{Sd_2}$	Drones Unmanned Aerial Vehicle	50	€ 600,000
3	$\boldsymbol{Sd_3}$	Aerial Patrol	30	€ 250,000

In Table 3, for each defensive strategy made by a single countermeasure or by a set of countermeasures we have assumed illustrative performance score and total cost.

4.2. Attacker

Strategies for attackers represent the level of efforts that potential adversaries are putting while targeting a specific pipeline segment.

$\boldsymbol{Sa_n}$**= The $\boldsymbol{n^{th}}$ attacker strategy, (which means the $\boldsymbol{n^{th}}$ Attack Effort Level (AEL))**

Five Attacker Effort Levels (AEL) are considered and numbered from 1 to 5. The higher its value, the higher the level of effort (AEL). Based on the AEL level an increasing amount of investment is required to perform the attack. Since in PSG all factors are expressed in monetary scale, each AEL is associated with an amount of money needed to perform a malicious act. Therefore, each AEL is paired with an approximated required budget. Table 4 represents five levels of attack effort with their associated required budgets. As stated in the introduction all cost values are based on the judgment from risk experts.

Table 4, AEL associated to a set of attacker's strategies

Attacker strategies	Effort level (AEL)	Required budget (Euro) (C_A)
$\boldsymbol{Sa_1}$	1	€ 5.000,00
$\boldsymbol{Sa_2}$	2	€ 25.000,00
$\boldsymbol{Sa_3}$	3	€ 100.000,00
$\boldsymbol{Sa_4}$	4	€ 250.000,00
$\boldsymbol{Sa_5}$	5	€ 500.000,00

In the PSG, it is assumed that an attack in a urban area will require more investment due to the higher complexity of the attack, which most likely entails more preparations and efforts to be successful. For this reason, Table 4 has been slightly modified, by raising the "Required budget" for an attack performed in a segment crossing an urban area, when using the PSG on an illustrative case in Section 7.1.

The PSG can be solved by applying two different methods. In the first approach (see Section 5.1), the attacker is using a "local optimization" approach focusing on a particular pipeline segment at a time and selecting the best attack strategy to maximize his payoff resulting from the potential consequences of an attack on that segment.

In the second solution method (see Section 5.2), a "global optimization" approach is adopted looking at the whole pipeline network as an available opportunity to attack. As a result, the attacker will choose one pipeline segment with a specific AEL to attack. In other words, following the "global optimization" approach and assuming a pipeline system with four route sections, the attacker can potentially target any route sections with one of the AELs. This means that the attacker has 20 strategic options, resulting from a wide spectrum of attack combinations potentially targeting 4 route sections with 5 different attack levels. In this solution, the attacker would be interested in the maximization of his payoff by attacking a pipeline segment having the highest consequence with the lowest possible AEL. In other words, a favourable attack strategy presents the lowest investment level (AEL) and triggers the highest possible damages. Considering the overall pipeline network made by K segments as possible targets for the attacker, the total number of attacker's strategies according to the "global optimization" approach is given by the following formula:

$$m = k * |\mathrm{AEL}| \qquad (1)$$

4.3. Likelihood grade

As mentioned before, during the segmentation phase the whole pipeline network is divided into some homogeneous segments based on different vulnerability and attractiveness parameters associated with these segments. In this Section, we present a model to calculate the likelihood grade, named LG for short and indicating the likelihood of a possible terrorist attack according to the vulnerability and the attractiveness of each segment.

For this purpose, we used the TePiTri model which is proposed by Reniers and Dullaert (2011). This model was developed as a screening method for assessing terrorist-related pipeline transport risks and has a similar procedure to the TRANS model derived by Reniers et al. (2010) for safety risk analysis.

Within the route segmentation process, a specific Likelihood Grade is computed for each route segment. This process is carried out in 4 consecutive steps as shown in Figure 1.

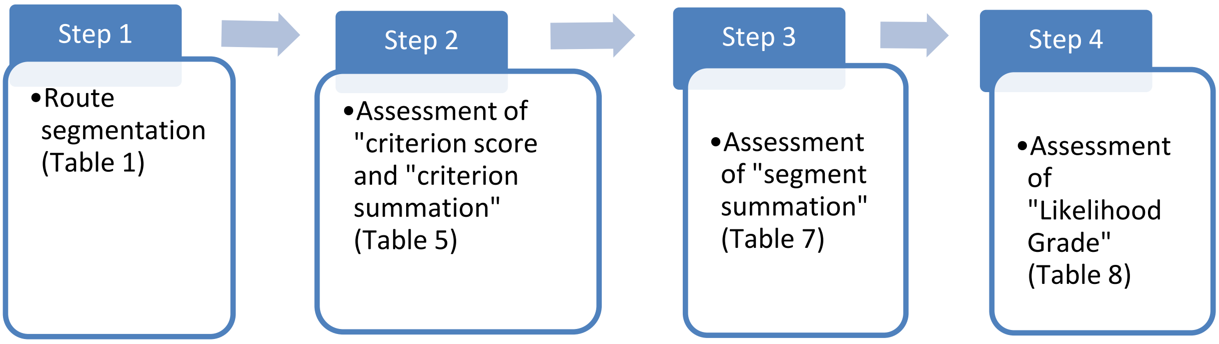

Step 1
•Route segmentation (Table 1)
Step 2
•Assessment of "criterion score and "criterion summation" (Table 5)
Step 3
•Assessment of "segment summation" (Table 7)
Step 4
•Assessment of "Likelihood Grade" (Table 8)

Figure 1, Flow chart for the application of segmentation procedure combined with the TePiTri model

The first step is the so called route segmentation already explained in Section 3. Then, in the second step, all the criteria which determine the vulnerability and attractiveness of pipeline segments are listed (see Table 5). Each criterion has a weighting factor (WF) indicating its relative contribution in the likelihood grade compared to the other parameters. These weighting factors (WF) have been determined by a group of experts which have developped the TePiTri model.

In addition, there are four classes named A, B, C, and D, having a relevance of 5, 3, 2 and 1 respectively. As shown in Table 5, for each criterion the weighting factor is multiplied by the relevance of the associated class and as a result, the contribution of the specific likelihood criterion is obtained as a “criterion score”. Then, all criteria scores are summed up generating the so-called “criteria summation” which indicates the overall contribution of all likelihood criteria in the “Likelihood Grade” measure. Table 6 provides an example to calculate the “criterion summation”.

Table 5, likelihood criteria

				Classes			
	Likelihood criteria		WF	A	B	C	D
Related to vulnerability	1	Visibility of pipeline	4	Above ground totally visible	not completely Above ground in duck or semi buried in soil	Not visible, but because of certain landscape characteristics, one may assume that a pipeline is present	Not visible, no indication of the presence of a pipeline whatsoever
	2	Accessibility of pipeline	3	Accessible with all vehicles	Accessible with agricultural vehicles	Accessible by motorcycle/bicycle	Only accessible by foot
	3	Patroles	1	Never	At least once a month	At least once every 2 weeks	At least once a week
Related to target attractiveness	4	Pipeline is located close to dense populated area	2	> 100 persons present within House Burning Distance (HBD)	10 – 100 persons present within HBD	About 10 persons present within HBD	< 10 persons present within HBD
	5	Pipeline is located close to industrial activities	2	Yes	Yes, but some countermeasures have been taken such that the pipeline is somewhat protected	Yes, but important countermeasures have been taken such that the pi	No
	6	Pipeline is situated close to major traffic route	2	Yes	Yes, but countermeasures have been taken	No	No
	7	Pipeline may be used to initiate a domino effect	2	Yes	Yes, but countermeasures have been taken	No	No
	8	Disruption of local, regional or national gas supply	2	National	Regional	Local	No
	9	Presence of symbolic building or national landmarks within 200m	1	Yes	-	-	No

Table 6, Example of scores for Likelihood criteria (see corresponding numbers in Table 5 for the definition of likelihood criteria)

		Classes				Criterion score
		A	B	C	D	
Criteria	WF	5	3	2	1	
1	4	20				20
2	3				3	3
3	1			2		2
4	2	10				10
5	2				2	2
6	2		6			6
7	2	10				10
8	2				2	2
9	1			2		2
criteria summation						57

In the third step, the hazardous property of the fluid that flows through the pipeline is considered to compute the likelihood grade evaluation. For this reason, we introduce a new parameter which is the so called “segment summation”. To add the contributon of the hazardous property in the calculation of the Likelihood Grade, the original TePiTri method is adjusted based on the NFPA diamond, Standard System for the Identification of the Hazards of Materials for Emergency Response, from NFPA 740 (2001) (National Fire Protection Association), and Dornette and Woodworth (1969). These features, associated to the hazardous properties of the fluids transported via pipeline, have a significant impact on both the vulnerability and attractiveness. In this step, by considering the hazardous properties the "segment summation" is calculated from "criteria summation". Similar to the assessment of the "criteria summation", there are five classes named A, B, C, D and E, having a relevance of 4, 3, 2, 1 and 0 respectively. According to the NFPA Diamond, hazardous materials are grouped into four categories. These properties are ranked from 0 to 4 from the lowest to the highest hazard.

As shown in Table 7, the values attached to the "criteria summation" for each type of hazardous property are tied-up to the corresponding class. Then, for each type of fluid a score is computed by multiplying the criteria summation with the relevance of the classes. Finally, all scores are summed up to obtain the so called "segment summation". From the previous example, the "segment summation" is calculated as below:

Table 7, Calculation "segment summation" according to hazardous properties of fluid based on NFPA 704

Type of HAZARD of fluid	Classes					
	A	B	C	D	E	Score
	4	3	2	1	0	
Flammability	57					4*57
toxicity			57			2*57
Instability/reactivity						0
Special notice						0
					segment summation	**342**

In order to compute the likelihood grade, ten intervals are assumed. A score from 1 to 10 is assigned to each of the intervals indicating a corresponding likelihood grade. Higher scores indicate a higher likelihood grade. The interval, which the "segment summation" falls into, represents the likelihood grade which is denoted by LG. As stated before, the value of LG is associated with a specific pipeline segment.

Table 8, Likelihood grade

Likelihood grade		
Grades	**Interval**	**LG**
LG 1	x≤100	1
LG 2	100<x≤300	2
LG 3	300<x≤400	3
LG 4	400<x≤500	4
LG 5	500<x≤510	5
LG 6	510<x≤650	6
LG 7	650<x≤700	7
LG 8	700<x≤800	8
LG 9	800<x≤1000	9
LG 10	x>1000	10

As also mentioned in the TepiTri model by Reniers and Dullaert (2011), the security management department, based on their policy, expertise, standards, etc. should determine the interval boundaries during a risk assessment phase. In Table 8, some interval boundaries are reported just as an illustrative example, and the same values will be used in Section 5 for a test case.

4.4. Socio-political Index

In the previous section, we have described the way in which the LG is evaluated mainly based on some design parameters associated with the pipeline system. In addition to these factors, there are other parameters, which might have a significant impact on both the vulnerability and the attractiveness of a pipeline segment for a terrorist group. It means that one pipeline segment with a particular design and thus a certain amount of likelihood grade (LG) could be more attractive or vulnerable in one location rather than in another one. Contrary to the LG, the Socio-political index (I) depends on social, political and economic situations, which are specific of a certain region. Political instability, existing terroristic groups, threat history and insufficient legislation are some examples of factors, which determine the Socio-political index I. Argenti et al. (2015) proposed a method to determine the Socio-political index I listing all social, political or economic factors, which can contribute to increase/decrease the attractiveness and vulnerability of process facilities. To achieve a systematic consideration, the authors ordered them in a hierarchical model. Furthermore, they proposed ranges of scores for each of the specification elements. We adapted their hierarchical model for the PSG application as shown in Figure 2.

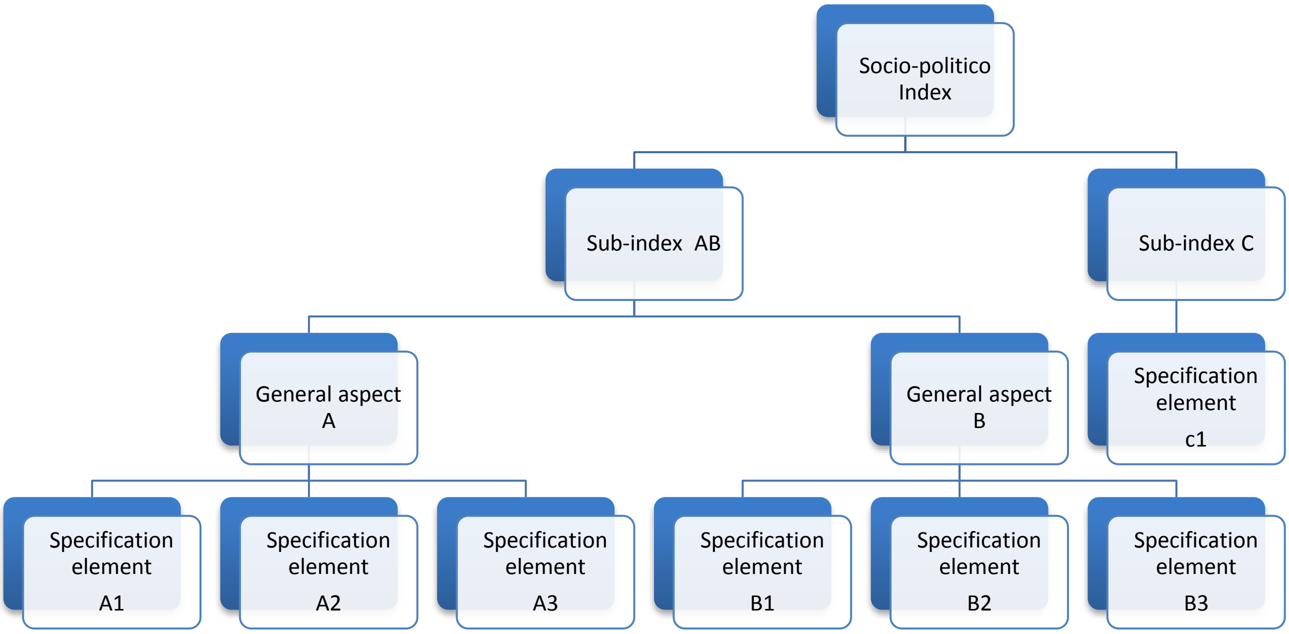


Figure 2, Hierarchical model

According to this method, the socio-political index is a summation of two sub-indexes: the “attractiveness increase” (sub-index C) and the “threat worsening” (sub-index AB).

The method of Argenti et al. (2015) was adapted and applied in the present framework to determine the socio-political index. As, some of the elements in the method have already been considered in the calculation of the likelihood grade like (e.g. the presence of symbolic buildings), were not considered. Some other factors are not applicable in a pipeline security risk assessment (e.g. chemicals that can be used in creating chemical weapons). It should be stated that the range of scores that Argenti et al. (2015) originally proposed applies to our study since this range is coherent with the probability function used in the PSG model (see Section 4.5).

Considering the attractiveness increase, in the PSG model, the sub-index C has one specification element named c1 (see Fig.2). The value of this sub-index C is equal to the value of the specification element c1. Originally, the “attractiveness increase” sub-index in Argenti’s method has two general aspects, but as explained before one of them is irrelevant in the PSG model.

In Table 9, we can find relevant scores linked to the pipeline network ownership situation of a Pipeline Company, and then assume this score equal to the specification element c1. It should be stated that some of the scores in Argenti et al. (2015) like the ownership situation score can vary from country to country due to different social and political situations. In this work, we used the original scores, which have been derived taking into account the social and political situation in Italy. However, in case the PSG model is applied to pipelines located in other countries with a completely different social and political situation, the user of the model should take into account these differences and if required update these scores according to feedback provided by risk experts.

Table 9, “attractiveness increase” sub-index C (Original scores proposed by Argenti, 2015)

Specification element	**Qualitative estimate**	**Description**	**Score**
c1	Presence	Public ownership/ State participation in company management. Company may be seen as a symbol of state authority	0.04
	Absence	Private ownership	0

The sub-index AB includes two general aspects: the first one (denoted by term A) refers to location-specific conditions, while the second one (referred to by using term B) relates to the public perception of the potential target. In Table 10 all general aspects, A and B, and their specification elements are summarized.

Table 10, "threat worsening" sub-index AB (Original scores proposed by Argenti)

General aspect	Specification elements	Qualitative level	Description	Score
A	A_1	Low	Threat history provides no records of attacks to similar facilities. The presence of terrorist cells or activist groups in the area can be excluded/has never been documented	0
		Medium	Threat history provides no records of attacks to similar facilities. Suspect of terrorist cells' or activist groups' presence in the area exists	0.05
		High	Threat history evidences attacks to similar facilities. The activity of terrorist cells or activist groups in the area is confirmed	0.1
	A_2	Low	Low A context of political stability and democracy exists. Governing authorities are legitimated and supported by populace	0
		Medium	Few opposition groups willing to mine government authority exist and may be blamed for violent actions. Existence of political factions	0.05
		High	Political instability and internal conflicts exist. Social order control and maintenance is periodically disrupted	0.1
	A_3	Low	Low Strict legislation concerning the transport, selling and detention of weapons of any nature. Effective and diffuse implementation of controls by police forces	0
		Medium	Legislation concerning the transport, selling and detention of weapons is present but control is not a priority.	0.05
		High	The transport, selling and detention of weapons is poorly ruled and uncontrolled. Third-party interests in favouring the weapons market	0.1
B	B_1	Low	Company reputation and image are extremely positive. Local community judge company activities beneficial	-0.05
		Medium	Local community accepts company activities. Few aversion motives of minor importance	0
		High	Company reputation and image are extremely negative. Existence of organized aversion groups	0.05
	B_2	Low	High level of engagement of local stakeholders. Transparency and continuous information sharing to enhance community awareness of company activities	-0.05
		Medium	Medium level of engagement of local stakeholders. Local community accepts company activities. Few aversion motives of minor importance	0
		High	No engagement of local stakeholders. Creation of a climate of suspicion and mistrust	0.05
	B_3	Low	No interactions with cultural/historical, archaeological, religious heritage. Absence of activists groups on the area/ No evidence of aversion by activist groups	-0.05
		Medium	No significant negative interactions with cultural/historical, archaeological, religious heritage. Sporadic demonstrations of aversion by local activist groups	0
		High	Negative interactions with cultural/historical, archaeological, religious heritage. Frequent demonstrations of aversion by activist groups attracting regional/national media attention	0.05

The following formulas are used to calculate the sub-index AB starting from the values of the general aspects A and B. The sub-index AB is simply computed by adding the values of A and B.

$$A = A_1 + A_2 + A_3 \qquad (2)$$

$$B = B_1 + B_2 + B_3 \qquad (3)$$

$$AB = A * (1 + B) \qquad (4)$$

Finally, the socio-political index I is calculated using the following equation:

$$I = 1 + 2.5 * (C + AB) \qquad (5)$$

This index is assumed to be a value between 1 and 2.

4.5. Probability of a successful attack

Based on the Contest Success function described in Skaperdas (1994) and on its extended form known as “Extended Contest Success” function in Clark and Riis (1998), the probability of a successful attack $p(\boldsymbol{Sd}, \boldsymbol{Sa})$ is computed as follows:

$$p(Sd, Sa) = \frac{I * LG * AEL}{I * LG * AEL \ + \ 4 * ps} \tag{6}$$

Where,
I: Socio-politico index
AEL: Attacker Effort level
ps: Performance score
LG: Likelihood grade.

It should be noted that all values in Eq. (6) are dimensionless. In fact, the AEL can range from 1 to 5, while the LG from 1 to 10. Therefore, the value of $LG * AEL$ can assume values from 1 to 50. The performance score (ps) can be equal to 1-100. The socio-political index I varies between 1 and 2.

In theory, ordinal numbers should not be multiplied, nevertheless to determine the payoff function according to contest success function we had to adopt the rank ordering parameters. Moreover, in this work measurements are intended to be relative with the only aim to compare different situations or locations with each other. In addition, the authors implemented a sensitivity analysis on the model. Afterwards the range of the parameters, weights and the equations have been fine-tuned. Although the validity of the security risk assessment is difficult and sometimes needs a large amount of confidential information, the results of the sensitivity analysis were discussed with experts in this domain and the main conclusions are presented. It should be stated that, this approach was taken before in other works like the MISTRAL game developed by Talarico et al. (2015).

4.6. Consequences

In order to evaluate the consequences (Co) of an attack assuming a specific strategy scenario for both the attacker (Sa) and the defender (Sd), three factors are assumed. The first one is the asset value, the second one is the monetary value associated with human losses or injures, and the last element to be assessed represents the cost associated to the environmental damages.

The value of Co is measured in monetary terms (e.g. in euro) as follows:

$$Co \ = \ S + \alpha * H \ + \ \beta * E \tag{7}$$

Where:
S: Asset value
H: Number of people affected
α: Coefficient to quantify the cost associated to human losses or injuries in monetary terms
E: Area that is affected
β: Coefficient to convert the impact of the accident on the environment in monetary terms

In general, to figure out the consequences of a terrorist attack, the effect distance for a certain accident scenario should be determined first. Because we are considering terrorist acts with major impacts, it is recommendable to assume the worst-case scenario. To do so we can use consequence modelling tools or software like PHAST, SAFETI, ALOHA or other simulators to estimate the affected areas and find useful information to approximate the possible damages on assets, on nearby population and on the environment.

The reader is referred to Reniers *et al.* (2006) for software employed as decision support tools to investigate major hazards in the chemical industry and to OGP (2010) for a more general consequence modelling tool.After modelling the accident scenario by using one of the aforementioned consequence modelling software, the next step is to assess the impact of a terrorist attack by using publicly available data and experimental formulas from the internationally well-known “Green Book” (TNO 1992) or VROM (The Netherlands Ministry of Housing 2005).

To compute the consequences of a terrorist act on assets S, two terms are to be assessed. The first one is represented by direct financial losses, while the second term consist of indirect costs associated to a terrorist attack. Direct losses include damages to the infrastructure, equipment and installations either inside the pipeline system or in the facilities located nearby the pipeline such as roads, pump stations, valves, etc. To better determine the direct financial losses the above mentioned software also provides the effect area in addition to the pressure increase and the heat radiation contours. The "Green Book" (TNO 1992) help us assessing damages caused by heat radiation and the consequences of explosion effects on structures respectively. Therefore, by assuming the worst-case scenario the possible loss associated to assets can be approximated. Indirect losses involve also psychological effects on society or in nations' economies such as losses in financial markets and reduction in foreign investments. To find out more details about the way in which financial losses are computed readers are referred to Enders and Olson (2012), and Sandler and Enders (2008).

As number of fatalities increase the public reaction increase consequently its associated costs increase as a non-linear function according to CCPS (2009), nonetheless as a simple example of considering the fatality costs in our PSG, we assume a linear relation in Eq.7. For implementing PSG for real cases, any PSG user can update this equation based on their assumptions. Therefore, for simplicity, in order to compute the monetary values associated to human losses or injuries, (the second term in Eq.7), a coefficient α and a parameter H are assumed. The coefficient α represents for any individual, involved in the accident, the societal value of a life i.e. how much money the society should pay for medical costs, insurance claims, and any other recovery expenses. It is clear that this value might be different from country to country or even from region to region within a country. Therefore, when using the PSG one should estimate the value of α in the region where the pipeline segment involved in the attack, lies. The parameter H indicates the number of injuries or fatalities. As stated before, the consequence modelling tools provide us the affected area. For the total amount of population potentially at risk, generic data and formula from the "Green Book" (TNO 1992), can be used for assessing the population figures (e.g. in an urban region 120 pers/ha and in an industrial area 40 pers/ha).

Finally, the monetary value associated to environmental damages, (third term in Eq. 7), requires a coefficient β and a parameter E. The coefficient β represents the amount of money that would be needed to recover any environmental damage within a unit area. It is clear that the value of β is based on regional or governmental regulations outlining the required investments to recover any environmental damages after unexpected accidents or incidents. This coefficient might vary depending on the type of pollution and/or on the type of polluted area (e.g. jungle, desert, river and/or national landmark). The parameter E specifies the polluted area and it can be determined via a consequence model.

4.7. Utility functions in the PSG

The payoff associated to the players of the PSG game is measured by using a monetary scale.

The Payoff function for the attacker is:

$$\boldsymbol{U_a}\ (\boldsymbol{S_d}, \boldsymbol{S_a}) = \mathrm{Co}^*\ \mathrm{p}(\boldsymbol{S_d}, \boldsymbol{S_a})\ \text{-}\ C_A \qquad (8)$$

Whereas the payoff function for the defender is:

$$\boldsymbol{U_d}\ (\boldsymbol{S_d}, \boldsymbol{S_a}) = \text{-}\ \mathrm{Co}^*\ \mathrm{p}(\boldsymbol{S_d}, \boldsymbol{S_a})\ \ \text{-}\ C_d \qquad (9)$$

In these formulas, Co is the total cost associated to the consequences of the attack, as described in the previous section, while the probability of a successful attack is $\mathrm{p}(S_d, S_a)$, C_A and C_d represent the expenses for that attack sustained by the attacker and by the defender respectively.

In short, the steps needed by the PSG can be presented in a schematic form as in Figure 3.

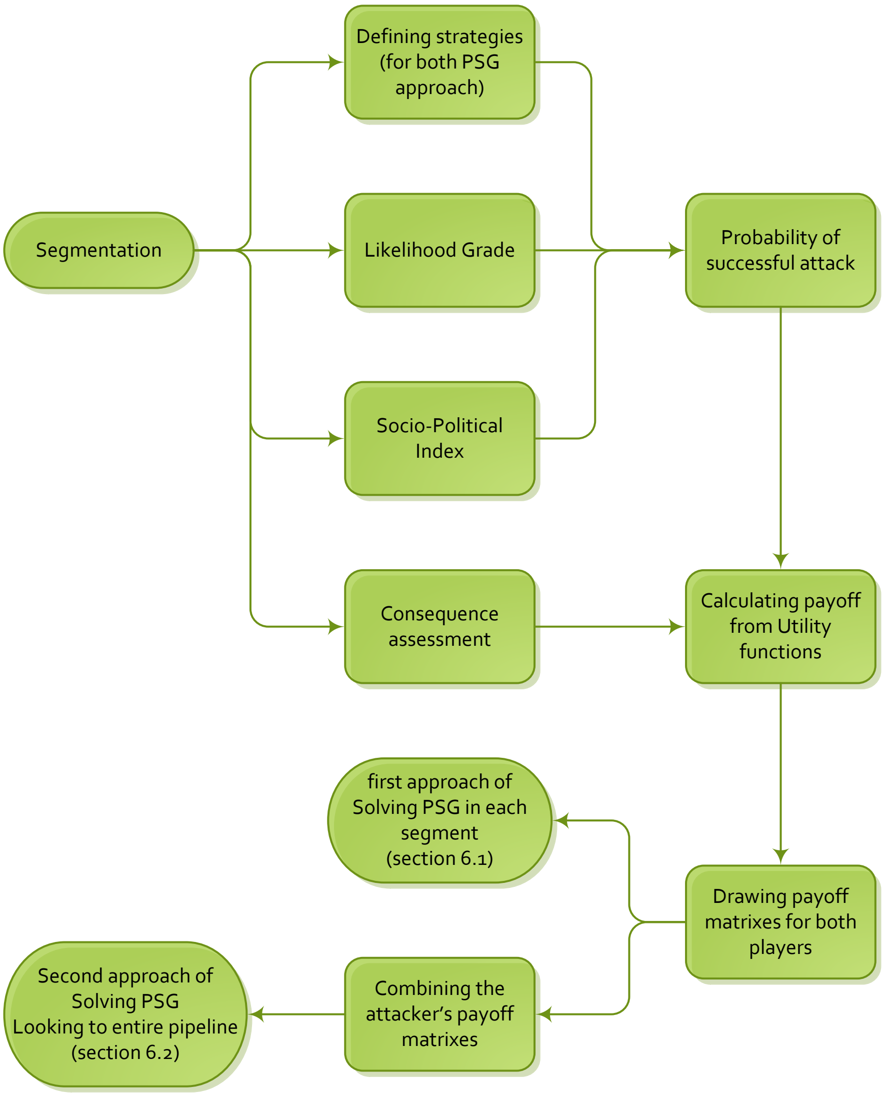

Defining strategies (for both PSG approach)
Segmentation
Likelihood Grade
Socio-Political Index
Consequence assessment
Probability of successful attack
Calculating payoff from Utility functions
first approach of Solving PSG in each segment (section 6.1)
Drawing payoff matrixes for both players
Second approach of Solving PSG Looking to entire pipeline (section 6.2)
Combining the attacker's payoff matrixes

Figure 3, PSG Procedure

5. Approaches to solve PPG

5.1. Local optimization approach

This approach helps security experts to find out the expected outcome for each of their strategies and enables the assessment of the available choices both the attacker and the defender have. In this way, they can compare different available countermeasure sets with each other. In addition, a defender can estimate the minimum and maximum expected losses under different scenarios of terrorist attacks. This model can also help to predict which strategy a fully rational attacker will choose in case of complete information. In the first step to solve the PSG game, the payoff matrixes are calculated for all segments. The payoff matrixes show the possible outcomes or payoffs for the attacker and the defender associated with different strategies that may be applied on each segment.

In each segment, each player has his/her own payoff matrix. A payoff matrix is an $m \times n$ matrix of real numbers, where m is the number of rows representing defender's strategies and n is the number of columns representing attacker's strategies. Such games with two different payoff matrixes, one for each player, are called "bimatrix games".

The Nash equilibrium can be determined for each route segment. The Nash equilibrium is a pair of strategies like p (strategy of first player) and q (strategy of second player) in a bimatrix game *(A,B),* if p is the best response of first player to q**,** while q is the best response of second player to p. A Nash equilibrium **i**s called pure if both p and q are pure strategies (see (Nash 1950) for more details).

The strategy of the defender is a probability distribution over the rows of her payoff matrix. Similarly, a strategy of the attacker is a probability distribution over the columns of his payoff matrix. A strategy p of the defender is called pure if there is a row *i* with $p_i = 1$, otherwise her strategy is called a mixed strategy. Similarly, a strategy q of the attacker is called pure if there is a column j with $q_j = 1$, otherwise his strategy is called a mixed strategy.

In a Nash equilibrium, none of the players tends to change his/her choice because it is the best result for both of them, and if one of them wants to increase his/her payoff, this will not happen unless the payoff of the other player decreases.

There are two possible solutions of this approach. The first one is a pure strategy and the other one is a mixed strategy. Therefore, we will explore the possible Nash equilibrium given a specific payoff matrix and find whether our game in each segment has a pure or a mixed solution.

For this purpose, we determined two stochastic vectors, which represent the probability distribution of pure strategies for the two players. These vectors show the optimal probability distribution that each player can achieve in response to another player and by which they can receive the highest payoff from their choice. If this probability distribution shows that a player will choose one of the available strategies with probability 100%, it means the solution is a pure strategy, and we will have a pure Nash equilibrium. Otherwise, the solution or the Nash equilibrium is a mixed strategy.

The pure equilibrium means finding the best answer, and the mixed equilibrium says that more than one strategy set is favorable. The defender can change and adjust their strategies to find a pure strategy equilibrium. It means that if we find a mixed equilibrium, we can change the configuration of each strategy and again run the game. As explained in the Paper, each strategy is a set of security countermeasures; therefore, in the case we find a mixed equilibrium, we may find more than one set of countermeasure favourable to implement on the pipeline system. Nonetheless, to reach to the best solution, we can change these sets of countermeasures and again compare them with each other. It should be stated that the cost of each type of security countermeasures play a crucial role in solving the game. Therefore, in changing the configuration of countermeasure sets, we can change the type and/or investment on each type within a set. For example, assume that the strategy one is Aerial patrol with a remote sensing system, and the second strategy is ground paroling with Distributed acoustic sensing. In this example, if we reach to a mixed equilibrium, we can combine somehow these two strategies and again solve the game. In another word, one of the strategies can be remote sensing system, distributed acoustic sensing and ground paroling, and the other strategy may be remote sensing system, distributed acoustic sensing and aerial patrol. Also, the amount of patrolling is the other important factor. Thus, it is possible to change the investment on Aerial or ground patrolling and compare them.

This Nash equilibrium is found through the Lemke-Howson algorithm, (Amin and Saberi 1964) and (Pritchard 2011). The algorithm is simulated in MATLAB, and two optimal stochastic vectors are obtained for each segment matrix.

5.2. Global optimization approach

In this approach, the PSG is solved treating the whole pipeline network in its entirety by assessing the terrorist threats from an attacker point of view. In other words, if all the pipeline segments are available for the attacker, and he plans to attack this pipeline, it would be interesting to find, which segment and with which AEL the attacker will most likely attack. The attacker copes with the whole pipeline at once, and he can decide to attack a single pipeline segment with a specific value of AEL to obtain the highest results.

In this approach, the strategy of the attacker is to choose one of the pipeline's segments with a particular AEL to attack; and the strategy of the defender is the displacement of his sets of available countermeasures.

6. Illustrative example

In this section, we represent a pipeline route as an example to be assessed by the PSG model. The pipeline network considered in the proposed example is a regional transportation pipeline transporting sweet methane (H2S concentration within the standard limit for urban usage) from a refinery to a metering station nearby a city and an industrial zone.

It is assumed that this regional pipeline belongs to a company with public ownership and that different states participate in its management (C=0.04). In that region, there is a threat history to similar facilities (A1=0.1) but the government is democratic and its authority is supported by population (A2=0). In addition, legislation concerning transportation and detecting weapons is present, but the control is not a priority (A3=0.05). The activities of the Pipeline Company are accepted by local communities (B1=0), but the engagement of local stakeholders lies in a medium level (B2=0). The activities of that company have no significant negative interactions with cultural or historical heritage; nonetheless, sporadic aversion by local activist groups is reported (B3=0.025). As a result, the socio-political index is evaluated to be equal to 1.35.

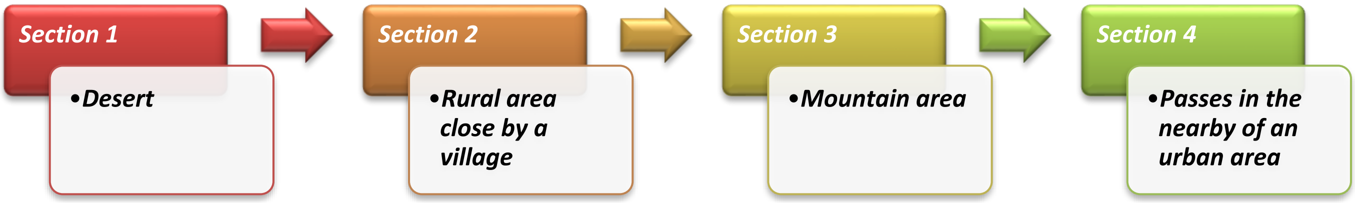

Section 1
•Desert
Section 2
•Rural area close by a village
Section 3
•Mountain area
Section 4
•Passes in the nearby of an urban area

Figure 4, Division of the pipeline network in four sections located in different areas

The overall pipeline network is divided into four sections as also described in Figure 4.:

- The first segment of the pipeline crosses a desert. The pipeline segment is above the ground, and it is accessible by off-road or agricultural vehicles. This segment is located in a remote area far away from any urban or industrial areas. Patrolling is done at least once a month.

- The second segment lies in a rural area close by a village (located at a certain distance). The population present in this area is limited to ten people at maximum. The pipeline is semi-buried under ground, and it is accessible by off-road and/or agricultural vehicles. Furthermore, there is not any symbolic building, a national landmark, nor major traffic route or industrial activity. Nonetheless, there is a high probability of domino effects. Natural factors such as the wind can amplify the impact of a possible incident for example by spreading its consequences to a wider area. Patrolling is done at least once every two weeks.

- The third segment of the pipeline is located above the ground and passes through a mountain area. Therefore, its accessibility is limited only to motorcycles or bikes. Due to the peculiarity of that geographical zone, there is no population living in that area and/or building. However, a national landmark is located in the nearby, so it is assumed that four climbers or mountaineers can stray near that pipeline route. Patrolling is performed at least once a month.

- The fourth segment is buried under ground and passes in the nearby of an urban area. It is predicted that, in case of security incident by terrorist attack about 21 people could be potentially affected. The pipeline is easily accessible by using all kinds of vehicles. In addition, the pipeline segment is close to industrial activities and it is located in the nearby of major traffic routes. Despite the pipeline is designed to cross the city by a certain safety distance, as time passes, the city might expand incorporating the areas crossed by the pipeline. Consequently, those pipelines that were designed to pass the city by a certain distance in past can be become closer to the city today and/or in the near future. Patrolling is performed at least once a week. As discussed in Section 4.2, the cost of a terrorist attack is assumed to be higher in a urban area.

As explained in Section 4.3 the values of LG are determined for all pipeline segments. Then, the probabilities of a successful attack are calculated (see Section 4.5). Three possible defender's strategies are assumed for each route segment. In addition, the consequences of terrorist attacks are determined for each segment based on the assumptions described before. The possible scenario for a terrorist attack is assumed to be an explosion of the pipeline. In addition, in all segments the H, which is the unit base for calculating the human related consequences is assumed equal to € 1.000.000.

Since the pipeline route in this example belongs to one single company, the "reducing consequence" countermeasures, including policies, standards, and employees, are the same along the pipeline except for the "Isolation Valve and ESD". Since the fourth segment is more critical, it presents a higher number of isolation valves located at closer intervals.

7. Results and discussion

The detailed calculations are presented in the Appendix; and in this section, we are going to discuss the final results of the illustrative case study, which are obtained using two different solution approaches: local and global optimization. These two approaches are explained separately in the following subsections.

The payoff for the defender, which is expressed on a monetary scale, is made of all negative values. The Defender's payoff is always assumed negative in the PSG game because the Defender invests in security countermeasures and she should also pay for the consequences of a terrorist attack. Therefore, she will be the player who is paying in all situations. The preferable condition for the Defender is spending as little as possible to operate the pipeline system safely and securely.

7.1. Illustrative case: local optimization approach

In this section, the results obtained by analysing the illustrative case using the approach described in section 5 are reported.

- Route Segment one (desert):

In this Route segment, the defender has three countermeasure sets as available options, which are Aerial Patrol, Aerial Patrol with Distributed acoustic sensing, and Drones with Thermal Infrared Sensor.

Furthermore, the consequence of the terroristic attack on the asset is assumed equal to € 3.000.000. The cost of environmental damages is assumed as € 750 and the whole affected area is 300 m^2.

The Defender's and the attacker's payoff are presented in a bimatrix as Table 11, in which each cell shows the outcome of the game for the Defender and the attacker respectively.

Table 11, Defender's and Attacker's Payoff Bimatrix

Section 1		Attacker				
		1	2	3	4	5
Defender	1	-€ 785.415, € 272.415	-€ 1.028.998, € 495.998	-€ 1.244.584, € 636.584	-€ 1.436.736, € 678.736	-€ 1.609.079, € 601.079
	2	-€ 913.919, € 150.919	-€ 1.058.858, € 275.858	**-€ 1.193.938,** **€ 335.938**	-€ 1.320.130, € 312.130	-€ 1.438.285, € 180.285
	3	-€ 1.344.057, € 131.057	-€ 1.471.715, € 238.715	-€ 1.591.729, € 283.729	-€ 1.704.766, € 246.766	-€ 1.811.416, € 103.416

Figure 5a and 5b present the attacker's payoff comparing his strategies versus each defender strategy, as well as the defender's payoff in comparison to each attacker strategy.

In the case of rational players, the attacker will choose strategy three from his five possible strategies (Sa_3) and the defender will prefer to play her second strategy (Sd_2). In other words, pure strategy Sd_2 for defender, (in this case selecting Aerial Patrolling with installing Distributed acoustic sensor) and pure strategy Sa_3 for attacker, (i.e. her third Attack Effort Level), have the best payoffs for both players and thus it represents the Nash equilibrium in route segment one. The Nash equilibrium in this case is equal to (-€1.193.938; €335.938), where the first and second numbers represent the payoffs for defender and attacker respectively. Probability distributions demonstrate that the game has a pure strategy solution and as a result has a pure Nash equilibrium.

As stated before if the attacker has larger budgets and can afford all the attack strategies, the most probable AEL is the level three (Sa_3). This means that, from the attacker point of view it is not worth investing in Sa_4 or Sa_5 (strategies with higher costs than Sa$_3$), because he can achieve the highest payoff with a smaller amount of investment. On the other hand, looking at the Nash equilibrium, it is better for the defender to implement the second countermeasure set on that pipeline segment instead of Sd_3 (the most expensive countermeasure set with the highest ps) and Sd_1 (the cheapest countermeasure set with the lowest ps).

- Route Segment two (rural area with a village):

For route segment two, the defender again has three countermeasure sets on hand, which are Ground Patrol with Not Open-Air Sensor, Ground Patrol with Remote Sensing Systems, and Fences with Open-Air Intrusion Detection Sensors.

Moreover, the consequences of the terroristic attack on the asset is assumed € 3.500.000. Also, the unit base for cost estimation of environmental damages is assumed equal to € 750 and the overall affected area is 400 m^2.

As mentioned before, the payoffs for the defender are always negative. The following bimatrix (Table 12) shows the defender’s and the attacker’s payoff respectively, in the case of different values of AEL and various defensive strategies. In this segment as the attacker invests more on his AEL, he will gain more. Hence, it is preferable for the attacker to choose the highest AEL, which also implies the most expensive preparation costs.

Table 12, Defender’s and Attacker’s Payoff Bimatrix

Section 2		Attacker				
		1	2	3	4	5
Defender	1	€ -2.609.338, € 796.338	€ -3.322.719, € 1.489.719	€ -3.961.872, € 2.053.872	€ -4.537.809, € 2.479.809	€ -5.059.466, € 2.751.466
	2	€ -3.059.257, € 696.257	€ -3.692.690, € 1.309.690	€ -4.267.686, € 1.809.686	€ -4.791.975, € 2.183.975	€ -5.271.980, € 2.413.980
	3	€ -3.218.124, € 505.124	€ -3.691.879, € 958.879	€ -4.133.020, € 1.325.020	€ -4.544.802, € 1.586.802	€ -4.930.063, € 1.722.063

Figure 6a and 6b show the trends of attackers and defenders payoffs respectively. In case of rational players, the attacker will choose strategy 5 ($\boldsymbol{Sa_5}$) from his five possible strategies and the defender will prefer to play her third strategy ($\boldsymbol{Sd_3}$). In other words, pure strategy three (i.e. Fences with Open-Air Intrusion Detection Sensors), for the defender and the highest AEL for the attacker ($\boldsymbol{Sd_3}, \boldsymbol{Sa_5}$) result in the best payoff for both players, being (-€ 4.930.063; € 1.722.063) the Nash equilibrium for this route segment. Probability distributions demonstrate that the game has a pure strategy solution and as a result has a pure Nash equilibrium. In conclusion, in this segment the attacker will choose the highest effort level ($\boldsymbol{Sa_5}$). In case the defender aims at maximizing the protection of the pipeline, increasing her payoff, and decreasing the payoff of her opponent as much as possible, it would be better to install Fences with Open-Air Intrusion Detection Sensors, which represents the most expensive defensive option.

- Route Segment three (mountain area):

In route segment three, there are three available countermeasure sets for the defender, which are Aerial Patrol with Thermal Infrared Sensor, Aerial Patrol with Not Open-Air Sensor, and Drones with Remote Sensing Systems.

The consequence of the terroristic attack on the asset is assumed equal to € 3.200.000.The area at risk measures 500 m^2 for which the cost of environmental damages is assumed equal to € 750 .

Similarly, Table 13 is the payoff bimatrix that shows the outcomes for the defender and the attacker respectively:

Table 13, Defender’s and Attacker’s Payoff Bimatrix

Section 3		Attacker				
		1	2	3	4	5
Defender	1	€ -2.003.258, € 340.258	€ -2.318.416, € 635.416	€ -2.607.244, € 849.244	€ -2.872.911, € 964.911	€ -3.118.095, € 960.095
	2	€ -2.321.638, € 308.638	€ -2.610.336, € 577.336	€ -2.876.956, € 768.956	€ -3.123.937, € 865.937	€ -3.353.372, € 845.372
	3	€ -3.454.037, € 241.037	€ -3.684.595, € 451.595	€ -3.901.089, € 593.089	€ -4.104.768, € 646.768	€ -4.296.737, € 588.737

Figure 7a and 7b show the attacker's payoff versus each defender strategy and the defender's payoff for each attacker.

In case of rational players, the attacker will choose strategy four from his five possible strategies ($\boldsymbol{Sa_4}$) and the defender will prefer to play her first strategy ($\boldsymbol{Sd_1}$). In other words, pure strategy one for the defender and pure strategy four for the attacker ($\boldsymbol{Sd_1}, \boldsymbol{Sa_4}$) present the best payoff for both players, and it is a Nash equilibrium for this segment with payoffs (- € 2.872.911; € 964.911) for defender and attacker respectively. Probability distributions demonstrate that the game has a pure strategy solution and as a result has a pure Nash equilibrium.

To conclude, similar to segment one, the attacker is expected not to choose strategy $\boldsymbol{Sa_5}$ having the highest efforts/investment level, since with lower AEL he can get better results. On the other side, for the defender, it is better to choose the cheapest option with the lowest ps as it is not worth investing in a more costly defence strategy. Despite more expensive defensive strategies might trigger higher results, in comparison to the Aerial Patrol with Thermal Infrared Sensor, the advantages are not as high as the incremental required investments. In other words investing much more money in defence will not necessarily bring enhanced performances.

- Route Segment four (urban area):

In this segment, the defender has three available countermeasure sets, which are Aerial and Ground Patrol with Other ground sensors, Aerial and Ground Patrol with Remote and other ground Sensing Systems, and Fences linked with Open-Air Intrusion Detection Sensors and Other ground sensors,

The terroristic attack consequences on the asset are assumed to be equal to € 5.000.000. Also, the cost of environmental damages is taken as 750 € $/m^2$. and the whole affected area is 400 m^2.

For both the defender and the attacker respectively all the associated payoffs are reported in Table 14:

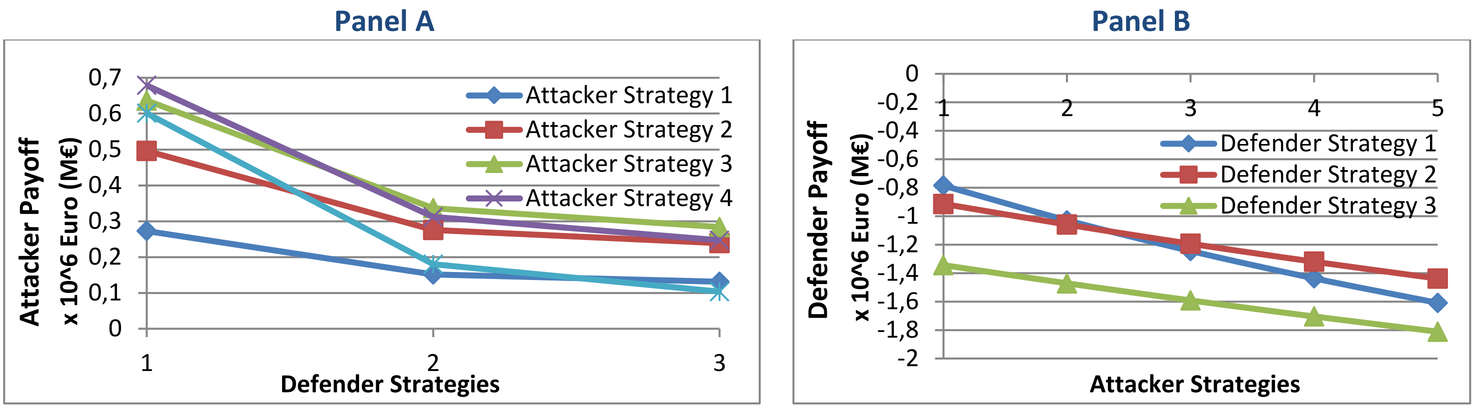
Table 14, Defender's and Attacker's Payoff Bimatrix

Section 4		**Attacker**				
		1	**2**	**3**	**4**	**5**
Defender	**1**	€ -4.265.844, € 854.844	€ -5.153.783, € 1.592.783	€ -5.981.613, € 2.170.613	€ -6.755.237, € 2.444.237	€ -7.479.809, € 2.768.809
	2	€ -4.892.282, € 581.282	€ -5.539.159, € 1.078.159	€ -6.154.173, € 1.443.173	€ -6.739.622, € 1.528.622	€ -7.297.587, € 1.686.587
	3	€ -5.437.642, € 676.642	€ -6.169.731, € 1.258.731	€ -6.860.994, € 1.699.994	€ -7.514.754, € 1.853.754	€ -8.133.981, € 2.072.981

See also Figure 8a and 8b, which show the attacker's payoff for each defender strategy, and defender's payoff versus each attacker strategy respectively.

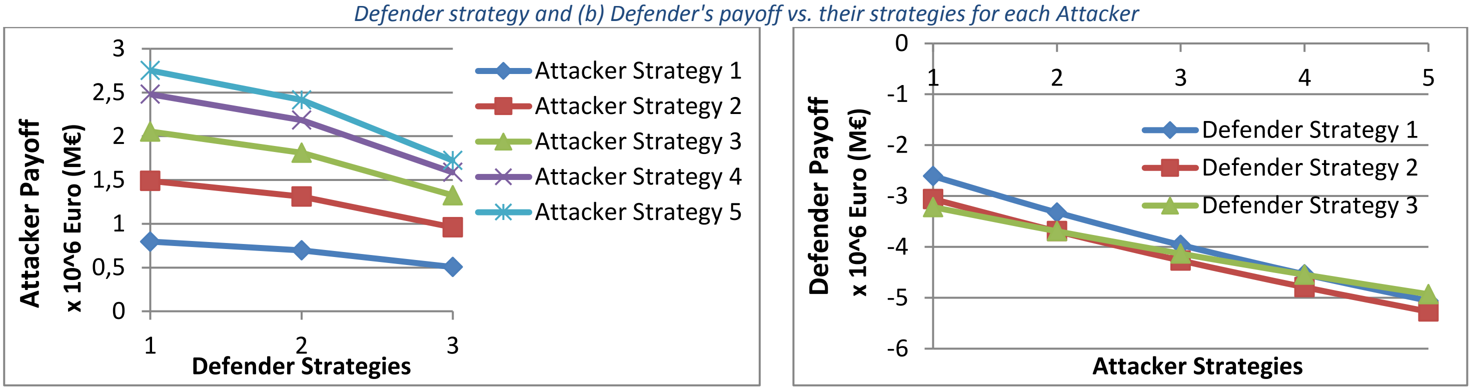
As a result in the case of rational players, the attacker will choose strategy five ($\boldsymbol{Sa_5}$) and the defender will prefer to play her second strategy ($\boldsymbol{Sd_2}$). In other words, pure strategy two for the defender and pure strategy five for the attacker ($\boldsymbol{Sd_2}, \boldsymbol{Sa_5}$) present the best payoff for both players representing the Nash equilibrium for this segment with payoffs (- € 7.297.587; € 1.686.587), for the defender and the attacker respectively. Probability distributions demonstrate that the game has a pure strategy solution and as a result has a pure Nash equilibrium.

In the last segment, the fence with Open ‐ Air Intrusion Detection Sensors represent a very expensive defensive strategy option, but its ps is not as high as its cost. Between the first and the second strategy for the defender, as the ps increase along its cost, the expected losses resulting from a terrorist attack will decrease. Therefore, the defence strategy $\boldsymbol{Sd_2}$ is more preferable. On the other side, because the urban area is so vulnerable and critical, as the attacker increases his effort level investing more on his attack, the resulting payoffs for the attacker will increase. As a result, we can predict that the attacker prefers to attack the urban area with the highest effort level he can make.



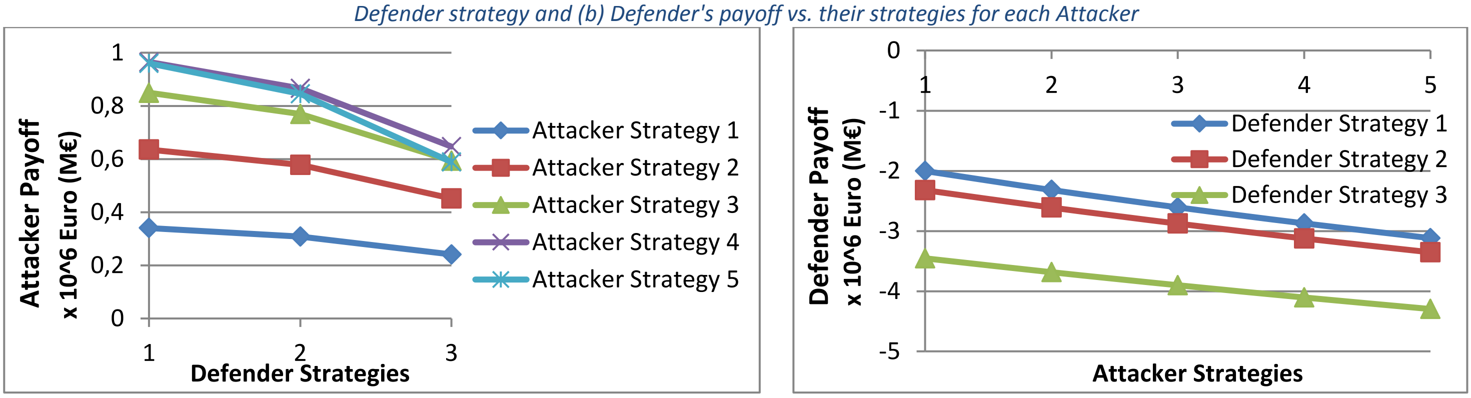
(a) (b)

Figure 5, in Route segment one (a) Attacker's payoff vs. their strategies for each Defender strategy and (b) Defender's payoff vs. their strategies for each Attacker



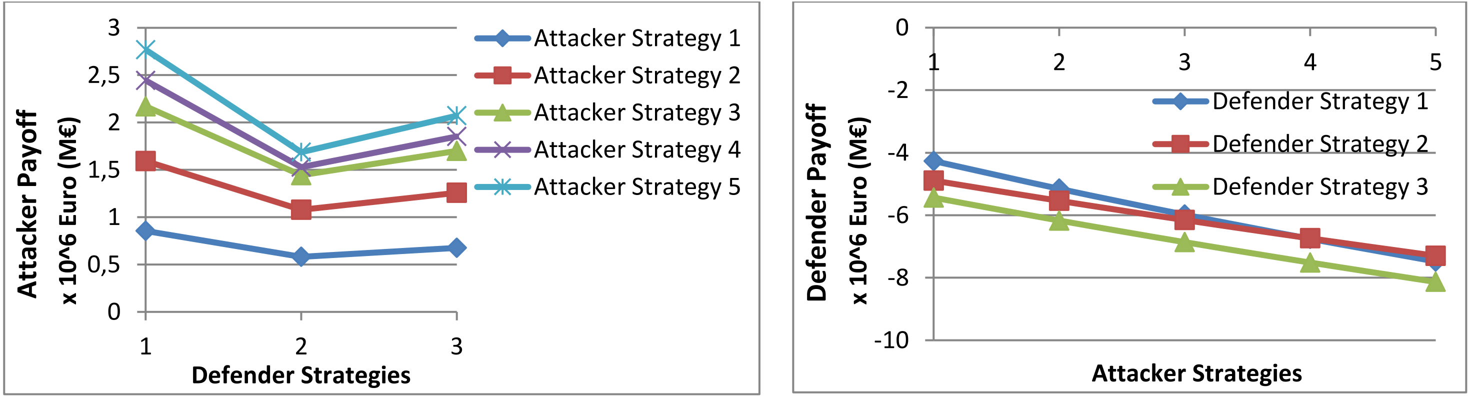
(a) (b)

Figure 6, in Route segment two (a) Attacker's payoff vs. their strategies for each Defender strategy and (b) Defender's payoff vs. their strategies for each Attacker



(a) (b)

Figure 7, in Route segment three (a) Attacker's payoff vs. their strategies for each Defender strategy and (b) Defender's payoff vs. their strategies for each Attacker



(a) (b)

Figure 8, in Route segment four (a) Attacker's payoff vs. their strategies for each Defender strategy and (b) Defender's payoff vs. their strategies for each Attacker

7.2. Illustrative case: global optimization approach

In this approach all the segment matrices (Table 11 to 14) are treated in a combined way. As a result, we have a matrix with three rows and 20 columns showing all the attacking strategies in one view.

A newly combined table can have three rows indicating three defender's strategies ordered from 1 to 3. The three strategies are ordered from the lowest to the highest ps. The columns represent the possible attacker's strategies for all segments (See Table A17 in Appendix).

Then the best mixed-strategy from the attacker's viewpoint will be obtained through the simplex optimization method using MATLAB software. The result shows that an attacker will choose strategy 10 (attacking segment two which is located nearby a village with effort 5) with the probability of 36%, and he can attack by using strategy 20 (attacking the vicinity of an urban area with AEL 5) with the probability of 64%. Probabilities of other strategies are close to zero (see Table A17 in Appendix).

It should be stated that the minimum expected payoff for the attacker is € 1.947.236 for this probability distribution, which is the highest minimum payoff (Maximin) in comparison to other mixed or pure strategies in this type of PSG.

8. Conclusions

In this paper, we have presented a new game theory model, which we called Pipeline Security Game (PSG). The PSG enables a decision maker to assess possible security threats and to explore the beneficial effects of the available countermeasures to prevent or mitigate the consequences of a terrorist attack. Also, a pipeline operator, while assessing possible terrorist threats, could identify weak points or the most likely locations for a terrorist to attack. The innovative predictive model for a possible terrorist attack on a pipeline system, which is developed in this paper, could increase the overall security level of a pipeline network with many practical applications. As a result, the PSG could support more efficient allocation of limited security resources for an oil & gas pipeline system.

The PSG represents a game theoretical model assisting the security risk assessment on a pipeline route in two different aspects. In this paper, two approaches, having different objectives, have been proposed to address two important security protection requirements.

The local optimization approach focuses on one route segment at a time and does not consider security risk on other segments. In this approach, for each specific segment, it is possible to compare different countermeasures or countermeasure sets with each other to find out the most beneficial one to protect a specific pipeline segment. Depending on the AEL in a specific segment, the local optimization assists decision maker to choose the countermeasure that triggers the highest payoff from a variety of available defensive options with various prices and effectiveness.

Conversely, the global optimization approach looks thoroughly at the pipeline network as a whole and compares all the segments with each other to find which one is a more probable target for a terrorist attack. This approach assumes that defender is fully aware of all available countermeasure sets for each route segments as well as all possible Attacker Effort Level from a potential attacked which might be provided by intelligent resources.

By analysing the results obtained, it can be observed that the attacker is a rational decision maker. Therefore, it is unlikely that he uses the highest effort levels whether with a low budget he can achieve his goals. Therefore, this model assists security managers to predict the effort levels that an attacker will most likely put on each route segment.

It should be stated that all costs and parameters might vary depending on the location of the pipeline and the time of the attack. In the proposed example, both location and time related parameters were determined after consultations with experts. In addition, weighting factors used in the PSG model have been taken from the literature. A sensitivity analysis was performed in this PSG model to examine the impact of the parameters on the solution. Since the validity of security risk assessment is difficult to be tested on real cases due to a lack of publicly available data that can be the subject of future studies and sometimes it needs exploring and analysing extensive number of confidential data. The results of this sensitivity analysis were discussed between the authors and security experts; at the end, outcomes are included in this paper.

The PSG model presented in this paper represents the first step in applying game theory in securing a pipeline network. In future research, we can process different assumptions on players' rationality into the calculations of the game. In fact, in many practical situations, a full rational assumption is not realistic. It should be stated that similarly to (Bo An et al. 2012), game theory for security purpose can also be developed and expanded to model cost-benefit analysis to decide how and when to protect pipelines by ground or aerial patrols.

Additional research directions, which are complementary to this study, include the study of other pipeline system facilities such as pump stations; metering or block valve stations which can be all modelled in the PSG game. In fact, these facilities can also be considered as possible targets for attackers along with any other pipeline segments. This would bring to an even more realistic risk assessment for whole pipeline system.

References

(NFPA), National Fire Protection Association. 2001. "NFPA 704." In *Standard System for the Identification of the Hazards of Materials for Emergency Response*. USA: National Fire Protection Association.

Amin, and Saberi. 1964. 'Lemke-Howson Algorithm', *Journal of the Society for Industrial and Applied Mathematics*, 12: 413-23.

Rezazadeh, Zhang, Reniers, Khakzad, and Cozzani. 2017. 'Optimal patrol scheduling of hazardous pipelines using game theory', *Process Safety and Environmental Protection*, 109: 242-56.

Argenti, Landucci, Spadoni, and Cozzani. 2015. 'The assessment of the attractiveness of process facilities to terrorist attacks', *Safety Science*, 77: 169-81.

Bier, and Azaiez. 2009. *Game theoretic risk analysis of security threats* (Springer: New York, USA).

Bo An, Shieh, Yang, Tambe, Baldwin, DiRenzo, Maule, and Meyer. 2012. "PROTECT - A Deployed Game-Theoretic System for Strategic Security Allocation for the United States Coast Guard." In *AI Magazine*. USA: Association for the Advancement of Artificial Intelligence.

CCPS, (Center for Chemical Process Safety). 2003. *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites* (America Institute of Chemical Engineers, John Wiley & Sons: New York, USA).

CCPS, (Center for chemical Process Safety). 2008. *Guidelines for chemical transportation safety, security, and risk management* (America Institute of Chemical Engineers, John Wiley & Sons: New York, USA).

CCPS, (Center for Chemical Process Safety). 2009. *Guidelines for Developing Quantitative Safety Risk Criteria* (John Wiley & Sons, Inc: New York, USA).

Clark, and Riis. 1998. 'Extended Contest Success functions', *Springer*, Economic Theory, Berlin Heidelberg, Germany.

DHS, US Department of Homeland Security. 2007. 'Chemical Facility Anti-Terrorism Standards (CFATS)'. https://www.dhs.gov/cfats-risk-based-performance-standards.

Dornette, and Woodworth. 1969. "Proposed Amendments on Revisions to the Recommended System for the Identification of The Fire Hazards of Materials." In *NFPA704M*. National Fire Protection Association.

Enders, and Olson. 2012. "Measuring the economic costs of terrorism." In *The Oxford Handbook of the Economics of Peace and Conflict*, 874. Online: Oxford University Press.

FAS, Federation of American Scientists. 2006. "Al Qaeda training manual." In. New York, USA: Federation of American Scientists (FAS).

Islam, Mohammad Saiful, Robert Nix, and Murat Kantarcioglu. 2012. "A Game Theoretic Approach for Adversarial Pipeline Monitoring using Wireless Sensor Networks." In *13th IEEE International Conference on Information Reuse and Integration*. Las Vegas, Nevada, USA: IEEE IRI 2012.

Nash, John F. 1950. "Equilibrium Points in n-Person Games." In *Proceedings of the National Academy of Sciences of the United States of America*. National Academy of Sciences.

OGP, (Oil & Gas Producers). 2010. "Consequence modelling." In *Risk Assessment Data Directory*. London, UK: International Association of Oil & Gas Producers.

Peters. 2015. *Game Theory muli-level approach* (Springer-Verlag: GmbH Berlin Heidelberg).

Pritchard, David. 2011. 'The Lemke-Howson Algorithm.' in, *Game Theory and Algorithms* (EPFL: Lausanne).

RAND. 2016. 'RAND Database of Worldwide Terrorism Incidents', National Security Research Division. http://www.rand.org/nsrd/projects/terrorism-incidents.html.

Reniers, and Dullaert. 2011. 'TePiTri: A screening method for assessing terrorist-related pipeline transport risks', *Security Journal*, 25: 173-86.

Reniers, Katleen De Jongh, Gorrens, Lauwers, Leest, and Witlox. 2010. 'Transportation Risk ANalysis tool for hazardous Substances (TRANS) – A user-friendly, semi-quantitative multi-mode hazmat transport route safety risk estimation methodology for Flanders', *Transportation Research Part D: Transport and Environment*, 15: 489-96.

Reniers, and Pavlova. 2013. *Using Game Theory to Improve Safety within Chemical Industrial Parks* (Springer Series in Reliability Engineering: Springer-Verlag London, UK).

Reniers, Ale, Dullaert, Foubert, . 2006. 'Decision support systems for major accident prevention in the chemical process industry: A developers survey', *Journal of loss prevention in the process industries*, 19: 604-20.

Sandler T, and Enders W. 2008. "Economic consequences of terrorism in developed and developing countries." In *Terrorism, economic development, and political openness*.

Skaperdas. 1994. 'Contest Success functions', *Springer-Verlag Berlin Heidelberg*, Economic Theory.

Talarico, Sorensen, Reniers, and Springael. 2015. 'pipeline secuiry.' in Hakim, Albert and Shiftan (eds.), *Securing Transportation Systems* (John Wiley & sons, Inc.).

Tambe. 2012. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned* (Cambridge University Press: United States of America).

TNO. 1992. *Methods for determination of possible damage - Green Book* (The Netherlands Organisation of Applied Science Research: The Hague, Netherlands).

VROM (The Netherlands Ministry of Housing, Spatial Planning and the Environment). 2005. *Methods for the determination of possible damage to people and goods* (Ministry of VROM: Den Haag, Netherlands).

Wadhawan, Yatin, and Clifford Neuman. 2016. "Defending Cyber-Physical Attacks on Oil Pipeline Systems." In, 1-8.

Appendix:

The detailed calculations in each route segment are presented in this annex. All the information from the text is summarized here. The calculations followed the Fig 3.

- **Route Segment one: (Desert)**

We can summarize the evaluation of consequences in Table A1.

Table A1, Consequences of security incident

Asset	**Health-related cost**		**Environmental cost**	
S	α	H	β	E
€ 3.000.000	0	€ 1.000.000	300	€ 500

Through the procedure of Section 4.3 the LG obtained is equal to 5 and the Co is calculated as € 3.150.000 by equation 7 in this route segment (see Section 4.6).

The strategies and associated costs for the attacker is reported in Table A2:

Table A2, Attacker's strategies

AEL	1	2	3	4	5
Strategies	$\boldsymbol{Sa_1}$	$\boldsymbol{Sa_2}$	$\boldsymbol{Sa_3}$	$\boldsymbol{Sa_4}$	$\boldsymbol{Sa_5}$
C_A	€ 5.000,00	€ 25.000,00	€ 100.000,00	€ 250.000,00	€ 500.000,00

While for strategies of the defender, we have Table A3:

Table A3, Defender's strategies

Countermeasure set	Strategies*	ps	C_d	Type of countermeasure
1	$\boldsymbol{Sd_1}$	18	€508.000	Aerial Patrol
2	$\boldsymbol{Sd_2}$	33	€758.000	Aerial Patrol, Distributed acoustic sensing
3	$\boldsymbol{Sd_3}$	38	€1.208.000	Drones, Thermal Infrared Sensor

*Note: these strategies are ordered from the lowest ps to the highest ps.

The reported probabilities of a successful attack in Table A4 were found by equation 6.

Table A4, Successful attack probabilities

Section 1		Attacker				
		1	2	3	4	5
Defender	1	0,088	0,165	0,233	0,294	0,349
	2	0,049	0,095	0,138	0,178	0,215
	3	0,043	0,083	0,121	0,157	0,191

Accordingly the bimatrix of payoffs in this segment is Table 11.

- **Route Segment two: (rural area with a village)**

The detailed consequence evaluation in segment two is given in Table A5.

Table A5, Consequences of security incident

Asset	**Health-related cost**		**Environmental cost**	
S	α	H	A	α
€ 3.500.000	10	€ 1.000.000	400	€ 750

Through the procedure of Section 4.3 the LG is 6, and the value of Co has been calculated by equation 7 as € 13.800.000 for this route segment (see Section 4.6).

In Table A6, the attacker strategies with their costs are reported.

Table A6, Attacker's strategies

AEL	1	2	3	4	5
Strategies	$\boldsymbol{Sa_1}$	$\boldsymbol{Sa_2}$	$\boldsymbol{Sa_3}$	$\boldsymbol{Sa_4}$	$\boldsymbol{Sa_5}$
C_A	€ 5.000,00	€ 25.000,00	€ 100.000,00	€ 250.000,00	€ 500.000,00

While for strategies of the defender, we have Table A7:

Table A7, Defender's strategies

Countermeasure set	Strategies*	ps	C_d	Type of countermeasure
1	$\boldsymbol{Sd_1}$	33	€ 1.808.000	Ground Patrol, Not Open-Air Sensor
2	$\boldsymbol{Sd_2}$	38	€ 2.358.000	Ground Patrol, Remote Sensing Systems
3	$\boldsymbol{Sd_3}$	53	€ 2.708.000	Fences, Open-Air Intrusion Detection Sensors

*Note: these strategies are ordered from the lowest to the highest ps.

The probabilities of a successful attack were found by equation 6 and they are shown in Table A8:

Table A8, Successful attack Probabilities

Section 2		Attacker				
		1	2	3	4	5
Defender	1	0,058	0,109	0,156	0,197	0,235
	2	0,050	0,096	0,138	0,176	0,211
	3	0,036	0,071	0,103	0,133	0,161

consequently Table 12 is the bimatrix payoff for this segment.

- **Route Segment three: (Mountain area)**

In this segment, the detailed consequence evaluation is given in Table A9.

Table A9, Consequences of security incident

Asset	**Health-related cost**		**Environmental cost**	
S	α	H	A	α
€ 3.200.000	4	€ 1.000.000	500	€ 750

Through the procedure of Section 4.3 the LG level is equal to 5 and by equation 7 the Co is equal to € 7.575.000 for this route segment (see Section 4.6).

For the attacker strategies and their costs are listed in Table A10:

Table A10, Attacker's strategies

AEL	1	2	3	4	5
Strategies	$\boldsymbol{Sa_1}$	$\boldsymbol{Sa_2}$	$\boldsymbol{Sa_3}$	$\boldsymbol{Sa_4}$	$\boldsymbol{Sa_5}$
C_A	€ 5.000,00	€ 25.000,00	€ 100.000,00	€ 250.000,00	€ 500.000,00

While for the defender, these strategies with related costs in Table A11 are available:

Table A11, Defender's strategies

Countermeasure set	Strategies*	ps	C_d	Type of countermeasure
1	$\boldsymbol{Sd_1}$	35.5	€ 1.658.000	Aerial Patrol, Thermal Infrared Sensor
2	$\boldsymbol{Sd_2}$	39.25	€ 2.008.000	Aerial Patrol, Not Open-Air Sensor
3	$\boldsymbol{Sd_3}$	50.5	€ 3.208.000	Drones, Remote Sensing Systems

*Note: these strategies are ordered from the lowest to the highest ps.

Table A12 represents the probabilities of successful attack that calculated by equation 6.

Table A12, Successful attack Probabilities

Section 3		Attacker				
		1	2	3	4	5
Defender	1	0,045	0,087	0,125	0,160	0,192
	2	0,041	0,079	0,114	0,147	0,177
	3	0,032	0,062	0,091	0,118	0,143

As a result Table 13 presents the bimatrix payoff for this segment.

- **Route Segment Four: (Urban area)**

Consequence evaluation of this segment can be summarized in Table A13.

Table A13, Consequences of security incident

Asset	**Health-related cost**		**Environmental cost**	
S	α	H	A	α
€ 5.000.000	21	€ 1.000.000	400	€ 750

Through the procedure of Section 4.3 the LG for this route segment is equal to 7 and as mentioned in Section 4.6 by equation 7 the Co associated to this segment is € 26.300.000.

The attacker has available strategies in Table A14:

Table A14, Attacker's strategies

AEL	1	2	3	4	5
Strategies	$\boldsymbol{Sa_1}$	$\boldsymbol{Sa_2}$	$\boldsymbol{Sa_3}$	$\boldsymbol{Sa_4}$	$\boldsymbol{Sa_5}$
C_A	€ 100.000	€ 250.000	€ 500.000	€ 1.000.000	€ 1.400.000

Note: As mentioned in Section 4.2, the cost of a terrorist attack is assumed to be higher in an urban area.

While for defender, the strategies are shown in Table A15:

Table A15, Defender's strategies

Countermeasure set	Strategies*	ps	C_d	Type of countermeasure
1	$\boldsymbol{Sd_1}$	63	€ 3.311.000	Aerial Patrol, Ground Patrol, Other ground sensors
2	$\boldsymbol{Sd_2}$	89.25	€ 4.211.000	Aerial Patrol, Ground Patrol, Other ground sensors, Remote Sensing Systems
3	$\boldsymbol{Sd_3}$	78	€ 4.661.000	Fences, Open-Air Intrusion Detection Sensors, Other ground sensors

*Note: these strategies are ordered from the lowest to the highest ps.

The probabilities that the attack successfully occurs are shown in the Table A16.

Table A16, Successful attack Probabilities

Section 4		Attacker				
		1	2	3	4	5
Defender	1	0,036	0,070	0,101	0,130	0,158
	2	0,025	0,050	0,073	0,096	0,117
	3	0,029	0,0573	0,0836	0,108	0,132

Accordingly for this segment the bimatrix payoff is Table 14.

Following section 7.2, the combined matrix is shown in table A17.

Table A17: Defender's payoff in all segments

		Attacker																			
Route Segment		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Defender	1	272415	495998	636584	678736	601079	796338	1489719	2053872	2479809	2751466	340258	635416	849244	964911	960095	854844	1592783	2170613	2444237	2768809
	2	150919	275858	335938	312130	180285	696257	1309690	1809686	2183975	2413980	308638	577336	768956	865937	845372	581282	1078159	1443173	1528622	1686587
	3	131057	238715	283729	246766	103416	505124	958879	1325020	1586802	1722063	241037	451595	593089	646768	588737	676642	1258731	1699994	1853754	2072981

Referring to section 7.2, Table A17 shows the probability distribution for the whole segments.

Table A18: probability distribution of likelihood of terrorist attack to whole pipeline

	Attacker																			
Route Segment	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Probability	0	0	0	0	0	0	0	0	0	37%	0	0	0	0	0	0	0	0	0	63%