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

Análise de Risco Adversário para alocação de recursos de contraterrorismo

Adversarial Risk Analysis in support of defensive resource allocation for counterterrorism

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

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.

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.*

1 Introdução

O Brasil é um país que vem crescendo, expondo-se cada vez mais no cenário mundial. Assim, a tendência é que o Brasil seja cada vez mais requisitado para sediar eventos de grandes proporções como aconteceu, por exemplo, por ocasião da Copa do Mundo de Futebol de 2014 e dos recém-realizados Jogos Olímpicos de 2016, na cidade do Rio de Janeiro. Megaeventos esportivos como os enumerados têm características intrínsecas que os tornam extremamente simbólicos (Jennings & Lodge, 2012). Camargo (2011) comenta que megaeventos esportivos são eventos que, além de envolverem enorme audiência, provocam concentração de nacionalidades diversas. Eventos desse porte reúnem autoridades representando Estados e governos, empresários e outras pessoas emblemáticas de condições que podem catalisar ódios, preconceitos etc. Assim, é possível apontar que eventos dessa magnitude podem mostrar-se atrativos para grupos terroristas que queiram perpetrar ataques com o objetivo de dar visibilidade à sua causa, projetando-a em âmbito internacional. Na maioria das vezes, tais grupos realizam seus ataques visando fama, reconhecimento de suas causas e, em alguns casos, vingança (Richardson, 2007). Com essa visão, embora

[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, Brasil, 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, Brasil, 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

Recebido em Out. 24, 2015 - Aceito em Maio. 15, 2016

Suporte financeiro: Nenhum.

não seja exatamente alvo, o Brasil, quando serve de palco para megaeventos como os comentados, pode ser cenário do terrorismo internacional (Diniz, 2004).

É interessante notar que a história mostra que grandes eventos esportivos têm sido escolhidos de forma frequente como teatro de operações por grupos terroristas, atentados como a bomba no Parque Centenário durante a Olimpíada de Atlanta de 1996; a explosão de um carro bomba nas imediações do estádio Santiago Bernabéu, no jogo semifinal da UEFA Champions League de 2002; o atentado suicida da maratona no Sri Lanka, em 2008, e, entre outros, o ataque à seleção do Togo, em 2010, quando homens armados abordaram a tiros o ônibus em que se encontravam os jogadores. Ainda, mais recentemente, os acontecimentos nos Estados Unidos no dia 15 de abril de 2013 (ataques terroristas na Maratona de Boston) indicam que a prática terrorista, aproveitando como palco grandes eventos esportivos é uma modalidade que vem se repetindo de forma frequente no âmbito internacional.

Historicamente, o Brasil não possui grande experiência no gerenciamento do assunto terrorismo e não conta com iniciativas, planejamentos e políticas que inibam práticas do terrorismo, como Inglaterra, Israel e Estados Unidos da América. Em tais países, a ameaça relativa a possíveis atentados terroristas tem motivado investimentos de bilhões de dólares, com o objetivo de melhorar a segurança pública (Kardes & Hall, 2005). Alguns estudos sobre o tema (Buzanelli, 2004) criticam o baixo nível de atenção dispensada, por parte dos órgãos governamentais brasileiros, ao assunto terrorismo e, aqui, especificamente, aponta-se a alocação de recursos para a proteção antiterrorismo como tema importante e merecedor de maior atenção.

Como apontado por Willis (2007), esforços relacionados à alocação de recursos para a consecução de atividades antiterroristas estão conectados de forma íntima com a necessidade de se avaliar riscos. Grande parte do desafio apresentado neste trabalho deriva do fato de que, diferentemente de ameaças naturais (ex.: fenômenos meteorológicos intensos) ou sistemas de engenharia (ex.: falhas em componentes sistêmicos), os riscos que devem ser avaliados são proporcionados por adversários inteligentes (como é o caso das organizações terroristas) e, por isso, as chances avaliadas nesse contexto deixam de ser regidas pelo acaso (Ayyub et al., 2007; Brown & Cox, 2011; Parnell et al., 2010; Zhuang & Bier, 2007). Afinal, a natureza pode ser sutil, mas não é maliciosa. Os terroristas, por outro lado, são tanto sutis quanto mal-intencionados (Woo, 2002). Em outras palavras, terroristas podem se adaptar a diferentes medidas que venham a ser adotadas para enfrentá-los (Cox, 2009a, b, 2012). Por isso, nem sempre as abordagens tradicionais usadas para a avaliação de riscos são suficientes para balizar a alocação de recursos visando o antiterrorismo.

Portanto, este artigo tem como objetivo principal apresentar para a comunidade científica brasileira a abordagem de pesquisa recentemente divulgada internacionalmente: Análise do Risco Adversário (ARA – Adversarial Risk Analysis) (Banks, 2009, 2011; Rios & Insua, 2011). Acredita-se que a introdução dessa ferramenta, que visa apoiar a avaliação dos riscos proporcionados por oponentes inteligentes, é uma contribuição relevante para a academia nacional. Enfatiza-se que, até o presente, no conhecimento dos autores, o assunto é inédito no Brasil.

O presente artigo apresenta, inicialmente, uma breve revisão das duas principais abordagens que constam na literatura a respeito de alocação de recursos para o gerenciamento do risco de ataques terroristas: Avaliação Probabilística de Riscos e Teoria dos Jogos. Na sequência, a proposta ARA é apresentada e um exemplo simulado ilustra a aplicação dessa abordagem. O artigo é encerrado com considerações sobre as vantagens que a ARA apresenta quando comparada com as duas abordagens comentadas anteriormente. Adicionalmente, enfatizam-se as contribuições que a abordagem ARA pode trazer e, finalmente, apresentam-se os desafios ainda a serem explorados em relação à proposta da ARA, os quais podem balizar futuras pesquisas.

2 O problema de alocação de recursos de defesa antiterrorismo

2.1 Avaliação Probabilística de Risco

A Avaliação Probabilística de Risco (PRA – Probabilistic Risk Assessment) vem sendo empregada por mais de 30 anos para avaliar os riscos (probabilidades e consequências da falha de um sistema) e orientar decisões relacionadas à gestão de riscos na área governamental e industrial, em diversas situações, como, por exemplo: na proteção do meio ambiente, na segurança industrial e em procedimentos médicos (Ezell et al., 2010; Paté-Cornell, 2007). Em termos de riscos de terrorismo, modelos construídos com base na abordagem PRA, normalmente, têm por objetivo estimar a diferença do risco que cada alvo em potencial corre, quando esses não contam e, depois, quando contam com as diversas medidas de proteção que podem ser adotadas. Então, como resultado, obtém-se uma ordenação dos riscos avaliados (*risk-scoring*), viabilizando a priorização na alocação dos recursos disponíveis (Ayyub et al., 2007; Cox, 2009a; Paté-Cornell, 2007; Willis et al., 2005).

De modo a operacionalizar a aplicação de PRA, grande parte dos trabalhos adotam como principal referência o modelo Risk Analysis and Management for Critical Asset Protection (RAMCAPTM) (Cox, 2008). Nesse modelo, uma estrutura conceitual

para o cômputo do risco (R) é sugerida como função de uma ameaça (A) existente, uma vulnerabilidade (V) apresentada por um alvo e uma consequência (C) para um ataque sofrido, ou seja, R = f (T, V, C) (Dillon et al., 2009).

Alguns casos interessantes em que PRA foi aplicada podem ser observados em, por exemplo, Willis et al. (2005), que comparam os resultados obtidos quando considera-se o uso da referida função com os resultados decorrentes do computo do risco considerando-se indicadores simples (por exemplo, população de uma região e densidade populacional ponderada de uma região). Os autores concluem que no primeiro caso os riscos se mostram mais concentrados em determinadas regiões urbanas do que no segundo caso. Winterfeldt & O'Sullivan (2006) e Kleinmuntz & Willis (2009) também se aprofundam no uso da função f (T, V, C) como indicadora de risco e analisam as incertezas que os parâmetros considerados na análise podem englobadar.

Não obstante diversas pesquisas proponham a aplicação da abordagem PRA, ainda permanecem alguns questionamentos que podem sugerir que ela não seria a mais indicada para lidar com a alocação de recursos de defesa visando o antiterrorismo. Por exemplo, Cox (2009a) comenta que bastaria que o terrorista soubesse que uma análise como a proposta pela abordagem PRA está sendo realizada para inferir que alvos com características semelhantes iriam receber prioridade semelhante na alocação de recursos para a proteção antiterrorismo. Uma informação como essa poderia ser valiosa para os atacantes, pois poderiam inferir o nível de proteção destinado a cada alvo. Cox (2009a) também aponta que métodos como PRA não permitem a exploração do sigilo, não levam em conta restrições orçamentárias que podem existir (não só para a defesa como também para os atacantes) e desconsideram o fato de que proteger um alvo muda a probabilidade de ataques a outros alvos. Por exemplo, como apontado por Sandler & Siqueira (2008), a instalação de detectores de metal em aeroportos em 5 de janeiro de 1973 resultou em uma queda vertiginosa no número de sequestros de aeronaves. No entanto, a partir desse momento foi possível notar uma grande diversificação nas táticas empregadas por organizações terroristas. Parnell et al. (2010) e Cox (2009a) apontam criticamente que PRA ignora o que o atacante vai fazer depois que as medidas de defesa são alotadas. Tal atitude equivale a descartar o fato de que os terroristas são inteligentes e que podem adaptar-se às medidas defensivas adotadas.

Isso posto, é possível concluir que, embora a abordagem PRA seja capaz de contribuir significativamente para apoiar a alocação de recursos para o enfrentamento/mitigação dos riscos em estudos antiterrorismo, algumas lacunas ainda não foram completamente preenchidas e, por isso, futuros estudos são necessários nesse campo. Alguns trabalhos buscaram na conhecida Teoria dos Jogos alternativas para eliminarr tais lacunas.

2.2 A visão estratégica da Teoria dos Jogos

Motivados pela observação de que cada parte do jogo age de acordo com suas crenças e de acordo com as antecipações que podem ser feitas sobre o adversário, diversos pesquisadores acreditam que a Teoria dos Jogos pode ser considerada uma ferramenta apropriada para apoiar a alocação de recursos de defesa objetivando o antiterrorismo. Observa-se que a Teoria dos Jogos está alinhada com uma série de pressupostos relevantes adotados em estudos dentro do contexto em questão, como os destacados por Sandler & Arce (2003):

- As interações entre os lados envolvidos no jogo são estratégicas;
- As ações são interdependentes e, portanto, não é possível analisar um dos lados como passivo;
- As interações estratégicas ocorrem entre atores racionais, que estão tentando agir de acordo com a forma que eles imaginam os homólogos irão agir e reagir.

De fato, essa teoria permite uma análise normativa simétrica conjunta na qual os jogadores têm por principal objetivo maximizar as suas utilidades esperadas enquanto esperam que os outros jogadores façam o mesmo. As análises permitidas pela Teoria dos Jogos ocorrem uma vez que as decisões de cada jogador podem ser antecipadas pelo processo da busca pelos equilíbrios de Nash (Rios & Insua, 2011), o conceito central em Teoria dos Jogos. O equilíbrio de Nash pode ser definido como a situação em que a estratégia escolhida por cada jogador é a melhor resposta para qualquer que seja a escolha do(s) outro(s) jogador(es). De modo formal, uma estratégia s_i^* de um jogador i é considerada a melhor resposta a uma dada estratégia s_{-i} de outro jogador quando não há outra estratégia disponível para o jogador i que produza uma recompensa mais elevada do que s_i^* quando S_{-i} é jogada, ou seja: $\pi_i\left(s_i^*, s_{-i}^*\right) \geq \pi i\, \pi_i\left(s_i, s_{-i}^*\right)$ para todo si e todo i, em que πi representa a função de recompensa de um jogador i; si é uma estratégia do jogador i; e o asterisco indica que a estratégia é um equilíbrio de Nash (Fiani, 2006).

O Quadro 1 apresenta de forma resumida alguns exemplos de aplicação da Teoria dos Jogos em situações nas quais o problema de alocação de recursos de defesa contra ações terroristas é explorado.

Embora a Teoria dos Jogos tenha sido extensamente aplicada para solucionar esse tipo de problema, essa abordagem enfrenta algumas críticas que merecem ser

Quadro 1. Aplicação da Teoria dos Jogos em problemas de alocação de recursos antiterrorismo.

Tema	Variações	Observações /Conclusões	Referências
Distribuição de recursos para proteção contra ações terroristas	Ameaças consideradas estratégicas.	As preferências do atacante se alteram de acordo com a alocação prévia dos recursos de defesa.	(Powell, 2007a)
	Ameaças consideradas não estratégicas.	Não se ataca o adversário onde ele é mais fraco e onde os ganhos esperados serão maiores. Preferências dos atacantes ficam inalteradas.	(Banks & Anderson, 2006; Farrow, 2007; Powell, 2007a; Zhuang & Bier, 2007)
	Medidas de defesa que apresentam sinergia entre si.	Uma única medida de defesa pode refletir na redução da vulnerabilidade de mais de um alvo.	(Farrow, 2007; Powell, 2007a)
Incertezas inerentes aos atacantes e aos defensores	Incertezas do defensor sobre como as preferências do atacante se modificam em relação aos alvos.	Recursos centralizados protegendo alvos mais valorizados têm desempenho melhor do que aqueles aplicados de forma descentralizada.	(Bier et al., 2007; Major, 2002)
		Com recursos escassos, a incerteza torna-se mais significativa e torna-se mais difícil proteger alvos que são mais valiosos.	(Wang & Bier, 2011)
		Uma otimização do tipo robusta pode contornar as incertezas sobre parâmetros do atacante.	(Nikoofal & Zhuang, 2011)
	Incertezas do atacante sobre a vulnerabilidade dos alvos.	A modelagem do jogo pode ser realizada como jogos de sinalização. Alocar muito recurso para a proteger um alvo pode sinalizar alvo de alto valor.	(Powell, 2007b)
	Incertezas sobre o valor dos alvos e sobre as preferências do atacante pelos alvos.	A incerteza sobre as preferências dos atacantes impactam pouco na forma de alocação dos recursos de defesa.	(Bier et al., 2008)
Vantagens e desvantagens em tornar a alocação de recursos pública		É melhor para a defesa tornar a sua estratégia pública do que fazê-la em segredo.	(Farrow, 2007; Major, 2002; Zhuang & Bier, 2010)
		O equilíbrio entre a divulgação das estratégias de defesa e a manutenção do segredo dessas informações é a melhor estratégia.	(Brown et al., 2005)
Proteção redundante de alvos críticos		É mais vantajoso proteger um maior número de componentes críticos do que optar pela redundância.	(Brown et al., 2005)
		O autor enfatiza a validade da redundância como uma estratégia defensiva.	(Bier, 2006)
Análise de *tradeoffs* na distribuição dos recursos para a proteção de vários alvos		Análise de como consideração da equidade e da eficiência impactam na distribuição de recursos para a proteção de diversos alvos.	(Shan & Zhuang, 2012)

discutidas. Sebenius (1992, 2006), por exemplo, aponta que um dos principais aspectos da Teoria dos Jogos que pode ser considerado problemático é a adoção das premissas que se referem ao conhecimento completo e perfeito sobre as possíveis metas e aspirações que os jogadores sustentam uns sobre os outros. Sandler & Arce (2003) colocam que nas situações reais onde alocação de recursos antiterrorismo é estudada, o cenário mais comum é que ambos, defesa e ataque, disponham de informações incompletas. Como apontado por Banks & Anderson (2006), a abordagem padrão que considera o conhecimento completo acaba por falhar na prática. Para contornar essa falha, teorias foram modificadas com pressupostos relaxados principalmente no que se refere a considerar o conhecimento completo do jogo ou sobre a consideração da racionalidade ilimitada (Gigerenzer & Reinhard, 2001) por parte dos jogadores. Da mesma forma, autores sugerem o uso de probabilidade, tratando o jogo por meio de uma análise Bayesiana, como, por exemplo, fazem Ezell et al. (2010), que consideram que a possibilidade da adoção dos jogos de informações incompletas, quando existem incertezas inerentes aos jogadores e suas preferências, seja uma boa solução.

Nesta pesquisa, acredita-se que, realmente, o encontro dos pontos que definem o equilíbrio de Nash pode permitir alguma introspecção interessante sobre a questão analisada. No entanto, é importante salientar aqui que alocar recursos para se proteger do pior cenário (aquele que o oponente tem em mente causar e aquele que a defesa irá buscar evitar) não equivale a proteger-se de todos os outros cenários menos nocivos. O resultado típico em uma procura pelos pontos de equilíbrio é que nenhum dos jogadores acaba ficando com a recompensa que mais gostaria, no entanto evitam-se os piores resultados (Insua et al., 2009). É exatamente em relação a essa busca que se faz, aqui, uma questão: seria a busca pelo equilíbrio de Nash suficiente para balizar a questão da alocação de recursos com fins antiterrorismo?

O que se conclui aqui é que a Teoria dos Jogos, como todas as abordagens, tem limitações que precisam ser levadas em consideração. Por fim, fica aberta a questão apontada por Ellis (2009): qual abordagem de avaliação de risco seria flexível e robusta, simultaneamente, de forma que servisse para balizar a alocação de recursos de defesa para essa situação, reconhecendo que a natureza das ameaças terroristas muda em resposta a qualquer estratégia de defesa adotada?

3 Análise do Risco Adversário: uma nova abordagem

De acordo com Insua et al. (2009), em uma visão geral, os desafios caracterizados pelo fato de existirem dois ou mais adversários inteligentes que tomam decisões, as quais culminam em um desfecho incerto, são cobertos por uma abordagem chamada de Avaliação do Risco Adversário – ARA (Adversarial Risk Analysis). Rios & Insua (2011) argumentam que a ARA é capaz de viabilizar uma sinergia entre a clássica Teoria dos Jogos e a Avaliação Probabilística de Risco.

Visando suportar um dos participantes de um jogo (chamemos esse de defesa), a ARA emprega a modelagem da estrutura de decisão da parte adversária (chamemos essa de ataque) para obter um modelo probabilístico descritivo do comportamento que o ataque poderá vir a ter. A grande contribuição da ARA ocorre quando essa descrição é usada, pela defesa, como informações úteis para resolver o seu próprio problema de decisão. Para isso, a estrutura montada leva em conta as possíveis alternativas de decisão que existem para a defesa e para o ataque, assim como outras informações que podem estar disponíveis, de forma assimétrica, para as partes envolvidas no jogo. Como forma de acomodar as informações possíveis de serem extraídas na análise realizada para a solução dos problemas de decisão de ambas as partes do jogo, a ARA adota uma estrutura com modelos de decisão "aninhados", viabilizado por um procedimento denominado *mirroring* (espelhamento) (Banks, 2009; Insua et al., 2009). Tal estrutura permite tornar a análise do problema mais próxima daquela que seria realizada em uma situação real (Insua et al., 2009). A estratégia básica contida no argumento de espelhamento é um procedimento no qual o decisor estuda a análise que o adversário provavelmente está realizando, considerando o fato de que o adversário irá, simultaneamente, realizar um estudo simétrico da análise da decisão do primeiro (a defesa). Rothschild et al. (2012) apontam que a técnica do espelhamento se assemelha à de jogos de nível-*k* (Level-k games) (Rothschild et al., 2012; McLay et al., 2012).

A abordagem ARA já está presente em alguns trabalhos na literatura internacional. Dentre esses, destacam-se as aplicações mais relevantes dentro do tema em voga: Insua et al. (2009) e Rios & Insua (2011) exploram como a ARA poderia ser aplicada para jogos simultâneos e sequenciais com informações privadas por uma das partes. Wang & Banks (2011) analisam a alocação de recursos em missões de comboios militares que se deslocam por rotas que podem ser atacadas por inimigos. Sevillano et al. (2012) apresentam um modelo de comportamento dos piratas utilizados na seleção da decisão a ser tomada no caso de se sofrer uma abordagem pirata no mar. Por fim, Banks et al. (2011) exploram a abordagem ARA quando se assume que uma das partes envolvidas no jogo pode estar blefando.

De forma a clarificar a filosofia da modelagem da abordagem ARA considera-se aqui uma situação

hipotética em que a defesa precisa optar por uma estratégia, sendo essas estratégias elementos do conjunto $D = \{d_1, d_2, d_3, ..., d_n\}$, em que d_n representa a *n-ésima* estratégia disponível para a defesa escolher, enquanto o atacante deve decidir qual tipo de ataque deve realizar, sendo os tipos de ataque os elementos do conjunto $A = \{a_1, a_2, a_3, ..., a_m\}$, em que a_m representa o *m-ésimo* tipo de ataque que o atacante pode adotar. A árvore mostrada na Figura 1 representa os eventos observados pela defesa e pelo ataque. O nó *D, A* (retângulo) representa as decisões da defesa e do atacante. O nó S representa a chance que existe de o ataque fracassar (representado pelo ramo s_0) ou ter sucesso (representado pelo ramo s_1). Considera-se aqui que sucesso significa que os danos esperados pelo atacante ocorrem. Nos casos em que os danos esperados não ocorrem, independentemente do motivo que impede tal ocorrência, o ataque é considerado um fracasso. A cada folha da árvore está associado um par de valores de utilidade (u_D, u_A), representando os valores atribuídos pela função de utilidade da defesa e do atacante, respectivamente.

3.1 Modelagem do jogo pela visão da defesa

Quando o problema analisado é aquele que a defesa precisa resolver, a decisão do atacante (qual tipo de ataque ele irá realizar) torna-se uma incerteza. Na nova árvore de decisão representada pela Figura 2 essa situação pode ser observada. O nó que representava uma decisão do atacante passa a ser percebido como um nó que representa uma incerteza para a defesa, ilustrada por um círculo ao invés de um quadrado. Percebe-se uma linha pontilhada ao redor das possíveis decisões do atacante. Tal representação indica que essas decisões são consideradas um conjunto de informações, uma vez que o atacante não sabe em qual ramo da árvore realmente está quando toma sua decisão (o jogo representado é um jogo simultâneo).

A defesa conhece sua função-utilidade $u_D(d, s)$. Pode-se definir também que especialistas que apoiam a defesa tenham condições de definir a probabilidade de sucesso e de fracasso $p_D(S = s \mid d, a)$ quando cada tipo de ataque é realizado, nos casos em que cada uma das estratégias da defesa tenham sido adotadas. No entanto, as probabilidades de o atacante escolher cada tipo de ataque não estão disponíveis para a defesa. A defesa expressa essa incerteza por meio de uma probabilidade $\pi_D(A = a)$.

Considerando-se que a defesa pretende adotar a decisão que maximiza a utilidade esperada, o principal problema de otimização que deve ser resolvido por ela é representado pela Equação 1.

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

Isso posto, conclui-se que o fator que a defesa realmente precisa avaliar é a probabilidade $\pi_D(A = a)$. Para obter tal parâmetro, a defesa passa a analisar a forma como seu oponente poderia estar realizando a análise de seu próprio problema de decisão: escolher qual tipo de ataque ele deve realizar.

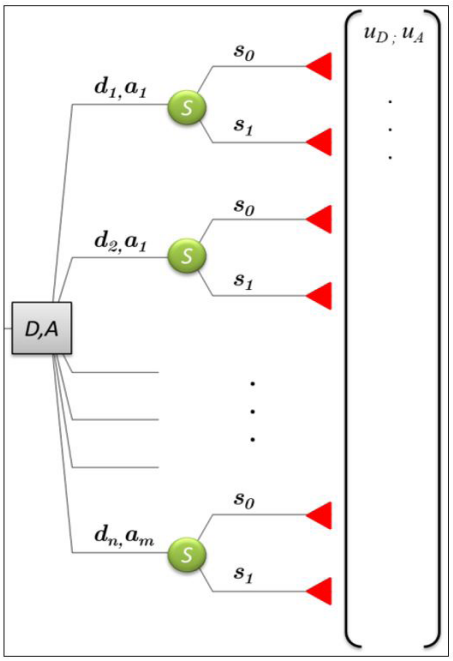

Figura 1. Árvore de decisão com os eventos enfrentados pela defesa e pelo atacante. Fonte: adaptação de Rios & Insua (2011).

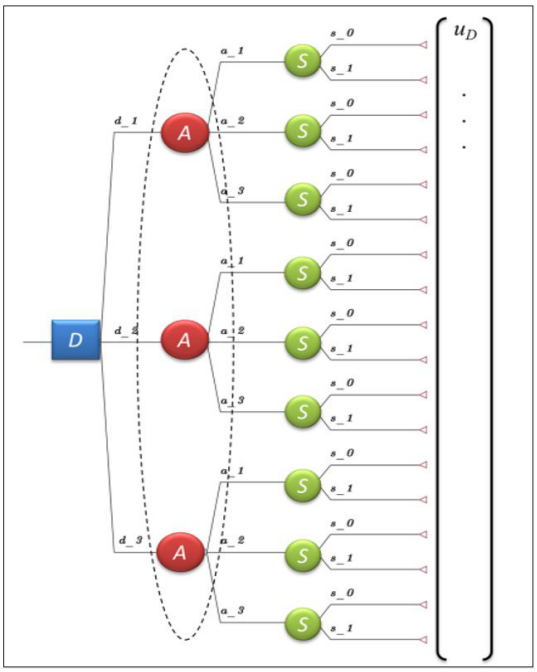

Figura 2. Árvore de decisão que representa o problema da defesa.

3.2 Modelagem do jogo pelo ponto de vista do atacante

O problema de decisão enfrentado pelo atacante é ilustrado pela árvore de decisão apresentada na Figura 3. Nessa árvore, os nós *D* representam a incerteza que o atacante sustenta a respeito de qual estratégia a defesa irá adotar. A defesa deve então colocar-se na posição do atacante e imaginar como ele estaria resolvendo o seu problema de decisão. Esse procedimento pode ser encontrado em trabalhos científicos e acadêmicos que exploram a modelagem do comportamento de agentes como terroristas e suas organizações (exemplos podem ser vistos em: Pat-Cornell & Guikema, 2002; Ushakov, 2006; Rios & Insua, 2011; Sevillano et al., 2012).

Como em diversos trabalhos nesse contexto, assume-se que os atacantes são maximizadores de utilidade (Ezell et al., 2010; McLay et al., 2012; Sevillano et al., 2012; Wang & Banks, 2011). Assim, o atacante procura pela opção $a \in A$ que forneça a ele a máxima utilidade esperada e, para tal, busca a solução para a Equação 2, construída por meio de um processo análogo ao realizado para a construção da Equação 1.

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

Durante a resolução da Equação 2, a defesa terá dúvidas sobre os valores de utilidade $u_A(a,s)$ que o atacante adotará ao resolver o seu problema.

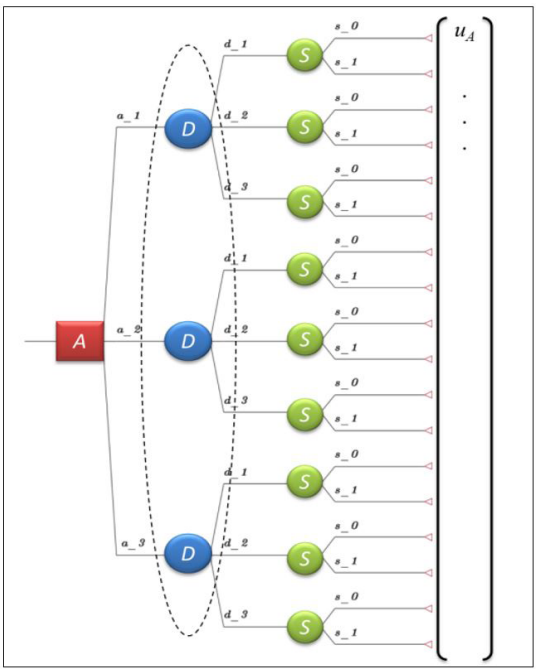

Figura 3. Árvore de decisão que representa o problema do atacante.

Da mesma forma, a defesa não sabe ao certo quais as crenças do atacante sobre as probabilidades de sucesso ou fracasso de seu ataque $p_A(S = s \mid d, a)$, quando cada uma das estratégias que a defesa pode adotar é a escolhida. Outro parâmetro que é incerto para a defesa refere-se a como o atacante pode estar avaliando as chances de a defesa optar por um das estratégias de defesa $\pi A (D = d)$. Insua et al. (2009) propõem a utilização de distribuições de probabilidades subjetivas para representar todas as quantidades que são desconhecidas para o decisor (defesa). Embora Banks (2011) aponte que formular as probabilidades subjetivas que representam o comportamento do seu oponente pode apresentar desafios, Kunreuther et al. (2013) comentam sobre a extensa literatura a respeito de métodos para se obter tais parâmetros, quando o conhecimento de especialistas pode ser explorado.

Dessa forma lança-se mão da modelagem das informações disponíveis para a defesa por meio de distribuições de probabilidade para representar, agora, as variáveis aleatórias U_A, P_A e $\prod_A$, que descrevem o comportamento de $u_A(a,d)$, $p_A(S = s \mid d,a)$ e $\pi_A(D = d)$, respectivamente. Agregando tal incerteza à Equação 2, temos a seguinte Equação 3:

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

Os parâmetros para as distribuições de probabilidades $U_A(a,s)$ e $P_A(S = s \mid d,a)$ podem ser propostos diretamente pela defesa com auxílio de especialistas. Porém, para a avaliação de $\prod_A (D = d)$ será necessário que a defesa se coloque no lugar do atacante e pense sobre como ele estaria pensando quando buscasse as respostas para o seu problema (qual tipo de ataque adotar). É exatamente por isso que na Equação 3 existe um condicionante a *D*. Isso mostra que a defesa, nessa etapa, precisa avaliar como o atacante estaria pensando sobre as suas recompensas e sobre as suas chances de sucesso quando opta por cada tipo de ataque. Da mesma forma, a defesa deve propor crenças a respeito de como o atacante estaria avaliando a probabilidade de ela, defesa, adotar cada pacote de medidas defensivas. Então a defesa, para obter os valores para $\prod_A (D = d)$, poderia considerar que o atacante também estaria resolvendo o seu problema de decisão dessa mesma forma. Se isso se confirmasse, o atacante estaria buscando a melhor forma de solucionar o problema que a defesa enfrenta, ou seja, aquele representado pela Equação 1.

Por conseguinte, o atacante estaria buscando obter os parâmetros da distribuição de probabilidade que regesse o comportamento da variável aleatória $D|A^1$ (Equação 4), assumindo que a defesa fosse capaz de avaliar $\prod_D (A^1)$, em que A^1 representa a decisão do atacante dentro do segundo nível do pensamento recursivo da defesa.

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

Para avaliar a distribuição da variável aleatória $D|A^1$, a defesa precisaria da distribuição de probabilidade que rege a variável aleatória $U_D\,(d,s)$, representando as suas crenças a respeito de como o atacante poderia ter estimado a função de utilidade da defesa $u_D\,(d,s)$. De uma forma geral, este processo exigiria futuros pensamentos recursivo por parte do defensor. Esta hierarquia de modelos aninhados encontraria um limite quando se atingisse um nível em que faltassem informações necessárias para o Defensor continuar a alimentar as equações associadas aos cômputos dos valores de A^I e D^I $(i = 1,2,3,...)$. Neste caso o uso de uma distribuição de probabilidade não informativa (como a distribuição de máxima entropia) associada aos parâmetros incertos seria suficiente para representá-los (Insua et al., 2009; Rios & Insua, 2011).

4 Um caso simulado de ARA

A intenção deste exemplo é, principalmente, detalhar a forma como se desenvolve a aplicação da abordagem ARA. Por isto, nesse caso simulado, pouca atenção será dada para a forma como foram escolhidos os valores hipotéticos assumidos para as distribuições de probabilidades adotadas. Igualmente, não será discutida a forma como as funções de utilidade adotadas foram construídas. Tampouco serão alvo de análise as técnicas de simulação utilizadas neste exemplo.

Considera-se aqui uma situação hipotética em que a defesa precisa proteger um estádio no qual ocorrerá um evento esportivo contra possíveis ataques terroristas. Para isso, supõe-se que a defesa precise escolher um dos "pacote de medidas defensivas" oferecidos por empresas especializadas em segurança pública para a proteção do estádio. Considera-se que tais pacotes sejam os elementos do conjunto $D = \{d_1, d_2, d_3\}$. Cada um desses pacotes tem suas diferenças de preço de aquisição e se mostram mais ou menos eficientes contra diferentes tipos de ataque que possam ser realizados. A defesa deseja adotar o pacote de medidas defensivas que minimize os danos esperados.

Por outro lado, o atacante deve decidir sobre qual tipo de ataque deve realizar. Definem-se os tipos de ataque como os elementos do conjunto $A = \{a_1, a_2, a_3\}$. Ataques que resultem em maiores efeitos, em termos de danos causados, retornam os maiores benefícios para a organização terrorista, ao mesmo tempo, são mais custosos e, quando frustrados (ataque sem sucesso), resultam em grandes perdas para essas organizações.

4.1 Recompensas e probabilidades de sucesso e fracasso quando ocorrem os ataques

Neste exemplo, a função de utilidade da defesa $u_D\,(d,s)$ é influenciada pela escolha do pacote de medidas defensivas e também pelo resultado do ataque. A defesa percebe suas recompensas de forma que ganhos estejam associados com o fracasso do atacante ao realizar o ataque; perdas estejam associadas com as situações em que o ataque ocorra com sucesso. No entanto, a defesa conta com os custos associados à adoção dos pacotes de medidas defensivas. Além disso, podem existir perdas específicas ao se adotarem determinados pacotes como, por exemplo: transtorno para a população e desconforto da opinião pública a respeito do esquema de segurança. Os valores de utilidade assumidos para a defesa estão apresentados no Quadro 2.

Por outro lado, o atacante percebe suas recompensas de acordo com os danos causados e os custos para a mobilização dos recursos necessários para a realização do atentado; possíveis perdas que possam causar para seus próprios recursos. Esse parâmetro pode englobar diversos valores representados de formas tangíveis como dinheiro ou aumento no número de membros recrutados para as organizações terroristas; ou intangíveis, como fama, satisfação, entre outros (Quadrifoglio, 2008; Sri Bhashyam & Montibeller, 2012). A defesa, porém, não pode definir de maneira determinística a utilidade $u_A\,(a,s)$ adotada pelo atacante. É possível que a defesa tenha informações históricas e de inteligência sobre as atividades executadas pela organização terrorista que esteja sendo considerada como geradora de ameaça. Tais informações podem ser englobadas nas estimativas que a defesa deve realizar a respeito de como o atacante poderia estar avaliando suas recompensas para cada tipo de ataque que poderia ser realizado (Ezell et al., 2010). Da mesma forma, essas informações podem orientar a defesa a respeito de como o atacante estaria avaliando as probabilidades de sucesso quando cada tipo de ataque estivesse sendo executado. Por isso acredita-se que é possível a realização de uma avaliação, por parte dos especialistas na área de defesa, sobre a distribuição obedecida por uma variável aleatória $U_A\,(a,s)$ que representará a utilidade $u_A\,(a,s)$ adotada pelo atacante. O Quadro 3 representa as distribuições do tipo triangular [Tri (mínimo; moda; máximo)] utilizadas aqui para descrever o comportamento da variável aleatória $U_A\,(a,s)$.

Assume-se que, com o apoio de especialistas, a defesa possa estabelecer o quanto o alvo (no caso deste exemplo, o estádio) é vulnerável a cada tipo de ataque que o oponente pode executar. Essa vulnerabilidade retrata a probabilidade de sucesso que o atacante tem ao atacar o alvo. Os valores de probabilidade

assumidos pela defesa para o sucesso e o fracasso do atacante, quando ele opta por usar cada tipo de ataque e a defesa adota cada um dos pacotes de medidas defensivas estão apresentadas no Quadro 4.

A defesa precisa estimar como o atacante estaria avaliando as probabilidades de sucesso e fracasso quando ele opta por usar cada tipo de ataque e considera que a defesa esteja adotando cada um dos pacotes de medidas defensivas. Neste exemplo, supõe-se que as crenças da defesa a levam a considerar que o atacante possui capacidades de avaliação de vulnerabilidades de alvos bastante similar à dela. Também assume-se que não exista qualquer informação à respeito das eficiências das medidas defensivas que sejam consideradas, por parte da defesa, surpresas estratégicas. Então, assume-se que a defesa fique satisfeita ao considerar que sua incerteza sobre como o atacante estimaria as suas probabilidades de sucesso e fracasso (para cada folha da árvore) possa ser representada por uma distribuição de probabilidade do tipo uniforme [U (mínimo; máximo)] com as seguintes características: o valor da média dessa distribuição é exatamente o valor de $p_D\,(S = s \mid d, a)$. O valor limite superior *dessa* distribuição é dado por $p_D\,(S = s \mid d, a)+0{,}2$, assim como o valor limite inferior é dado por $p_D\,(S = s \mid d, a)-0{,}2$. Assim, as distribuições a serem levadas em conta para representar o valor da variável aleatória $P_A\,(S = s \mid d, a)$ em cada ramo da árvore de decisão do atacante são as mostradas no Quadro 5. Observa-se, no entanto, que como sucesso e fracasso são os dois únicos desfechos para o ataque, considera-se aqui que o valor assumido pela variável aleatória $P_A\,(S = s \mid d, a)$ para os casos de sucesso do ataque (s_1) são dados pelo valor complementar da probabilidade atribuída para os casos de fracasso.

Por fim, a defesa deve explicitar suas crenças a respeito de como o atacante estaria avaliando a probabilidade de ela (a defesa) adotar cada pacote de medidas defensivas. Neste exemplo, considera-se que a defesa não possui qualquer informação que possa ser significativa para auxiliar na avaliação dessas probabilidades. Assim, define-se aqui que a variável aleatória representada por $\prod_A\,(D = d)$ deverá ser regida pela distribuição de probabilidade de máxima entropia, ou seja, a distribuição do tipo Uniforme U (0, 1).

Quadro 2. Valores de utilidade assumidos para a defesa.

Proteção	s_0 (utilidade)	s_1 (utilidade)
d_1	55	–45
d_2	40	–60
d_3	65	–35

Quadro 3. Distribuições de probabilidade que representam as recompensas do atacante.

Tipo de ataque	s_1 (probabilidade)	s_0 (probabilidade)
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)]

Quadro 4. Valores de probabilidade assumidos pela defesa para o sucesso e o fracasso do atacante.

Valores de probabilidade de sucesso e fracasso		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%

4.2 A solução do problema de decisão da defesa

Inicialmente, percebe-se que uma maneira intuitiva de iniciar a solução do problema proposto seria uma abordagem em ordem inversa. Isso significa que a primeira resposta a ser procurada é a forma como se comportaria a variável aleatória $A \mid D$ (Equação 3). Aplicando-se simulação de Monte Carlo (nesse exemplo realizaram-se 10 mil iterações), observou-se que a variável aleatória $A \mid D$ comportou-se como mostra o histograma apresentado na Figura 4.

Conclui-se pelos resultados apresentados que em aproximadamente 8,85% das vezes o atacante optaria pela realização do ataque tipo a_1; 4,63% das vezes optaria por a_2; e em 86,52% das vezes optaria por a_3. Tais valores poderiam ser considerados satisfatórios o suficiente para representarem os valores de $\pi_D\,(A = a)$. No entanto, pode-se admitir aqui que a defesa, no seu íntimo, apresente determinada confiança dos

Quadro 5. Distribuições de probabilidades para sucesso e fracasso do atacante pelo ponto de vista da defesa.

Distribuição de probabilidade		s_0	s_1
d_1	a_1	U(0,1; 0,5)	Complementar
	a_2	U(0,2; 0,6)	Complementar
	a_3	U(0,35; 0,75)	Complementar
d_2	a_1	U(0,15; 0,55)	Complementar
	a_2	U(0,05; 0,45)	Complementar
	a_3	U(0,15; 0,55)	Complementar
d_3	a_1	U(0,15; 0,55)	Complementar
	a_2	U(0,20; 0,60)	Complementar
	a_3	U(0,05; 0,45)	Complementar

valores obtidos. Por isso, supõe-se que a defesa prefira estabelecer uma distribuição de probabilidade para representar a, agora, variável aleatória $\prod_D(A=a)$. Para o exemplo em questão, assume-se que a defesa opte por adotar uma distribuição do tipo Beta para incorporar essa confiança em suas análises. Supõe-se *Be* (a; b), onde *a* e *b* são os parâmetros de formato dessa distribuição, com média π_D *(A = a)* e uma determinada precisão (η). Por definição tem-se que $\eta = a + b$, ou seja, $Be\,(a;\eta - a)$. Reorganizando as equações apresentadas por Myriam & Pongo (1997) pode-se definir que a média (μ) de uma distribuição Beta é dada pela Equação 5 e sua variância (σ^2) é definida pela Equação 6:

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

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

Pode-se então fazer os parâmetros a e b em função de $\mu e \sigma^2$.

Adota-se, nesse caso em particular, que a defesa estabeleceu que um desvio padrão de 10% sobre o valor da média seria o suficiente para representar sua confiança nos resultados obtidos pela simulação realizada. Assim, tem-se que $\sigma = \frac{\mu}{10}$. Os parâmetros *a*, *b* e μ são apresentados no Quadro 6. Têm-se assim os valores calculados para os parâmetros de $\prod_D(A=a)$, ou seja, a forma como a defesa acredita que se comportam as probabilidades de o ataque adotar cada um de seus possíveis tipos de ataque $a \in A$.

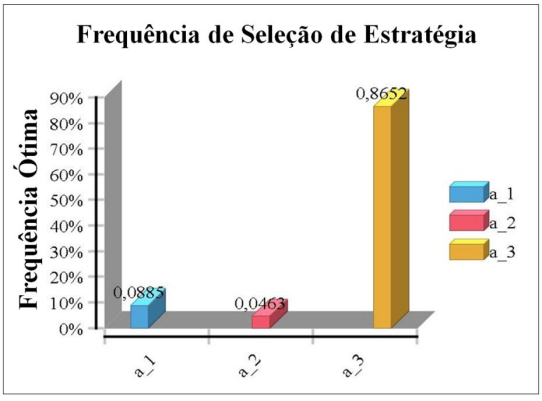

Figura 4. Ocorrências de a_1, a_2 e a_3 com a simulação de Monte Carlo.

Agora, pode-se dizer que a defesa possui todas as informações necessárias para resolver o seu problema original. Os valores de utilidade adotados pela defesa são apresentados deterministicamente. Porém a defesa opta por usar distribuições de probabilidades para contemplar incertezas sobre as suas avaliações quanto às probabilidades de sucesso e fracasso de um ataque. Assim, ela representa esses valores por meio de distribuições de probabilidades do tipo triangular, ilustradas no Quadro 7.

As probabilidades associadas à escolha do atacante serão dadas pelas distribuições de probabilidade apresentadas no Quadro 6, sendo assim consideradas variáveis aleatórias $\prod_D(A=a)$. A Equação 7 ilustra a forma como a defesa resolve o seu problema, ou seja, escolher qual dentre as três alternativas (pacotes de medidas defensivas) é a que retorna o maior valor de utilidade esperada. Aplicando-se nova simulação de Monte Carlo com os parâmetros da Equação 7 pode-se estimar as frequências com que cada uma de suas opções retorna o maior valor de utilidade esperada, quando adotada pela defesa.

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

De acordo com a simulação de Monte Carlo realizada, as frequências com que cada uma das opções retorna o maior valor de utilidade esperada, quando adotada pela defesa, está representada pela Figura 5.

Com esses resultados, em uma visão prescritiva (Merrick & Parnell, 2011; Rothschild et al., 2012), o conselho dado para a defesa seria: seus recursos deveriam ser alocados para adquirir o pacote de medidas de segurança d_1. Essa opção retornaria o maior valor para a utilidade esperada da defesa em aproximadamente 93% das simulações que foram realizadas.

5 Discussão

Primordialmente, uma diferença e, ao mesmo tempo, vantagem apontada para a abordagem ARA, quando comparada com a aplicação clássica da Teoria dos Jogos e PRA, é que as descrições do comportamento do atacante não são dados de entrada do problema

Quadro 6. Valores dos parâmetros de $\prod_D(A=a) \sim Be(a;b)$ adotados pela defesa.

	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	$Be(12,61;1,9654)$

Quadro 7. Distribuições de probabilidade para representar crenças da defesa sobre sucesso e fracasso de um ataque.

Distribuição de probabilidade		s_0	s_1
d_1	a_1	Tri (0,10; 0,30; 0,50)	Complementar
	a_2	Tri (0; 0,20; 0,40)	Complementar
	a_3	Tri (0,35; 0,55; 0,75)	Complementar
d_2	a_1	Tri (0,15; 0,35; 0,55)	Complementar
	a_2	Tri (0,05; 0,25; 0,45)	Complementar
	a_3	Tri (0,15; 0,35; 0,55)	Complementar
d_3	a_1	Tri (0,15; 0,35; 0,55)	Complementar
	a_2	Tri (0,20; 0,40; 0,60)	Complementar
	a_3	Tri (0,05; 0,25; 0,45)	Complementar

a ser resolvido. De acordo com Merrick & Parnell (2011), trabalhos que partem da premissa que esses valores são dados normalmente adotam distribuições de probabilidades subjetivas, advindas de especialistas. Geralmente, essas estimativas são muito genéricas. O que se consegue nessa abordagem é, exatamente, encontrar tais probabilidades. Para tanto, o modelo requer como entrada crenças que a defesa possui sobre como os oponentes veem as consequências dos ataques (recompensas) e as chances de sucesso para esses ataques, o que, nesta pesquisa, em comum acordo com Merrick & Parnell (2011), julga-se muito mais realista e viável. Banks (2011) comenta que seria perfeitamente razoável imaginar que os jogadores têm conhecimentos probabilísticos relevantes sobre os valores e as crenças que seus oponentes nutrem. Esses conhecimentos poderiam ser, por exemplo, derivados de estudos realizados pela comunidade de inteligência. Por outro lado, é importante notar que alguns fatores englobados no exemplo ilustrado devem ser analisados em relação a sua variação, como em uma espécie de análise de sensibilidade. Certamente um aspecto que merece atenção está relacionado ao grau de incerteza atribuído pela defesa aos valores de utilidade do atacante quando se definiu a representação dessa variável aleatória (U_4). Da mesma forma, análises interessantes podem surgir quando se estudam as variações para as distribuições de probabilidade associadas aos casos de sucesso e fracasso do atacante, quando avaliadas pelo atacante, de acordo com o ponto de vista da defesa. Análises interessantes sobre valores de recompensas atribuídas a atentados realizados por organizações terroristas estão disponíveis em pesquisas (Keeney, 2007; Dillon et al., 2009; Keeney & Winterfeldt, 2011).

Caso as informações obtidas por meio dos especialistas que apoiam a defesa fossem mais acuradas, o natural seria que as análises contemplassem um nível de incerteza menor e, portanto, fossem mais confiáveis. Embora a redução das incertezas inerente às informações seja possível de ser obtida por meio dos resultados coligidos pelos serviços de inteligência

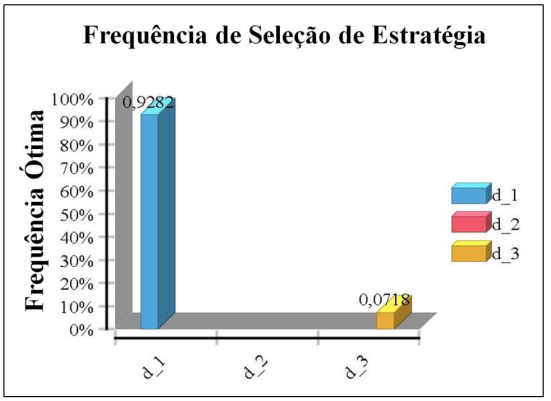

Figura 5. Ocorrências de d_1, d_2 e d_3 com a simulação de Monte Carlo.

que apoiam a defesa, Banks (201) e Rios & Insua (2011) apontam que a disponibilização de informações para a modelagem proposta por ARA ainda é tida como grande desafio. Tal fato é importante de ser observado e deve ser explorado em trabalhos futuros, pois as decisões de alocação de recursos de defesa estarão intimamente ligadas ao grau de qualidade e confiabilidade das informações.

Outra análise interessante poderia ser realizada em relação ao procedimento de espelhamento proposto na abordagem ARA. Qual seria o nível de recursividade que esse modelo deveria atingir? No exemplo ilustrado optou-se por explorar apenas até o segundo nível do pensamento recursivo da defesa. No entanto, uma sondagem que se aprofundasse em outros níveis de recursividade, tanto na modelagem do problema enfrentado pela defesa como naquele resolvido pelo ataque, poderia trazer interessantes resultados, em futuras pesquisas. Alguns trabalhos, como o de Farias (2013), exploram esse assunto, inclusive verificando a convergência dos resultados para jogos com informações completas e para aqueles com informações incompletas.

Assim, conclui-se que a ARA possui estrutura para avaliar riscos oferecidos por oponentes inteligentes e que apresenta a vantagem de embutir informações

assimétricas na modelagem dos jogadores. Além disso, a ARA descarta a necessidade de que os especialistas forneçam julgamentos subjetivos sobre as prováveis estratégias que serão adotadas pelos oponentes, uma vez que o próprio modelo chega a uma descrição probabilística delas. Porém, ao mesmo tempo, carece de uma quantidade considerável de informações sobre os oponentes, o que ainda pode ser considerado como uma fragilidade da proposta.

6 Considerações finais

Este artigo teve como objetivo apresentar uma nova abordagem de avaliação de riscos para o apoio à alocação de recursos antiterrorismo. Foram revisadas as duas principais abordagens tradicionalmente utilizadas para apoiar esse tipo de decisão. Ao se comentar a respeito das aplicações de Avaliação Probabilística de Riscos, pôde-se perceber que embora essa seja a teoria que atualmente baliza as decisões do governo estadunidense sobre a melhor forma de alocar recursos para antiterrorismo existem críticas relevantes à sua aplicação. A principal delas refere-se a não observar o oponente como adaptável e estratégico e, dessa forma, não considerar a maneira como ele se comportará após observar como a defesa aloca seus recursos. Na sequência, comentou-se sobre pesquisas que se apoiam na Teoria dos Jogos. Nesse caso, o oponente leva em conta as ações da defesa quando escolhe sua estratégia, no entanto descarta-se a possibilidade de considerar informações de inteligência e outras que possam ser relevantes para a modelagem dos agentes envolvidos no jogo, além de considerar como premissa a disponibilidade de informações sobre o oponente que, na realidade, sabe-se que seriam bem críticas de se obter. Finalmente, foi apresentada a proposta Avaliação do Risco Adversário (ARA). Essa recente abordagem pode ser vista como uma contribuição de potenciais aplicações e como relevante para a academia, no contexto brasileiro. Como parte final, um caso simulado foi apresentado de forma a ilustrar a aplicação do ARA. Considera-se aqui que a aplicação apresentada permitiu que ficasse claro como as probabilidades das ações dos adversários podem ser estimadas antes de a defesa calcular sua utilidade máxima esperada. Isso permite um tratamento mais realístico e ao mesmo tempo mais simples para o ambiente de tomada de decisão quando se trata de contraterrorismo e é uma vantagem que a ARA sustenta perante as aplicações clássicas da Teoria dos Jogos.

Ressalta-se neste trabalho que em situações em que se possui pouca experiência em assuntos relacionados a antiterrorismo é importante enfatizar que o planejamento das atividades que visam à redução da ocorrência de um atentado é distinto de mitigar os riscos de desastres naturais. Por isso, em situações de megaeventos esportivos, por exemplo, a proteção da infraestrutura, das autoridades mundiais e do público precisa ser planejada levando-se em consideração as características de adaptabilidade do oponente que está sendo enfrentado. Concorda-se com o apontado por Rios & Insua (2011), que comentam que a criação de uma estrutura conceitual como a apresentada (ARA) é apenas um primeiro passo necessário e relevante para que, a partir dele, sejam realizadas melhorias significativas que permitam aplicações em situações reais.

Como conclusão final, acredita-se que a exploração em profundidade dessa nova abordagem possa trazer novas ideias, a serem somadas às abordagens tradicionais propostas pela Teoria dos Jogos. Portanto, a estrutura apresentada pode ser considerada uma contribuição para a área de estudo sobre avaliação de riscos não só no contexto relacionado ao terrorismo mas em qualquer situação em que duas partes sejam oponentes e reajam de forma estratégica e inteligente uma às ações da outra.

Agradecimentos

O autor agradece ao pesquisador doutor João José de Farias Neto, do Instituto de Estudos Avançados, e a Amaury Caruzzo, do Grupo de Estudos de Análise de Decisão – GEAD (Instituto Tecnológico de Aeronáutica) pelas contribuições proporcionadas por relevantes discussões a respeito do tema.

Referências

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.