Gest. Prod., São Carlos, v. 24, n. 3, p. 450-463, 2017
http://dx.doi.org/10.1590/0104-530X1814-16

Adversarial Risk Analysis in support of defensive resource allocation for counterterrorism

Análise de Risco Adversário para alocação de recursos de contraterrorismo

Marcelo Zawadzki[1]*
André Negrão Costa[1]
Mischel Carmen Neyra Belderrain[2]
Gilberto Montibeller[3]

Abstract: Terrorism risk assessment is one of the biggest challenges that authorities must face to define the defensive resource allocation policy for a country. This article provides a brief review of two approaches that have been traditionally used for this purpose: Probabilistic Risk Assessment and Game Theory. Additionally, it introduces the Adversary Risk Analysis approach to the Brazilian context; an innovative methodology that aims to assess risks caused by intelligent opponents. Finally, an application of Adversarial Risk Analysis in a hypothetical situation is presented. The results show that Adversarial Risk Analysis can be useful to support decisions about defensive resource allocation in contexts such as sports mega events, a reality for many countries around the world.

Keywords: Adversarial Risk Analysis; Resource allocation, Terrorism risk; Terrorism in sports events; World Soccer Cup; Olympic Games.

Resumo: *Análise de risco de terrorismo é um dos maiores desafios enfrentados pelas autoridades que definem a política de alocação de recursos de uma nação. Este artigo provê uma breve revisão de duas abordagens tradicionalmente usadas para esse propósito: Análise de Risco Probabilística e Teoria dos Jogos. Adicionalmente, ele introduz no contexto brasileiro a Análise de Risco Adversário, uma metodologia inovadora que objetica analisar os riscos causados por oponentes inteligentes. Finalmente, uma situação hipotética da Análise de Risco Adversário é apresentada. Os resultados mostram que essa metodologia pode ser utilizada para apoiar decisões sobre a alocação de recursos de defesa no contexto de megaeventos esportivos que são de interesse de diversos países.*

Palavras-chave: *Análise de Risco Adversário; Alocação de recursos; Risco de terrorismo; Terrorismo em eventos esportivos; Copa do Mundo; Jogos Olímpicos.*

1 Introduction

As a growing country, Brazil has been progressively exposing itself on the world stage. Thus, the trend is for Brazil to be increasingly selected to host major events such as the 2014 FIFA World Cup and the 2016 Summer Olympics Games in Rio de January. Mega sporting events like those listed above have intrinsic characteristics that make them extremely symbolic (Jennings & Lodge, 2012). Camargo (2011) states that mega sporting events are events that, besides including a huge audience, gather diverse nationalities. Events of this size bring together authorities representing states and governments, businessmen and other emblematic individuals that can catalyze hatred, prejudice, etc. Thus, events of this magnitude can be very attractive to terrorist groups that want to perpetrate attacks with the goal of enhancing the visibility of their cause, projecting it internationally. In most cases, such groups carry out their attacks for fame, for recognition of their causes and, sometimes, for revenge (Richardson, 2007). In this context, although Brazil is not exactly the target, it can be a scenario for international terrorism

[1] Subdivisão de Sistemas de Apoio à Decisão, Instituto de Estudos Avançados – IEAv, Trevo Coronel Aviador José Alberto Albano do Amarante, 1, CEP 12228-001, São José dos Campos, SP, Brazil, e-mail: mzawa@ieav.cta.br, negrao@ieav.cta.br

[2] Departamento de Produção, Instituto Tecnológico de Aeronáutica – ITA, Praça Marechal Eduardo Gomes, 50, CEP 12228-900, São José dos Campos, SP, Brazil, e-mail: carmen@ita.br

[3] Management Science and Operations Management Group, Loughborough University, LE11 3TU, Leicestershire, England, United Kingdom, e-mail: G.Montibeller@lboro.ac.uk

Received Oct. 24, 2015 - Accepted May. 15, 2016

Financial support: None.

as it serves as the stage for mega events such as the aforementioned (Diniz, 2004).

It is interesting to note that history shows that major sporting events have been frequently chosen as theater of operations by terrorist groups. Some unforgettable examples are: the bombings at Centennial Park during the 1996 Atlanta Summer Olympics; The explosion of a car bomb in the vicinity of Santiago Bernabéu stadium in the 2002 UEFA Champions League semi-final; The suicide bombing at a marathon in Sri Lanka in 2008, and, among others, the attack on the Togolese soccer team in 2010, when gunmen shot the bus on which the players were. More recently, events on April 15, 2013 in the United States (terrorist attacks at the Boston Marathon) indicate that terrorist practices, taking advantage of major sporting events as their main stage, have been repeatedly employed with increased frequency.

Historically, Brazil does not have much experience in managing terrorist threats, not counting on many initiatives, plans, and policies for inhibiting terrorism practices, as do countries such as England, Israel and the United States of America. In such countries, the risks of terrorist attacks have led to billions of dollars of investment in order to improve public security (Kardes & Hall, 2005). Some studies (Buzanelli, 2004) criticize the low level of attention paid by the Brazilian government's agencies to the subject of terrorism, specifically the allocation of resources for anti-terrorism protection as an important matter that would deserve more attention.

As pointed out by Willis (2007), efforts related to resource allocation to anti-terrorist activities are intimately connected to the need to assess risks. Much of the challenge presented in this paper is motivated by the fact that, unlike natural threats (eg, intense meteorological phenomena) or engineered systems (*e.g.*, failures in systemic components), the risks to be evaluated here are provided by opponents (as in the case of terrorist organizations), and therefore the risks evaluated in this context are no longer governed by chance (Ayyub et al., 2007; Brown & Cox, 2011; Parnell et al., 2010; Zhuang & Bier, 2007). After all, nature may be subtle, but it is not malicious. Terrorists, on the other hand, are both subtle and malicious (Woo, 2002). In other words, terrorists can adapt to different measures that may be taken to deal with them (Cox, 2009a, b, 2012). So, the traditional approaches used for risk assessment are not always sufficient to guide the resource allocation for counterterrorism.

Therefore, this article focuses on the contextualization and application of a method called Adversarial Risk Analysis (ARA) (Banks, 2009, 2011; Rios & Insua, 2011). The introduction of this tool, which aims to support the risk assessment of the information provided by intelligent opponents, is a relevant contribution to the Brazilian context. It is emphasized that until the present, as far as the authors know, the subject is still unpublished in Brazil.

This paper presents, initially, a brief review of the first two approaches available in the literature with respect to resource allocation for risk management in face of terrorist attacks: Probabilistic Risk Assessment and Game Theory. Following, an ARA proposal is presented and simulated to illustrate the application of this approach. The article concludes with considerations about the advantages that ARA presents when compared to the two approaches previously discussed. Additionally, it emphasizes what contributions the ARA approach can bring and, finally, presents the challenges that persist in the ARA methodology.

2 The antiterrorism defense resource allocation problem

2.1 Probabilistic Risk Assessment

Probabilistic Risk Assessment (PRA) has been used for more than 30 years to evaluate risks (probabilities and consequences of a system failure) and to orient decisions in risk management in the governmental and industrial arenas in several situations, such as in environment protection, industrial safety and medical procedures (Ezell et al., 2010; Paté-Cornell, 2007). In terms of terrorist risks, models constructed based on the PRA approach usually aim to estimate the difference between the risks of each target, when they do not count, and, when they count, the various protection measures that can be adopted. Then, as a result, a risk ordering is obtained and evaluated (risk-scoring) and in this way it is feasible to prioritize the available resources to be allocated (Ayyub et al., 2007; Cox, 2009a; Paté-Cornell, 2007; Willis et al., 2005).

In order to operationalize the PRA application, most of the approaches are based on the Risk Analysis and Management for Critical Asset Protection Model (RAMCAPTM) (Cox, 2008). In this, a conceptual framework for risk (R)computation is suggested as a function of an existing threat (A), a vulnerability (V) presented by a target and a consequence (C) for an attack suffered, *i.e.*, $R=F(T,V,C)$ (Dillon et al., 2009).

Some interesting cases where PRA has been applied are presented by Willis et al. (2005), that compare the results obtained when considering the use of the function above with the results derived from the calculation of the risk considering simple indicators (for example, population of a region and the weighted population density of a region). The authors conclude that in the first case the risks are more concentrated in certain urban regions than in the second case. Winterfeldt & O'Sullivan (2006), Kleinmuntz & Willis (2009) go deeper into the use

of the $f(T,V,C)$ function as an indicator of risk and analyze the uncertainties that may be included in the parameters considered in the analysis.

Although several research efforts propose the application of the PRA approach, there are still some questions that may suggest that it would not be the most appropriate for dealing with defense resource allocation aimed at counterterrorism. For example, Cox (2009a) comments that if the terrorist group knows that an analysis like the one proposed by the PRA approach is being conducted, it would be able to infer that targets with similar characteristics would receive similar priorities in allocating resources for counter-terrorism protection. Such information could be valuable to attackers, as they could infer the level of protection that would be assigned to each target. Cox (2009a) also points out that methods such as PRA do not allow secrecy to be exploited, do not take into account budget constraints that may exist (not only for defense but also for offense) and disregard the fact that protecting a target changes probabilities of attacks on other targets. For example, as presented by Sandler & Siqueira (2008), the installation of metal detectors at airports on January 5th, 1973, resulted in a dramatic drop in the number of aircraft abductions. However, from this moment, it was possible to notice a great diversification in the tactics employed by terrorist organizations. Parnell et al. (2010) and Cox (2009a) critically point out that PRA ignores what the attacker will do after defense measures are allocated. Such an attitude is equivalent to ruling out the fact that terrorists are intelligent and can adapt to the defensive measures taken.

That said, it is possible to conclude that although the PRA approach is able to contribute significantly to support the allocation of resources for risk coping / mitigation in counterterrorism studies, some gaps have not yet been fully met and therefore further studies are needed in this field. Some papers sought to employ the well-known Game Theory in an attempt to fill in these gaps.

2.2 The strategic vision of Game Theory

Motivated by the observation that each part of the game acts according to its beliefs and according to the anticipations that can be made about the opponent, several researchers believe that Game Theory can be considered an appropriate tool to support the resource allocation for defense aiming at counter-terrorism. It is noted that Game Theory is aligned with a series of relevant assumptions adopted in studies within the context in question, such as those highlighted by Sandler & Arce (2003):

- The interactions between sides in the game are strategic;
- Actions are interdependent and therefore it is not possible to analyze one side as passive;
- Strategic interactions occur between rational actors, who are trying to act according to the way they imagine their counterparts will act and react.

In fact, this theory allows for joint symmetric normative analysis, in which players aim to maximize their expected utilities while expecting other players to do the same. The analyses through Game Theory are enabled once the decisions of each player can be anticipated by the process of the search for the Nash equilibria (Rios & Insua, 2011), the central concept in Game Theory. Nash equilibrium can be defined as the situation in which the strategy chosen by each player is the best answer for whatever the other players choose. Formally, a single-player strategy s_i^* is considered the best response to a given player's strategy when there is no other strategy available to the player to produce a higher reward than s_i^* when s_{-i} is played, *i.e.*, $\pi_i\left(s_i^*, s_{-i}^*\right) \geq \pi_i\left(s_i, s_{-i}^*\right)$ for all s_i and all i, where π_i represents the reward function of a player i; s_i is a player strategy i; And the asterisk indicates that the strategy is a Nash equilibrium (Fiani, 2006).

Chart 1 presents some examples of Game Theory applications in the problem of allocating defense resources against terrorist actions.

Although Game Theory has been extensively applied to solve this type of problem, this approach faces some criticisms that deserve to be discussed. Sebenius (1992, 2006), for example, points out that one of the main aspects of Game Theory that can be considered problematic is the adoption of premises that refer to complete and perfect knowledge about possible goals and aspirations that the players sustain, some about the others. Sandler & Arce (2003) argue that in real situations where counter-terrorism resource allocation is being studied, the most common scenario is that both defense and attack have incomplete information. As pointed out by Banks & Anderson (2006) the standard approach that considers complete knowledge ends up failing in practice. To circumvent this flaw, there are modified theories with relaxed assumptions, mainly in regard to considering the complete knowledge of the game or the consideration of unlimited rationality (Gigerenzer & Reinhard, 2001) by the players. In the same way, authors suggest the use of probabilities, treating the game through a Bayesian analysis, as does Ezell et al. (2010), who consider that the possibility of adopting incomplete information games, when there are inherent uncertainties about the players and their preferences, is a good solution.

In this research, it is believed that, in fact, the meeting of the points that define the Nash equilibrium may allow some interesting insight on the analyzed

Chart 1. Application of the theory of games in problems of allocation of antiterrorism resources.

Topic	Variations	Comments/Conclusion	References
Distribution of resources for protection against terrorist actions	Strategic threats	The attacker's preferences change according to the prior allocation of defense resources.	(Powell, 2007a)
	Non-strategic threats	The opponent is not attacked where it is the weakest and where the expected gains will be greater. Preferences of attackers are unchanged.	(Banks & Anderson, 2006; Farrow, 2007; Powell, 2007a; Zhuang & Bier, 2007)
	Synergic defensive measures	A single defense measure may result in reducing the vulnerability of more than one target.	(Farrow, 2007; Powell, 2007a)
Uncertainties inherent to attackers and defenders	Defender uncertainties about how the attacker's preferences change over targets.	Centralization of resources protecting high valued targets performs better than those acting in a decentralized manner.	(Bier et al., 2007; Major, 2002)
		With scarce resources the uncertainty becomes more significant and it is more difficult to protect targets that are more valuable.	(Wang & Bier, 2011)
		A robust type optimization can circumvent the uncertainties about the attacker's parameters.	(Nikoofal & Zhuang, 2011)
	Attacker's uncertainty related to the targets.	Game modeling can be performed as signaling games. Allocating too much resource to protect a target can signal high value target.	(Powell, 2007b)
	Uncertainties about the targets' values and about the attacker's target preference.	Uncertainty about attackers' preferences has little impact on how defense resources are allocated.	(Bier et al., 2008)
Advantages and disadvantages of making resource allocation public		It is better for the defense to make its strategy public than to make it a secret.	(Farrow, 2007; Major, 2002; Zhuang & Bier, 2010)
		The balance between disclosure of defense strategies and maintaining the secrecy of this information is the best strategy.	(Brown et al., 2005)
Redundant protection of critical targets		It is more advantageous to protect more critical components than to opt for redundancy.	(Brown et al., 2005)
		The author emphasizes the validity of redundancy as a defensive strategy.	(Bier, 2006)
Tradeoff analysis in the distribution of resources for the protection of several targets		Analysis of how considering equity and efficiency impacts on the distribution of resources for the protection of various targets.	(Shan & Zhuang, 2012)

question. However, it is important to point out here that allocating resources to protect oneself from the worst scenario (the one the opponent has in mind to cause and the one the defense will seek to avoid) is not tantamount to protecting against all other less harmful scenarios. The typical result in searching for balance points is that none of the players end up getting the reward they would like the most, however, they avoid the worst results (Insua et al., 2009). It is exactly in relation to this search that one makes a question here: would it be the search for the Nash equilibrium sufficient to mark the issue of the allocation of resources for antiterrorism purposes?

What we conclude here is that Game Theory, as well as all other approaches, has limitations that need to be taken into account. Finally, the question raised by Ellis (2009) is open: what approach to risk assessment would be both flexible and robust in a way that would serve to guide the allocation of defense resources to this situation, recognizing that the nature of terrorist threats changes in Response to any defense strategy that is adopted?

3 Adversarial Risk Analysis: a new approach

According to Insua et al. (2009), the challenges characterized by the existence of two or more intelligent opponents making decisions that culminate in an uncertain outcome are covered by an approach called Adversarial Risk Analysis (ARA). Rios & Insua (2011) argue that ARA is capable synergistically integrate classic Game Theory and Probabilistic Risk Assessment.

In order to support one of the participants of a game (called defense), ARA employs the modeling of the opponent's decision structure (called attack) to obtain a descriptive probabilistic model of the behavior that the attack may take. The great contribution of ARA occurs when this description is used by the defense as useful information to solve its own decision problem. For this, the assembled structure takes into account possible decision alternatives that exist for defense and attack, as well as other information that may be available, asymmetrically, for the parties involved in the game. As a way to accommodate the possible information to be extracted in the analysis performed, to solve the decision problems of both parts of the game, ARA adopts a structure with "nested" decision models made possible by a procedure called mirroring (Banks, 2009; Insua et al., 2009). This structure makes it possible to make the analysis of the problem closer to what would be done in a real situation (Insua et al., 2009). The basic strategy contained in the mirroring argument is a procedure in which the decision maker studies the analysis the opponent is likely to perform, considering the fact that the opponent will simultaneously conduct a symmetrical study of the defense's decision analysis. Rothschild et al. (2012), the technique of mirroring resembles level-k games (Rothschild et al., 2012; McLay et al., 2012).

The ARA approach is already present in some works in the international literature. Among these, we highlight the most relevant applications within the current theme: Insua et al. (2009), and Rios & Insua (2011) explore how ARA could be applied to simultaneous and sequential games with private information by one party. Wang & Banks (2011) analyze the allocation of resources in missions of military convoys that travel by routes that can be attacked by enemies. Sevillano et al. (2012) present a behavioral model of the pirates used in the selection of the decision to be made in case of a pirate approach at sea. Finally, Banks et al. (2011) explore the ARA approach when it is assumed that one of the parties involved in the game may be bluffing.

In order to clarify the modeling philosophy of the ARA approach, it is considered here a hypothetical situation where the defense needs to opt for a strategy, these strategies being elements of the set $D=\{d_1,d_2,d_3,...,d_n\}$ where d_n represents the n-th strategy available for the defense to choose, while the attacker must decide on which type of attack to carry out, the attack types being the elements of set $A=\{a_1,a_2,a_3,...,a_m\}$, Where am represents the m-th type of attack the attacker can adopt. The tree shown in Figure 1 represents the events observed by the defense and the attack. The node *D, A* (rectangle) represents the decisions of the defense and the attacker. The node *S* represents

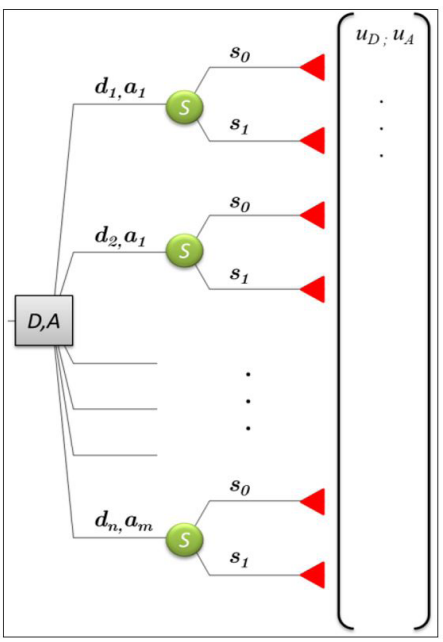

Figure 1. Decision tree with the events faced by the defense and the attacker. Source: adaptation Rios & Insua (2011).

the chance that the attack has to fail (represented by the branch s_0) or success (represented by branch s_1). It is considered here that success means that the damages expected by the attacker have occurred. In cases where the expected damages do not occur, regardless of the reason that did not allow such occurrence, the attack is considered a failure. Each pair of utility values (u_D, u_A) is associated to each leaf of the tree, representing the values assigned by the utility function of the defense and the attacker, respectively.

3.1 Game modeling by the defense's point of view

When the problem analyzed is the one that the defense needs to solve, the attacker's decision (which type of attack he will perform) becomes uncertain. In the new decision tree represented by Figure 2, this situation can be observed. A knot that represented an attacker's decision is now perceived as a knot that represents an uncertainty for the defense, illustrated by a circle, rather than a square. One can see a dotted line around the attacker's possible decisions. Such a representation indicates that these decisions are considered a set of information, since the attacker does not know in which branch of the tree it actually is, when it makes its decision (the game represented is a simultaneous game).

The defense knows its utility-function $u_D(d,s)$. One can also define that defense specialists are able to define the probability of success and failure $p_D(S=s\,|d,a)$, when each type of attack is carried out, in cases where each of the defensive strategies have been adopted. However, the chances of the attacker choosing each type of attack are not available for the defense. The defense expresses this uncertainty by means of a probability $\pi_D(A=a)$.

Considering that the defense intends to adopt the decision that maximizes its expected utility, the main optimization problem that must be solved by it is represented by Equation 1.

$$\mathrm{d}^* = \arg\max_{d\in D} \sum_{a\in A}\left[\sum_{s\in\{0,1\}} u_D(d,s)\,p_D(S=s\,|d,a)\right]\times\pi_D(A=a) \qquad (1)$$

With that, it is possible to conclude that the factor that the defense really needs to evaluate is the probability $\pi_D(A=a)$. In order to obtain such a parameter the defense starts to analyze how its opponent could be performing the analysis of its own decision problem: to choose what type of attack it should carry out.

3.2 Game modeling from the attacker's point of view

The decision problem faced by the attacker is illustrated by the decision tree shown in Figure 3. In this tree, nodes *D* represent the uncertainty that the attacker maintains as to which strategy the defense will adopt. The defense must then put itself in the position of the attacker and imagine how it would be solving its decision problem. This procedure can be found in academic efforts that explore the behavioral modeling of agents such as terrorists and their organizations (examples can be seen in: Pat-Cornell & Guikema, 2002; Ushakov, 2006; Rios & Insua, 2011; Sevillano et al., 2012).

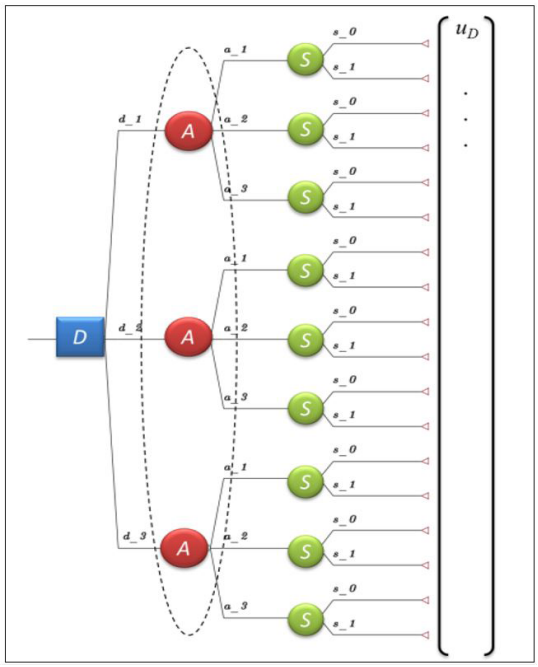

Figure 2. Decision tree representing the defense problem.

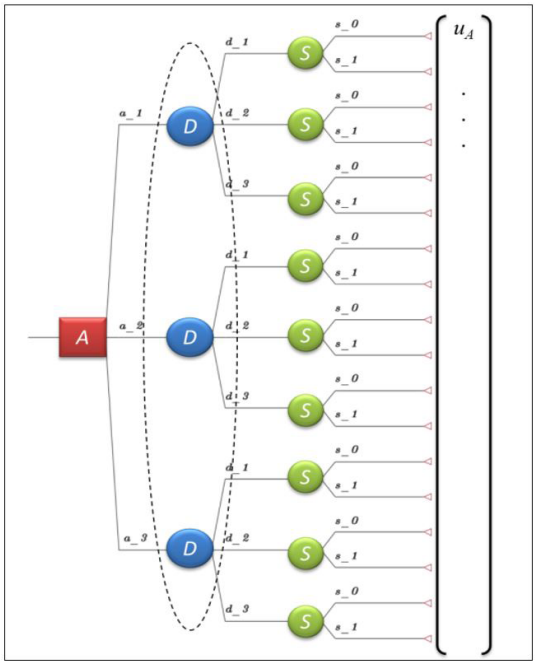

Figure 3. Decision tree representing the attacker's problem.

As in several works in this context, it is assumed that the attackers are utility maximizers (Ezell et al., 2010; McLay et al., 2012; Sevillano et al., 2012). Thus, the attacker looks for the option $a \in A$ that provides the maximum expected utility and, to this end, seeks the solution to Equation 2 that was constructed by means of a process analogous to that realized for the construction of Equation 1.

$$a^* = \arg\max_{a \in A} \sum_{d \in D} \left[\sum_{s \in \{0,1\}} u_A(a,s)\, p_A(S = s \mid d,a) \right] \times \pi_A(D = d) \qquad (2)$$

During the resolution of Equation 2, the defense will have doubts concerning the utility values $u_A(a,s)$ that the attacker will adopt when solving its problem. Likewise, the defense is not sure about what are the attacker's beliefs about the odds of success or failure of its attack $p_A(S=s \mid d, a)$, when each of the strategies that the defense can adopt is chosen. Another parameter that is uncertain for the defense refers to how the attacker may be evaluating the defense's chances of opting for one of the defense strategies $\pi_A(D=d)$. Insua et al. (2009) propose the use of subjective probability distributions to represent all quantities that are unknown to the decision maker (defense). Although Banks (2011) points out that formulating the subjective probabilities that represent the behavior of the opponent may present challenges, Kunreuther et al. (2013) comment on the extensive literature on methods for obtaining such parameters, when expert knowledge can be explored.

In this way, the modeling of the information available for the defense by means of probability distributions is now used to represent the random variables U_A, P_A e Π_A, which describe the behavior of $u_A(a,d)$, $p_A(S=s \mid d,a)$, and $\pi_A(D=d)$, respectively. Adding such uncertainty to Equation 2, the following Equation 3 is obtained:

$$A|D \sim \arg\max_{a \in A} \sum_{d \in D} \left[\sum_{s \in \{0,1\}} U_A(a,s) P_A(S = s \mid d,a) \right] \times \prod_A (D = d) \qquad (3)$$

The parameters for the probability distributions $U_A(a,s)$ and $P_A(S=s \mid d,a)$ can be proposed directly by the defense with the help of specialists. However, for the evaluation of $\Pi_A(D=d)$ it will be necessary for the defense to take the attacker's place and think about how it would be thinking, when it sought the answers to its problem (which type of attack). That is exactly why Equation 3 there is conditioned to D. This shows that the defense at this stage needs to evaluate how the attacker would be thinking about its rewards and its chances of success when it chooses each type of attack. Likewise, the defense must propose beliefs about how the attacker would be assessing its likelihood (the defense) to adopt each pack of defensive measures. Then, the defense, to get the values for $\Pi_A(D=d)$, could consider that the attacker would also be solving its decision problem in the same way. If this was confirmed, the attacker would be looking for the best way to solve the problem that the defense faces, that is, the one represented by Equation 1.

Therefore, the attacker would be seeking to obtain the parameters of the probability distribution that governed the behavior of the random variable $D \mid A^1$ (Equation 4), assuming that the defense was able to evaluate $\Pi_D(A^1)$, where A^1 represents the attacker's decision in the second level of the recursive defense thinking.

$$D \mid A^1 \sim \arg\max_{d \in D} \sum_{a \in A} \left[\sum_{s \in \{0,1\}} U_D(d,s) P_D(S = s \mid d,a) \right] \times \prod_D (A^1 = a) \qquad (4)$$

To evaluate the distribution of the random variable $D \mid A^1$, the defense would need the probability distribution that governs the random variable $U_D(d,s)$, representing its beliefs as to how the attacker could have estimated the utility function $u_D(d,s)$. Generally speaking, this process would require future recursive thoughts on the part of the defender. This hierarchy of nested models would find a limit when it reached a level where it lacked information necessary for the defender to continue to feed the equations associated with the computations of A^i and D^i $(i=1,2,3,...)$. In this case, the use of a non-informative probability distribution (such as the maximum entropy distribution) associated with the uncertain parameters would be sufficient to represent them (Rios & Insua, 2011).

4 A simulated ARA case

The purpose of this example is mainly to detail how an application of the ARA approach is conducted. Therefore, in this simulated case, little attention will be paid to the way in which the assumed hypothetical values were chosen to define the adopted probability distributions. Likewise, it will not be discussed how the utility functions adopted were constructed. Nor will the simulation techniques used in this example be analyzed.

It is considered here a hypothetical situation where the defense must protect a stadium, where a sporting event will occur, against possible terrorist attacks. For this, it is assumed that the defense needs to choose one of the "packages of defensive measures" that are being offered by companies specializing in public safety for the protection of the stadium. It is considered that such packages are the elements of a set $D=\{d_1,d_2,d_3\}$. Each of these packages have their differences in purchase price and are more or less efficient against different types of attacks that can be carried out. The defense wants to adopt the package of defensive measures that will minimize the expected damage.

On the other hand, the attacker must decide on what type of attack to perform. Attack types are defined as elements of a set $A=\{a_1,a_2,a_3\}$. Attacks that result in greater effects in terms of damage, return the greatest benefits to the terrorist organization and, at the same time, are costlier. Besides, when frustrated (unsuccessful attack), these attacks result in heavy losses for these organizations.

4.1 Rewards and probabilities of success and failure when attacks occur

In this example, the utility function $u_D(d,s)$ is influenced by the defensive package choice and also by the result of the attack. Defense perceives its rewards in such a way that gains are associated with the attacker's failure to perform the attack and losses are associated with situations where the attack occurs successfully. However, defense counts on the costs associated with adopting defensive measures packages. In addition, there may be specific losses when adopting certain packages, such as: disorder for the population and discomfort of public opinion regarding the security scheme. The utility values assumed for the defense are presented in Chart 2.

On the other hand, the attacker computes his rewards according to the caused damages, the mobilization costs of the necessary resources to carry out the attack, and the losses it may cause to its own resources. This parameter can encompass various values represented in tangible forms as money and the number of member recruitment to terrorist organizations, or intangibles such as fame and satisfaction (Quadrifoglio, 2008; Sri Bhashyam & Montibeller, 2012). The defense, however, cannot define, in a deterministic way, the utility $u_A(a,s)$ that is adopted by the attacker. It is possible that the defense has historical and intelligence information about the activities carried out by the threatening terrorist organization. This information can be included in the estimates that the defense must carry out as to how the attacker could be assessing its rewards for each type of attack that could be carried out (Ezell et al., 2010). In the same way, this information can guide the defense as to how the attacker would be assessing the odds of success when each type of attack was being executed. Therefore, it is believed that it is possible to carry out an evaluation, by defense specialists, on a random variable distribution $U_A(a,s)$ that will represent the utility $u_A(a,s)$ adopted by the attacker. Chart 3 represents the triangular distributions (Tri (minimum, fashion, maximum)) used here to describe the behavior of the random variable $U_A(a,s)$.

It is assumed that, with the support of specialists, the defense can establish how much the target (in this case a stadium) is vulnerable to each type of attack the opponent can perform. This vulnerability depicts the attacker's probability of success in attacking the target. The probability values assumed by the defense for the success and failure of the attacker when it chooses to use each type of attack and the defense adopts each of the packages of defensive measures are presented in Chart 4.

The defense needs to estimate how the attacker would be assessing the odds of success and failure when it chooses to use each type of attack and considers the defense to be adopting each of the defensive packages. In this example, it is assumed that the defense's beliefs lead it to consider that the attacker has very similar target vulnerability assessment capabilities to that of the attacker. It is also assumed that there is no information about the efficiency of the considered defensive measures. Then, it is adopted that the defense is satisfied by considering that its uncertainty as to how the attacker would estimate its probabilities of success and failure (for each leaf of the tree) can be represented by a uniform probability distribution (U (minimum; Maximum)) with the following characteristics. First, the mean value of this distribution is exactly the value of $p_D(S=s\,|d,a)$. Second, the upper limit value of this distribution is given by $p_D(S=s\,|d,a)+0.2$, just as the lower limit value is given by $p_D(S=s\,|d,a)-0.2$. Thus, the distributions to be taken into account to represent

Chart 2. Values of utility assumed for the defense.

Protection	s_0 (utility)	s_1 (utility)
d_1	55	–45
d_2	40	–60
d_3	65	–35

Chart 3. Probability distributions that represent the attacker's rewards.

Attack Types	s_1 (probability)	s_0 (probability)
a_1	Tri(35; 55; 75)	100-[u(a_1;s_1)]
a_2	Tri(20; 40; 60)	100-[u(a_2;s_1)]
a_3	Tri(45; 65; 85)	100-[u(a_3;s_1)]

Chart 4. Probability values assumed by the defense for the success and failure of the attacker.

Success and failure probabilities		s_0	s_1
d_1	a_1	30%	70%
	a_2	20%	80%
	a_3	55%	45%
d_2	a_1	35%	65%
	a_2	25%	75%
	a_3	35%	65%
d_3	a_1	35%	65%
	a_2	40%	60%
	a_3	25%	75%

the value of the random variable $P_A(S=s\,|d,a)$, in each branch of the decision tree of the attacker, are shown in Chart 5. It is observed, however that since success and failure are the only two outcomes for the attack, it is considered here that the value assumed by the random variable $P_A(S=s\,|d,a)$ for success cases of the attack (s_1) is given by the complementary value of the probability assigned to failure cases.

Finally, the defense should precise its beliefs about how the attacker would be assessing its likelihood to adopt each package of defensive measures. In this example, it is considered that the defense does not have any information that could be significant to aid in the evaluation of these probabilities. Thus, it is defined here that the random variable represented by $\Pi_A + A(D=d)$ should be governed by the maximum entropy probability distribution, that is, the uniform distribution $U(0,1)$.

4.2 The solution of the defense decision problem

Initially, it is perceived that an intuitive way of starting the solution of the proposed problem would be an inverse order approach. This means that the first response to be sought is how the random variable $A\,|\,D$ would behave (Equation 3). Applying Monte Carlo simulation (in this example, 10,000 iterations were performed), it was observed that the random variable behaved as shown in the histogram from Figure 4.

It is concluded from the results presented that in approximately 8.85% of the times the attacker would choose to carry out the attack type a_1; 4.63% of the time would opt for a_2; and at 86.52% of the time it would choose a_3. Such values could be considered satisfactory enough to represent the values of $\pi_D(A=a)$. However, it can be admitted here that the defense, in its inmost, presents certain confidence on the obtained values. Therefore, it is assumed that the defense prefers to establish a probability distribution to represent the now random variable $\prod_D(A=a)$.

Chart 5. Probability distributions for success and failure of the attacker from the defense point of view.

Probability distribution		s_0	s_1
d_1	a_1	U(0.1, 0.5)	Complementary
	a_2	U(0.2, 0.6)	Complementary
	a_3	U(0.35, 0.75)	Complementary
d_2	a_1	U(0.15, 0.55)	Complementary
	a_2	U(0.05, 0.45)	Complementary
	a_3	U(0.15, 0.55)	Complementary
d_3	a_1	U(0.15, 0.55)	Complementary
	a_2	U(0.20, 0.60)	Complementary
	a_3	U(0.05, 0.45)	Complementary

For the example in question, it is assumed that the defense chooses to adopt a Beta-type distribution to incorporate this confidence into its analyzes. It is considered $Be\,(a;\,b)$, where a and b are the format parameters of this distribution, with mean $\pi_D(A=a)$ and a given precision (η). By definition one has that $\eta = a+b$, that is, $Be\,(a;\ \eta-a)$. By rearranging the equations presented by Myriam & Pongo (1997) one can define that the mean (μ) of a Beta distribution is given by Equation 5 and its variance (σ^2) is defined by Equation 6, both presented below:

$$\mu = \frac{a}{a+b} \tag{5}$$

$$\sigma^2 = \frac{ab}{(a+b+1)(a+b)^2} \tag{6}$$

One can then define the parameters a e b in function of $\mu e \sigma^2$.

It is adopted, in this particular case, that the defense established that a standard deviation of 10% over the average value would be enough to represent its confidence in the results obtained by the performed simulation. Hence, $\sigma = \frac{\mu}{10}$. The parameters a, b, and μ are presented in Chart 6. Therefore, parameters of $\prod_D(A=a)$ are defined, that is, the way the defense believes that the probabilities of the attacker to adopt each type of attack behave, $a\ to \in A$.

Now, it can be said that the defense has all the information it needs to solve its original problem. The utility values adopted by the defense are presented deterministically. However, the defense chooses to use probability distributions to contemplate uncertainties about its assessments of the likelihood of success and failure of an attack. Thus, it represents these values by triangular probability distributions, as shown in Chart 7.

The probabilities associated with the attacker's choice attacker will be given by the probability distributions presented in Chart 6, thus being considered random variables ($\prod_D(A=a)$). Equation 7 illustrates

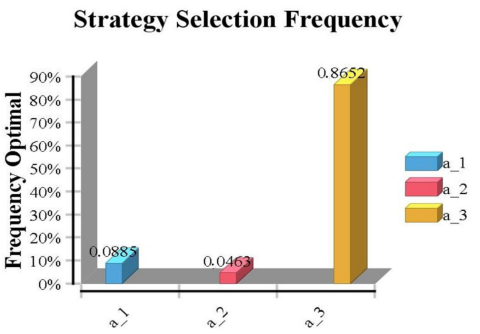

Figure 4. Occurrences of a_1, a_2 and a_3 with the Monte Carlo simulation.

Chart 6. $\prod_D(A=a) \sim Be(a;b)$ parameter values adopted by the defense.

	μ	A	B	H	$\prod_D(A=a)$
a_1	0.0885	91.06	937.88	1028.94	$Be(91,06;937,88)$
a_2	0.0463	95.32	1963.50	2058.83	$Be(95,32;1963,50)$
a_3	0.8652	12.61	1.9654	14.58	$Be(12,61;1,9654)$

Chart 7. Probability distributions to represent defense beliefs about success and failure of an attack.

Probability Distribution		s_0	s_1
d_1	a_1	Tri (0.10; 0.30; 0,50)	Complementary
	a_2	Tri (0; 0.20; 0.40)	Complementary
	a_3	Tri (0.35; 0.55; 0.75)	Complementary
d_2	a_1	Tri (0.15; 0.35; 0.55)	Complementary
	a_2	Tri (0.05; 0.25; 0.45)	Complementary
	a_3	Tri (0.15; 0.35; 0.55)	Complementary
d_3	a_1	Tri (0.15; 0.35; 0.55)	Complementary
	a_2	Tri (0.20; 0.40; 0.60)	Complementary
	a_3	Tri (0.05; 0.25; 0.45)	Complementary

how the defense solves its problem, *i.e.*, how it chooses which of the three alternatives (packages of defensive measures) is the one that returns the highest expected utility value. Applying a new Monte Carlo simulation for the parameters of Equation 7 it is possible to estimate the frequencies with which each of its options returns the highest expected utility value, when adopted by the defense. These results are presented in Figure 5.

$$D \mid A \sim arg\max_{d \in D} \sum_{a \in A} \left[\sum_{s \in \{0,1\}} u_D(d,s) P_D(S=s \mid d,a) \right] \times \prod_D \qquad (7)$$

With these results, in a prescriptive view (Merrick & Parnell, 2011; Rothschild et al., 2012) the advice given to the defense is that its resources should be allocated to acquire the package of measures d_1. This option would return the highest value for the expected defense utility in approximately 93% of the simulations that were performed.

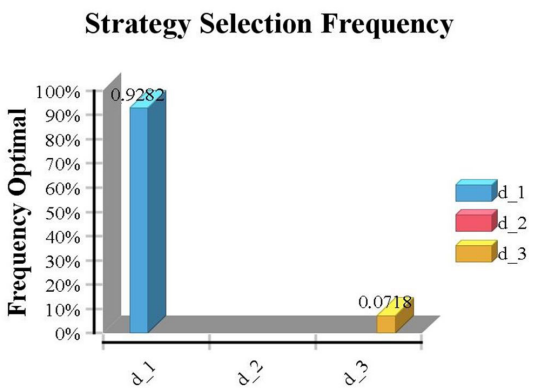

Figure 5. Occurrences of d1, d2 and d3 with the Monte Carlo simulation.

5 Discussion

Primarily, a difference and, at the same time, advantage to the ARA approach, when compared to the classic application of Game Theory and PRA, is that the descriptions of the attacker's behavior are not input data for the problem to be solved. According to Merrick & Parnell (2011), works starting from the premise that these values are given, usually adopt subjective probability distributions that come from specialists, which are, in most cases, very generic. That is what ARA addresses, allowing for precisely finding such probabilities. For this, the model requires as input the beliefs the defense has about how opponents perceive the consequences of the attacks (rewards) and the chances of success for these attacks, which in this research, as advocated by Merrick & Parnell (2011), is judged to be much more realistic and feasible. Banks (2011) comments that it would be perfectly reasonable to imagine that players have relevant probabilistic knowledge about the values and beliefs their opponents hold. This knowledge could be, for instance, derived from studies conducted by the intelligence community. On the other hand, it is important to note that some factors encompassed in the illustrated example should be analyzed in relation to their variation, as in a type of sensitivity analysis. Another aspect that deserves attention is related to the degree of uncertainty that was attributed by the

defender to the attacker's utility values when they were defined for the representation of this random variable (UA). In the same way, interesting analyzes may arise when studying the variations of the probability distributions associated to the attacker's successes and failures, when evaluated by the attacker, according to the point of view of the defense. Interesting analyzes of rewards values attributed to terrorist attacks are available in Keeney (2007), Dillon et al. (2009), Keeney & Winterfeldt (2011).

If the information obtained from defense specialists was more accurate, it would be natural for the analyzes to contemplate a lower level of uncertainty and therefore to be more reliable. Although the reduction of uncertainties inherent to the information can be obtained through the results collected by the intelligence services that support the defense, Banks (2011), Rios & Insua (2011) point out that the provision of information for the method proposed by ARA is still considered a great challenge. This fact is important to be observed and should be explored in future work, since decisions to allocate defense resources will be closely linked to the quality and reliability of the information.

Another interesting analysis could be performed in relation to the mirroring procedure proposed in the ARA approach. What would be the level of recursion that this model should achieve? In the illustrated example, we opted to explore only up to the second level of recursive defensive thinking. However, a survey that delves into other levels of recursion, both in modeling the problem faced by defense and by the attack, could bring interesting results in future research. Some works, such as Farias (2013), explore this subject, including verifying the convergence of results for games with complete information, as well as those with incomplete information.

Thus, it is concluded that ARA has a structure to evaluate risks offered by intelligent opponents with the advantage of embedding asymmetric information in the models of the players. In addition, ARA rules out the need for experts to provide subjective judgments about the likely strategies to be adopted by opponents, since the model itself defines a probabilistic description of them. At the same time, however, it lacks a considerable amount of information about opponents, which can still be seen as a fragility of the proposal.

6 Final considerations

This article aimed to present a new risk assessment approach to support the allocation of antiterrorism resources. The two main approaches traditionally used to support this type of decision were reviewed. Firstly, in analyzing the applications of Probabilistic Assessment of Risks, the authors concluded that, although being the theory currently used to guide the US government's decisions on how to allocate antiterrorism resources, there are some relevant caveats to its applicability. The main one is not considering the opponent as adaptive and strategic, thus not regarding how it will behave after observing how the defense allocates its resources. Secondly, the analysis focused on research work based on Game Theory. In this case, the opponent takes into account the defense actions when choosing his or her strategy, however, it is discarded the possibility of considering intelligence information and other sources, which may be relevant for modeling the agents involved in the game. Moreover, it considers the availability of information about the opponent as a premise, what, in fact, is known to be very critical to obtain. As an alternative, the authors propose the use of Adversarial Risk Assessment (ARA). This recent approach can be seen as a contribution of potential applications and as relevant to academia, specially in the Brazilian context. Lastly, a simulated case was presented to illustrate the application of ARA. The presented application clarified how the odds of the opponents' actions can be estimated before the defense calculates its maximum expected utility. This allows a more realistic and, at the same time, simpler treatment of the decision-making environment when it comes to counterterrorism, which is an advantage that ARA holds in face of classic applications of Game Theory.

This paper advocates that in situations where there is little experience in counterterrorism, it is important to emphasize that the planning of activities aimed at reducing the occurrence of an attack is different from mitigating the risks of natural disasters. Therefore, in mega sporting events, for example, the protection of infrastructure, world authorities and the public, needs to be planned taking into account the adaptive characteristics of the opponent that is being faced. The authors agree with Rios & Insua (2011) that the creation of a conceptual structure such as that presented (ARA) is only a necessary and relevant first step that allows for significant improvements, which can be applicable to real situations.

As a final conclusion, the authors advocate that the in-depth exploration of this new approach may bring new ideas to be added to the traditional approaches proposed by Game Theory. Therefore, the structure presented can be considered as a contribution to the area of study on risk assessment, not only in the terrorism-related contexts, but also in any situation where two parties oppose themselves and react strategically and intelligently to each other's actions.

Acknowledgements

The authors thank Dr João José de Farias Neto researcher at the Institute for Advanced Studies and Amaury Caruzzo from the Decision Analysis Studies Group - GEAD (Instituto Tecnológico de Aeronáutica)

for the contributions provided by relevant discussions on the subject.

References

Ayyub, B. M., Mcgill, W. L., & Kaminskiy, M. (2007). Critical asset and portfolio risk analysis: an all-hazards framework. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 27(4), 789-801. http://dx.doi.org/10.1111/j.1539-6924.2007.00911.x.

Banks, D. (2009, Junho). Adversarial risk analysis: decision making when there is uncertainty during conflict. *IHSS Research Brief*, 1-8.

Banks, D. (2011). *Adversarial risk analysis for dynamic network routing*. Durham: Duke University. Recuperado em 11 de novembro de 2013, de http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA547011

Banks, D., & Anderson, S. (2006). Combining game theory and risk analysis in counterterrorism: a smallpox example. In A. G. Wilson, G. D. Wilson & D. H. Olwell *(Eds.), Statistical methods in counterterrorism* (pp. 9-22). New York: Springer.

Banks, D., Petralia, F., & Wang, S. (2011). Adversarial risk analysis: analyses of borel games. *Applied Stochastic Models in Business and Industry*, 27(2), 72-86. http://dx.doi.org/10.1002/asmb.890.

Bier, V. M. (2006). Game-theoretic and reliability methods in counter-terrorism and security. In In A. G. Wilson, G. D. Wilson & D. H. Olwell *(Eds.), Statistical methods in counterterrorism* (pp. 23-40). New York: Springer.

Bier, V. M., Haphuriwat, N., Menoyo, J., Zimmerman, R., & Culpen, A. M. (2008). Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 28(3), 763-770. http://dx.doi.org/10.1111/j.1539-6924.2008.01053.x.

Bier, V. M., Oliveros, S., & Samuelson, L. (2007). Choosing what to protect: strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, 9(4), 563-587. http://dx.doi.org/10.1111/j.1467-9779.2007.00320.x.

Brown, G. G., & Cox, L. A., Jr (2011). How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 31(2), 196-204. http://dx.doi.org/10.1111/j.1539-6924.2010.01492.x.

Brown, G. G., Carlyle, M. W., Salmerón, J., & Wood, K. (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In H. J. Greenberg & J. C. Smith (Eds.), *Tutorials in operations research: emerging theory, methods, and applications* (pp. 102-123). Catonsville: INFORMS.

Buzanelli, M. P. (2004). Introdução. In Secretaria de Acompanhamento e Estudos Institucionais, *II Encontro de Estudos: terrorismo*. Brasília: Gabinete de Segurança Institucional. 123 p.

Camargo, C. A. (2011). *Planejamento da segurança antiterrorismo na copa do mundo.* São Paulo: Visão Consultoria. Recuperado em 11 de novembro de 2013, de http://www.universidadedofutebol.com.br/Artigo/15062/Planejamento-da-seguranca-antiterrorismo-na-Copa-do-Mundo

Cox, L. A. (2009a). Improving risk-based decision making for terrorism applications. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 29(3), 336-341.

Cox, L. A., Jr (2009b). Game theory and risk analysis. *Risk Analysis*, 29(8), 1062-1068. http://dx.doi.org/10.1111/j.1539-6924.2009.01247.x.

Cox, L. A., Jr (2008). Some limitations of "Risk = Threat x Vulnerability x Consequence" for risk analysis of terrorist attacks. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 28(6), 1749-1761. http://dx.doi.org/10.1111/j.1539-6924.2008.01142.x.

Cox, L. A. (2012). Evaluating and improving risk formulas for allocating limited budgets to expensive risk-reduction opportunities. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 32(7), 1244-1252.

Dillon, R. L., Liebe, R. M., & Bestafka, T. (2009). Risk-based decision making for terrorism applications. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 29(3), 321-335. http://dx.doi.org/10.1111/j.1539-6924.2008.01196.x.

Diniz, E. (2004). Considerações sobre a possibilidade de atentados terroristas no Brasil. In Secretaria de Acompanhamento e Estudos Institucionais, *II Encontro de Estudos: terrorismo*. Brasília: Gabinete de Segurança Institucional. 123 p.

Ellis, G. (2009). Grand challenges for engineering. *IEEE Engineering Management Review*, 37(1), 3-3. http://dx.doi.org/10.1109/EMR.2009.4804341.

Ezell, B. C., Bennett, S. P., von Winterfeldt, D., Sokolowski, J., & Collins, A. J. (2010). Probabilistic risk analysis and terrorism risk. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 30(4), 575-589. http://dx.doi.org/10.1111/j.1539-6924.2010.01401.x.

Farias, J. J., No. (2013). Can adversarial risk analysis define a new equilibrium concept in games? In *Proceedings of the INFORMS Annual Meeting*. Minneapolis: INFORMS.

Farrow, S. (2007). The Economics of homeland security expenditures: foundational expected cost-effectiveness approaches. *Contemporary Economic Policy*, 25(1), 14-26. http://dx.doi.org/10.1111/j.1465-7287.2006.00029.x.

Fiani, R. (2006). *Teoria dos jogos*. Rio de Janeiro: Elsevier.

Gigerenzer, G., & Reinhard, S. (2001). *Bounded rationality: the adaptive toolbox*. Cambridge: The MIT Press.

Insua, D. R., Rios, J., & Banks, D. (2009). Adversarial risk analysis. *Journal of the American Statistical Association*, 104(486), 841-854. http://dx.doi.org/10.1198/jasa.2009.0155.

Jennings, W., & Lodge, M. C. (2012). The Olympic Games: coping with risks and crises at a mega-event. In I. Helsloot, A. Boin, B. Jacobs & L. K. Comfort *(Eds.) Mega-Crises: Understanding the Prospects, Nature, Characteristics and Effects of Cataclysmic Events* (pp. 263-278). Springfield: Charles C. Thomas Publisher.

Kardes, E., & Hall, R. (2005). *Survey of literature on strategic decision-making in the presence of adversaries* (Paper 115). Los Angeles: Center for Risk and Economic Analysis of Terrorism Events. Recuperado em 2 de maio de 2012, de http://www.usc.edu/dept/create/assets/001/50765.pdf

Keeney, R. L. (2007). Modeling values for anti-terrorism analysis. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 27(3), 585-596.

Keeney, R. L., & Winterfeldt, V. D. A value model for evaluating homeland security decisions. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 31(9), 1470-1487, 2011.

Kleinmuntz, D. N., & Willis, H. (2009). *Risk-based allocation of resources to counter terrorism* (Research Project Summaries, 37). Los Angeles: Center for Risk and Economic Analysis of Terrorism Events.

Kunreuther, H., Michel-Kerjan, E., & Porter, B. (2013). *Assessing, managing and financing extreme events: dealing with terrorism* (NBER Working Paper, No. 10179). Cambridge: NBER.

Major, J. A. (2002). Advanced techniques for modeling terrorism risk. *The Journal of Risk Finance*, 4(1), 15-24. http://dx.doi.org/10.1108/eb022950.

McLay, L., Rothschild, C., & Guikema, S. (2012). Robust adversarial risk analysis: a level-k approach. *Decision Analysis*, 9(1), 41-54. http://dx.doi.org/10.1287/deca.1110.0221.

Merrick, J. R. W., & Parnell, G. S. (2011). A comparative analysis of PRA and intelligent adversary methods for counterterrorism risk management. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 31(9), 1488-1510. http://dx.doi.org/10.1111/j.1539-6924.2011.01590.x.

Myriam, R., & Pongo, R. (1997). Uma metodologia bayesiana para estudos de confiabilidade na fase de projeto: aplicação em um produto eletrônico. *Gestão & Produção*, 4(3), 305-320.

Nikoofal, M. E., & Zhuang, J. (2011). Robust allocation of a defensive budget considering an attacker's private information. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 32(5), 930-943. http://dx.doi.org/10.1111/j.1539-6924.2011.01702.x.

Parnell, G. S., Smith, C. M., & Moxley, F. I. (2010). Intelligent adversary risk analysis: a bioterrorism risk management model. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 30(1), 32-48. http://dx.doi.org/10.1111/j.1539-6924.2009.01319.x.

Pat-Cornell, E., & Guikema, S. (2002). Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. *Military Operations Research*, 7(4), 5-23. http://dx.doi.org/10.5711/morj.7.4.5.

Paté-Cornell, E. (2007). Probabilistic risk analysis versus decision analysis: similarities, differences and illustrations. In M. Abdellaoui, R. D. Luce, M. J. Machina & B. Munier (Eds.), *Uncertainty and Risk* (Theory and Decision Library C, Vol. 41, pp. 223-242). New York: Springer.

Powell, R. (2007a). Defending against terrorist attacks with limited resources. *The American Political Science Review*, 101(3), 527-541. http://dx.doi.org/10.1017/S0003055407070244.

Powell, R. (2007b). Allocating defensive resources with private information about vulnerability. *The American Political Science Review*, 101(04), 799-809. http://dx.doi.org/10.1017/S0003055407070530.

Quadrifoglio, L. (2008). A Bottom-up risk-based resource allocation methodology to counter terrorism. *International Journal of Society Systems Science*, 1(1), 4. http://dx.doi.org/10.1504/IJSSS.2008.020043.

Richardson, L. (2007). What terrorists want. *Rennerinstitutat*, 13(1), 1-6.

Rios, J., & Insua, D. R. (2011). Adversarial risk analysis for counterterrorism modeling. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 32(5), 894-915. http://dx.doi.org/10.1111/j.1539-6924.2011.01713.x.

Rothschild, C., McLay, L., & Guikema, S. (2012). Adversarial risk analysis with incomplete information: a level-k approach. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 32(7), 1219-1231. http://dx.doi.org/10.1111/j.1539-6924.2011.01701.x.

Sandler, T., & Arce, M. (2003). Terrorism & game theory. *Simulation & Gaming*, 34(3), 319-337. http://dx.doi.org/10.1177/1046878103255492.

Sandler, T., & Siqueira, K. (2008). Games and terrorism: recent developments. *Simulation & Gaming*, 40(2), 164-192. http://dx.doi.org/10.1177/1046878108314772.

Sebenius, J. K. (1992). Negotiation analysis: a characterization and review. *Management Science*, 38(1), 18-38. http://dx.doi.org/10.1287/mnsc.38.1.18.

Sebenius, J. K. (2006). Negotiation Analysis: Between Decisions and Games. In W. E. R. Miles & D. Von Winterfeldt (Eds.), *Advances in decision analysis* (pp. 469-488). New York: Cambridge University Press.

Sevillano, J. C., Rios Insua, D., & Rios, J. (2012). Adversarial risk analysis: the somali pirates case. *Decision Analysis*, 9(2), 86-95. http://dx.doi.org/10.1287/deca.1110.0225.

Shan, X., & Zhuang, J. (2012). Cost of equity in homeland security resource allocation in the face of a strategic

attacker. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 33(6), 1083-1099. https://doi.org/10.1111/j.1539-6924.2012.01919.x.

Sri Bhashyam, S., & Montibeller, G. (2012). Modeling state-dependent priorities of malicious agents. *Decision Analysis*, 9(2), 172-185. https://doi.org/10.1287/deca.1120.0237

Ushakov, I. (2006). Counter terrorism: protection resources allocation. *Reliability: Theory & Applications*, 1(2), 71-78.

Wang, C., & Bier, V. M. (2011). Target-hardening decisions based on uncertain multiattribute terrorist utility. *Decision Analysis*, 8(4), 286-302. http://dx.doi.org/10.1287/deca.1110.0218.

Wang, S., & Banks, D. (2011). Network routing for insurgency: an adversarial risk analysis framework. *Naval Research Logistics*, 58(6), 595-607. http://dx.doi.org/10.1002/nav.20469.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis*, 27(3), 597-606. http://dx.doi.org/10.1111/j.1539-6924.2007.00909.x.

Willis, H. H., Morral, A. R., Kelly, T. K., & Medby, J. J. (2005). *Estimating terrorism risk*. Santa Monica: Rand Corporation.

Winterfeldt, V. D., & O'Sullivan, T. M. (2006). Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? *Decision Analysis*, 3(2), 63-75. http://dx.doi.org/10.1287/deca.1060.0071.

Woo, G. (2002). Quantitative terrorism risk assessment. *The Journal of Risk Finance*, 4(1), 7-14. http://dx.doi.org/10.1108/eb022949.

Zhuang, J., & Bier, V. M. (2007). Balancing terrorism and natural disasters: defensive strategy with endogenous attacker effort. *Operations Research*, 55(5), 976-991. http://dx.doi.org/10.1287/opre.1070.0434.

Zhuang, J., & Bier, V. M. (2010). Reasons for secrecy and deception in homeland-security resource allocation. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 30(12), 1737-1743. http://dx.doi.org/10.1111/j.1539-6924.2010.01455.x.