UMA CONTRIBUIÇÃO AO GERENCIAMENTO DE RISCO DA SEGURANÇA DOS SISTEMAS DE TRANSPORTE: UM MODELO *FUZZY*-HIERÁRQUICO PARA A AVALIAÇÃO DO NÍVEL DE AMEAÇA INTENCIONAL A UM SISTEMA.

Getúlio Marques Martins

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM ENGENHARIA DE TRANSPORTES.

Aprovada por:

_____
Prof. Amaranto Lopes Pereira, Dr. Ing.

_____
Prof. Paulo Cezar Martins Ribeiro, Ph. D.

_____
Prof. Carlos Alberto Nunes Cosenza, D. Sc.

_____
Prof. Jorge Lopes de Sousa Leão, Dr. Ing.

_____
Prof. Félix Mora-Camino, Dr. Ing., Dr. d'État

RIO DE JANEIRO, RJ – BRASIL

MARÇO DE 2008

MARTINS, GETÚLIO MARQUES

Uma Contribuição ao Gerenciamento de Risco da Segurança dos Sistemas de Transporte: Um Modelo *Fuzzy*-Hierárquico para a Avaliação do Nível de Ameaça Intencional a um Sistema [Rio de Janeiro] 2008

XIV, 147 p. 29,7 cm (COPPE /UFRJ, D.Sc., Engenharia de Transportes, 2008)

Tese - Universidade Federal do Rio de Janeiro, COPPE

1. Gerenciamento de Risco da Segurança dos Sistemas de Transporte 2. Análise de Risco 3. Avaliação da Ameaça 4. Teoria dos Conjuntos *Fuzzy* 5. Processo de Hierarquia Analítica

I. COPPE / UFRJ II. Título (série).

DEDICATÓRIA

A meus filhos, Giselle e Guilherme,
por me incentivarem e apoiarem nesta jornada.

A minha mulher, Monika, pela compreensão, paciência,
apoio, incentivo, carinho e momentos de paz e amor ao longo do
caminho.

A meus pais, Benedito† e Dinorah, por terem-me passado a crença de
que é com trabalho, perseverança, determinação e fé, que se atinge as metas escolhidas.

AGRADECIMENTOS

Antes de tudo, agradeço a Deus, pela vida, livre-arbítrio, diversidade de sendas que conduzem à consciência cósmica e pela intuição para escolher a senda do *espírito da verdade* (*ciência*).

Ao Professor AMARANTO LOPES PEREIRA, pela orientação sempre serena e sábia; pela amizade, paciência e consideração; pelo incentivo e pela irrestrita confiança em mim depositada ao longo de todo curso de doutorado.

Ao Professor CARLOS ALBERTO NUNES COSENZA, pela amizade e consideração e pelo incentivo à adoção da Lógica *Fuzzy* como alternativa de modo de raciocínio para abordar o problema objeto desta tese.

Ao Professor FÉLIX MORA-CAMINO, pela consideração e apreço e por me conceder a honra de participar da Banca Examinadora desta Tese, como professor externo à UFRJ.

Ao Professor JORGE LOPES DE SOUZA LEÃO pelas pertinentes considerações referentes à inferência bayesiana como possibilidade de abordar o tema e por me dar a honra de participar da Banca Examinadora desta Tese.

Ao Professor PAULO CEZAR MARTINS RIBEIRO, pela consideração e apreço e pela honra concedida em participar da Banca Examinadora desta Tese.

Ao amigo e Professor ORLANDO NUNES COSSENZA, pelo apreço, consideração, amizade e inestimáveis discussões acadêmicas havidas ao longo do período de pesquisa desta tese.

Em especial à Professora MARIA KARLA VERVLOET SOLLERO, por compartilhar de sua sabedoria comigo nos trabalhos acadêmicos da disciplina Introdução a Lógica *Fuzzy* e pela inestimável amizade.

Ao colega e amigo Engenheiro e Mestre JOÃO CARLOS DE ANDRADE LOPES PEREIRA, pela consideração, incentivo e inestimável apoio, durante todo o tempo de pesquisa desta tese, desenvolvido nas dependências do LESFER/PET/COPPE.

Aos colegas e amigos entusiastas do LESFER/PET/COPPE, o Engenheiro, Mestre e Doutor EDUARDO GONÇALVES DAVID e seu filho o Mestre RAPHAEL KLING DAVID, pela enriquecedora troca de idéias, pelas instigantes discussões acadêmicas e pelo agradável convívio.

ALGUNS PENSAMENTOS INSPIRADORES

"A textura básica da pesquisa constitui-se de sonhos dentro dos quais os fios do raciocínio, da medição e do cálculo são entrelaçados."

Albert Szent Gyorgyi

"Não deveria ser escolha nossa decidir que quantidades são observáveis; estas deveriam ser dadas a nós, ser indicadas a nós, pela teoria."

Albert Einstein

"Não há esperanças para Teorias que, à primeira vista, não pareçam malucas."

Freeman Dyson

"O mundo real é repleto de imprecisão, incerteza e parcialidade, especialmente parcialidade de verdade, incerteza e possibilidade."

"No mundo real, quase tudo é uma questão de gradação; os absolutos são poucos e distantes uns dos outros."

"O modelo de referência da lógica *fuzzy* é a mente humana e sua notável capacidade de manipular informações baseadas na percepção sem quaisquer mensurações ou computações".

Lotfi Zadeh

Resumo da Tese apresentada à COPPE / UFRJ como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D. Sc.).

UMA CONTRIBUIÇÃO AO GERENCIAMENTO DE RISCO DA SEGURANÇA DOS SISTEMAS DE TRANSPORTE: UM MODELO *FUZZY*-HIERÁRQUICO PARA A AVALIAÇÃO DO NÍVEL DE AMEAÇA INTENCIONAL A UM SISTEMA.

Getúlio Marques Martins

Março / 2008

Orientador: Amaranto Lopes Pereira
Programa: Engenharia de Transportes

Esta tese propõe um **modelo *fuzzy*-hierárquico** para abordar o **problema da avaliação do nível de ameaça intencional a um sistema de transporte**. O nível de ameaça intencional é um dado crítico para a *provisão de segurança contra ameaças intencionais* nos sistemas de transporte, porque determina o *risco* associado às ameaças. A constante revisão desse nível e o compatível ajuste dos programas de segurança associados são requisitos internacionais do setor, que estabelecem o **gerenciamento de risco** como prática para essa provisão. Por analogia ao conceito de potencial de energia de um corpo em um campo gravitacional, define-se o **potencial de uma ameaça intencional a um sistema de transporte** como o produto de três atributos relevantes associados às ameaças intencionais - a ***impactabilidade adversa***, a ***perpetrabilidade*** e a ***probabilidade de perpetração***. O **nível de ameaça intencional ao sistema** é, então, definido como o **maior dos potenciais de ameaça** assim avaliados.

Agregados conjunturais de condições e fatores *vagos* e *ambíguos*, internos e externos ao sistema, esses atributos são usualmente **avaliados por percepção**, recebendo para valores ***expressões em linguagem natural***, em *termos absolutos*, naturalmente *imprecisas* e difíceis de manipular formalmente por métodos quantitativos clássicos. Para superar essa dificuldade, o problema é abordado pelo **Processo de Hierarquia Analítica** em associação com a **Teoria dos Conjuntos *Fuzzy*.** Por essa abordagem, o problema é estruturado em uma *hierarquia*, na qual aqueles atributos são avaliados em *termos relativos fuzzy*. Assim, o modelo reduz a *imprecisão* inerente aos resultados, provendo um formalismo matemático adequado à resolução do problema.

Abstract of Thesis presented to COPPE / UFRJ as a partial fulfillment of the requirements for the degree of Doctor of Science (D.Sc.)

A CONTRIBUTION TO SECURITY RISK MANAGEMENT OF TRANSPORT SYSTEMS: A FUZZY-HIERARCHIC MODEL FOR THE ASSESSMENT OF THE LEVEL OF INTENTIONAL THREAT TO A SYSTEM.

Getúlio Marques Martins
March / 2008

Advisor: Amaranto Lopes Pereira
Department: Transport Engineering

This thesis proposes a **fuzzy-hierarchic model** for approaching the problem of **assessing the level of intentional threat to a transport system**. The level of intentional threat is a critical input for the *provision of security* in transport systems, because it determines the ***risk*** associated to the threats. Constant revision of the intentional threat level and the commensurate adjustment of the related *security programs* are international requisites of the sector, which establish *risk management* as a practice for that provision. By analogy to the concept of potential energy of a body in a gravitational field, the **potential of an intentional threat to a transport system** is defined as the product of three relevant attributes associated to intentional threats - the ***adverse impactability***, the ***perpetratability*** and the ***probability of perpetration***. The **level of intentional threat** to that system is, then, defined as the ***largest threat potential*** among the potentials thus assessed.

Conjunctural aggregates of *vague* and *ambiguous* conditions and factors, internal and external to the system, these attributes are usually **assessed by perception**, receiving as values ***expressions in natural language***, in *absolute terms*, naturally *imprecise* and difficult to manipulate formally by classical quantitative methods. For overcoming this difficulty, the problem is approached by the **Analytic Hierarchy Process** in association with the **Fuzzy Set Theory**. By this approach**,** the problem is structured as a *hierarchy*, in which those attributes are assessed in *fuzzy relative terms*. Thus, the model reduces the *imprecision* inherent in the results, providing an adequate mathematical formalism for the solution of the problem.

SUMÁRIO

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

LISTA DE SÍMBOLOS E NOMENCLATURAS

AHP: *Analytical Hierarchy Process*

ANAC: Agência Nacional de Aviação Civil

ATSA: *Aviation and Transportation Security Act*

AVSEC: *Aviation Security*

BNDES: Banco Nacional de Desenvolvimento Econômico e Social

DAC: Departamento de Aviação Civil

DHS: *Department of Homeland Security*

IMO: *International Maritime Organization*

OACI: Organização de Aviação Civil Internacional

TSA: *Tansportation Security Administration*

FMEA: *Failure Mode and Effects Analysis*

FMECA: *Failure Mode and Effects and Criticality Analysis*

FTA: *Fault Tree Analysis*

PHA: *Preliminary Hazard Analysis*

UITP: *Union Internationelle de Transport Publique*

EDS: *Explosive Detection System*

ETD: *Explosive Trace Detection System*

CAPÍTULO 1
INTRODUÇÃO

1.1 APRESENTAÇÃO DO TEMA

O considerável aumento do custo de implementação das medidas de segurança contra ameaças intencionais no sistema de transporte aéreo, decorrente da elevação dos padrões de severidade destas medidas e da maior intensificação de seu emprego após os atentados de 11 de setembro de 2001 nos EUA (GAO, 2002), colocou, em destaque, nos fóruns internacionais do setor, a questão da *compatibilidade* e *proporcionalidade* dessas medidas ao **nível de ameaça intencional** aos sistemas de transporte.

Um adequado equacionamento e uma solução prática dessa questão são críticos para uma provisão de serviços de transportes segura e eficiente, porque permitem racionalizar os gastos com segurança, mediante o emprego de medidas preventivas e de proteção proporcionais aos níveis de ameaça intencional avaliados. Assim, o resultado das discussões internacionais setoriais não podia ser outro, senão a recomendação do uso do **gerenciamento de risco da segurança contra ameaças intencionais** como prática de gestão para essa provisão, *considerando* o risco da segurança uma *função* dos níveis de ameaça intencional aos sistemas de transporte.

Entretanto, é exatamente nesse *considerando* que se encontra o problema central do gerenciamento de risco da segurança contra ameaças intencionais nos sistemas de transporte, a saber: *a avaliação do nível de ameaça intencional* - o problema de que se ocupa esta tese.

Tal avaliação, diferente do que possa parecer, não é, absolutamente, uma tarefa simples e trivial. Ao contrário, sua característica marcante é justamente a complexidade, que, de acordo com nosso entendimento, é caracterizada por três aspectos relevantes,

claramente identificáveis em uma análise mais criteriosa do problema, conforme veremos com mais detalhes adiante. Estes aspectos são:

1º) a falta de uma definição convencionalmente aceitável no setor para a grandeza *nível de ameaça intencional*;

2º) a notória *vagueza* e *ambigüidade* que caracterizam as diferentes variáveis identificadas como concorrentes, contribuintes ou influentes na formação dessa grandeza; e

3º) a inexistência de um modelo, método ou processo *específico* para avaliar essa grandeza, capaz de tratar a vagueza e ambigüidade das variáveis envolvidas, de uma forma matematicamente adequada.

Em face dessa complexidade, a recomendação internacional do uso do gerenciamento de risco da segurança acabou implicando a adoção da **abordagem sistêmica** para a análise da segurança dos sistemas de transporte e, por conseqüência também, para a análise das ameaças intencionais. Para explicitar essa complexidade, identificando as interações entre os diferentes componentes, funções e interfaces pertinentes ao problema, esta abordagem, no entanto, deve ser entendida não como uma teoria ou uma ciência, mas sim como uma *metodologia* que tem por objetivo *reunir e organizar os conhecimentos, com vistas a uma maior eficácia da ação* (Pereira, 2006). E, neste caso particular, a *ação* para a qual se busca maior eficácia não é outra senão a *avaliação do nível de ameaça intencional a um sistema de transporte*.

Com esse entendimento, a implicação referida anteriormente é perfeitamente justificável, porque, com a abordagem sistêmica, ativos físicos e operacionais essenciais dos sistemas de transporte, assim como funções e interfaces sensíveis, podem ser melhor estudados em termos de **importância** (ou **criticalidade**) para esses sistemas e em termos de **vulnerabilidade** às ameaças intencionais, dois atributos de tais ativos ou

funções, reconhecidamente relevantes para a determinação do nível de ameaça intencional e, conseqüentemente, para o risco da segurança contra ameaças intencionais.

Além disso, a abordagem sistêmica das ameaças intencionais, ao caracterizar relevantes atributos destas ameaças, entre os quais a **perpetrabilidade** e a **impactabilidade adversa**, e analisar suas interações com os atributos relevantes da segurança, permite visualizar a natureza, a dimensão e a intensidade dessas interações, possibilitando inferir correlações capazes de viabilizar avaliações consistentes do **risco** associado.

Assim, por meio do **gerenciamento** desse **risco**, torna-se possível otimizar as decisões sobre a alocação dos recursos disponíveis para a segurança (tais como equipamentos de inspeção, pessoal treinado, sistemas de vigilância etc.), priorizando o emprego destes recursos nos ativos avaliados como de maior risco. Isto possibilita prevenir e evitar atentados a tais ativos, bem como mitigar eventuais conseqüências adversas, com maior eficácia em termos de custo, contribuindo, assim, para uma provisão de uma **segurança contra ameaças intencionais,** compatível e adequada nos sistemas de transporte.

Tendo em vista que os sistemas modais de transporte operam em uma rede relativamente integrada, a priorização do emprego desses recursos pode ser ainda mais eficaz em termos de custo, se tais ativos de risco puderem ser identificados e analisados da perspectiva dos sistemas integrados de transporte. De fato, dessa perspectiva, componentes com funções intermodais integradas, cujas características físicas, operacionais ou de segurança exibam elementos de visibilidade e de acessibilidade capazes de torná-los **alvos atrativos** a essas ameaças, podem receber mais recursos para segurança. Desta forma, não apenas os sistemas modais, mas também, por extensão, os

chamados *sistemas nacionais de transporte*, estruturas mais complexas, identificadas como formadas pelos sistemas modais de um país, podem ter sua segurança aumentada.

Por isso, conseqüências de ameaças intencionais perpetradas contra componentes individuais de sistemas de transportes não podem ser explicadas simplesmente por avaliações dos efeitos adversos isolados nesses componentes, sejam estes veículos de transporte, peças fixas da infra-estrutura de transporte ou funções críticas. Os impactos da perpetração de uma ameaça contra um componente específico devem ser analisados de uma perspectiva mais ampla, isto é, de uma perspectiva que permita observar todo o sistema modal a que esse componente pertence. Da mesma forma, impactos em sistemas modais específicos, pelos possíveis reflexos em outros sistemas modais, num efeito "cascata" em todo o sistema nacional de transportes, acaba requerendo que a análise dos impactos se estenda a todo este sistema.

Por estas razões, a identificação e a caracterização de tais *ativos,* em termos de **criticalidade** e de **vulnerabilidade a ameaças intencionais**, são cruciais para o **gerenciamento de risco da segurança**.

Os atentados de 11 de setembro de 2001, envolvendo o sistema de transporte aéreo dos EUA, e os atentados de 11 de março de 2004, em Madrid, Espanha, contra o sistema de transporte ferroviário, e de 07 de julho de 2005, em Londres, Inglaterra, contra o sistema de transporte público urbano por Metrô, evidenciaram de forma trágica e definitiva a *vulnerabilidade* desses sistemas de transporte a atos terroristas (ameaças intencionais), ressaltando as conseqüências fatídicas da exploração deste atributo dos sistemas de transporte e de suas graves repercussões na sociedade.

Desde então, a provisão de segurança contra ameaças intencionais passou a ter maior importância na gestão operacional dos sistemas de transporte, mudando de forma

radical os quadros de referência das análises de decisão sobre os investimentos e a alocação de recursos no setor.

Elementos críticos desses quadros de referência, os custos adicionais estimados da implementação de medidas de segurança mais severas redirecionaram o foco das análises para a comparação do custo total dos investimentos em segurança frente aos benefícios esperados, incluindo, nessa comparação, as *estimativas dos riscos de segurança associados*. Assim, o **gerenciamento de risco** acabou emergindo naturalmente como estratégia gerencial para a provisão da segurança contra ameaças intencionais nos sistemas de transporte.

Um claro exemplo disto aparece nas considerações utilizadas para justificar as ações propostas pela Resolução A33/1 ("*Declaração sobre o uso indevido de aeronaves civis como armas de destruição em massa e outros atos terroristas envolvendo a aviação civil*"), da 33ª Sessão Assembléia da Organização de Aviação Civil Internacional (OACI), realizada em Montreal, Canadá, entre 25 de setembro e 5 de Outubro de 2001. Nessas considerações, o custo adicional da segurança aumentada para combater "*esse novo tipo de ameaça imposta pelas organizações terroristas*"[1] e a necessidade dos Estados-Contratantes da Convenção sobre Aviação Civil Internacional empreenderem "*novos esforços concertados com uma nova política de cooperação*"[2] para a segurança da aviação civil são implicitamente reconhecidos como uma questão central a ser resolvida (OACI, 2001), levando em conta os aspectos do risco associado às ameaças.

Entre essas ações, destaca-se a de nº 5, que instou explicitamente e com urgência os Estados-Contratantes da Convenção sobre Aviação Civil Internacional a "***tomar medidas adicionais de segurança, apropriadas e proporcionais ao nível de ameaça***, *a*

[1] Tradução da Resolução A33-1 das "*Resolutions adopted at the 33rd Session of the Assembly of the International Civil Aviation Organization"*. http://www.icao.int/icao/en/assembl/a33/resolutions_a33.pdf.
[2] Ibid.

fim de prevenir e erradicar atos terroristas envolvendo a aviação civil", conforme bem mostra o trecho a seguir:

> "The Assembly solemnly:
> […] 5. Urges all Contracting States to intensify their efforts in order to achieve the full implementation and enforcement of the multilateral conventions on aviation security, as well as of the ICAO Standards and Recommended Practices and Procedures (SARPs) relating to aviation security, to monitor such implementation, and to take within their territories ***appropriate additional security measures commensurate to the level of threat*** in order to prevent and erradicate terrorist acts involving civil aviation;..."(grifo nosso)(OACI, 2002).
>
> (Tradução):
> "A Assembléia solenemente:
> [...] 5. Conclama com urgência todos os Estados Contratantes a intensificarem seus esforços para alcançar plena implementação das convenções multilaterais sobre segurança da aviação contra atos ilícitos, bem como dos Padrões, Práticas e Procedimentos Recomendados, relativos à segurança da aviação; para monitorar tal implementação; e tomar, dentro de seus territórios, ***medidas adicionais de segurança apropriadas e proporcionais ao nível de ameaça***, a fim de prevenir e erradicar atos terroristas envolvendo a aviação civil;..."(grifo nosso)(OACI, 2002).

Iniciativas similares, tomadas posteriormente pela Organização Marítima Internacional (OMI, 2002) e pela União Internacional de Transporte Público (UITP, 2004), para os respectivos modais de transporte, conforme mostram documentos dessas organizações, também requereram, explicitamente, ***ações preventivas e de proteção compatíveis e proporcionais* ao *nível de ameaça*** a esses modais de transporte.

A consolidação desse requisito nos documentos normativos setoriais procurava dar resposta urgente a três demandas decorrentes dos atentados:

1) introdução imediata de novos padrões técnico-normativos de segurança contra ameaças intencionais emergentes;

2) aperfeiçoamento de alguns dos padrões já existentes; e

3) exigência do imediato cumprimento de ambos pelos Estados-Contratantes das convenções internacionais de transporte.

Em 19 de novembro de 2001, pouco mais de dois meses após os ataques ao *World Trade Center* e ao Pentágono, os EUA lançavam sua primeira reação político-normativa a esses atentados, promulgando a Lei N.º 07–71, *Aviation and Transportation Security Act* (ATSA) que, entre outras medidas, criou uma nova instituição governamental para tratar da segurança dos transportes contra ameaças intencionais naquele país: a *Transportation Security Administration* (TSA). Embora reativa, essa iniciativa estabelecia medidas para aumentar rapidamente os níveis de segurança e a confiabilidade nos serviços de transporte prestados por esses sistemas, e, dessa forma, resgatar a confiança dos usuários nesses serviços.

A revisão dos documentos técnico-normativos setoriais, pelos organismos internacionais, também teve esse objetivo, introduzindo novos e aperfeiçoados requisitos e padrões mínimos na regulação de segurança do setor. No caso da aviação civil, essa revisão incluiu programas internacionais de *auditorias de segurança contra ameaças intencionais* (“*security”*), destinados à verificação do cumprimento desses novos requisitos e padrões de segurança pelos países-membros dessas organizações. O objetivo era obviamente assegurar o cumprimento da segurança aumentada.

Entretanto, como é de conhecimento geral, a demora na maturação das novas e aperfeiçoadas medidas de segurança e no seu processo de aprovação pelas organizações internacionais, bem como na sua posterior inclusão na regulamentação dos países membros dessas organizações, acabaram frustrando as expectativas imediatas de tais esforços. No transporte aéreo civil internacional, essa demora acabou gerando uma crise de confiança que se desdobrou em uma crise de demanda, com sérias conseqüências para a saúde financeira de várias empresas aéreas e para o desempenho dos serviços aéreos, conforme foi amplamente divulgado pela mídia internacional.

No sistema de transporte ferroviário e no sistema de transporte público por metrô, as repercussões econômicas, embora não tão drásticas quanto as vivenciadas pelo sistema de transporte aéreo civil, provocaram, ainda assim, reavaliações das práticas de gestão da segurança contra ameaças intencionais, que passaram a incluir a adoção da *análise de risco* no planejamento e na implementação de novas medidas preventivas e de proteção nesses sistemas.

Por todo o setor dos transportes, a provisão de uma segurança aumentada, caracterizada pela intensificação e aperfeiçoamento das medidas preventivas e de proteção, era reconhecida como uma ação necessária para restaurar confiabilidade aos serviços prestados pelos sistemas. Problemas de sustentabilidade econômico-financeira, entretanto, impediam sua pronta implementação, já que os custos adicionais decorrentes dessa intensificação e desse aperfeiçoamento tendiam a exceder as receitas operacionais, particularmente em componentes ou funções de baixa densidade tráfego. Nesses componentes ou funções, havia forte possibilidade da manutenção dos serviços de transporte com a segurança aumentada tornar-se economicamente inviável.

Do ponto de vista econômico-operacional, essa possibilidade é considerada irracional e indesejável, principalmente se resultar da provisão de um aumento da segurança em operações ou componentes, cujo risco de segurança se mostre baixo ou, em outras palavras, cujo risco estiver associado a um nível de ameaça intencional baixo. Esta consideração consolidava, definitivamente, a proposta de adotar o *gerenciamento de risco da segurança* como alternativa gerencial para a provisão dos serviços de segurança dos transportes contra ameaças intencionais.

Com o ***risco da segurança*** admitido como uma função do **nível de ameaça**, este ***nível*** passava a condição de *elemento de informação determinante* do grau de severidade a adotar nas medidas preventivas e, em conseqüência, um fator decisivo para

auxiliar na redução dos altos custos inerentes à implementação dessas novas medidas e equipamentos de segurança (GAO, 1998). Em conseqüência disso, a ***avaliação do nível de ameaça intencional*** aos sistemas de transporte passou a constituir uma atividade crítica do gerenciamento de risco da segurança.

Essa mudança de atitude gerencial no setor respaldava-se, portanto, em sólidos argumentos econômicos. Ao adotar o gerenciamento de risco na provisão da segurança dos transportes contra ameaças intencionais, a alocação dos recursos disponíveis no setor para essa atividade ficaria racionalizada pelo emprego de medidas de segurança apropriadas e comensuráveis com os riscos estimados ou, em outras palavras, ***apropriadas e proporcionais ao nível de ameaça intencional avaliado*** para cada sistema de transporte considerado.

Dessa forma, a eficácia das medidas de segurança tenderia a ser aumentada, ao compatibilizar a implementação das medidas de segurança a esse risco, reduzindo, eventualmente, os custos totais incorridos com a provisão de segurança contra ameaças intencionais e com a provisão dos serviços de segurança como um todo.

1.2 RELEVÂNCIA DO TEMA.

No contexto da intensificação da segurança contra ameaças intencionais, medidas tais como a *blindagem das portas das cabines de comando*, o *Programa do Agente Federal Aéreo* (*Air Marshall Program*), a *inspeção de 100% da bagagem despachada*, entre outras aplicadas no transporte aéreo e, ressalvadas as devidas particularidades, também em outros modais, reduziram sensivelmente o risco de atentados similares aos de 11 de setembro de 2001, mas também provocaram, por um processo igualmente reativo e característico das ameaças intencionais, mudanças na forma de atuar e nos elementos de interferência adversa destas.

Entre tais elementos, incluem-se os agentes químicos, biológicos, radioativos e nucleares, conhecidos como agentes CBRN (sigla derivada das iniciais de ***C**hemical, **B**iological, **R**adioactive and **N**uclear*). Entretanto, hoje, apesar de uma justificada preocupação com o potencial emprego desses agentes, há um *sentimento,* compartilhado por vários profissionais do setor, identificando os explosivos como as ameaças de maior probabilidade de risco aos sistemas de transportes (GAO, 2005).

Por essa razão, medidas preventivas tais como a inspeção dos passageiros e de sua bagagem de mão, cuja procura por itens de embarque proibido nas aeronaves consumia um razoável tempo, resultando em filas e demoras nesse embarque, passaram por extensa revisão. Baseada em análises das ameaças, vulnerabilidades e conseqüências, essa revisão resultou na retirada de alguns itens identificados como relativamente inócuos, isto é, não mais representativos de risco significativo para o sistema, sendo o tempo e o esforço de busca a eles destinados revertidos para a busca por explosivos.

Essa mudança, no entanto, intensificou o debate a respeito da adequação e eficácia dos equipamentos de inspeção utilizados na triagem de passageiros e carga, levantando sérias questões técnicas e de custo. As tecnologias disponíveis até então funcionavam relativamente bem na detecção de objetos e explosivos com componentes metálicos, mas não na detecção de armas não-metálicas ou explosivos plásticos.

Estas limitações exigiam o aprimoramento dos sistemas de inspeção existentes e o desenvolvimento de novas tecnologias de detecção de tais tipos de armas e dispositivos. Entre essas modernas tecnologias de inspeção, incluem-se:

- Tecnologias de imagem – sistemas existentes e novos equipamentos;
- Tecnologias eletromagnéticas não geradoras de imagens;
- Tecnologias de detecção de explosivos químicos e plásticos (*Explosive Detection Systems* – EDS);

- Tecnologias de detecção de vestígios de explosivos (*Explosive Traces Detection Systems* – ETD);
- Tecnologias de detecção de vestígios de agentes biológicos; etc.

Duas dessas tecnologias - a de detecção de explosivos (EDS) e a de detecção de vestígios de explosivos (ETD) - já se encontram bem desenvolvidas e em uso em vários países. Os problemas identificados no seu emprego estão mais relacionados ao seu financiamento, devido aos altos custos de aquisição, operação e manutenção, principalmente os da tecnologia EDS.

Por exemplo, o custo de aquisição de uma máquina EDS para uso no transporte aéreo varia de trezentos mil a um milhão e duzentos mil dólares (GAO, 2006), enquanto, para o transporte marítimo pode chegar a cinco milhões de dólares. Com custos de operação e manutenção variando, respectivamente, de 200 mil a 500 mil dólares por ano, o emprego desta tecnologia exige uma análise de investimento mais cuidadosa, principalmente porque, além desses custos, é necessário ainda levar em consideração os custos inerentes à disponibilização e preparo de áreas para instalação e operação desses sistemas, bem como os de seleção e treinamento especializado para pessoal de operação.

Áreas para a instalação e operação de um EDS em terminal aeroportuário, por exemplo, requerem reforços estruturais nos pisos existentes nos terminais aeroportuários, rearranjos arquitetônicos e novos procedimentos operacionais, para acomodar os fluxos de passageiros e cargas aos novos canais de inspeção de segurança criados. Já o recrutamento, a seleção e o treinamento de pessoal especializado requerem programas de treinamento novos e específicos. Em ambos os casos, os custos podem ser expressivos, quando comparados aos custos de aquisição, operação e manutenção.

Uma análise da produtividade média anual de única máquina EDS (cerca de 400 a 500 mil itens de bagagem por ano), frente aos custos totais estimados de aquisição, operação e manutenção, pode facilmente inibir seu emprego nos terminais de passageiros e cargas de um modal específico de transporte, uma solução que, embora extremamente onerosa, tem sido considerada para adoção.

Aliás, a adoção dessa solução em alguns sistemas de transporte envolveu o investimento de centenas de milhões de dólares. Os benefícios, contudo, ainda são discutíveis. O problema principal tem sido justamente o financiamento dos custos de investimento.

Apenas para dar uma idéia do volume de recursos financeiros envolvidos, a Tabela 1, a seguir, apresenta um extrato dos custos estimados em 2005 para dotar o Aeroporto Internacional de Los Angeles (LAX) e o Aeroporto de Ontário (ONT), ambos na Califórnia, de EDS nas esteiras de bagagem. Esses dados foram obtidos no Relatório GAO–07-445 do General Accountability Office dos EUA, de março de 2007 (GAO, 2007).

Tabela 1 – Custo Estimado de Instalação de EDS em Aeroportos

Aeroporto	**Custo (US$ milhões)**
Los Angeles	439,3
Ontário	53,3
Total	492,6

Fonte: US GAO Report 07-445, Março/2007.

Como se pode observar, os investimentos necessários para equipar estes dois aeroportos com EDS, são da ordem de 500 milhões de dólares. Diante de tal soma, é interessante e necessário fazer algumas contas.

Suponhamos que esses dois aeroportos juntos movimentem 50 milhões de passageiros por ano[3] e cada passageiro despache apenas uma peça de bagagem (uma hipótese conservativa). Consideremos ainda uma produção de inspeção de 500 mil peças de bagagem/ano por EDS, uma vida útil de 10 anos, uma taxa de desconto de 6% a.a. e custos de O&M anuais de 500 mil dólares. Nessas condições, para implementar o requisito normativo de *inspeção de 100% da bagagem despachada*, seriam necessárias 100 máquinas EDS. Tal operação resultaria num acréscimo de US$2.80 / passageiro na tarifa doméstica de embarque (*Passenger Facility Charge – PFC*), um impacto de mais de 50% nos US$4,50 atualmente praticados no Aeroporto de Los Angeles. Em razão disso, é, no mínimo, uma ingenuidade não admitir que o investimento em tais tecnologias necessite de modelos de provisão baseados nos riscos associados às ameaças intencionais.

Nos esforços de revisão da legislação internacional, essa necessidade foi claramente contemplada. O Anexo 17 – *Security* à Convenção sobre a Aviação Civil Internacional incluiu, expressamente, como requisito, que "*cada Estado-Contratante"* da Convenção *"revise constantemente o* ***nível de ameaça*** *às operações da aviação civil dentro de seus territórios e* ***ajuste os elementos relevantes de seu programa nacional de segurança da aviação civil de conformidade com esse nível****"* (ICAO, 2002).

De modo similar, o *International Ship and Port Facility Security Code* (Código ISPS), da OMI, também incluiu requisito, instando os governos dos países membros da Organização a *combater as ameaças com ações de redução da vulnerabilidade dos navios e instalações portuárias, mediante a* ***implementação de medidas de segurança compatíveis e proporcionais aos níveis de ameaça avaliados*** (IMO, 2002).

[3] Estatísticas do tráfego de passageiros no Aeroporto Internacional de Los Angeles estão em torno de 45 milhões anuais.(Fonte: Anuário Estatístico da FAA 2006)

O cumprimento de tais requisitos implica, no entanto, a utilização de duas ferramentas gerenciais: um *método* que possibilite *avaliar* o *nível de ameaça intencional a um sistema de transporte* e um *modelo de gerenciamento de risco* que use essa informação como fator de decisão quanto às medidas e procedimentos de segurança a serem implementados. Aliás, esta implicação é plenamente reconhecida pela OACI (2002), ao afirmar que:

> "[...] juntas, essas duas ferramentas formam os fundamentos de uma gestão de segurança contra atos ilícitos viável e efetiva em termos de custo...". [Threat Assessment Methodology. Appendix 4, § 1, Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, ICAO, 2002].

Com essa afirmativa, a OACI reiterava mais uma vez a decisão e o compromisso dos Estados-Membros em adotar o gerenciamento de risco na provisão dos serviços de segurança contra ameaças intencionais.

A presente pesquisa, ao propor um modelo para a avaliação do nível de ameaça intencional a um sistema de transporte, procura aportar recursos técnicos de suporte a essa decisão e a esse compromisso, proporcionando uma alternativa metodológica para a avaliação do risco associado às ameaças intencionais, como contribuição ao gerenciamento de risco da segurança dos sistemas de transporte.

1.3 CARACTERIZAÇÃO E DEFINIÇÃO DO PROBLEMA

A ***avaliação do nível de ameaça intencional a um sistema de transporte***, como atividade crítica do **gerenciamento de risco da segurança**, é, portanto, o ***problema objeto*** desta tese. Aparentemente simples em seus termos, esse problema, na verdade, envolve conceitos e definições que necessitam de uma análise mais detalhada para serem melhor entendidos, avaliados e utilizados adequadamente. A razão disto é que o

próprio conceito de nível de ameaça intencional a um sistema de transporte, embora tenha um forte caráter intuitivo, não é simples e objetivo, nem passível de auto-elucidação; nem tampouco tem uma definição capaz de permitir avaliações diretas de seu valor.

Diferentes fatores e condições dos sistemas de transporte e do ambiente nos quais estes operam têm afetação sobre os atributos ou componentes identificados como relevantes para a formação dessa grandeza, pragmática e tacitamente denominada no setor de *nível de ameaça*. Com efeito, um levantamento superficial identifica, pelo menos, uma dúzia de fatores e condições relevantes, a saber:

a) a conjuntura política, social, econômica e de segurança internacional;

b) a conjuntura política, social, econômica e de segurança interna do país;

c) a existência de antagonismos internos;

d) a importância relativa dos ativos físicos e operacionais dos sistemas de transporte para seu funcionamento;

e) o valor monetário desses ativos;

f) as vulnerabilidades "genéticas" ou adquiridas desses ativos;

g) as condições de implementação e controle das medidas e procedimentos de segurança;

h) a existência de grupos adversos;

i) a capacidade de perpetração das ameaças por esses grupos;

j) a capacidade de liderança e organização desses grupos para perpetração das ameaças;

k) as demandas de ordem técnica e logística para perpetração das ameaças;

l) a disponibilidade e facilidade de obtenção de meios técnicos e materiais para perpetração das ameaças;

m) etc.

Pela quantidade de variáveis envolvidas e pelas características de vagueza e ambigüidade que apresentam, este problema, na realidade, é complexo e, em geral, enfrenta dificuldades de ser resolvido por métodos clássicos quantitativos, tais como, por exemplo, a análise de risco tradicional que é fortemente dependente de um tratamento estocástico das variáveis envolvidas. Apesar disso, são os fundamentos desta análise que constituem o referencial teórico primário para a pesquisa deste tema.

De fato, no contexto da análise de risco tradicional, a abordagem deste problema geralmente tem sido feita por técnicas de cenários, nos quais o cálculo das probabilidades de ocorrência das ameaças potenciais é definido a partir de quadros conjunturais específicos, formados por "valores" específicos de variáveis associadas às ameaças, identificadas por especialistas como explicativas do risco. Além da ***probabilidade de ocorrência***, as variáveis mais comuns utilizadas nos cenários são a ***vulnerabilidade*** de alvos potenciais e as ***conseqüências ou impactos*** sobre o sistema. O risco em geral é visto como uma função dessas três variáveis.

Todas essas variáveis são geralmente avaliadas por percepção, recebendo para valores, "***expressões em linguagem natural***" do tipo: ***alta vulnerabilidade, graves conseqüências*** etc. Porém, a variável *nível de ameaça intencional*, com um valor específico, resultante da agregação de valores de determinados atributos relevantes das ameaças intencionais capazes de serem perpetradas contra sistemas de transporte, do estado dos sistemas e das condições do ambiente em que estes operam, tal como se espera de um indicador com essa finalidade, e como é requerido pelas normas internacionais, não é avaliada.

No meu entender, essa não avaliação, conforme descrito acima, deriva da complexidade de definir e avaliar um indicador com esse grau de agregação, isto é, um

indicador capaz de representar os diferentes potenciais das diferentes ameaças intencionais capazes de serem perpetradas contra um sistema de transporte. De uma perspectiva formal, uma solução para esse problema envolve primeiramente o esclarecimento de três questões primárias, intrinsecamente relacionadas entre si, referentes a esse conceito: a *questão conceitual*, a *questão metodológica* e a *questão computacional*; que passo a discutir a seguir.

A QUESTÃO CONCEITUAL

Esta questão caracteriza-se, a meu ver, pela falta de uma definição formal para o conceito *nível de ameaça intencional*, quer dizer, uma definição capaz não apenas de descrever coerentemente a estrutura e a dimensão dessa grandeza, mas também de viabilizar-lhe uma avaliação racional de valor, valor este que possa ser utilizado como fator crítico determinante do risco associado às ameaças intencionais a um sistema de transporte. Na literatura pesquisada, não encontrei uma definição nesses termos.

A falta dessa definição apresenta um sério entrave ao problema da avaliação. Como avaliar uma grandeza para a qual não se tem uma definição formal? Quer dizer, uma grandeza cujas características estruturais e dimensionais não são a priori conhecidas? Fundamental para o processo de avaliação da grandeza, esta questão deveria provocar, normalmente, abstenções do uso desse conceito.

No entanto, em que pese este argumento, não é o que acontece. Ao contrário, verifica-se um uso indiscriminado deste conceito, sem uma definição formal, bem disseminado no setor, configurando um *consenso tácito* sobre o seu significado entre os profissionais de segurança. Uma clara evidência desse uso é a inclusão do termo "*nível de ameaça*" em requisitos técnicos de documentos normativos internacionais, conforme já mencionado anteriormente. Essa inclusão, sem a definição formal, leva a supor que o

conceito é auto-explicativo em termos de significado, bem como auto-suficiente para fins de avaliação, o que, conforme veremos nesta discussão, está longe de ser o caso.

De fato, em termos práticos, uma definição não apenas é necessária, mas também constitui condição básica para a avaliação dessa grandeza, porque, ao explicitar seus elementos constituintes, sua estrutura de formação e sua dimensão, provê os elementos fundamentais para estimar seu valor, que deve emergir de uma manipulação racional e coerente dos valores desses elementos constituintes, de conformidade com as correlações estabelecidas pela definição.

Não havendo essa definição, a tendência é descrever essa grandeza apenas como um dos atributos mais relevantes das ameaças intencionais ou a elas associados, enfraquecendo sensivelmente sua percepção intuitiva de agregado de atributos e seu potencial de uso como indicador da ameaça. Ao limitar obviamente o valor da grandeza ao conjunto dos valores de um único atributo, introduzem-se imprecisões nos resultados impossíveis de serem reduzidas apenas com a manipulação desses valores.

Amplamente compartilhada entre os profissionais de segurança e disseminada pela literatura de análise de risco é a percepção de nível de ameaça como *probabilidade da ameaça* ou *probabilidade de ocorrência da ameaça* (Haimes, 1998 e 2004; GAO, 2005). Uma evidência expressiva e recente dessa disseminação pode ser verificada no discurso de Michael Chertoff, Secretário do *Department of Homeland Security* (DHS), dos EUA, ao se referir ao tratamento que o DHS pretende dar à ameaça terrorista naquele país. Ao explicar as prioridades do DHS baseadas no risco, Chertoff afirma:

> "[W]e must make tough choices about how to invest finite human and financial capital to attain the optimal state of preparedness. The Department will use three variables, corresponding to the three questions of classic risk assessment: vulnerability (What can go wrong?), threat (What is the likelihood?), and consequences. DHS will concentrate first and foremost -- most relentlessly -- on addressing threats that pose catastrophic consequences," (Por Marisa Katz, The New Republic, Editorial Page, acessado em abril de 2007, disponível em http://www.tnr.com/doc.mhtml)

> Tradução:
> "[D]evemos tomar sérias decisões sobre como investir capital humano e financeiro finitos para alcançar o estado ótimo de prontidão. O Departamento usará as três variáveis correspondentes às três questões clássicas da avaliação de risco: vulnerabilidade (O quê pode dar errado?), ameaça (Qual é a probabilidade?), e conseqüências. DHS concentrará primeiro e antes de tudo – e mais inexoravelmente -- nas ameaças que representem conseqüências catastróficas".

Nota-se, no discurso de Chertoff, a preocupação em bem aplicar recursos humanos e financeiros limitados. Assim, diz ele, "o DHS irá usar as três questões clássicas da avaliação de risco: a *vulnerabilidade*, a *ameaça* e as *conseqüências"*. Na referência à ameaça - "*...threat (What is the likelihood?)*" ["*...ameaça (Qual é a probabilidade?*)"], vê-se claramente a percepção desse problema como de *avaliação da probabilidade (de ocorrência) da ameaça*, numa evidente prova do uso desse único atributo para representar a ameaça.

Infelizmente, isto introduz um erro de entendimento fatal, por meio do qual o próprio termo *ocorrência* e não *perpetração* (semanticamente mais apropriado a *atos intencionais*) produz a percepção deturpada de que tais *ameaças intencionais* são *eventos aleatórios*. Como conseqüência direta dessa percepção deturpada, *nível* é implicitamente *percebido* como *probabilidade de ocorrência*, caracterizando esta *percepção deturpada* provavelmente uma das causas principais da falta de uma definição. Aparentemente irrelevante, esta questão é, na verdade, crítica, porque dela derivam as escolhas dos processos ou métodos de avaliação dessa grandeza.

Ameaças intencionais, ou, em termos mais objetivos, atos intencionais, não "*ocorrem*", no sentido semântico comum deste verbo. Atos intencionais são "*perpetrados"*. Tal perpetração, normalmente, envolve um processo complexo, que inclui um *planejamento* detalhado por parte de um *agente perpetrador, motivado* e com um *objetivo bem definido*. Em geral, a escolha do tipo da ameaça pelo perpetrador está

intimamente ligada a este objetivo que, normalmente, transcende o mero dano ao ou destruição dos componentes de um sistema de transporte[4]. Mais adiante nesta tese, esta questão é abordada com mais detalhes.

Entretanto, o que importa ressaltar neste ponto é que tal planejamento baseia-se em *avaliações* de diversos *atributos* pertinentes à perpetração das ameaças pelo agente perpetrador. Entre tais fatores incluem-se: *a* ***própria capacidade do agente perpetrar*** as ameaças (incluindo aspectos tais como sua ***organização, capacitação técnica e logística***); a ***oportunidade*** (***ocasião e condições gerais do ambiente***); a ***impactabilidade adversa*** das ameaças no sistema, a ***perpetrabilidade*** destas etc.

Devido ao caráter vago e ambíguo dessas variáveis, essas avaliações são normalmente feitas com base na *percepção* do agente perpetrador, percepção esta que internaliza seu conhecimento e experiência sobre as *afetações* desses atributos por condições operacionais, de segurança e de criticalidade do sistema-alvo, ou por condições e fatores gerais do ambiente em que o sistema opera, todas estas também igualmente vagas e ambíguas, também avaliadas por percepção, e que, agregadas, concorrem para formação do que denomino nesta tese de ***probabilidade de perpetração*** das ameaças intencionais.

Por essas razões, o conceito de ***nível de ameaça intencional a um sistema de transporte*** proposto nesta tese procura internalizar aquele atributo, agregando-o, de uma forma original, à ***perpetrabilidade*** e à ***impactabilidade adversa***, atributos mais próprios das ameaças intencionais, quase propriedades destas, identificados como relevantes para a formação desse conceito.

[4] Uma análise de diferentes ameaças intencionais ou atos de interferência ilícita perpetrados contra sistemas de transporte mostra que os objetivos dos atos raríssimas vezes foram os danos ou a destruição de componentes desses sistemas. Normalmente, os objetivos são mais amplos e de outro jaez.

Uma definição formal e coerente de *nível de ameaça intencional,* nesses termos, constitui, portanto, a primeira contribuição desta tese à resolução do problema e um elemento central do modelo aqui proposto.

A QUESTÃO METODOLÓGICA

A questão metodológica, por sua vez, emerge do fato de não ter sido encontrado, na literatura pesquisada, um método ou processo que tenha a finalidade específica de *avaliar o nível de ameaça intencional a um sistema de transporte*. Parecendo uma decorrência natural da questão conceitual, este fato pode ser facilmente constatado na literatura existente sobre análise de risco da segurança (McCormick, 1981; Rasche, 2001; Haimes, 1998 e 2004).

Na análise de risco tradicional, este problema normalmente é abordado sob a denominação de *avaliação da ameaça*, e não *avaliação do nível de ameaça*. Como instrumentos de avaliação, encontram-se métodos qualitativos, quantitativos e híbridos (qualitativo-quantitativos). Porém, com denominação e finalidade específicas de *avaliar o nível de ameaça intencional*, não encontrei nenhum método na literatura pesquisada.

Não obstante, a modelagem e os procedimentos de alguns dos métodos clássicos de *avaliação da ameaça* existentes baseiam-se em conceitos e princípios que podem ser utilizados como referencial teórico para uma análise e avaliação aceitável deste índice. No capítulo 3 desta tese, ao fazer uma revisão dos métodos utilizados, apresento com mais detalhes esses aspectos.

A QUESTÃO COMPUTACIONAL

Por último nesta discussão, temos a questão computacional. Esta questão é caracterizada pela dificuldade relativa que as atuais metodologias encontram em tratar, formalmente, a vagueza e a ambigüidade que caracterizam, não apenas os atributos

intrínsecos das ameaças intencionais, mas também os atributos físicos, operacionais e de segurança do sistema, e, ainda, os fatores e/ou condições do ambiente em que o sistema opera. Devido a essa vagueza e ambigüidade, essas variáveis, conforme já mencionado anteriormente, tendem a ser avaliadas mais com base na *percepção* de especialistas do que com base em mensurações físicas (instrumentais).

Por esse motivo, seus valores são expressões em linguagem natural ou expressões lingüísticas ou, ainda, "valores lingüísticos", que internalizam o conhecimento profissional, a experiência e o "*feeling*" dos especialistas em segurança dos transportes. Formadas a partir de interações desses fatores, essas expressões embutem, naturalmente, toda a subjetividade inerente a esse tipo de avaliação, sendo, por esse motivo, permitam-me dizer, "geneticamente*" imprecisas* e, em geral, difíceis de serem estimadas em valores absolutos, mesmo quando estes valores são de natureza qualitativa.

Além disso, ao serem representadas por "valores lingüísticos", essas variáveis enfrentam certa dificuldade em serem manipuladas por métodos de avaliação clássicos tradicionais. Tal dificuldade, portanto, remete à escolha ou ao desenvolvimento de um modelo, cujo formalismo matemático seja capaz de viabilizar essa manipulação de forma racional e coerente, eventualmente aumentando o rigor científico do processo de avaliação e reduzindo a imprecisão inerente aos resultados, que é, justamente, o que se pretende dar, em termos de contribuição, com o modelo proposto nesta tese.

Esclarecidas essas questões, passo a definir, nos parágrafos a seguir, o problema objeto desta tese em seus aspectos mais específicos.

DEFINIÇÃO DO PROBLEMA

Em termos práticos, a segurança dos sistemas de transporte contra ameaças intencionais pressupõe a implementação de medidas e procedimentos de segurança

destinados a prevenir e a proteger o sistema contra a perpetração de tais ameaças. Geralmente, para cada ameaça intencional específica, é possível listar um elenco das medidas e procedimentos de segurança, destinados a prevenir o sistema contra aquela ameaça.

Todavia, a provisão simultânea de medidas e procedimentos preventivos e de proteção contra todas as ameaças intencionais possíveis de serem perpetradas contra o sistema é, obviamente, uma decisão irracional, extremamente onerosa e ineficiente em termos de custo. Pelo menos dois motivos podem explicar isso: (1) a *redundância* das medidas preventivas, em face da similaridade de modos de perpetração de diferentes ameaças; e (2) a *desproporcionalidade* do grau de severidade dessas medidas, em relação ao potencial diversificado de interferência adversa que as ameaças podem apresentar contra o sistema.

Em razão disso, a estratégia de gestão a ser adotada na provisão da segurança deve ser a do gerenciamento de risco da segurança, que prevê a implementação de medidas e procedimentos de prevenção e de proteção em quantidade e grau de severidade compatíveis e proporcionais às estimativas do risco correspondente ao *nível de ameaça* ao sistema.

Depreende-se daí, portanto, que níveis de ameaça avaliados de forma imprecisa resultam em estimativas imprecisas do risco e, por conseguinte, no estabelecimento de medidas e procedimentos de segurança inapropriados. Tal estabelecimento de medidas e procedimentos de segurança inapropriados, por sua vez, compromete a eficácia dessa segurança, e, por conseguinte, sua eficiência econômica.

DECLARAÇÃO FORMAL DO PROBLEMA

O cerne do problema objeto desta tese é, portanto, o de avaliar o nível de ameaça intencional a um sistema de transporte, considerados o estado de funcionamento e de

segurança deste sistema e a conjuntura política, social, econômica e de segurança do ambiente no qual este opera. Para tanto, é necessário primeiro que se tenha uma definição coerente e aceitável desse conceito. Considerando haver essa definição (que, aliás, será provida no devido momento mais adiante nesta tese), podemos declarar esse problema em termos formais, da seguinte maneira:

"*Dado um sistema de transporte, com todos seus componentes funcionais (veículos, terminais, vias, sistemas de comunicação e controle de tráfego etc.), operando com regularidade diferentes serviços (domésticos urbanos, interurbanos e internacionais); um conjunto de* **n** *ameaças intencionais relevantes* (A_1, A_2,...,A_n)*, identificadas como capazes de serem perpetradas contra o sistema; caracterizadas por três atributos relevantes: a* impactabilidade adversa (*IMPAC*), *a* perpetrabilidade (*PERPE*) *e a* probabilidade de perpetração (*PROBA*)*; um conjunto de* **p** *condições e fatores* (C_1, C_2,..., C_p)*, identificados como os de afetação mais significativa sobre esses atributos; e um grupo de* **m** *especialistas em segurança dos transportes* (E_1, E_2,..., E_m)*, hierarquizados em termos de capacitação, experiência e"feeling" sobre segurança contra ameaças intencionais, determine o* nível de ameaça intencional *(NAI) a esse sistema de transporte"*.

1.4 OBJETIVO DA TESE

O objetivo desta tese é resolver esse problema, procurando, com essa resolução, dar uma contribuição original e inédita ao gerenciamento de risco da segurança dos sistemas de transporte. Tendo em vista o caráter ambíguo e vago das variáveis envolvidas e a propensão de serem avaliadas mais por percepção, a abordagem adotada para o problema desvia-se das convencionais, que são baseadas em modos de raciocínio clássico, para apoiar-se em outra, baseada em modos de raciocínio aproximado.

Esta outra abordagem consiste de um **modelo analítico-quantitativo** que combina conceitos e princípios do **Processo de Hierarquia Analítica (AHP)** e da **Lógica *Fuzzy*,** em outras palavras, um modelo ***Fuzzy*-Analítico-Hierárquico**, ***Fuzzy*-AHP** ou, simplesmente, ***Fuzzy*-Hierárquico**.

Os conceitos e princípios dessas duas técnicas são utilizados, respectivamente, para **estruturar hierarquicamente o problema** em subproblemas de menor complexidade e **manipular formalmente** os valores lingüísticos atribuídos às variáveis envolvidas pela Teoria dos Conjuntos Fuzzy.

Como **elementos de originalidade,** temos os conceitos propostos de ***potencial de ameaça intencional*** e de ***nível de ameaça intencional***, bem como, obviamente, o uso dessa **associação de técnicas** para manipular os valores das variáveis envolvidas. Com tal modelo, pretende-se reduzir a imprecisão inerente aos resultados e dotar o processo de avaliação de um adequado formalismo matemático, aumentando seu rigor científico.

1.5 METODOLOGIA ADOTADA NA PESQUISA

A **hipótese central** admitida nesta tese é que o problema objeto de interesse da pesquisa, isto é, o **problema da avaliação do nível de ameaça intencional a um sistema de transporte,** é complexo, subjetivo e, por essa razão, mais passível de avaliação por métodos qualitativos ou híbridos. Tendo em vista que as variáveis envolvidas nessa avaliação têm características de variáveis lingüísticas, assumindo para valores normalmente expressões em linguagem natural, estimadas com base na percepção de especialistas em segurança, a resolução do problema implica **processos de avaliação** classificados como essencialmente **subjetivos** e/ou **qualitativos.**

Portanto, a pesquisa concentrou-se principalmente em processos de avaliação de perfil qualitativo, utilizando métodos de pesquisa exploratória. A pesquisa exploratória (Gil, 2002) é descrita como tendo por objetivo proporcionar mais familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. Esse autor acrescenta ainda que seu planejamento é, portanto, bastante flexível, possibilitando a consideração dos mais variados aspectos relativos ao fato estudado.

Consideraram-se também alguns elementos de natureza **descritiva** para a sua elaboração, já que a pesquisa visa a descrever as características de uma "grandeza", no caso relacionada às dimensões que condicionam a evolução das ameaças intencionais no setor dos transportes, e como estas afetam os fatores estruturantes do atual modelo de provisão de segurança. Cooper e Schindler (2003) apontam os elementos de pesquisa descritiva como:

> [...] descrições de fenômenos ou características associadas com a população-alvo (o quem, que, quando, onde e como de um tópico); estimativa de proporções de uma população que tenha essas características, e descoberta de associações entre as diferentes variáveis. (COOPER e SCHINDLER, 2003, p. 136)

Quanto às técnicas ou meios de pesquisa empregados, utiliza-se a **pesquisa bibliográfica,** incluindo um exame da literatura existente sobre o assunto, tanto em livros acadêmicos, teses e dissertações, quanto em artigos publicados em periódicos, anais de congressos e de conferências realizados no setor. Verifica-se que, embora o acervo existente de artigos tratando da avaliação da ameaça a sistemas de transportes seja razoavelmente grande e diversificado, de um modo geral, esta questão é abordada como uma etapa crítica da análise de risco da segurança e do gerenciamento de risco (Haimes, 1998, 2004; GAO, 2005). Em conseqüência, grande parte desta pesquisa tem por base essa literatura.

Outro caminho metodológico foi a **pesquisa documental** (elaborada a partir de materiais que não receberam tratamento analítico), e adicionalmente da **observação informal**, incluindo a pesquisa de relatórios técnicos, artigos independentes de associações especializadas, "white papers" etc., disponíveis na internet, nos *sites* de instituições que se dedicam aos estudos deste tipo de ameaça. Entre os principais *sites* pesquisados, destacamos o *National Threat Assessment Center* (NTAC), com artigos dedicados especialmente ao terrorismo, e o *General Accountability Office* (GAO), ambos dos EUA, naqueles artigos e relatórios que versam sobre metodologias de avaliação das ameaças intencionais (terrorismo internacional).

A pesquisa relativa ao desenvolvimento do modelo proposto teve como referencial teórico os princípios, conceitos e referências bibliográficas introduzidos pelas disciplinas "Confiabilidade e Segurança nos Sistemas de Transporte" e "Tópicos Especiais em Análise de Risco", do Programa de Engenharia de Transportes, e "Introdução à Lógica Fuzzy", do Programa de Engenharia de Produção, ambos da COPPE/UFRJ.

Parte da argumentação conceitual utilizada nesta tese deriva da experiência do autor, adquirida no desempenho de cargos e funções no sistema de aviação civil brasileiro, vinculados ao objeto da pesquisa, bem como do acesso a informações e dados utilizados nessas instâncias. Entre tais cargos e funções, são pertinentes os desempenhados no Sub-departamento de Infra-Estrutura do ex-Departamento de Aviação Civil, do Comando da Aeronáutica, nas áreas de análise da regulamentação e controle da segurança da aviação civil, do desenvolvimento e operações da infra-estrutura aeroportuária, bem como os desempenhados no Painel de Especialistas em Segurança da Aviação Civil e no Painel de Especialistas em Facilitação do Transporte Aéreo, ambos da Organização de Aviação Civil Internacional (OACI).

Por razões de sigilo, a maioria dos documentos internacionais e nacionais sobre o assunto recebe a classificação de RESERVADO, condicionando sua consulta apenas a pessoas que tenham sido credenciadas com o grau de acesso correspondente. Por esse motivo, material contido nesses documentos deixa de ser incluído nesta tese.

Dados e informações de segurança utilizados nesta tese restringem-se exclusivamente àquilo que se encontra divulgado publicamente pelos órgãos responsáveis, em publicações e *sites* do setor. Contudo, como os documentos sigilosos podem ser eventualmente de interesse para uma consulta suplementar, sua referência é incluída nas referências bibliográficas, ficando, no entanto, o acesso aos interessados condicionado à autorização pela autoridade competente.

Em particular, dados e informações de segurança que poderiam servir para compor um estudo-de-caso são também, em sua maioria, sigilosos, não estando disponíveis para manipulação. Desta forma, limitar-me-ei a apresentar um exemplo ilustrativo.

Em se tratando de um modelo, a utilização de um exemplo ilustrativo, a rigor, até comporta certas vantagens, porque torna possível explorar situações hipotéticas de ameaça, nas quais é possível simular, dentro de intervalos paramétricos aceitáveis, os valores das variáveis relevantes que entram na formação dos potenciais das ameaças específicas ao sistema.

Pelas mesmas razões, é possível simular diferenças nos valores dos atributos que caracterizam o conhecimento, a experiência e o "feeling" em segurança contra ameaças intencionais dos profissionais em atuação no setor, designados para o grupo de avaliação do nível de ameaça ao sistema. Da perspectiva dos objetivos desta tese, tais possibilidades, são interessantes para fins de explicitação das potencialidades e de simplificação de apresentação do modelo.

1.6 ORGANIZAÇÃO DO CONTEÚDO

O restante desta tese está organizado da seguinte forma. No capitulo 2, uma breve descrição dos estudos de segurança e confiabilidade dos sistemas de transportes é apresentada, logo no início do capítulo, com a finalidade de explicitar as diferenças conceituais existentes entre segurança operacional e segurança contra ameaças intencionais, a partir das características das faltas envolvidas, bem como da relação de dependência entre segurança e confiabilidade. A noção de segurança de funcionamento (*dependability*) de um sistema é também discutida em seus aspectos conceituais. Em seguida, faz-se uma descrição mais detalhada de ameaças intencionais. Neste ponto, introduz-se formalmente o conceito de potencial de uma ameaça intencional específica a um sistema de transporte. A partir desse conceito, o nível de ameaça a um sistema de transporte é definido também em termos formais. Finalmente, a filosofia e os princípios básicos do gerenciamento de risco da segurança são descritos, com destaque para o papel que a avaliação da ameaça tem no contexto da análise de risco da segurança.

No Capítulo 3, os atuais métodos de avaliação da ameaça são examinados *vis-à-vis* os objetivos da presente proposta. Ainda neste capítulo, apresentamos os conceitos e princípios da Teoria dos Conjuntos "Fuzzy" e do Processo de Hierarquia Analítica. Um contraponto da Lógica Fuzzy com o Método de Inferência Bayesiana é incluído para fundamentar a escolha da Lógica Fuzzy como modo de raciocínio de suporte ao modelo. Complementam ainda este capítulo, uma descrição sucinta do conceito de variável lingüística e sua importância para os objetivos desta tese. Os modelos Analíticos Hierárquicos Fuzzy são apresentados em seus aspectos teórico-práticos.

No capítulo 4, o Modelo "*Fuzzy-Analítico-Hierárquico*" é apresentado, iniciando com uma descrição geral do modelo. Em seguida, o problema é decomposto

em uma hierarquia de elementos pelo Processo de Hierarquia Analítica (AHP) e a escala fundamental de correspondência numérico-conceitual adotada neste processo é convertida em números "fuzzy" triangulares. A forma de avaliar o grau relativo de conhecimento e experiência em segurança é então apresentada. Os dois próximos tópicos do capítulo abordam respectivamente as metodologias de avaliação da Importância Relativa de Fatores e Condições para o Potencial de Ameaça e dos Potenciais das Ameaças Específicas Relevantes Identificadas. Finalmente concluímos o capítulo com a agregação que determina o Nível de Ameaça Intencional ao Sistema de Transporte.

O capítulo 5 apresenta um exemplo ilustrativo de aplicação do modelo para a segurança da aviação civil contra atos de interferência ilícita de um país hipotético, com o objetivo de melhor explicitar as etapas, passos e manipulações computacionais do modelo.

No capítulo 6, faz-se uma síntese da tese, repassando os principais aspectos da pesquisa, as características particulares do problema abordado, reforçando os principais argumentos apresentados, descobertas e as principais conclusões sobre os resultados obtidos com a aplicação do modelo. Algumas recomendações para pesquisa futura são incluídas ao final.

Capítulo 2

SEGURANÇA E CONFIABILIDADE, SEGURANÇA DE FUNCIONAMENTO, AMEAÇAS INTENCIONAIS E GERENCIAMENTO DE RISCO.

Atos intencionais adversos perpetrados contra sistemas de transporte não podem ser estudados da mesma forma que falhas de natureza estrutural ou operacional destes, nem como falhas decorrentes de causas naturais. Por terem origem na intenção humana, sua perpetração envolve a análise de motivações, objetivos, condições e fatores, a maior parte dos quais externos à estrutura física e operacional desses sistemas. Por essa razão, as ameaças intencionais necessitam de outra forma de estudo e tratamento.

A análise de eventos intencionais passados mostra que a **visibilidade e repercussão dos eventos** são os principais atributos associados aos objetivos dos perpetradores. Porém, a escolha de um sistema para a perpetração de determinado ato intencional depende parcialmente da **vulnerabilidade** relativa da estrutura física e operacional do sistema às ameaças intencionais e da **criticalidade** dos componentes e processos dessa estrutura. A gravidade das conseqüências adversas dependerá, naturalmente, da importância para o funcionamento do sistema dos componentes ou processos escolhidos como alvos. Assim, esses dois atributos são importantes para a análise da ***segurança*** desses sistemas contra ameaças intencionais e, obviamente, para o ***gerenciamento de risco*** dessa ***segurança***.

Numa análise abrangente do funcionamento dos sistemas, ambos atributos têm relação direta com a *integridade,* a *confidencialidade e* a *disponibilidade* dos serviços prestados pelo sistema, três atributos que dependem drasticamente da *segurança contra ameaças intencionais* (*security*).

Este capítulo visa a discutir essa dependência, situá-la no contexto da taxonomia da segurança de funcionamento dos sistemas e justificar a adoção da abordagem proposta nesta tese para a avaliação do nível de ameaça intencional, fora do referencial teórico tradicional dos estudos de tolerância a falhas.

Iniciamos com as noções de segurança e confiabilidade. Em seguida, abordamos sucintamente a segurança de funcionamento dos sistemas, para nos concentrarmos nas ameaças intencionais, introduzindo, neste momento, os conceitos de *potencial de uma ameaça específica* a um sistema de transporte e o de *nível de ameaça intencional* a um sistema de transporte. Um item específico é dedicado à segurança dos transportes contra ameaças intencionais. Finalmente, fechamos o capítulo com uma discussão sobre o gerenciamento de risco da segurança.

2.1 SEGURANÇA E CONFIABILIDADE

Segurança e **confiabilidade** são dois atributos de extrema importância para o desempenho dos sistemas de transportes. Enquanto a confiabilidade é um agregado de vários outros atributos, entre os quais a **segurança**, esta, por sua vez, é mais primária e independente, servindo, normalmente, de sustentação para outros atributos, especialmente a **confidencialidade**, a **integridade** e a **disponibilidade**. Todavia, os dois conceitos são vagos e ambíguos.

Com efeito, uma análise da segurança realizada com o propósito de definir o processo de avaliação de risco e o correspondente tratamento preventivo associado, mostra uma clara diferença dos conceitos. Essa diferença relaciona-se diretamente à natureza das causas dos eventos adversos que podem sobrevir a esses sistemas.

Como estas causas podem ser *naturais, acidentais ou intencionais,* não apenas o processo de avaliação de risco pode variar como também pode variar o conseqüente tratamento preventivo. Por exemplo, se os eventos tiverem causas *naturais* ou

acidentais, avaliações de risco baseadas em processos estatísticos e probabilísticos são normalmente indicadas. Neste caso, o tratamento preventivo geralmente inclui redundâncias operacionais ou políticas de manutenção mais rigorosas.

Por outro lado, se os eventos ou ameaças tiverem causas *intencionais*, os conceitos e princípios da estatística e da probabilidade já não se mostram tão adequados como ferramentas de análise ou de avaliação. A razão disso, entretanto, não está na ausência ou insuficiência de dados e/ou informações sobre os atributos que caracterizam essas causas, mas no fato de que análises estocásticas tradicionais de tais dados e/ou informações pouco contribuem para aumentar o conhecimento sobre os eventos.

Nestes casos, processos alternativos, com outras capacidades analíticas para tratar a vagueza e a ambigüidade, devem ser pesquisados e utilizados, no intuito de assegurar o rigor científico necessário a uma avaliação de risco com um grau aceitável de imprecisão. O tratamento preventivo, em geral, incluirá medidas e procedimentos de segurança, tais como o controle de acesso a instalações ou informações, o credenciamento de pessoas e veículos, a inspeção física de veículos ("varredura"), a revista de pessoas e de seus pertences, etc.

Confiabilidade (*"reliability"*), por sua vez, também apresenta aspectos conceituais vagos e ambíguos. Segundo Pereira (2003), em seu sentido comum, o termo "*confiabilidade*" corresponde à "*confiança do usuário no material (ou serviço) que ele utiliza (ou consome)*", enquanto, no sentido estrito, pode ser definido como a "*característica (ou aptidão) de um dispositivo, expressa pela probabilidade que este tenha de cumprir uma dada (requerida) função, em* ***condições de segurança****, durante uma duração dada*".

Verifica-se, portanto, que a confiabilidade de um sistema de transporte é conceitualmente dependente das condições ***de segurança,*** de forma que, na prática,

espera-se que, proporcionando mais segurança ao sistema, estaremos necessariamente contribuindo para aumentar sua confiabilidade. Examinemos, então, um pouco mais a questão da vagueza e ambigüidade do conceito de segurança e sua relação com a **segurança de funcionamento**, já que esta última, por constituir um conceito mais amplo, inclui o atributo da confiabilidade.

A Noção de Segurança

No estudo da segurança dos sistemas, a nomenclatura científica internacional registra dois termos em inglês, ***safety*** e ***security*** (ou, respectivamente, *sécurité* e *sûreté,* em francês), que veiculam a noção de segurança. O que distingue um conceito do outro, mas também reforça suas características de ambigüidade, é justamente, a natureza da causa das falhas que podem sobrevir aos sistemas. Quer dizer, se a ocorrência tem como causa um evento (ameaça) acidental, estamos diante de um problema de *safety* (*sécurité*), mas se a causa é um evento (ou ameaça) intencional, defrontamo-nos com um problema de *security* (*sûreté*).

Assim, a *safety* de um sistema está ou pode ser comprometida se a *falha* ocorrida (ou passível de ocorrer) tiver, como causa, um *evento acidental*. Esse evento acidental tanto pode ser *físico* (produzindo um erro físico-estrutural em algum componente – então visto como um sistema) quanto *de concepção* (caracterizado por imperfeições na estrutura operacional ou na arquitetura do sistema, tanto na fase inicial de produção quanto nas modificações posteriores). Esses tipos de *eventos* são ditos *internos ao sistema*. Entretanto, podem ocorrer falhas no sistema derivadas de *eventos externos*, capazes de produzir *erros de interação homem-máquina* ou *erros de entrada* de dados ou informações para o sistema. Mesmo nestes casos, a natureza dos eventos é tipicamente *acidental*.

A *security* de um sistema, por sua vez, está ou pode ser comprometida, se a *falha* ocorrida (ou passível de ocorrer) no sistema tiver como causa um *evento intencional*. Neste caso, a *intenção humana* aparece como o elemento constituinte central do *evento*, cuja concretização se dá pelo aproveitamento de *vulnerabilidades* ou *deficiências* (genéticas ou adquiridas) da estrutura física ou operacional do sistema, bem como das suas interfaces com o ambiente em que opera. *Erros de interação homem-máquina* ou *erros de entrada* de dados ou informações no sistema podem também resultar de atos de interferência maliciosa, com a *intenção humana* aproveitando-se de eventuais vulnerabilidades (deficiências de autenticidade ou de acessibilidade) na segurança do sistema.

Um aspecto importante, por vezes negligenciado nas análises de segurança, é que a provisão de *security* tem por finalidade assegurar a *safety* do sistema e que estes dois atributos, *safety* e *security*, concorrem para garantir a *segurança de funcionamento do sistema*.

Examinemos, então, o conceito de *segurança de funcionamento* ou "*dependability"* de um sistema, um conceito relativamente recente, utilizado no contexto da ***tolerância a faltas,*** em princípio, passível de extensão à análise de risco, em sua relação com a segurança operacional (*safety*) e a segurança contra atos de interferência adversa (*security*).

2.2 SEGURANÇA DE FUNCIONAMENTO ("*DEPENDABILITY*")

Originariamente direcionados para sistemas de computação e para a tecnologia da informação, os estudos de *segurança de funcionamento* ("*dependability"*) vêm ganhando espaço e aplicação em outros sistemas. Tal fato parece dever-se, em parte, à síntese dos conceitos fundamentais de tolerância a faltas, formulada por Laprie, no livro

"*Dependability: Basic Concepts and Terminology*", editado em 1985, e disseminada mais tarde em seu artigo de 1989 (Laprie, 1989).

Nessa síntese, Laprie descreve a estrutura da *segurança de funcionamento* como sendo composta por seis **atributos** de um sistema: *disponibilidade*, *confiabilidade*, "*safety*", *confidencialidade*, *integridade* e *manutenibilidade.* Além desses ***atributos***, Laprie inclui ainda, nesta estrutura, os ***entraves*** ou impedimentos, que ele classifica de *faltas, erros e falhas*, e os ***métodos***, classificados como *prevenção, tolerância, remoção e previsão de faltas*. Em razão do seu formato, essa estrutura foi por ele denominada de "Árvore da *Dependability*" ou Taxonomia da Segurança de Funcionamento.

Segurança de funcionamento, de acordo com essa taxonomia, "*caracteriza a aptidão de um sistema realizar suas funções dentro de determinadas condições dadas"*. Reafirmando esse conceito, Pereira (2003), ressalta que "*em sentido estrito, segurança de funcionamento de um sistema é um atributo do serviço prestado pelo sistema, capaz de inspirar em seus usuários uma confiança justificada*". Justificada, esclarece Pereira, naturalmente por níveis adequados dos seis atributos referidos.

Nota-se, entretanto, que "*security*" não é incluída nesse conjunto de atributos. Numa primeira tentativa de integrar "*security*" aos estudos da "*dependability*", faltas intencionais (lógica maliciosa, invasões, etc.) foram grupadas em uma classe específica de faltas, diferente da classe das faltas acidentais (deficiências físicas, erros de concepção ou de interação), com o objetivo de obter uma clara identificação e caracterização dos entraves e seus elementos, bem como uma apropriada identificação dos métodos.

Após 1985, outros autores (Dobson & Randell, 1986; Joseph & Avizienis, 1988; Fray *et al*. 1986) iniciam uma pesquisa exploratória sobre a integração da segurança contra faltas intencionais na análise da tolerância a faltas. O resultado de tal pesquisa

indicou que a "*security*" proporciona à estrutura física e operacional dos sistemas as condições para que os serviços prestados exibam valores aceitáveis de *integridade, confidencialidade e disponibilidade*. Assim, "*security*" seria um atributo compósito desses três atributos. Em outras palavras, a informação de que um sistema é *seguro contra eventos intencionais* implicaria que os serviços prestados pelo sistema seriam *íntegros*, *confidenciais* e *disponíveis*.

Nos sistemas de transportes, valores aceitáveis desses três atributos da segurança de funcionamento são obviamente capazes de inspirar uma *confiança justificada* nos usuários dos serviços. O problema nos sistemas de transportes é que, tradicionalmente (pelo menos no contexto técnico-normativo), outros atributos são vistos como importantes.

Por exemplo, na aviação civil, prevalece a doutrina de que todos os padrões técnicos e procedimentos operacionais devem, no mínimo, assegurar a *safety* e a *regularidade* das facilidades e dos serviços prestados. De fato, ao definir o *status* dos padrões incluídos nos Anexos Técnicos à Convenção sobre Aviação Civil Internacional, a OACI estabelece expressamente que estes são:

> "Qualquer especificação de característica física, configuração, material, desempenho, pessoal ou procedimento, cuja aplicação uniforme é reconhecida como necessária para a segurança operacional (*safety*) ou regularidade da navegação aérea internacional, que os Estados Contratantes se obrigam a cumprir, de acordo com o estabelecido na Convenção".

Já a *security* tem por finalidade, em princípio, assegurar a integridade física e operacional dos sistemas de transporte contra ameaças intencionais. Isto é geralmente feito mediante a implementação de medidas preventivas e de contingência contra tais ameaças. Para o estabelecimento dessas medidas, os sistemas de transporte devem ter sua estrutura física e operacional analisada de uma forma tal que suas principais componentes físicas e funcionais, bem como suas interfaces, possam incluir atributos

correlacionados aos quesitos de segurança, ao serem caracterizadas. Nessa análise, dois atributos são considerados como de relevância primária: a *criticalidade* dessas componentes físicas, funções e interfaces e sua *vulnerabilidade* a ameaças intencionais.

Para facilitar essa análise, os serviços prestados por um sistema de transporte são geralmente divididos em duas classes específicas: (1) os serviços prestados pelos veículos de transporte; e (2) os serviços prestados pela infra-estrutura de transporte. A percepção dos usuários parece ser mais crítica em relação à segurança dos serviços prestados pelo veículo de transporte, quer dizer, do deslocamento propriamente dito. Porém a conscientização sobre a segurança dos serviços prestados pela infra-estrutura de transporte, caracterizados pela oferta de estradas, terminais, instalações e serviços de informações, de comunicações e de controle tráfego, vem se intensificando cada vez mais.

O outro atributo importante dos sistemas de transporte, do ponto de vista dos serviços prestados, é a ***regularidade*** desses serviços. Conforme já mencionado, organismos internacionais, tais como a OACI e a OMI, enfatizam que os padrões técnicos estabelecidos em seus documentos normativos destinam-se a garantir a *segurança operacion*al (*safety*) e a ***regularidade*** dos serviços e facilidades ofertadas pelos respectivos sistemas de transporte.

Embora não conste da taxonomia geral proposta por Laprie (1985, 1989, 1990), a regularidade dos serviços de transporte tem um papel crítico no desempenho dos sistemas, com fortes reflexos na economia. "*Trade-offs*" entre custos de estoque e custos do transporte ressaltam a importância da regularidade dos serviços de transporte na "performance" dos sistemas logísticos, muitas vezes estabelecendo-o como o fator-chave para tomadas de decisão no setor. A inclusão da regularidade desses serviços, no escopo dos estudos da segurança de funcionamento e particularmente na análise de risco

da segurança contra ameaças intencionais, é também importante para os sistemas de transporte.

Nosso próximo item destina-se a apresentar com mais detalhes o conceito de ameaça intencional aos sistemas de transporte. Embora até este ponto da tese, o termo *ameaça intencional* já tenha sido utilizado várias vezes, o seu significado talvez ainda não tenha sido completamente assimilado, de forma que achamos necessário apresentá-lo de maneira mais formal, para consolidar não apenas o conceito, mas também as noções dos atributos condições e fatores relevantes a ele associados.

2.3 AMEAÇAS INTENCIONAIS A SISTEMAS DE TRANSPORTES

Sistemas de transporte, assim como outros sistemas de produção de bens e serviços, estão sujeitos a diferentes tipos de ameaças. Entre estes tipos incluem-se:

a) catástrofes naturais;

b) eventos acidentais externos ao sistema, com repercussão no sistema;

c) falhas estruturais ou operacionais internos ao sistema; e

d) atos ou atentados contra a integridade / confidencialidade / regularidade dos serviços prestados pelo sistema.

A diferença primária entre estes tipos de ameaça está na origem ou natureza das causas. Enquanto nos três primeiros tipos, a natureza das ameaças é reconhecida como eminentemente *acidental*, isto é, completamente independente da vontade ou intenção humana, no último tipo, essa intenção constitui o atributo determinante da ameaça e aquilo que a faz distinta das demais.

O objeto de exame desta tese são as ameaças de natureza intencional aos sistemas de transporte. Ameaças de natureza intencional aos sistemas de transportes podem ser definidas como ***quaisquer atos capazes de serem perpetrados contra a***

integridade física e / ou operacional dos sistemas de transporte, com o intento de comprometer-lhe o funcionamento regular, por meio de dano a ou destruição de algum componente, interface ou função[5].

Estas ameaças têm, portanto, na intenção humana, o elemento central e determinante, sem o qual sua natureza fica descaracterizada. Como essa intenção vale-se normalmente de meios ilegais para se concretizar, estas ameaças são também comumente denominadas de *atos ilícitos* ou *atos de interferência ilícita*. Este último termo, aliás, já é de uso bem consagrado no sistema de transporte aéreo civil internacional (ICAO, 2002).

Um fator importante e condicionante das ameaças intencionais é a motivação. Teorias comportamentais clássicas da psicologia social (Maslow, 1954; Vroom, 1964) defendem a tese de que o ser humano só age motivado. Segundo essas teorias, motivação é o processo responsável pela intensidade, direção e persistência dos esforços de uma pessoa para a concretização de uma intenção. Vroom (1964), em particular, acredita que a "*motivação é o processo que governa ou condiciona a escolha de comportamentos intencionais alternativos*". Pode-se admitir, portanto, que a qualquer ato intencional está associada uma motivação. Por exemplo, o *vandalismo*, um dos atos intencionais ilícitos mais comuns, admite uma motivação: o prazer mórbido dos vândalos.

Entretanto, a maioria dos motivos pelos quais atos intencionais ilícitos têm sido praticados contra os sistemas de transporte tem sido vinculada a interesses ou objetivos ideológicos políticos ou religiosos. Entre tais interesses e objetivos, incluem-se, por exemplo, o reconhecimento internacional da soberania sobre territórios ocupados por etnias, a libertação de presos políticos, o radicalismo religioso, lutas sociais, etc.

[5] A destruição de todo um sistema de transporte pela perpetração de atos intencionais é, naturalmente, uma possibilidade de ameaça intencional descartada da análise de possibilidades, por ser considerada irrealizável do ponto de vista prático.

São raríssimos os casos de atos intencionais adversos perpetrados com o objetivo específico de provocar dano ou destruir ativos de sistema de transporte. Assim, a constante análise da conjuntura política, social, econômica e de segurança internacional e regional é vital como instrumento de avaliação do nível de ameaça aos sistemas de transporte.

A perpetração de um ato intencional ilícito contra um sistema de transporte, entretanto, depende de vários outros fatores e condições intrínsecos e extrínsecos ao ato. Um fator intrínseco relevante é a propriedade que o ato tem de poder ser perpetrado, sob determinadas condições, que aqui denomino de ***perpetrabilidade***.

Diferentes gradações de perpetrabilidade são possíveis, dependendo da interação do conjunto de características ou atributos do ato com as características e atributos do agente perpetrador, assim como com as condições de segurança do sistema e as condições do ambiente. Conforme seja a forma e intensidade dessa interação, a ameaça poderá ser percebida como mais facilmente perpetrável ou menos facilmente perpetrável, isto é, a ameaça terá *maior* ou *menor perpetrabilidade*.

A organização e porte do agente perpetrador têm relação direta com a ameaça e o grau de deterrência das medidas de segurança em vigor. Com efeito, face ao atual poder de deterrência das medidas de segurança em vigor nos sistemas de transportes, a perpetração por uma única pessoa vem se tornando um caso raro. Excluindo-se os chamados "homens-bomba", as ameaças intencionais mais comuns contra os sistemas de transporte têm sido perpetradas por grupos de pessoas dotados de um mínimo de organização, liderança e suporte logístico, tais como certas facções radicais extremistas, de ideologia política ou religiosa.

Exemplos notórios deste fato são os grandes atentados aos sistemas de transportes divulgados pela mídia, cuja perpetração tem sido reclamada por grupos ou

células pertencentes a facções terroristas de motivação étnico-político-religiosa. Entre tais facções, destaca-se a Al Qaeda, de origem islâmica, que se responsabilizou pelos atentados de 11 de setembro de 2001, ao *World Trade Center,* em Nova Iorque, e ao Pentágono, em Washington, D.C., nos EUA, bem como pelos atentados do Metrô de Londres, em 07 de julho de 2005.

Conceito de Potencial de Ameaça Intencional Específica e de Nível de Ameaça Intencional a um Sistema de Transporte.

Nesta tese, parte-se do ***pressuposto*** de que, para toda *ameaça intencional* a um sistema de transporte, isto é, para todo *ato intencional* (o que exclui ato involuntário ou acidental) capaz de interferir adversamente em um sistema de transporte, é possível associar uma grandeza, que aqui denomino de ***potencial de ameaça intencional***, conceituada de forma análoga à energia potencial de um corpo em um campo gravitacional.

Tal como na energia potencial de um corpo, essa grandeza é determinada pelo produto de três variáveis associadas às ameaças intencionais: duas mais inerentes a essas ameaças - a *impactabilidade adversa* e a *perpetrabilidade* - e uma mais inerente à conjuntura e condições do ambiente em que o sistema opera - a *probabilidade de perpetração da ameaça*. Essas três variáveis seriam os análogos respectivos da *massa* de um corpo (*m*), da *altura* (*h*) do corpo em relação a um nível de referência gravitacional, e da *constante do campo gravitacional* (*g*), do conceito de energia potencial de um corpo em um campo gravitacional.

A ***impactabilidade adversa*** pode ser definida como a propriedade intrínseca que as ameaças intencionais têm de comprometer o funcionamento regular dos sistemas de transporte, por meio de dano ou destruição de algum componente, função ou interface

do sistema de transporte. A impactabilidade adversa deve ser capaz de expressar a *gravidade* e o *alcance (extensão)* da *interferência adversa* no sistema. A impactabilidade adversa decorre da interação circunstancial de fatores e condições tais como a ***criticalidade do alvo,*** o ***potencial de interferência*** em outros componentes, funções ou interfaces do sistema, a ***letalidade da ameaça,*** etc.

A ***perpetrabilidade***, conforme já mencionado anteriormente, é definida como a propriedade que as ameaças intencionais têm de poderem ser concebidas e perpetradas com maior ou menor facilidade pelo agente perpetrador. A perpetrabilidade deriva também da combinação interativa de fatores e condições tais como a ***capacidade de liderança e de organização do perpetrador,*** as ***demandas de ordem técnica e logística da perpetração***, a ***disponibilidade e facilidade de obtenção de meios técnicos e materiais para perpetração*** no mercado doméstico e internacional, etc.

Já a ***probabilidade de perpetração*** é definida como uma variável associada à ameaça que depende da interação conjuntural de fatores e condições mais externos ao sistema, tais como a ***conjuntura político-social, econômica e de segurança*** da ***região*** ou ***país***, a ***conjuntura político-social, econômica e de segurança internacional,*** o ***status de implementação e controle das medidas de segurança***, um eventual histórico de perpetração da ameaça etc.

As medidas desses três atributos relevantes da ameaça variam com a forma e intensidade dessa interação, podendo ser obtidas com agregações coerentes e adequadas desses fatores e condições**.**

A partir dessas definições, é possível obter alguns agregados conceituais interessantes. Por exemplo, a agregação por multiplicação da *impactabilidade adversa* e da *probabilidade de perpetração* em uma única variável pode constituir o conceito de

"*poder de interferência adversa da ameaça*", uma grandeza capaz de atualização pela variável *perpetrabilidade* da ameaça.

Este raciocínio permite representar ameaças intencionais como vetores de três componentes. A representação vetorial é ao mesmo tempo interessante, prática e conveniente, porque retém a informação desagregada dos valores dos atributos relevantes que caracterizam a ameaça. Para os profissionais de segurança, essa retenção desagregada de informação pode constituir uma "virtude" que falta em representações por um único atributo.

Além disso, a agregação desses valores em uma grandeza significativa, tal como o potencial específico de uma ameaça intencional a um sistema, conforme aqui proposto, é, ao mesmo tempo, interessante e útil para fins de comparação relativa entre as ameaças e de definição da severidade das medidas preventivas e de proteção a serem adotadas.

No contexto do problema examinado nesta tese, o que se busca é um indicador mais abrangente, capaz de representar de forma adequada e racional as condições de ameaça intencional ao sistema de transporte. Considerando todos os potenciais específicos das ameaças identificadas como capazes de serem perpetradas contra esse sistema, esse indicador, denominado **nível de ameaça intencional ao sistema de transporte** é definido como o *maior potencial entre os potenciais de ameaça específicos avaliados*.

Formalização Matemática dos Conceitos

Assim, em termos formais, se $\boldsymbol{IMPAC_i}$, $\boldsymbol{PERPE_i}$ e $\boldsymbol{PROBA_i}$ são, respectivamente: a *impactabilidade adversa da ameaça intencional* ***i*** *a um sistema de transporte;* a *perpetrabilidade dessa ameaça;* e sua *probabilidade de perpetração*

contra esse sistema, todas avaliadas por percepção, de conformidade com as definições anteriores, então a ***ameaça intencional i*** ($\boldsymbol{A_i}$) pode ser representada pelo vetor:

$$\boldsymbol{A_i = (IMPAC_i, PERPE_i, PROBA_i)} \qquad \text{(I)}$$

O potencial dessa ameaça ao sistema ($\boldsymbol{POTA_i}$), de acordo com a analogia mencionada, será determinado pelo produto dessas componentes, isto é, por:

$$\boldsymbol{POTA_i = (IMPACi) \otimes (PERPEi) \otimes (PROBAi)} \qquad \text{(II)}$$

onde ⊗ significa um operador de agregação por multiplicação de variáveis lingüísticas.

Portanto, consideradas todas as *n* ameaças intencionais específicas relevantes, A_1, A_2, A_3,..., A_i,..., A_n, identificadas como capazes de serem perpetradas contra o sistema de transporte, o ***nível de ameaça intencional*** *a esse sistema,* (***NAI***), grandeza de interesse do modelo aqui proposto, seria, então, determinado por:

$$\boldsymbol{NAI = máx\ (POTA_i)} \qquad \text{(III)}$$

onde: i = 1, ..., n,

n = número de ameaças intencionais identificadas como capazes de serem perpetradas contra o sistema.

No capítulo 4, trataremos com maior detalhamento estas definições, tendo em vista que esses valores deverão derivar de manipulações dos valores dessas variáveis, conforme a aplicação do modelo proposto.

Tipos de Ameaças

Entre as ameaças intencionais mais comuns e passíveis de serem perpetradas contra os sistemas de transporte, incluem-se:

a) a sabotagem de instalações, veículos, funções ou interfaces do sistema;
b) o apoderamento ilícito de instalações ou veículos de transporte (com manutenção ou não de reféns);
c) a colocação e detonação de explosivo a bordo de veículos ou em instalações de transporte;
d) a interferência adversa nos sistemas de comunicação e de controle das operações de transporte;
e) etc.

A sabotagem constitui ameaça intencional em que o perpetrador visa comprometer a segurança de funcionamento do sistema, mediante a introdução de algum dispositivo nocivo ou a retirada, desativação ou destruição de algum componente funcional, ou qualquer interferência adversa em uma função ou processo, com o objetivo de provocar uma pane ou um colapso no sistema, dessa forma, comprometendo a prestação dos serviços pelo sistema. Dependendo da impactabilidade da sabotagem, além de danos ou destruição de componentes do sistema, as conseqüências podem também incluir vítimas.

O apoderamento ilícito (*unlawful seizure*) de veículos ou instalações de transporte consiste da tomada do controle desses componentes do sistema pela força (normalmente com o uso de armas), podendo ocorrer ou não a feitura de reféns. No caso do apoderamento ser perpetrado durante a viagem dos veículos de transporte, com desvio de rota ou destino programado, o ato ilícito é comumente denominado de *seqüestro*.

A colocação de explosivos a bordo de veículo ou em instalação de transporte e a interferência adversa nos sistemas de comunicações e de controle das operações de transporte são ameaças intencionais de significado óbvio, dispensando definições mais detalhadas.

Um aspecto importante e característico de todas essas ameaças, muitas vezes esquecido nas avaliações, é que sua concretização depende, primariamente, do acesso físico ou virtual não autorizado do agente perpetrador e/ou da introdução do artefato às áreas ou setores sensíveis, normalmente de acesso restrito, dos sistemas ou de seus componentes.

Os eventos de 11 de setembro de 2001, em que aeronaves do transporte aéreo comercial foram utilizadas como armas de destruição contra o *World Trade Center*, em Nova Iorque, e contra o Pentágono, em Washington DC, configuraram a perpetração um ato de interferência ilícita, o *apoderamento ilícito de veículo de transporte em operação* (seqüestro de aeronave em vôo), pela força com o *uso de arma introduzida a bordo*, burlando as inspeções de segurança.

Os ataques terroristas ao transporte ferroviário em Madrid, Espanha, em 11 de marco de 2004, e ao Metrô de Londres, Inglaterra, em 07 de julho de 2005, por sua vez, configuraram a colocação e conseqüente detonação de explosivo a bordo de veículo de transporte.

Em cada um destes atos, os perpetradores conseguiram burlar os controles de acesso e os sistemas de vigilância remota, ultrapassando os postos de controle de acesso e os canais de inspeção, com a introdução de artefatos ou dispositivos explosivos em setores sensíveis do sistema.

A Perpetração de Ameaças Intencionais e as Contramedidas de Segurança

Ao longo dos últimos 40 anos, vários atos ilícitos contra a segurança dos transportes foram perpetrados, com resultados trágicos para a população ou o governo dos países alvos. Tais atos, além da destruição de componentes dos sistemas de transportes, como veículos, terminais e instalações diversas, provocaram a morte de várias pessoas e a destruição de ativos públicos e privados.

Uma cronologia histórica dos principais incidentes terroristas no mundo, de 1961 a 2003, feita pelo Bureau de Assuntos Públicos do Departamento de Estado dos EUA (2004), inclui vários atos ilícitos contra veículos e instalações de transporte, envolvendo a morte de milhares de pessoas, além da destruição dos alvos dos ataques.

De acordo com Pate (2001), pesquisador assistente sênior do Instituto de Estudos Internacionais de Monterey, Califórnia – EUA:

> "As tendências terroristas durante os últimos quinze anos indicam que redes internacionais com uniões fracas, motivadas principalmente por ideologias religiosas que querem vítimas em massa, estão substituindo os terroristas mais 'tradicionais', cuja motivação principal é política".

Afirma ainda Pate que "*estas tendências ameaçadoras sugerem potencial de ataques em massa e, como os agentes biológicos podem ser usados para esse fim, o potencial para o bioterrorismo em massa pode vir a calhar*".

Os atentados de 11 de setembro de 2001 nos EUA, os de 11 de março de 2004 em Madrid e os de Sete de julho de 2005, em Londres, confirmaram estas tendências de destruição em massa, evidenciando, de forma trágica e sem precedentes, a vulnerabilidade dos sistemas de transporte a tais atos de interferência ilícita.

O embarque dos terroristas em vôos domésticos de empresas aéreas dos EUA, cuja competência em termos de prevenção contra atos ilícitos no sistema de transporte

aéreo gozava de reconhecimento mundial, evidenciou ainda mais essa vulnerabilidade, ressaltando a necessidade e a urgência de fortalecer e priorizar a segurança nesse modal. Drásticas repercussões na forma de tratar a segurança dos transportes contra atos de interferência ilícita em todo o mundo se fariam sentir após esses atentados.

No sistema de transporte aéreo civil internacional, a reação consistiu do estabelecimento imediato de alertas de segurança nos mais elevados níveis, em praticamente todos os países membros da Organização de Aviação Civil Internacional (OACI).

Para a segurança da aviação civil, isto significou o emprego de medidas e procedimentos de segurança no mais alto grau de severidade. A conseqüência do emprego de medidas de segurança nesse grau de severidade foi a quase paralisação, em alguns países, das operações aéreas do segmento internacional, com graves reflexos no segmento doméstico.

Conforme já mencionado no capítulo 1, a primeira resolução da 33ª Assembléia da OACI, realizada entre 25 de setembro e 05 de outubro de 2001 (a Resolução 33-1), instou os 188 Estados-membros daquela organização a desenvolver com urgência esforços no sentido de aperfeiçoar e de fortalecer as medidas de segurança contra atos de interferência ilícita (ICAO, 2001).

Nessa resolução, a Assembléia também instou o Conselho da OACI a revisar com urgência o Anexo 17 – *Security* à Convenção sobre a Aviação Civil Internacional, com a finalidade de aperfeiçoar os padrões de segurança ali estabelecidos.

No sistema de transporte marítimo, diante da possibilidade de navios e portos sofrerem ataques similares aos de 11 de setembro de 2001, a Organização Marítima Internacional (*International Maritime Organization* - IMO), em Conferência do setor realizada em Londres, no dia 13 de dezembro de 2002, desenvolveu um conjunto

abrangente de medidas, denominado *International Ship and Port Facility Security Code* (Código ISPS), para melhorar a segurança contra ameaças aos navios e instalações portuárias. O Código ISPS entrou em vigor em julho de 2004, provendo uma estrutura consistente e padronizada para avaliar o risco das ameaças. Com o Código ISPS, os Governos dos países membros da Organização passavam a dispor de orientações para combater tais ameaças com ações de redução da vulnerabilidade dos navios e instalações portuárias, mediante a implementação de medidas de segurança compatíveis e comensuráveis com os níveis de ameaça avaliados (IMO, 2002).

Na Conferência Internacional sobre Segurança Pessoal no Transporte Público, realizada em 4 de junho de 2004, em Genebra, Suíça, a *International Association of Public Transport* (UITP) e a *International Union of Railways* (UIC) assinaram uma declaração conjunta contra o terrorismo, com a finalidade de demonstrar o compromisso das duas entidades em combater o terrorismo no transporte público. Essa iniciativa conjunta reconhecia que o transporte internacional não era o alvo exclusivo dos ataques terroristas. Ao contrário, o transporte público doméstico estaria se tornando um dos principais alvos do terrorismo, principalmente por causa da sua vulnerabilidade física e operacional.

Na declaração conjunta, a UITP e a UIC conclamaram os operadores do transporte público a realizar análises de vulnerabilidade em suas redes, mas reconheceram também que a *avaliação e o monitoramento de ameaças terroristas* são uma *responsabilidade primária das autoridades nacionais*, a quem cabe manter os operadores informados sobre o *nível da ameaça*, para permitir-lhes estabelecer as necessárias medidas de prevenção (UITP, 2004). De fato, por serem abertos, completamente acessíveis e por transportarem diariamente uma quantidade considerável de passageiros, os sistemas de transporte público apresentam alto grau de

vulnerabilidade a ações terroristas. Como não existe controle de acesso dos passageiros nem designação de assento (uma rotina comum no transporte aéreo) e as redes de serviço, de extensa cobertura geográfica, terem múltiplas paradas, conexões e alta rotatividade de veículos e passageiros, o transporte público, além de proporcionar inúmeras opções de acesso e fuga a terroristas, torna difícil um monitoramento de segurança efetivo e eficiente. A paralisação de suas operações pode confundir e levar o público ao pânico, uma vez que constrange a mobilidade das pessoas, um atributo geralmente percebido e considerado uma liberdade fundamental.

Nos EUA, em 19 de novembro de 2001, o Congresso aprovou o *Aviation and Transportation Security Act*, um estatuto que criou a Administração de Segurança dos Transportes (TSA) no Ministério dos Transportes americano (*The Department of Transport*), para ser responsável pelas questões de segurança contra atos ilícitos em todas as modalidades de transporte naquele País. A TSA absorveu as responsabilidades de segurança da aviação civil da Administração Federal de Aviação (FAA), passando a regulamentar as atividades de segurança no transporte aéreo civil, antes atribuídas àquele órgão (*US Congress*, 2001).

Como se pode notar, os atentados de 11 de setembro de 2001, nos EUA, deram origem a uma mobilização geral em quase todos os modais de transporte quanto à questão da segurança contra atos de interferência ilícita. Embora não tenha havido um sincronismo nas ações de resposta decorrentes dessa mobilização, é interessante observar que houve consenso sobre a necessidade de adotar o gerenciamento de risco na provisão da segurança contra ameaças intencionais nesses modais. No próximo item, veremos como se processa normalmente essa provisão de segurança contra ameaças intencionais nos sistemas de transporte.

2.4 A SEGURANÇA CONTRA AMEAÇAS INTENCIONAIS AOS SISTEMAS DE TRANSPORTES

A segurança dos sistemas de transporte contra ameaças intencionais consiste primariamente da implementação de medidas e procedimentos destinados a prevenir e a proteger os componentes e os processos operacionais dos sistemas de transporte contra tais ameaças, preservando a integridade física e/ou operacional desses sistemas. Incluída na provisão de segurança está também a implementação de medidas e procedimentos de contingência, para o caso de tais ameaças chegarem a ou estarem em via de se concretizar.

Medidas e procedimentos de segurança adotados para combater as ameaças aos sistemas de transportes, em suas características gerais, praticamente não apresentam variação de um modal para outro. Tal sucede porque as ameaças aos sistemas de transporte também não variam muito de modal para modal.

No sistema de transporte aéreo civil, no qual esta atividade tem tido mais divulgação, são definidos não mais que seis atos ilícitos típicos capazes de ameaçar o sistema de aviação civil (ICAO, 2002). O conjunto de medidas e procedimentos de segurança, portanto, é também limitado. Além disso, outras limitações podem derivar de diferenças nas características físicas e / ou operacionais específicas de cada modal.

Podem-se verificar casos em que uma medida eficaz em um modal pode mostrar-se pouco aplicável ou completamente inaplicável em outro. Por exemplo, a inspeção de passageiros e de seus pertences de mão, medida preventiva extensamente utilizada no transporte aéreo, antes do embarque dos passageiros nas aeronaves, é praticamente inaplicável ao transporte público por ônibus ou Metrô.

De forma similar, o patrulhamento da cerca de segurança que protege áreas operacionais de acesso restrito em um modal, medida preventiva de extrema

importância em um aeroporto, pode ser uma medida difícil de ser praticada em uma faixa de domínio de uma ferrovia, em razão de sua extensão.

Uma outra questão central verificada no combate às ameaças é que estas evoluem, estando sempre um passo a frente das ações de prevenção. Aliás, a maioria dos avanços nas medidas preventivas acontece após medidas em vigor terem sido superadas por uma nova forma de atuação das ameaças.

Classificação das Medidas de Segurança

Em geral, as medidas de segurança são classificadas em medidas de prevenção e medidas de contingência. As medidas de prevenção destinam-se a evitar a prática de atos de interferência ilícita mediante a aplicação de procedimentos e controles de segurança, em pontos sensíveis ou vulneráveis do sistema, ou mediante a introdução de mecanismos ou processos que reforçam as barreiras físicas ou operacionais existentes ou eliminam vulnerabilidades latentes ou adquiridas.

Já as medidas de contingência destinam-se a viabilizar ações de negociação, de repressão, de socorro a vítimas e de mitigação geral dos efeitos de uma ameaça em curso ou já concretizada. Medidas de contingência requerem um alto grau de coordenação entre os operadores do sistema e os diferentes órgãos e instituições públicas e privadas envolvidas, tais como Defesa Civil, Polícia Federal, Hospitais etc. Essas ações normalmente são reunidas em um Plano de Contingência do Operador do Sistema de Transporte, do qual a autoridade deve exigir no mínimo um exercício de treinamento anual.

Enquanto o conjunto de medidas de contingência é quase estático, em razão das conseqüências das ameaças no máximo variarem de lugar ou escala, o conjunto de medidas preventivas tende sempre a crescer e/ou a evoluir, acompanhando o eventual

aparecimento de novas ameaças ou novas formas de atuação das já existentes. A rigor, com a sofisticação dos métodos adotados pelas ameaças, as medidas de segurança vão se aperfeiçoando, incluindo novas tecnologias de detecção de armas e explosivos e monitoramento remoto, credenciamento, entre outras.

Medidas e procedimentos de segurança são às vezes customizados por ameaças específicas e outras vezes abrangentes para várias ameaças específicas. Neste último caso, a capacidade de prevenção da medida ou procedimento cobre uma ampla faixa de vulnerabilidades do sistema, possíveis de serem explorados pelas ameaças.

Duas das vulnerabilidades mais propícias à exploração por várias ameaças aos sistemas de transportes são a inexistência ou a deficiência dos controles de acesso não autorizado, físico ou virtual, e a debilidade das barreiras das áreas restritas de segurança ou dos componentes sensíveis do sistema. A maioria dos atos de interferência ilícita procura explorar essas vulnerabilidades ou deficiências nos sistemas.

Por esse motivo, uma medida de segurança considerada básica nos sistemas de transporte é o controle de acesso de pessoas e de veículos e a inspeção de seus pertences, visando a prevenir a introdução de itens considerados perigosos nas áreas restritas de segurança. O controle de acesso inclui, no mínimo, procedimentos de credenciamento de pessoas e veículos, a verificação de identidade e procedimentos de inspeção de pessoas e seus pertences, por meios técnicos ou manuais.

Responsabilidade pela Segurança

Na maioria dos países, a segurança dos transportes contra atos de interferência ilícita é de responsabilidade da autoridade nacional dos transportes, normalmente um Ministério dos Transportes ou órgão similar. Nos EUA, essa responsabilidade era do *Department of Transport*, porém, desde 19 de novembro de 2002, passou a ser do então

criado *Department of Homeland Security* (DHS), que anexou a TSA como uma de suas administrações federais. No Brasil, essas responsabilidades são atribuídas ao Ministério dos Transportes, ao Ministério da Defesa e ao Ministério da Justiça.

O cumprimento dessas responsabilidades inclui normalmente Programas Nacionais de Segurança, no qual, além das alocações de atribuições e responsabilidades entre os diferentes entes da federação, operadores e agentes diversos, com ingerência ou interesse nos serviços de transporte, são estabelecidas normas gerais referentes às estruturas dos sistemas de segurança, com respectivas remissões a regulamentos, instruções e manuais específicos por modal.

Elementos centrais desses Programas são as auditorias sistemáticas de segurança, compulsórias e regulares, destinadas a possibilitar a avaliação das medidas de segurança, com vistas a identificar e a corrigir deficiências e não-conformidades na implementação dos padrões estabelecidos.

Conforme já mencionado, normas de segurança, estabelecidas por organizações internacionais de transporte já incluem a revisão constante do *nível de ameaça* das operações e o *gerenciamento de risco da segurança* como requisitos ou recomendações a serem cumpridos pelos países membros dessas organizações. No próximo item, veremos em que consiste basicamente o gerenciamento de risco da segurança nos sistemas de transporte.

2.5 GERENCIAMENTO DE RISCO DA SEGURANÇA EM SISTEMAS DE TRANSPORTE

Várias são as definições para gerenciamento de risco existentes na literatura (Haimes, 1998 e 2004; NIPC, 2002; Walker e Guthrie, 1999; Casada et al., 2001; GAO, 2005). Todas, de um modo geral, são unânimes em descrever essa atividade como um

processo contínuo de avaliar riscos, estabelecer e implementar medidas preventivas e de contingência, para reduzir a probabilidade de ocorrência de eventos adversos e mitigar os impactos negativos derivados de uma eventual contingência.

GAO (2005), por exemplo, descreve gerenciamento de risco como sendo "uma estratégia para auxiliar as autoridades a tomar decisões que envolvem risco, tais como alocações de recursos humanos, materiais ou financeiros para o desenvolvimento de ações sob condições de incerteza".

O gerenciamento de risco tem sido usado por décadas nos setores público e privado, em áreas tais como seguros e finanças, entre outras, mas sua aplicação ao terrorismo e a outras ameaças intencionais ainda não tem precedentes. O gerenciamento de risco pode ser aplicado tanto para atentados terroristas quanto para desastres naturais, tais como terremotos e tempestades, bem como para acidentes.

Contudo, diferente de tempestades e acidentes, ameaças intencionais envolvem um adversário com a intenção deliberada de causar dano ou destruição. Por essa razão, os riscos associados a essas ameaças, em termos de probabilidades e conseqüências, ainda são mal compreendidos e difíceis de avaliar e prever.

No campo dos seguros, por exemplo, utiliza-se uma grande variedade de técnicas estatísticas para avaliar e gerenciar o risco associado aos produtos e serviços segurados. No setor público, diversos órgãos usam o gerenciamento de risco para estabelecer normas, proteger o ambiente, a saúde e a segurança dos cidadãos.

Embora algumas metodologias e processos de gerenciamento de risco possam ser complexos e requerer assessoria e apoio de especialistas, outros aspectos dessa atividade - tais como o estabelecimento de metas e o uso de medidas de performance para acompanhar seu alcance - são bem compreendidos e largamente praticados.

No gerenciamento de risco, a avaliação do risco é a atividade pivotal, porque dela decorrem as demais. No entanto, como o risco é um fator associado diretamente à natureza do evento adverso, é fundamental identificar e caracterizar essa natureza, para instruir a escolha do processo de avaliação.

O Gerenciamento de Risco da Segurança Contra Ameaças Intencionais nos Sistemas de Transporte

Na segurança dos sistemas de transporte contra ameaças intencionais, o gerenciamento de risco tem essas mesmas funções. Em termos práticos, gerenciar o risco da segurança dos sistemas de transporte contra ameaças intencionais significa empreender esforços gerenciais no sentido de empregar medidas e procedimentos de segurança compatíveis e proporcionais aos riscos associados aos níveis de ameaça intencional aos sistemas.

O propósito central do gerenciamento de risco da segurança nos sistemas de transporte não difere dos propósitos em outros sistemas. O que se pretende com o gerenciamento do risco é alocar racionalmente os recursos disponíveis, para proporcionar prevenção e proteção das instalações e operações desses sistemas a um custo que resulte na eficiência econômica nessa alocação.

Baseado nas práticas da indústria americana, GAO (2005) desenvolveu uma estrutura para o gerenciamento de risco, dividida em cinco etapas:

(1) o estabelecimento de metas e objetivos estratégicos e a determinação de restrições;

(2) a avaliação dos riscos;

(3) a avaliação das alternativas para lidar com esses riscos;

(4) a escolha das alternativas apropriadas; e

(5) a implementação das alternativas e a monitoração do progresso e resultados alcançados.

Essa estrutura é mostrada na figura 1, a seguir. Pode-se observar que apenas ao completar o ciclo é possível reavaliar os resultados obtidos.

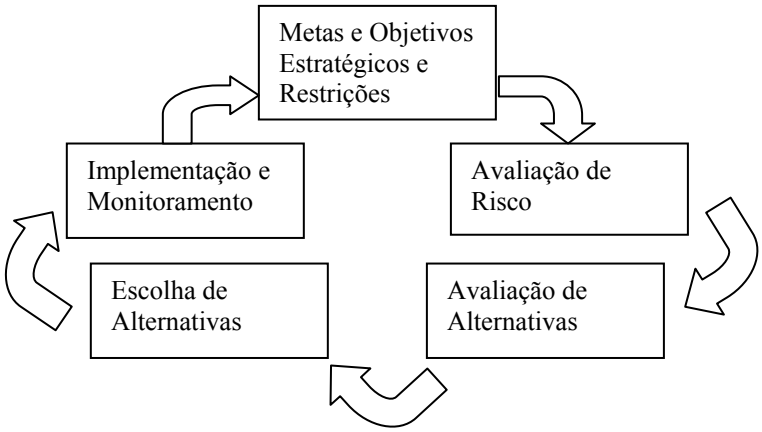

Figura 1: Estrutura de Gerenciamento de Risco
Fonte: GAO (2005)

A avaliação do nível de ameaça aos sistemas de transporte tem profundas implicações no gerenciamento do risco da segurança contra atos intencionais. Ações preventivas decorrentes destas avaliações tendem a melhorar a *segurança operacional* (*safety*) dos veículos, terminais, passageiros e carga, mas os custos incorridos com tais ações podem aumentar significativamente os custos da indústria, ocasionando eventuais crises de provisão. A habilidade em quantificar apropriadamente os riscos para os sistemas de transporte permite desenvolver políticas operacionais destinadas a equilibrar os custos das ações preventivas / corretivas com os benefícios de uma segurança aumentada.

A rigor, precisa-se de meios para avaliar em que setores ou componentes do sistema de transporte os riscos são maiores, para priorizar as respostas de segurança, isto é, para priorizar o emprego de contramedidas de segurança, de maneira que a quantidade limitada de recursos financeiros disponíveis seja utilizada da forma mais

eficaz possível e as contramedidas de segurança sejam proporcionais e compatíveis aos riscos identificados em cada componente do sistema (terminais, veículos, empresas de transporte ou rotas praticadas).

O uso do gerenciamento de risco da segurança contra ameaças intencionais nos sistemas de transporte é, portanto, relevante e requer um comprometimento pró-ativo de todos os envolvidos na provisão dos serviços de transporte, incluindo as autoridades públicas, os operadores dos veículos de transporte e da infra-estrutura dos transportes, mormente no tocante ao transporte de passageiros, em razão dos prêmios de seguro envolvido nas operações.

Embora existam na literatura da modelagem de risco várias metodologias de avaliação da ameaça à segurança, poucas se preocupam em agregar os potenciais individuais das ameaças determinados, para a obtenção de um índice representativo de sua combinação. A idéia de um índice assim, para assistir à autoridade competente a estabelecer o alerta apropriado, é, no entanto, intuitiva, tanto que a denominação dos alertas existentes pouco varia de um País para outro, limitando-se geralmente a alguns adjetivos tais como, *baixo, médio, alto, severo, moderado* etc.

Nos EUA, por exemplo, são adotados cinco alertas de segurança. Denominados de *condições de ameaça* ("*Threat Conditions*" ou abreviadamente THREATCON), tais alertas são definidos com os seguintes rótulos, cores e significados:

Tabela 2 – Níveis de Ameaça Adotados nos EUA

Rótulo	**Cor**	**Significado**
SEVERO	VERMELHA	Risco Severo de um Ataque Terrorista
ALTO	LARANJA	Risco Alto de um Ataque Terrorista
ELEVADO	AMARELA	Risco Significativo de um Ataque Terrorista
EM GUARDA	AZUL	Risco Geral de um Ataque Terrorista
BAIXO	VERDE	Baixo Risco de um Ataque Terrorista

Na Inglaterra, são utilizados também cinco níveis de ameaça que informam as decisões sobre os níveis de segurança necessários para proteger a Infra-Estrutura Crítica Nacional (CNI). Esses níveis são:

Tabela 3 – Níveis de Ameaça Adotados na Inglaterra

Rótulo	**Significado**
CRÍTICO	Um Ataque Terrorista é Iminente
SEVERO	Um Ataque Terrorista é Altamente Provável
SUBSTANCIAL	Um Ataque Terrorista é uma Forte Possibilidade
MODERADO	Um Ataque Terrorista é Possível, mas não Provável
BAIXO	Um Ataque Terrorista é Improvável

No Anexo 2 desta tese, apresenta-se um informativo do Governo Britânico esclarecendo sobre definição do nível de ameaça naquele país.

Na França, o novo Plano Governamental VIGIPIRATE, de 26 de março de 2003, estabelece quatro níveis de ameaça, baseados numa avaliação e caracterização da ameaça. Esses quatro níveis são definidos pelas cores: amarela, laranja, vermelha e escarlate.

Tabela 4 – Níveis de Ameaça Adotados na França

Cor	**Significado**
ESCARLATE	**Risco de atentados maiores, simultâneos ou não, com efeitos devastadores.**
VERMELHA	**Risco avéré de um ou vários atentados graves.**
LARANJA	**Risco de uma ação terrorista considerada plausível.**
AMARELA	**Riscos reais, mas ainda imprecisos.**

Fonte: http://www.auvergne.pref.gouv.fr/pdf/plan_vigipirate.pdf

A habilidade em antecipar eventos adversos futuros e escolher entre alternativas de segurança situa-se no centro do processo de gerenciamento de risco e proporciona um guia baseado em boas práticas de gerenciamento que, apoiado por controles internos bem estabelecidos, pode melhorar o processo de tomada de decisão e a implementação da segurança. Embora o gerenciamento de risco venha, há muito, sendo usado em

alguns setores, tais como o ambiental, o da saúde, das finanças e da indústria dos seguros, a aplicação dos princípios do gerenciamento de risco à segurança dos sistemas de transporte contra ameaças intencionais é relativamente recente.

Os diferentes componentes e atividades desses sistemas que devem ser protegidos contra as ameaças enfrentam desafios difíceis e ainda não testados. A razão disso é que a fonte de risco é um adversário inteligente, contra o qual ainda não existe muita experiência.

Como resultado, as probabilidades e conseqüências da perpetração de uma ameaça tornam-se difíceis de prever. Apesar deste alto grau de incerteza e o reconhecimento de que nem todo risco pode ser eliminado, o melhoramento da proteção contra ameaças potenciais ou conhecidas pode ajudar a prevenir ou mitigar os eventos adversos.

Capítulo 3
REVISÃO DA LITERATURA

Conforme já mencionado nesta tese, não encontramos na literatura pesquisada nenhum método ou processo com a finalidade específica de *avaliar o nível de ameaça intencional a um sistema de transporte*. No Manual de Segurança da OACI e no Código ISPS da OMI, podem ser encontradas, respectivamente, uma metodologia para avaliação da ameaça e algumas instruções sobre a definição de níveis de ameaça. Ambos os documentos provêem procedimentos para obter uma avaliação da probabilidade de ocorrência de ameaças específicas consideradas conhecidas a priori. O Código ISPS da OMI pode ser encontrado com facilidade na Internet. O Manual da OACI é classificado como RESERVADO. Porém, nem o Manual nem o Código apresentam um processo de avaliação do nível de ameaça intencional, nos termos propostos nesta tese.

Tal fato parece ser uma decorrência natural da inexistência de uma definição para essa grandeza, uma definição que explicite o entendimento intuitivo, mediante uma descrição das interações dos atributos das ameaças intencionais, dos sistemas de segurança e do ambiente interno e externo aos sistemas de transporte. A abordagem mais próxima dos interesses de pesquisa desta tese é encontrada na literatura existente sobre análise de risco da segurança (McCormick, 1981; Rasche, 2001; Haimes, 1998 e 2004).

Na análise de risco da segurança, este problema é denominado de *avaliação da ameaça*. A modelagem e os procedimentos adotados nessa abordagem baseiam-se em conceitos e princípios que podem ser utilizados como referencial teórico primário para a análise e avaliação aqui pretendidas.

Este capítulo destina-se a examinar as técnicas existentes na literatura do setor e justificar aquela que escolhemos como base teórica do modelo proposto. Inicia-se com uma revisão da abordagem tradicional da análise de risco da segurança. Depois, apresenta-se uma síntese das metodologias de avaliação das ameaças intencionais; os métodos de inferência bayesiana; o modo de raciocínio *fuzzy*; o Processo de Hierarquia Analítica e, finalmente, descreve-se o potencial oferecido pela associação da Lógica *Fuzzy* com o Processo de Hierarquia Analítica.

3.1 ANÁLISE DE RISCO DA SEGURANÇA CONTRA AMEAÇAS INTENCIONAIS

Diversas definições existem para análise de risco da segurança. De acordo com GAO (2005), *análise de risco é o processo de determinar* ***qualitativamente*** *ou* ***quantitativamente*** *a probabilidade de um evento adverso e a severidade de seu impacto sobre um ativo.* O risco é uma função da *ameaça,* da *vulnerabilidade* e da *conseqüência* do impacto. A avaliação de risco inclui a simulação da interação desses três componentes em cenários possíveis, onde os valores a eles atribuídos podem ser agregados entre si, produzindo uma percepção ou permitindo a mensuração dos valores do risco. Esses valores tornam possível ordenar os riscos e estabelecer prioridades para aplicação de contramedidas de segurança.

No artigo intitulado "Estimando o Risco do Terrorismo", publicado pela RAND Corporation, Willis et al. (2005) desenvolvem uma abordagem de análise de risco da segurança que, embora similar à de GAO (2005) e a outras existentes na literatura, é interessante em um aspecto específico: o risco é determinado para cada um dos possíveis alvos das ameaças intencionais.

Assim, os componentes do risco são: a *ameaça a um alvo*, a *vulnerabilidade daquele alvo à ameaça* e as *conseqüências ou impacto para esse alvo, caso a ameaça*

seja perpetrada com sucesso contra ele. A generalização para qualquer e apenas um alvo de cada vez é a parte interessante da abordagem, porque permite apreciar todas as variáveis envolvidas por ameaças possíveis de serem perpetradas contra cada alvo de *per se*.

De acordo com Willis, ameaças a um alvo podem ser medidas como a probabilidade de que um alvo específico seja atacado de um modo específico durante um período específico. Dessa forma, uma ameaça pode ser medida como a probabilidade anual de que um sistema ou um componente do sistema estará sujeito a um ataque com, digamos, o uso de uma bomba. Vulnerabilidade pode ser medida como a probabilidade de que um dano ocorra, considerada uma determinada ameaça.

Danos podem ser fatalidades, ferimentos, estragos em propriedades ou outros prejuízos; cada um associado a sua própria avaliação de vulnerabilidade. Conseqüências são as magnitudes e os tipos de dano resultante, devido a um ataque terrorista bem sucedido (sic). Risco, novamente, é uma função desses três componentes: ameaça, vulnerabilidade e conseqüências. Estes construtos podem ser usados para medir consistentemente o risco, expressando-os em termos das conseqüências anuais esperadas.

A Abordagem Tradicional

A abordagem tradicional de análise de risco da segurança envolve os seguintes procedimentos:

1) Identificação das ameaças ao sistema;
2) Identificação dos ativos sob risco;
3) Determinação da probabilidade das ameaças serem perpetradas;
4) Computação da perda esperada para cada ativo e ameaça.

5) Análise do impacto de controles existentes.

6) Análise para determinar o domínio da exposição ao risco.

O resultado destes procedimentos deve gerar, para o sistema, metas de exposição ao risco expressas em valores monetários. Esta abordagem admite a possibilidade de identificar e caracterizar a ameaça de forma realista. É importante destacar que o método requer que um conjunto significativo de estimativas para as probabilidades requeridas esteja disponível.

Probabilidades objetivas, subjetivas ou uma combinação das duas podem ser parte das hipóteses de probabilidade. A abordagem depende da percepção de uma correta estimativa probabilística de cada componente por parte dos analistas de segurança. Sem essa estimativa, o analista tem que realizar um processo de levantamento de dados, seleção e tratamento, estimando curvas de probabilidade para cada variável randômica da análise.

3.2 MÉTODOS DE AVALIAÇÃO DE RISCO

Essencialmente, a avaliação do risco da segurança é a atividade crítica da análise de risco da segurança, porque produz o parâmetro-chave para a decisão sobre a alocação dos recursos humanos e materiais disponíveis para a segurança no setor. A maioria das técnicas de avaliação de risco procura fazer uso de análises racionais, destinadas a viabilizar a comparação de possíveis perdas, decorrentes da ausência de um determinado controle de segurança, com os custos de implementar esse controle.

A taxa anual de ocorrência (ARO –*Annual Rate of Occurrence)*) é um dos parâmetros considerados. Para o cômputo desse parâmetro, a análise de risco emprega agregações de probabilidades de ameaças, parâmetros de vulnerabilidades e estimativas

de conseqüências (normalmente em dólares), com a finalidade de obter valores que permitam realizar essa comparação.

Métodos de avaliação de risco são classificados geralmente em qualitativos e quantitativos. Métodos qualitativos são caracterizados pelo emprego de ferramentas de avaliação baseadas no conhecimento prático, experiência e percepção de risco dos profissionais de segurança. Entre essas ferramentas, incluem-se escalas de avaliação subjetivas, que adotam conceitos tais como *alto*, *médio, baixo, crítico, sério, grave* e outros adjetivos pertinentes, para estimar probabilidades de ocorrência dos eventos adversos, graus de vulnerabilidade dos ativos e de seus sistemas de segurança, importância de ativos e conseqüências de suas perdas ou danos. Alguns métodos adotam escalas de correspondência conceitual-numérica, com o objetivo de permitir a manipulação computacional dos conceitos, visando a aportar algum formalismo matemático e rigor científico aos resultados.

Métodos quantitativos, por outro lado, procuram estimar valores numéricos para esses atributos, empregando ferramental matemático analítico normalmente baseado na Estatística e na Teoria da Probabilidade. Os métodos quantitativos são fortemente dependentes de dados históricos e de outras informações sobre os eventos adversos, requerendo análises estatísticas para interpretar, tratar e preparar esses dados e informações, de forma que sirvam de elementos de entrada consistentes para os modelos matemáticos utilizados.

Note-se que a categoria ou tipo de evento adverso a ser estudado normalmente define o método ou técnica de avaliação de risco que deve ser utilizada. Entretanto, mesmo quando a categoria está perfeitamente identificada, alguns cuidados devem ser tomados na escolha da técnica, uma vez que técnicas similares podem produzir resultados não necessariamente similares.

De um modo geral, para acidentes ou desastres naturais, erros de projeto e perdas financeiras, a análise de risco tem-se valido mais de métodos quantitativos de análise. Para estas categorias de eventos, a **Análise de Árvore de Eventos** (ETA – *Event Tree Analysis*) e a **Análise de Árvore de Falha** (FTA – *Fault Tree Analysis*) (Stamatelatos et al., 2002) têm sido utilizadas com relativo sucesso para determinar os riscos associados, normalmente como parte de uma metodologia de análise probabilística de riscos (PRA – *Probabilistic Risk Analysis*).

Para falhas ou erros de funcionamento de sistemas mecânicos, eletromecânicos ou eletrônico-digitais diversos, a FTA associada à PRA tem sido extensamente utilizada (Stalamelatos, 2002). A **Análise de Causa-Conseqüência** (CCA – *Cause-Consequence Analysis)*, uma combinação da FTA e da ETA, também tem uso nesses sistemas. Entretanto, métodos totalmente probabilísticos, vinculados à teoria da confiabilidade e segurança dos sistemas, tais como o *método de confiabilidade de primeira ordem* (FORM – *First Order Reliability Method)*, vêm tendo boa aceitação pelos analistas.

Os eventos adversos, ou as ameaças, de interesse desta tese, entretanto, são os atentados contra a integridade física e operacional dos ativos e funções dos sistemas de transporte. Estes eventos, conforme já mencionado, são de natureza intencional. Assim, na análise dos riscos associados a tais eventos, a avaliação dos fatores subjacentes a essa intenção desempenha um papel central. Entre tais fatores, estão a capacitação, organização, disciplina e liderança dos agressores ou terroristas potenciais e sua determinação para perpetrar a interferência adversa no sistema. Nesta tese, esses fatores são internalizados no atributo *perpetrabilidade da ameaça*.

O que é interessante e necessário destacar neste ponto é que para este tipo de evento adverso, a avaliação da ameaça constitui a atividade crítica do processo de análise de risco e, como tal, é necessário que as técnicas de avaliação adotadas ou

desenvolvidas sejam capazes de apropriar os valores desses fatores e agregá-los de *forma adequada e coerente*. Por *forma adequada e coerente* queremos dizer que essa agregação deve ser realizada por métodos ou processos capazes de explicitar coerentemente as contribuições desses fatores na composição do atributo e que este possa ser utilizado na determinação dos riscos associados à ameaça ou, então, que ele próprio possa expressar tais riscos.

3.3 MÉTODOS DE AVALIAÇÃO DE AMEAÇAS INTENCIONAIS

Para a avaliação de ameaças intencionais, a análise de risco tem utilizado metodologias híbridas, que associam elementos da análise de "inteligência", na identificação e caracterização do perfil de agressores ou terroristas, a técnicas subjetivas de obtenção e calibração do conhecimento, determinando probabilidades subjetivas de ocorrência dos eventos e avaliação conceitual da criticalidade dos alvos potenciais, bem como da conseqüência dessas ameaças (Willis et al., 2005).

Entre os métodos que podem ser aplicados isoladamente ou em combinação para abordar esta categoria de ameaça estão os qualitativos PHA (*Preliminary Hazard Analysis),* o HAZOP (*Hazard Operability studies)* e os semiquantitativos FMEA (*Failure Mode and Effect Analysis)* e FMECA (*Failure Mode and Effect Criticality Analysis).*

O método PHA (Andrews & Moss, 1993; Aven, 1992; Henley & Kumamoto, 1992; Roland & Moryaty, 1990; Fullwod & Hall, 1988) consiste de uma técnica qualitativa que envolve uma análise estruturada da seqüência dos eventos que podem fazer com que uma ameaça potencial seja perpetrada. Nesta técnica, os possíveis eventos indesejáveis são primeiramente identificados e depois analisados

separadamente. Para cada evento indesejável, ou ameaça, possíveis melhoramentos ou medidas preventivas são formuladas.

O resultado desta técnica provê uma base para determinar que categorias de ameaça devem ser examinadas mais detalhadamente e que métodos de análise são mais adequados. Com o auxílio de diagramas de freqüência / conseqüência (Tabela 5), as ameaças identificadas podem ser ordenadas pelo risco avaliado, permitindo que medidas sejam priorizadas para prevenir sua perpetração.

Tabela 5 – Diagrama de Freqüência vs. Conseqüência/Severidade da Ocorrência.

FREQÜÊNCIA DE OCORRÊNCIA	CONSEQÜÊNCIA/ SEVERIDADE		
	BAIXA	MÉDIA	ALTA
BAIXA			
MÉDIA			
ALTA			

Nesses diagramas, podem ser extraídos cinco cenários de risco, de conformidade com as combinações dos valores assumidos pelo atributo freqüência e pelo atributo conseqüência. Tais cenários podem ser distinguidos pelas diferentes cores das células da Tabela 5. O cenário amarelo é o de risco mais baixo, enquanto o vermelho é o de mais alto risco. Cenários intermediários são o verde, o azul e o roxo.

A técnica HAZOP, desenvolvida no início da década de 1970 (Sutton, 1992) pela *Imperial Chemical Industries Ltd.* (Andrews & Moss, 1993; Aven, 1992; Sutton, 1992; Suokas & Rouhiainen,1993), pode ser definida como a aplicação de um exame crítico sistemático formal, quanto ao processo e critérios de engenharia, de instalações novas ou existentes, para avaliar a ameaça potencial que resulta de desvios das especificações do projeto e os conseqüentes efeitos sobre tais instalações. Esta técnica utiliza um conjunto de palavras-guia: NENHUM/NÃO, MAIS OU/MENOS DE,

TANTO QUANTO, PARTE DO REVERSO, e EM VEZ DE. A partir destas palavras-guia, cenários que possam resultar em uma ameaça ou um problema operacional são identificados. As conseqüências da ameaça e as medidas para reduzir a freqüência com que a ameaça possa ocorrer são então discutidas. Esta técnica angariou ampla aceitação nos processos industriais como uma ferramenta eficaz para melhorar a segurança operacional em instalações fabris. Detalhes dos procedimentos adotados na técnica encontram-se disponíveis na literatura (Sutton, 1992; Suokas & Rouhiainen, 1993).

A técnica de análise *Failure Mode and Effect Analysis* (FMEA) foi desenvolvida nos anos 50 por engenheiros de confiabilidade, para identificar problemas que poderiam surgir do mau funcionamento de sistemas militares. FMEA (Stamatelatos et al., 2002; Andrews & Moss, 1993; Aven, 1992; Henley & Kumamoto, 1992; Fullwood & Hall,1992; Sutton, 1992; Bouti & Kadi, 1994; Stamatis, 1995; Russomano et al., 1992; 26, 27, 28, 29, 30, Pelaez e Bowles, 1995 58) é um procedimento por meio do qual cada modo de falha potencial em um sistema é analisado para determinar seu efeito no sistema e para classificá-lo de acordo com seu grau de severidade. Quando a FMEA é ampliada por uma análise de criticalidade, a técnica é denominada de *Failure Mode and Effects* ***Criticality*** *Analysis* (FMECA). Esta técnica foi amplamente aceita na indústria aeroespacial e militar (Sutton, 1992).

Procedimentos detalhados de como conduzir uma FMEA e suas várias aplicações nas diferentes indústrias encontram-se documentados em (Stamatis, 1995). Melhoramentos da FMEA/FMECA, que utilizam uma combinação de matrizes para modelar os sistemas e um conjunto de índices derivados de um tratamento probabilístico dos fatores envolvidos, têm tido aceitação e aplicação na avaliação de riscos desta categoria (Kara-Zaitri et al., 1991 e 1992). Uma abordagem similar encontrada na

literatura (Pelaez e Bowles, 1995) modela os sistemas utilizando mapeamento cognitivo *fuzzy*.

Contudo, nenhum desses métodos ou técnicas, em que pesem suas potencialidades, apresenta características metodológicas capazes de atender adequadamente aos interesses e objetivos desta tese ou se alinha com a lógica utilizada com o modo de raciocínio adotado no modelo proposto. O principal motivo disso é que, neste modo de raciocínio adotado, a *incerteza* e a *imprecisão* são entendidas como derivadas da *ambigüidade* e da *vagueza* das variáveis envolvidas e não da falta de conhecimento sobre elas ou da aleatoriedade de seus valores.

O modo de raciocínio adotado no modelo aqui proposto desvia-se, portanto, do modo de raciocínio clássico, no qual uma proposição é *verdadeira* ou *falsa*, sem que se admita gradação. No modelo proposto, o modo de raciocínio *aproximado* comporta alternativas teóricas que simulam o raciocínio em condições de incerteza. Nestes métodos, não se conhece com absoluta certeza a verdade ou a falsidade de uma proposição ou hipótese. Sua característica principal é justamente admitir uma faixa de variação possível entre tais extremos. Estas características de raciocínio aproximado podem ser encontradas nos ***métodos de inferência bayesiana*** e na ***Lógica Fuzzy***.

Em face disso e da importância e potencial de aplicação desses métodos em vários problemas nos quais a variável de interesse não dispõe de um histórico razoável de valores ou informações, é interessante examinar, com mais detalhes, seus fundamentos básicos, para verificar sua possibilidade de emprego no problema em consideração nesta tese.

Começaremos por examinar a inferência bayesiana e, em seguida, analisaremos a *Lógica Fuzzy*.

3.4 MÉTODOS DE INFERÊNCIA BAYESIANA

Fundamentados no conhecido teorema de Bayes, todos os métodos de inferência bayesiana têm em comum a atribuição de uma ***probabilidade a priori*** como medida inicial de confiança da hipótese. A *inferência* deve ser entendida como um ***processo de atualização das medidas de confiança***, ao se conhecerem ou serem observadas ***novas evidências***. Matematicamente, trata-se de obter as probabilidades das hipóteses, condicionadas às evidências que se conhecem. A atualização das probabilidades das hipóteses condicionadas às evidências se baseia na aplicação do teorema de Bayes. A diferença entre os métodos bayesianos, modelos causais e redes bayesianas deriva da hipótese de independência condicional entre hipóteses e evidências (Berger, 1985).

Em outras palavras, a inferência bayesiana utiliza aspectos do método científico, envolvendo a coleta de evidências que se pretende sejam consistentes ou inconsistentes com determinada hipótese. À medida que as evidências se acumulam, o grau de confiança na hipótese se altera. Com suficiente evidência, esse grau freqüentemente se torna muito alto ou muito baixo.

Por essa razão, proponentes da inferência bayesiana dizem que o grau de confiança pode ser usado para distinguir hipóteses conflitantes: hipóteses com um alto grau de confiança devem ser aceitas como verdadeiras, enquanto aquelas com um grau de confiança muito baixo devem ser rejeitadas como falsas. Contudo, há argumentos controversos, afirmando que este método de inferência pode ser tendencioso, devido ao grau de confiança inicial, que é preciso ter, antes que qualquer evidência seja coletada (Gull, 1988).

Na realidade, a inferência bayesiana utiliza estimativas numéricas do grau de confiança numa hipótese, antes que a evidência seja observada, e calcula uma estimativa numérica do grau de confiança da hipótese, depois da evidência ser observada. No

processo de indução, a inferência bayesiana confia nos graus de confiança ou probabilidades subjetivas, mas não afirma necessariamente que proporciona um método objetivo de indução. Não obstante, alguns estatísticos bayesianos acreditam que as probabilidades utilizadas podem ter um valor objetivo e, portanto, a inferência bayesiana pode ser considerada um método objetivo de indução (Gull, 1988).

Em termos formais, o processo utiliza o teorema de Bayes para ajustar as probabilidades, dada uma nova evidência, pela seguinte equação:

$$P(H_0 \mid E) = [P(E \mid H_0)\, P(H_0)] / P(E). \qquad \text{(IV)}$$

Onde:

- H_0: representa uma hipótese, chamada de hipótese nula, inferida antes que a nova evidência, E, esteja disponível.
- $P(H_0)$: é chamada de probabilidade a priori de H_0.
- $P(E \mid H_0)$: é chamada de probabilidade condicional de observar a evidência E, dado que a hipótese H_0 é verdadeira. É também chamada de função de verossimilhança, quando é expressa como uma função de E, dada H_0.
- $P(E)$: é chamada de probabilidade marginal de E, ou seja, a probabilidade de testemunhar a nova evidência E, sob todas as hipóteses mutuamente exclusivas. Pode ser calculada como a soma do produto de todas as probabilidades das hipóteses mutuamente exclusivas pelas correspondentes probabilidades condicionais: $\sum P(E \mid H_i)\, P(H_i)$.
- $P(H_0 \mid E)$ é chamada de probabilidade a posteriori de H_0, dada E.

O fator $P(E|H_0)/P(E)$ representa o impacto que a evidência tem sobre a confiança na hipótese. Se, quando a hipótese sob consideração é verdadeira, for provável que a evidência será observada, então este fator será grande. Multiplicando a probabilidade a priori da hipótese por este fator resultaria numa grande probabilidade a posteriori da hipótese, dada a evidência. Sob a inferência bayesiana, o teorema de Bayes *mede*, portanto, *quanto a nova evidência deve alterar uma confiança numa hipótese*.

Estatísticos bayesianos (Box and Tiao, 1973) argumentam que, mesmo quando as probabilidades subjetivas a priori são muito diferentes, novas evidências de repetidas observações tenderão a trazer suas probabilidades subjetivas a posteriori mais próximas de si. Contudo, outros argumentam que, quando as probabilidades subjetivas a priori são bem diferentes, suas probabilidades subjetivas a posteriori podem nunca convergir, mesmo com repetidas coletas ou observações de evidências. Estas análises argumentam que pontos de vista completamente diferentes inicialmente podem permanecer completamente diferentes com o passar do tempo, a despeito de uma grande acumulação de evidência (O'Hagan e Forster, 2003).

A probabilidade bayesiana tem sido utilizada por alguns analistas na avaliação de probabilidades de um ataque terrorista bem sucedido contra um alvo específico. Na análise Bayesiana, os analistas avaliam o estado atual do conhecimento relativo ao ataque terrorista em apreço, coletam novos dados e informações para determinar as questões remanescentes e então atualizam e refinam sua compreensão para incorporar tanto os dados e informações, novos quanto os velhos. ([http://www.bayesian.org/], acessado em 26Jan2007).

Com tais características, a inferência bayesiana bem poderia servir de base ao modelo proposto nesta tese, não fosse a estrutura desta já definida a partir de uma analogia mecânica. Entretanto, é inegável seu potencial de aplicação em problemas similares, já que possibilita superar a dificuldade de prover estimativas da probabilidade a priori, tomando por base a ***percepção dos analistas*** sobre o ***conhecimento empírico inicial da variável de interesse***. Contudo, verifica-se que, na seqüência do processo de inferência, as avaliações dependem da coleta de ***mais evidências***, o que caracteriza um tipo de incerteza que pode ser chamada de ***incerteza estocástica*** (Zimmerman, 1990), em contraste com a incerteza, derivada da ambigüidade concernente ao significado

semântico dessas evidências (eventos, fenômenos, atributos etc.), que pode ser chamada de ***incerteza difusa*** (ou *fuzziness*), característica identificada nas variáveis inerentes ao problema em análise.

Em razão desse argumento e do fato do conceito de *nível de ameaça intencional a um sistema de transporte* exibir essa ambigüidade e, portanto, o tipo de incerteza identificado ser a ***difusa***, decidi explorar o modo de raciocínio aproximado proporcionado pela Lógica *Fuzzy*, já que este modo de raciocínio "*provê uma maneira natural de abordar problemas nos quais a fonte de imprecisão é a ausência de critérios bem definidos de pertinência de classe* (derivada da incerteza difusa ou *fuzziness*)*, e não a presença de variáveis randômicas*" (Zadeh, 1965), situação típica do problema abordado nesta tese.

Visando a tornar mais claros os argumentos desta opção, apresento, a seguir, uma síntese dos conceitos e princípios filosóficos da Lógica *Fuzzy* e da Teoria dos Conjuntos *Fuzzy*. Embora esta síntese, se incluída como anexo ao texto principal, ficasse mais de acordo com as normas de apresentação de uma tese de doutorado, peço vênia para incluí-la no item a seguir, para não distanciar demasiadamente a contra-argumentação dela ao método de inferência bayesiana aqui apresentado.

3.5 LÓGICA "FUZZY"

A idéia de uma lógica re-inserindo o "*meio excluído*" da dicotomia aristotélica já existe desde o período pré-socrático. O filósofo grego Platão teria lançado as bases para essa lógica, ao propor uma terceira região entre o verdadeiro e o falso, onde as duas noções coexistiriam.

Bem mais recentemente, em artigo publicado em 1920, intitulado "***On three-valued logic",*** Jan Lukasiewicz propõe a extensão da lógica bivalente de Aristóteles

para uma lógica trivalente, na qual um novo valor é adicionado ao valor ***verdade (1)*** e ao valor ***falso (0)***. Este terceiro valor é denominado de "***possível***", recebendo o símbolo lógico ***( )***.

No entanto, as primeiras publicações generalizando a noção de conjunto *fuzzy* e propondo a idéia de uma lógica multivalente surgiram, apenas na década de 60, com Zadeh (1965) e Goguen (1967, 1968). Em 1965, Zadeh argumenta:

> "A noção de um conjunto fuzzy provê um ponto de partida conveniente para a construção de uma estrutura conceitual que é paralela em muitos aspectos à estrutura usada para os conjuntos comuns, mas é mais geral do que esta e, potencialmente, pode comprovar ter um escopo muito mais amplo de aplicabilidade, particularmente nos campos da classificação de padrões e processamento da informação. Essencialmente, tal estrutura provê um modo natural de tratar problemas, nos quais a fonte de imprecisão é a ausência de critérios bem definidos de pertinência de classe, em vez da presença de variáveis randômicas". [Zadeh L.A. (1965) Fuzzy Sets. Information and Control, 8, pp. 338-353]

Nestas mais de quatro décadas, desde que esse artigo foi publicado, a lógica *fuzzy* evoluiu consideravelmente, abrangendo uma ampla faixa de conceitos e técnicas direcionados para o tratamento de fenômenos que não se prestam à análise por métodos clássicos baseados na lógica bivalente e na teoria da probabilidade.

Aplicações atuais da lógica *fuzzy* podem ser encontradas em várias áreas do conhecimento humano, entre as quais, a da inteligência artificial, ciência da computação, engenharia de controle, reconhecimento de padrões, robótica, teoria da decisão, sistemas especialistas, pesquisa operacional, sistemas especialistas etc.

Os avanços teóricos têm sido tantos e tão rápidos que é difícil para um iniciante no assunto manter-se atualizado com o "estado-da-arte". Um número relativamente grande de artigos e livros tem surgido na literatura, em princípio voltados para as áreas de controle (Sugeno, 1985; Pedrycz, 1989), Teoria da Possibilidade (Dubois e Prade, 1988), ciências sociais e do comportamento (Smithson, 1987) e análise de decisão (Zimmermann, 1994), apenas para citar alguns.

Na área de análise de risco da segurança de sistemas, o uso da Lógica *Fuzzy* ainda é limitado. Em artigo publicado na revista Computers and Security, Kato et al. (1996) propõem a modelagem de um processo de análise de risco, numa instalação de computação, com o uso da Lógica *Fuzzy*. Moscato (1998), em um periódico similar, também apresenta um artigo abordando o uso da Lógica *Fuzzy* para a análise de risco. Sodyia et al. (2007) desenvolvem uma técnica de modelagem de ameaças à segurança dos sistemas de computação, em Lógica *Fuzzy*, baseado no modelo de inferência de Mandani (1981).

De um modo geral, no entanto, todas essas aplicações são devotadas à segurança dos processos de informática e da tecnologia da informação.

Teoria dos Conjuntos "*Fuzzy*"

A Teoria dos Conjuntos *Fuzzy* (Zadeh, 1965) constitui o arcabouço matemático formal da Lógica *Fuzzy*. Esta teoria vem sendo amplamente utilizada como uma alternativa adequada para a abordagem de problemas nos quais existam critérios ou fatores de mensuração vaga e ambígua.

Apesar das aparências, a Teoria dos Conjuntos *Fuzzy* provê um formalismo matemático estrito, no qual fenômenos ou atributos conceituais vagos e ambíguos podem ser estudados com precisão e rigor. Aliás, pode-se considerar essa teoria uma técnica de modelagem bem apropriada para situações nas quais fenômenos, critérios e relações *fuzzy* (difusas) existam.

Gin-Shuh Liang et alii (1991) fazem uma síntese bastante simples, clara e concisa dos fundamentos básicos dessa teoria, que reproduzimos a seguir, com eventuais paráfrases. Ressalte-se, porém, que, embora concisa, esta síntese contempla os principais conceitos e princípios necessários à compreensão da teoria.

Em um universo de discurso X, um subconjunto *fuzzy* A de X é definido por uma *função de pertinência* $f_A(x)$, que mapeia cada elemento x de X em um número real no intervalo fechado [0, 1]. O valor da função em x, isto é, $f_A(x)$, representa a *pertinência* de x em A. Quanto maior for $f_A(x)$, maior será a pertinência de x em A.

Por exemplo, se A for um subconjunto *fuzzy*, no conjunto dos números reais *R*, definido por {x | x são números reais próximos de 5}, a função de pertinência desse subconjunto pode ser definida como

$$f_A(x) = \begin{cases} 1, & \text{se} \quad 4 \leq x \leq 6 \\ 1 / (x - 5)^2, & \text{se} \quad x < 4 \ \text{ou} \ x > 6 \end{cases} \qquad \text{(V)}$$

Números *Fuzzy*

Um número *fuzzy* ***B*** é um subconjunto especial de números reais (Jain, 1976; Dubois e Prade, 1978). Sua função de pertinência f_B é um mapeamento contínuo de *R* em um intervalo fechado [0, 1], que tem as seguintes características:

1) $f_B(x) = 0$, para todo $x \in (-\infty, \alpha] \cup [\delta, +\infty)$;

2) $f_B(x)$ é estritamente crescente em $[\alpha, \beta]$ e estritamente decrescente em $[\gamma, \delta]$;

3) $f_B(x) = 1$, para todo $x \in [\beta, \gamma]$.

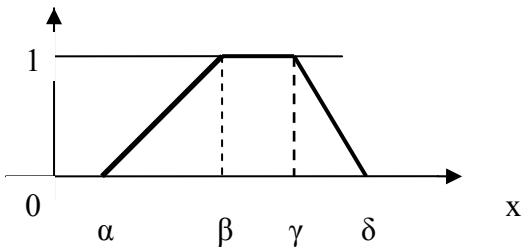

Figura 2 – Representação Gráfica de um Número *Fuzzy* Trapezoidal

Eventualmente, pode ocorrer que $\alpha = -\infty$ ou $\alpha = \beta$ ou $\beta = \gamma$ ou $\gamma = \delta$ ou $\delta = +\infty$. Segmentos de reta para $f_B(x)$ são adotados nos intervalos $[\alpha, \beta]$ e $[\gamma, \delta]$. Este tipo de número *fuzzy* é chamado de trapezoidal (ver representação gráfica na figura 3). Entretanto, se fizermos $\beta = \gamma$, em vez de uma representação trapezoidal, obtemos uma representação triangular, de forma que o número *fuzzy* passa a chamar-se *triangular*. Números *fuzzy* triangulares têm função de pertinência linear contínua e a seguinte representação gráfica.

$$f_B(x) = \begin{cases} (x - b) / (a - b), & b \le x \le a \\ 1, & x = a \\ (c - x) / (c - a), & a \le x \le c \\ 0, & x \text{ fora de } [c, b] \end{cases} \qquad \text{(VI)}$$

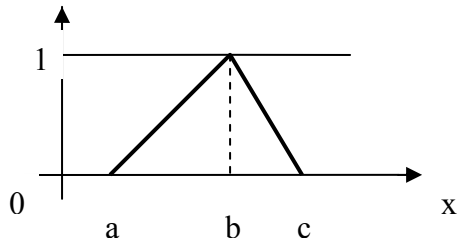

Figura 3 – Representação Gráfica de um Número *Fuzzy* Triangular

Números *fuzzy* triangulares, conforme expressos pela função de pertinência anterior, podem ser denotados por (a, b, c). Com esta notação e pelo *princípio de extensão* proposto por Zadeh (1965), as operações algébricas estendidas podem ser realizadas conforme mostrado a seguir:

Simetria

$$-(a, b, c) = (-c, -b, -a) \qquad \text{(VII)}$$

Adição ⊕

$$(a_1, b_1, c_1) \oplus (a_2, b_2, c_2) = (a_1 + a_2 , \ b_1 + b_2 , c_1 + c_2) \qquad \text{(VIII)}$$

Subtração (= Adição do simétrico)

$$(a_1, b_1, c_1) \oplus - (a_2, b_2, c_2) = (a_1 - c_2, b_1 - b_2, c_1 - a_2) \quad \text{(IX)}$$

Multiplicação ⊗

$$k \otimes (a, b, c) = (ka, kb, kc) \quad \text{(X)}$$

$$(a_1, b_1, c_1,) \otimes (a_2, b_2, c_2) \cong (a_1a_2, b_1b_2, c_1c_2) \quad \text{(XI)}$$

com $a_1 \geq 0$, $a_2 \geq 0$

Divisão ∅

$$(a_1, b_1, c_1) \varnothing (a_2, b_2, c_2) \cong (a_1/c_2 , b_1/b_2 , c_1/a_2) \quad \text{(XII)}$$

com $a_1 \geq 0$, $a_2 \geq 0$

Com base nestas definições, números *fuzzy* triangulares são fáceis de manipular e interpretar. Por exemplo, "aproximadamente igual a 50" pode ser representado por (49, 50, 51); e "50 exato" pode ser representado por (50, 50, 50). Suas agregações algébricas, conforme o princípio de extensão para as operações algébricas mostrado anteriormente, são também fáceis de manipular e processar computacionalmente.

Ambigüidade e Vagueza – Fontes de Incerteza e Imprecisão

Em um artigo de janeiro de 2005, intitulado "*Toward a Generalized Theory of Uncertainty* (GTU) – *an Outline",* Zadeh rompe com a tradição científica de considerar a *incerteza* uma *província* da Teoria da probabilidade, propondo-se a examiná-la de uma perspectiva mais ampla. De acordo com ele, a *incerteza*, sendo um atributo da informação, pode ser representada como uma *restrição generalizada*.

Assim, pela GTU, o *raciocínio sob incerteza* seria tratado com uma *propagação de restrições generalizadas*, envolvendo os *aspectos semânticos dessa propagação*.

O conceito de *restrição generalizada*, peça central da GTU, é um conceito extraído da lógica *fuzzy*. A característica fundamental que distingue a lógica *fuzzy* da

lógica aristotélica, normalmente utilizada no raciocínio científico tradicional, é que, na lógica *fuzzy, tudo é, ou é permitido ser, uma questão de gradação*.

Na GTU, a incerteza é percebida como uma *estrutura granular* – um conceito que desempenha um papel-chave na percepção do mundo real pela mente humana (Zadeh, 1979; 1997). Informalmente, um *grânulo* de uma variável *X* é um bloco de valores de *X*, grupados por *indistinção (de forma, quantidade ou qualidade)*, *equivalência*, *similaridade*, *proximidade* ou *funcionalidade*. Por exemplo, um intervalo de números reais é um grânulo.

Da mesma forma, um intervalo *fuzzy* também é um grânulo, assim como uma distribuição de probabilidade. Granulação é uma propriedade que permeia a cognição humana. Por exemplo, os grânulos (ou valores) de *Idade* são conjuntos *fuzzy* rotulados de *jovem*, *meia-idade* e *velho*. E os grânulos da Verdade podem ser *não verdadeiro*, *verdadeiro*, *não muito verdadeiro*, etc. Enquanto os grânulos de *potencial de uma ameaça* podem ser, em termos absolutos, *baixo*, *médio*, *alto* e *muito alto*.

O conceito de *granularidade* é subjacente ao conceito de variável lingüística - um conceito que foi introduzido, em 1973, por Zadeh, em seu artigo "*Outline of A New Approach to the Analysis of Complex Systems and Decision Processes*", Zadeh (1973; 1975). O conceito de variável lingüística desempenha um papel central em quase todas as aplicações da lógica *fuzzy* (Filev e Yager, 1994; Pedryc e Gomide, 1998; Ross, 2004; Yen e Langari, 1998).

No próximo item, exploramos com mais detalhes o conceito de variável lingüística e sua utilidade para a proposta da presente tese. Na realidade, veremos que, praticamente, todas as variáveis envolvidas no problema de avaliação do nível de ameaça intencional a um sistema de transporte exibem características de variável lingüística.

Variáveis Lingüísticas

O conceito de variável lingüística (Zadeh, 1973) é muito útil para abordar problemas complexos, cujos atributos sejam difíceis de descrever por expressões quantitativas convencionais. Uma variável lingüística, em princípio, é uma variável cujos valores são palavras ou sentenças em linguagem natural ou artificial. De um modo geral, a tendência destas palavras ou sentenças é serem expressas em valores absolutos.

Em muitos casos, porém, valores absolutos de variáveis lingüísticas são difíceis de avaliar e descrever e, caso sejam obtidos, sua eventual utilização pode aumentar a imprecisão dos resultados. Nestes casos, é interessante explorar a conveniência e praticidade de essas variáveis serem expressas em valores relativos.

Por exemplo, a *perpetrabilidade* de uma ameaça pode ser classificada como uma variável lingüística, cujos valores absolutos podem ser expressões tais como: *alta perpetrabilidade*, *média perpetrabilidade*, etc. A *probabilidade de perpetração* é outra variável que pode ser classificada como lingüística e cujos valores absolutos podem ser: *baixa probabilidade, moderada probabilidade, média probabilidade, elevada probabilidade;* etc. Em vez desses valores absolutos, cuja avaliação pode envolver esforço desnecessário por parte dos avaliadores, pode ser mais conveniente e apropriado, bem como menos impreciso, atribuir valores relativos, comparando pares de ameaça por atributo. Por exemplo: *a ameaça A_1 tem probabilidade moderadamente maior que a ameaça A_2*; a *ameaça A_2 tem probabilidade igual à ameaça A_3,* etc.

Valores lingüísticos podem ser analisados pelo raciocínio aproximado da teoria dos conjuntos *fuzzy* e representados por *números fuzzy triangulares*. Por exemplo, os valores lingüísticos definidos para a variável "*probabilidade relativa de perpetração da ameaça*" podem ter funções de pertinência, conforme mostradas nas representações

gráficas das figuras a seguir, nas quais se estabelece uma correspondência das bases desses valores em um intervalo fechado [0, 1].

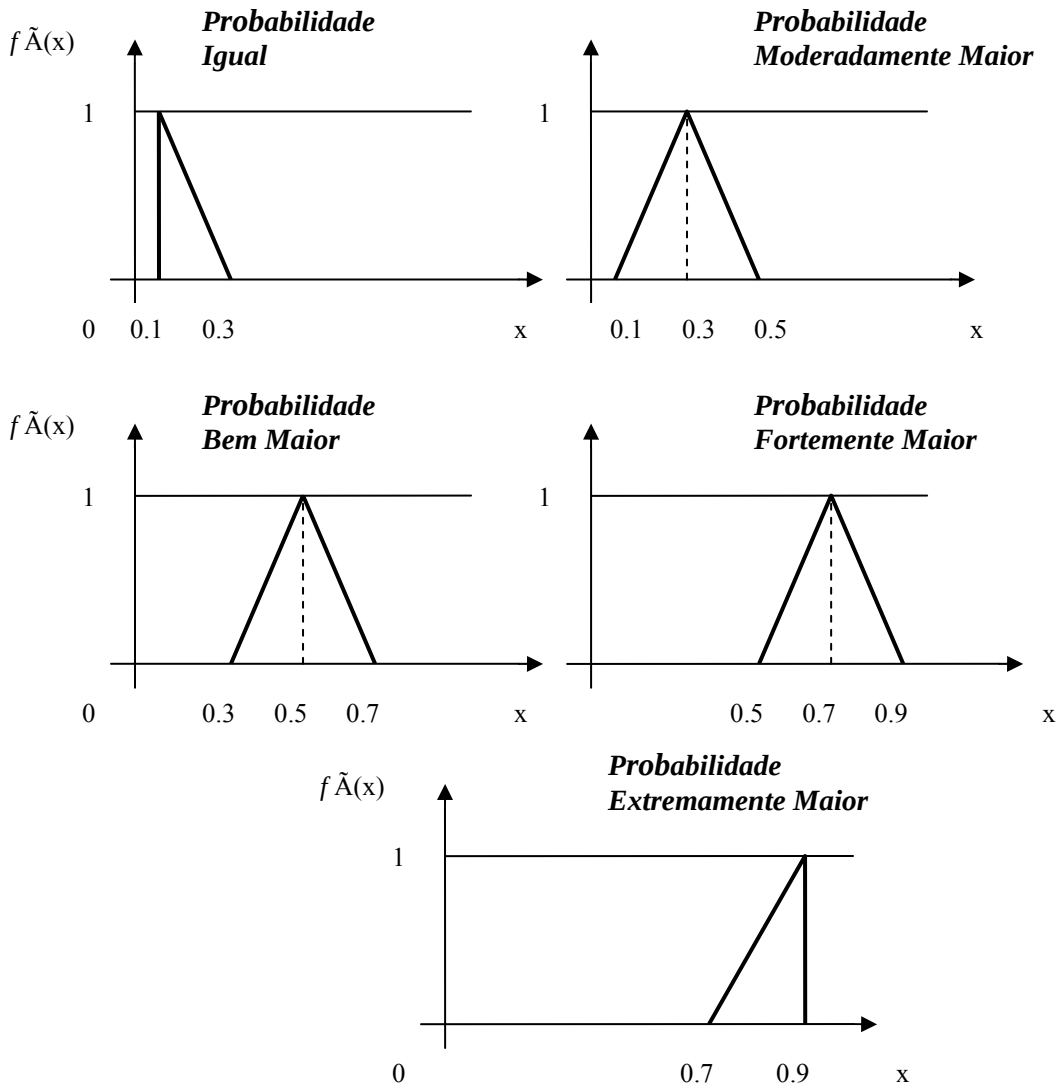

Figura 4. Representações Gráficas de Valores Fuzzy Triangulares da Variável Lingüística "*Probabilidade de Perpetração da Ameaça*".

Os números *fuzzy* correspondentes aos valores lingüísticos são:

Probabilidade Igual: ***(0.1, 0.1, 0.3)***

Probabilidade Moderadamente Maior: ***(0.1, 0.3, 0.5)***

Probabilidade Bem Maior: ***(0. 3, 0.5, 0.7)***

Probabilidade Fortemente Maior: ***(0.5, 0.7, 0.9)***

Probabilidade Extremamente Maior: ***(0.7, 0.9, 0.9)***

De modo similar, os valores lingüísticos “baixo”, “moderado”, “médio”, “elevado” e “alto”, passíveis de serem utilizados para descrever o potencial de uma ameaça intencional a um sistema de transporte ou mesmo o nível geral de ameaça intencional a esse sistema, podem ter essas mesmas representações em números “*fuzzy*” triangulares normalizados. As funções de pertinência desses números “*fuzzy*” triangulares, representadas em um único gráfico, ficariam assim:

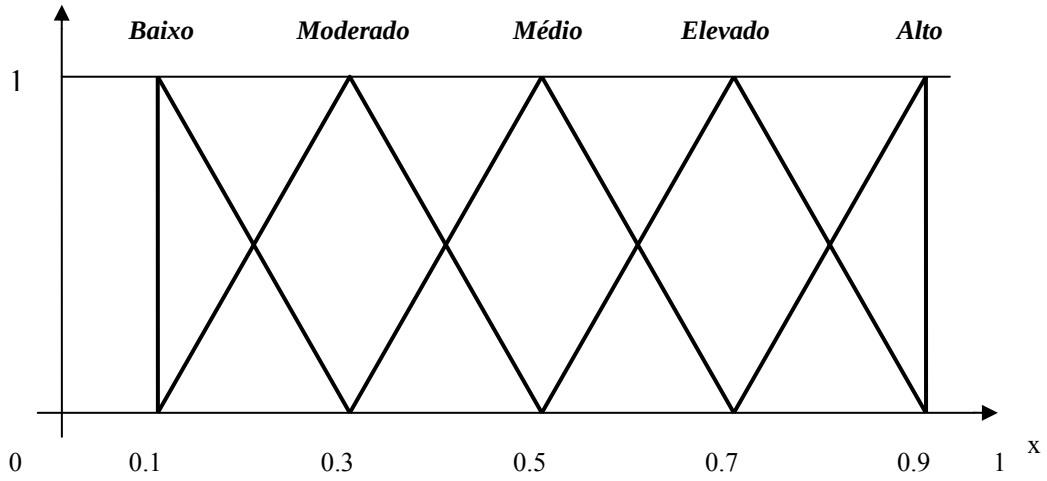

Figura 5. Números *Fuzzy* Triangulares Representativos da Variável Lingüística “Potencial de uma Ameaça Intencional a um Sistema de Transporte”

De modo similar, a variável “*importância relativa*” também é uma variável lingüística, cujos valores podem ter funções de pertinência, conforme mostradas na figura 6, de acordo com uma das diferentes adaptações *fuzzy* que a escala de preferência relativa de Saaty pode ter.

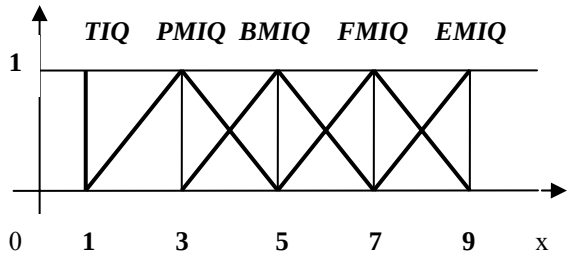

Figura 6 - Representação Gráfica dos Valores Lingüísticos da Variável Importância Relativa em Números *Fuzzy* Triangulares.

Na figura 6, as *abreviaturas* correspondem às expressões lingüísticas e seus respectivos números *fuzzy* triangulares, conforme apresentados a seguir:

TIQ - Tão Importante Quanto: (1, 1, 1)
MMIQ – Moderadamente Mais Importante Que: (1, 3, 5)
BMIQ – Bem Mais Importante Que: (3, 5, 7)
FMIQ – Fortemente Mais Importante Que: (5, 7, 9)
EMIQ - Extremamente Mais Importante Que: (7, 9, 9)

3.6 PROCESSO DE HIERARQUIA ANALÍTICA (AHP)

O Processo de Hierarquia Analítica (AHP) é uma técnica bem conhecida de solução de problemas, que provê uma base lógica para abordar problemas complexos (Saaty, 1980). Aplicações do método AHP podem ser encontradas várias áreas de análise de decisão e em diversos outros campos de interesse. O método é aplicável sempre que seja possível modelar os problemas em uma hierarquia de objetivos, critérios, subcritérios e alternativas.

Segundo Saaty (1980), "*a natureza holística de um dado problema*", tal como, por exemplo, o abordado nesta tese, "*necessita que ele seja dividido em áreas de assuntos menores, dentro das quais diferentes grupos de especialistas determinam quanto cada área afeta o problema total"*. Em outras palavras, um problema grande e complexo necessita ser decomposto em problemas de menor complexidade, cujas soluções possam ser combinadas para a solução do problema maior. Tais problemas, entretanto, argumenta Saaty, "*requerem expertise especializado para serem modelados adequadamente em uma estrutura e incluir o processo de avaliação nessa estrutura*".

Na *abordagem de tomada de decisão*, proposta pelo AHP, são necessários vários tipos de conhecimento, informação e dados técnicos, entre os quais:

a) detalhes sobre o problema que se deseja avaliar;

b) pessoas ou atores envolvidos;

c) objetivos e diretrizes;

d) atributos relevantes que entram na formação do problema principal;

e) fatores e condições que afetam esses atributos e os resultados; e

f) circunstâncias, cenários e outras restrições.

No AHP, fatores intuitivos, racionais e vagos podem ser avaliados simultaneamente nos julgamentos. Julgamentos e propósitos podem ser integrados em uma síntese geral e o processo não requer que tais julgamentos sejam consistentes. Na verdade, a consistência dos julgamentos só é revelada no final do processo, isto é, quando a síntese das prioridades relativas dos critérios com as preferências das alternativas por critério é realizada, mediante o cômputo do autovetor (*eigenvector*) normalizado de prioridades globais.

Após esse cômputo, é possível verificar a consistência dos resultados, a partir dos parâmetros das matrizes de comparações relativas de prioridades locais ou de preferências alternativas do processo e dos valores das componentes do autovetor de prioridades globais. A determinação da razão de consistência (CR) é feita, dividindo o índice de consistência (IC) pelo índice de consistência randômico (IR), com IR obtido da seguinte tabela:

Tabela 6: Índice de Consistência Randômico

n (= número de elementos da diagonal principal)	1	2	3	4	5	6	7	8	9	10
Índice de Consistência Randômico (IR)	0	0	.52	.89	1.11	1.25	1.35	1.40	1.45	1.49

O AHP tem sido mais utilizado para formalizar tomadas de decisão para um número limitado de escolhas ou alternativas, cada uma com uma quantidade também limitada de atributos, alguns dos quais com dificuldades em serem formalizados (Saaty, 1980). No AHP, frases tais como "*fortemente mais importante que*" são utilizadas para

expressar a avaliação da importância relativa de atributos, fatores, condições e/ou critérios, em comparação com outros do mesmo nível na hierarquia. Essa comparação é formalmente feita por pares de atributos.

Na formulação tradicional do AHP, os julgamentos humanos (normalmente de profissionais ligados à área de análise da decisão) são representados como números "*crisp*" (exatos), de acordo com a tabela fundamental de correspondência numérico-conceitual de Saaty a seguir (Tabela 7).

Tabela 7: A Escala Fundamental de Saaty

VALOR (Intensidade da importância)	**DEFINIÇÃO (Descrição da comparação)**
1	Importância igual
3	Importância moderada de um sobre o outro
5	Importância forte ou essencial
7	Importância muito forte
9	Importância extrema

Nota: Valores intermediários (2, 4, 6, 8) são permitidos, quando necessários para resolver um compromisso. Zero (0) não é permitido.

Contudo, em muitos casos práticos, o modelo de avaliação humana é incerto e impreciso e os profissionais podem mostrar-se relutantes ou incapazes de atribuir valores numéricos exatos aos julgamentos da comparação (Mikhailov, 2003). Por exemplo, quando avaliando a importância relativa de diferentes atributos, fatores ou condições associadas com uma ameaça intencional, os "experts" podem demonstrar insegurança em suas avaliações, devido a dados e informações vagos e ambíguos sobre aquelas variáveis.

Embora o método já tenha sido tema de muitas pesquisas e o consenso geral seja o de que ele é não apenas válido, tecnicamente, mas também útil, em termos práticos, existem críticas quanto a sua capacidade de tratar a incerteza inerente aos julgamentos. Estas críticas geralmente argumentam que as avaliações obtidas apenas representam alguma precisão aritmética que não reflete o real julgamento; que, apesar da escala

discreta de 1 a 9 do Saaty ter as vantagens da simplicidade e da facilidade de uso, ela não leva em conta a incerteza associada com o mapeamento da percepção humana sobre um número.

Este aspecto é exatamente o que torna interessante uma associação da Teoria dos Conjuntos *Fuzzy* com o AHP (Buckley, 1985; Chang, 1996; Van Laarhoven, 1983). Por esta associação, em princípio, é possível conferir maior formalismo matemático à abordagem da ambigüidade e vagueza dessas variáveis, mediante a utilização de números *fuzzy* na escala fundamental, o que reduziria a imprecisão inerente aos julgamentos.

Na proposta desta tese, o *problema da avaliação do nível de ameaça intencional a um sistema de transporte* é estruturado hierarquicamente em cinco níveis. Porém, em termos de aplicação do AHP, essa estrutura apresenta apenas três subproblemas específicos, cada um com três níveis hierárquicos. Tais subproblemas são justamente os das avaliações dos atributos do 3º nível da hierarquia: a ***impactabilidade adversa***, a ***perpetrabilidade*** e a ***probabilidade de perpetração***. O motivo disto é que, por definição, o objetivo global – a ***avaliação do nível de ameaça intencional*** – é alcançado pela mera hierarquização dos potenciais de ameaças obtidos no 2º nível, que, por sua vez, nada mais são que o produto dos valores dos atributos do 3º nível, tomados sem qualquer diferença em importância. Assim, nenhuma computação de importância relativa entre estes atributos para a formação do potencial das ameaças intencionais específicas a um sistema é necessária. A figura 7, a seguir, mostra essa estrutura hierárquica, com a indicação de alguns subatributos propostos por mim como mais pertinentes para a resolução do problema.

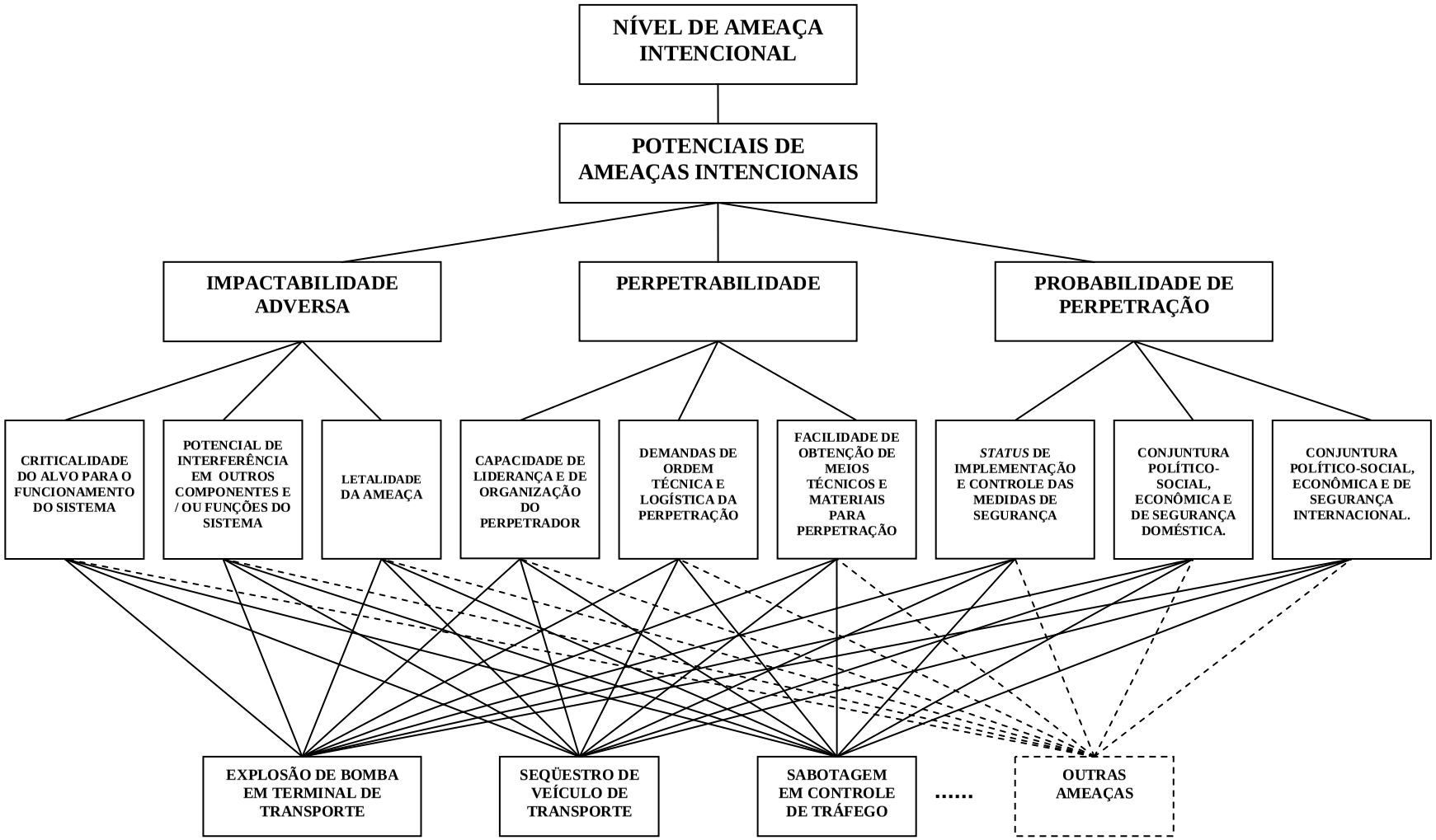

Figura 7 – Estrutura Hierárquica do Problema de Avaliação do Nível de Ameaça Intencional a um Sistema de Transporte

3.7 MODELOS *FUZZY*-HIERÁRQUICO-ANALÍTICOS (*FUZZY*-AHP)

Pesquisas associando a Lógica *Fuzzy* ao Processo de Hierarquia Analítica (AHP) são relativamente recentes. Em 1979, o próprio Thomas Saaty, criador do AHP, explorou interfaces entre hierarquias, objetivos múltiplos e conjuntos *fuzzy*, estabelecendo sobre o assunto, provavelmente, as bases para a exploração de outros modelos *Fuzzy*-AHP.

Todavia, um dos primeiros artigos explorando essa associação de forma mais prática parece ter sido o de P.J.M. van Laarhoven e W. Pedrycz (1983). Nesse artigo, intitulado "*A fuzzy extension of Saaty's priority theory*", os autores apresentam um método *fuzzy* para apoiar a decisão da escolha de uma entre várias alternativas, sob critérios de decisão conflitantes, quer dizer, uma versão *fuzzy* do método de comparação por pares de Saaty (1980). Nessa versão, os tomadores de decisão são solicitados a expressar seus julgamentos em números *fuzzy* triangulares.

Num artigo publicado em 1985, Buckley estende a análise hierárquica ao caso em que os participantes empregam números *fuzzy*, em vez de números exatos, nas comparações dos pares de critérios. A comparação produz matrizes recíprocas positivas *fuzzy*. O método da média geométrica é utilizado para calcular os pesos *fuzzy* para cada matriz *fuzzy* e estas são combinadas da forma usual para determinar os pesos finais *fuzzy* para as alternativas. Esses pesos finais *fuzzy* são usados para priorizar as alternativas de cima para baixo.

Mon (1994) desenvolveu um método para avaliar sistemas de armamento, usando um modelo *fuzzy*-AHP, baseado em cálculos entrópicos dos pesos. Chen (1996), para o mesmo problema, propôs um método modificado, usando operações aritméticas simplificadas de números fuzzy, em vez dos cálculos entrópicos de Mon. Cheng (1996) propôs um algoritmo para avaliar sistemas de mísseis táticos navais por um método

fuzzy-AHP e conceitos entrópicos para calcular pesos agregados. Estes estudos calculam prioridades *fuzzy* baseadas em operações aritméticas para números *fuzzy* triangulares ou trapezoidais.

Weck et al. (1997) desenvolveram um método para avaliar diferentes ciclos alternativos de produção, integrando a matemática da Lógica *Fuzzy* ao clássico Processo de Hierarquia Analítica (AHP). Qualquer ciclo de produção avaliado desta maneira gera um conjunto *fuzzy*. O resultado da análise pode finalmente ser defuzzificado pela formação do centróide de quaisquer dos conjuntos fuzzy encontrados e os ciclos alternativos de produção investigados podem ser ordenados hierarquicamente em termos dos objetivos gerais do problema.

Kuo et al. (1999) desenvolveram um sistema de suporte à decisão para selecionar localizações de novas lojas de conveniência por meio de um modelo *fuzzy*-AHP.

Karsak and Kuzgunkaya (2002) apresentam uma abordagem *fuzzy* de programação de objetivos múltiplos para facilitar a tomada de decisão na seleção de um sistema de manufatura flexível. Yu (2002) incorporou uma técnica de linearização de termos absolutos e uma expressão de pontuação *fuzzy* em um modelo de programação AHP para resolver problemas de tomadas de decisão em grupo.

Mais recentemente, Mikhailov (2003) propõe uma nova abordagem para derivar prioridades a partir de uma comparação aos pares *fuzzy* de julgamentos. Esta abordagem é baseada em decomposição α-*cuts* dos julgamentos *fuzzy* numa série de intervalos de comparação. A avaliação das prioridades a partir dos intervalos de comparação é formulada como um problema de otimização, maximizando a satisfação do tomador de decisão com um vetor de prioridade "crisp" específico. Um método de programação de preferência *fuzzy*, que transforma a atividade de priorização do intervalo em problema

de programação linear *fuzzy* é aplicado para derivar prioridades "crisp" ótimas. Agregando as prioridades ótimas, que correspondem ao diferentes níveis de α-cut, torna possível a obtenção dos escores dos elementos de priorização.

O modelo *fuzzy*-hierárquico-analítico, ou *Fuzzy*-AHP, ou simplesmente *fuzzy*-hierárquico, aqui proposto procura aproveitar as contribuições desses artigos, mantendo-se o máximo possível fiel aos princípios básicos do Processo de Hierarquia Analítica (AHP), estabelecidos por Saaty (1980). Contudo, visando a simplificar o processo em termos computacionais, na modificação introduzida na escala fundamental de Saaty, isto é, na substituição dos números "crisp" da escala por números *fuzzy* triangulares, mantemos, para o conceito "*igual importância*" ou "*tão importante quanto*" (TIQ), o *triplet* (1, 1, 1) como número *fuzzy* triangular 1, conforme já mostrado anteriormente.

A estrutura hierárquica do problema, apresentada na Figura 7, tem cinco níveis, sendo o primeiro o objetivo global, ou seja, o nível de ameaça intencional. O modelo é dividido em três etapas: (1ª) a determinação dos *índices de capacitação, experiência e "feeling"* (ou *pesos*) dos especialistas; (2ª) a implementação do processo *Fuzzy*-Hierárquico para determinação dos atributos relevantes – a *impactabilidade adversa*, a *perpetrabilidade* e a *probabilidade de perpetração*; e (3ª) a determinação dos potenciais específicos das ameaças intencionais consideradas e do *nível de ameaça intencional ao sistema*. No exemplo ilustrativo a ser apresentado no capítulo 5, todos os subatributos mostrados na figura 8 são utilizados, três ameaças capazes de serem perpetradas contra o sistema são consideradas e três especialistas formam o grupo de avaliação.

O próximo capítulo se ocupa da descrição do modelo fuzzy-hierárquico proposto para a avaliação do nível de ameaça intencional a um sistema de transporte.

CAPÍTULO 4

O MODELO "*FUZZY*"-HIERÁRQUICO

4.1 DESCRIÇÃO GERAL DO MODELO

O modelo *Fuzzy*-Hierárquico, ou *Fuzzy*-AHP, proposto nesta tese começa com a determinação dos *índices agregados de capacitação profissional, experiência profissional e "feeling"* ou, simplesmente, "*pesos de percepção*", dos especialistas designados para realizar as avaliações comparativas do problema. Por razões de coerência de abordagem, essa determinação, cujo desenvolvimento é mostrado no item 4.2 deste capítulo, também é feita com o auxílio do Processo de Hierarquia Analítica (AHP), porém na versão tradicional de Saaty, isto é, na versão que utiliza números "crisp".

Computados os "*pesos de percepção*" dos especialistas, o modelo prossegue para a segunda etapa - a aplicação do Processo *Fuzzy*-Hierárquico para determinação dos valores dos atributos relevantes. Esta etapa começa com o estabelecimento de uma estrutura hierárquica para o problema. Esta estrutura, conforme mostrado na figura 7, no capítulo anterior, já se encontra estabelecida, contendo cinco níveis. Entretanto, é apenas a partir do 3º nível que de fato são aplicados os procedimentos computacionais do Processo *Fuzzy*-AHP. Quer dizer, a rigor, apenas três subproblemas são abordados por esse processo: os subproblemas da avaliação da *impactabilidade adversa,* da *perpetrabilidade* e da *probabilidade de perpetração,* atributos localizados no 3º nível da hierarquia.

De acordo com a heurística do Processo *fuzzy*-AHP, a solução destes subproblemas começa com a construção das matrizes de comparações de pares de subatributos do 4º nível da hierarquia, para determinar sua importância relativa para a formação dos atributos do 3º nível, diretamente a eles conectados na hierarquia, isto é, a

impactabilidade adversa, a *perpetrabilidade* e a *probabilidade de perpetração*. Essas comparações são obtidas mediante os julgamentos dos especialistas, baseados em suas percepções, e pela conseqüente atribuição das expressões lingüísticas (ou valores lingüísticos) correspondentes a esses julgamentos.

As matrizes de valores lingüísticos assim construídas são depois convertidas em matrizes de números *fuzzy* triangulares, por meio da substituição de cada valor lingüístico pelo correspondente número *fuzzy* triangular, conforme escala de comparação relativa modificada, mostrada na figura 6.

Cada matriz de comparações relativas em números *fuzzy*, gerada por cada um dos especialistas, é, então, multiplicada pelo respectivo *índice relativo de capacitação, experiência e "feeling" em segurança* desse especialista, resultando nas matrizes *fuzzy* de comparações relativas ponderadas por especialista. Em seguida, somam-se todas essas matrizes *fuzzy* de comparações relativas ponderadas e divide-se a matriz resultante pelo número de especialistas. O resultado é uma matriz recíproca *fuzzy* de comparações relativas médias ($\tilde{\boldsymbol{A}}$). Até aqui, apenas as células acima da diagonal principal dessas matrizes receberam valores, de forma que é preciso completar a matriz com os correspondentes recíprocos desses valores na parte de baixo dessa diagonal.

O próximo passo desta etapa é a determinação dos autovetores (*eigenvectors*) normalizados *fuzzy* ($\boldsymbol{R}$) de cada matriz *fuzzy* ($\tilde{\boldsymbol{A}}$) assim obtida. Formalmente, esses autovetores são determinados por meio da seguinte equação matricial:

$$\tilde{\boldsymbol{A}} \bullet \boldsymbol{R} = \lambda \bullet \boldsymbol{R}, \qquad \text{(XIII)}$$

onde λ é um autovalor (*eigenvalue*) associado à matriz $\tilde{A}$.

Pelas características da matriz $\tilde{\boldsymbol{A}}$, este é um sistema de equações lineares homogêneas que tem uma solução não trivial se e somente se o determinante $\tilde{\boldsymbol{A}} - \lambda \boldsymbol{I}$ for igual a zero, isto é, λ é um autovalor de $\tilde{\boldsymbol{A}}$. Porém, como toda fileira dessa matriz é um

múltiplo constante da primeira fileira, a matriz tem posto unitário. Assim, todos os autovalores dessa matriz são iguais a zero exceto um. Como a soma de todos os autovalores de uma matriz é igual a seu traço que, neste caso, é igual à própria ordem da matriz, esta ordem é um autovalor de $\tilde{\boldsymbol{A}}$, de forma que se tem uma solução não trivial. Para encontrar esta solução, o AHP adota um algoritmo simplificado, que será mostrado mais adiante.

O autovetor principal normalizado *fuzzy* $\boldsymbol{R}$ da matriz *fuzzy* $\tilde{\boldsymbol{A}}$ determina a *importância relativa* de cada um dos subatributos do 4º nível para a formação do atributo do 3º nível a eles diretamente conectado na hierarquia. Em outras palavras, cada uma das componentes r_k desses autovetores normalizados *fuzzy R* representa a *importância relativa* do correspondente subatributo do 4º nível para a formação do atributo do 3º nível diretamente a ele conectado na hierarquia. Denominaremos esses autovetores principais normalizados *fuzzy* $\boldsymbol{R}$ de **autovetores *fuzzy* de importâncias relativas.**

Como são três os subproblemas a resolver, teremos obviamente que computar três *autovetores principais normalizados fuzzy R* específicos ($\boldsymbol{R}_{\text{IMPAC}}$, $\boldsymbol{R}_{\text{PERPE}}$ e $\boldsymbol{R}_{\text{PROBA}}$), um para cada conjunto de subatributos do 4º nível, conectados diretamente aos *atributos do 3º nível da hierarquia* (a *impactabilidade adversa*, a *perpetrabilidade* e a *probabilidade de perpetração*).

Depois que esses três **autovetores *fuzzy* de importância relativa** do 4º nível forem computados, repete-se esta mesma rotina de computações para as ameaças intencionais incluídas no 5º nível da hierarquia em relação aos subatributos do 4º nível da hierarquia, isto é, começamos pela construção das matrizes de comparações de pares das ameaças em relação aos subatributos, em valores lingüísticos, e concluímos com a

computação dos *autovetores principais normalizados fuzzy* ***S*** das matrizes *fuzzy* $\tilde{A}$ de comparações médias obtidas.

Esses autovetores normalizados *fuzzy* ***S*** determinam a dominância relativa das ameaças entre si, em relação aos subatributos do 4º nível. Quer dizer, cada uma das componentes s_{ik} desses autovetores representa a dominância relativa daquela ameaça A_i em relação ao subatributo C_k. Denominaremos esses *autovetores normalizados fuzzy* ***S*** de **autovetores *fuzzy* de dominâncias relativas**.

Naturalmente, são computados tantos *autovetores normalizados fuzzy S* quantos sejam os subatributos do 4º nível da hierarquia diretamente conectados aos atributos (ou subproblemas) do 3º nível.

O produto das *matrizes* formadas pelos **autovetores *fuzzy* de dominâncias relativas** do 5º nível da hierarquia pelos correspondentes **autovetores *fuzzy* de importância relativa** do 4º nível resulta nos ***vetores fuzzy de prioridades relativas globais*** (***IMPAC, PERPE*** e ***PROBA) das ameaças***, para cada um dos atributos relevantes do 3º nível.

Essas prioridades relativas globais por atributo nada mais são do que as respectivas *impactabilidades adversas, perpetrabilidades* e *probabilidades de perpetração* em termos relativos das ameaças consideradas. Essas prioridades relativas globais por ameaça são agregadas por multiplicação, pelo princípio de extensão da Teoria dos Conjuntos *Fuzzy*, resultando no ***potencial relativo específico de cada uma das ameaças ao sistema de transporte***. Finalmente, o ***nível de ameaça intencional ao sistema de transporte*** é determinado, mediante a definição do maior desses potenciais relativos específicos avaliados. Esta definição do máximo potencial é realizada pelo Método dos Conjuntos Maximizantes e Minimizantes (Chen, 1985), um método empírico prático para hierarquizar números *fuzzy* em ordem de grandeza.

4.2 DETERMINAÇÃO DOS ÍNDICES AGREGADOS DE CAPACITAÇÃO, EXPERIÊNCIA E "FEELING" EM SEGURANÇA CONTRA AMEAÇAS INTENCIONAIS DOS ESPECIALISTAS.

O primeiro passo de nosso modelo, portanto, consiste da determinação dos ***índices agregados relativos de capacitação, experiência e "feeling"*** ou "***pesos de percepção***" (w_g) em segurança contra ameaças intencionais nos sistemas de transporte dos especialistas que compõem o grupo de avaliação. O objetivo desses índices é ponderar as avaliações das demais variáveis pertinentes ao problema por esses especialistas.

Na *avaliação por percepção*, esta etapa é extremamente importante, porque calibra o instrumento utilizado para mensurar as variáveis, isto é, a ***percepção dos avaliadores***, refinando os resultados obtidos com o modelo.

Esses índices são justificados pela existência de *diferenças de percepção* dos profissionais de segurança em relação às diferentes comparações das importâncias dos subatributos das ameaças intencionais entre si, para o atributo a eles conectado na hierarquia, e das dominâncias destas ameaças quanto aos subatributos correspondentes.

Diferenças de percepção derivam de diferenças individuais em *capacitação/treinamento profissional*, *tempo de serviço em cargos e funções exercidas*, *participação em emergências* e/ou *investigações* de segurança e no "*feeling*" dos especialistas sobre as questões de segurança.

Esses fatores são considerados suficientes para apropriar as diferenças de percepção relevantes sobre segurança e possibilitar, mediante uma agregação adequada destas, a formação de um índice específico por especialista, capaz de ponderar as demais avaliações das variáveis do problema, reduzindo a imprecisão dos resultados. Essa agregação será feita por meio da aplicação do Processo de Hierarquia Analítica

clássico a este problema. Uma hierarquia de três níveis, mostrada na Figura 8 a seguir, é empregada para modelar o problema.

De acordo com os procedimentos computacionais do AHP, o primeiro passo para determinar este índice consiste em avaliar a importância relativa desses três atributos ("feeling", capacitação e experiência) para a formação desse índice.

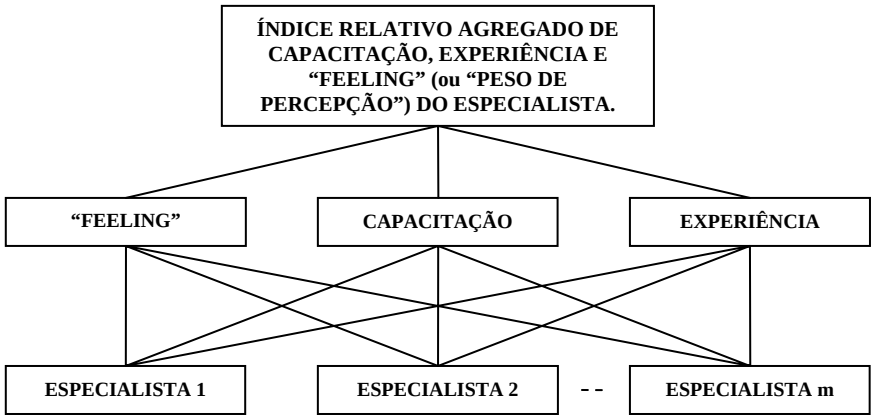

Figura 8: Estrutura Hierárquica para o Problema da Avaliação do Índice Relativo de Capacitação, Experiência e "Feeling" dos Especialistas em Segurança.

Para tanto, os especialistas são solicitados a construir matrizes de comparações de pares de atributos, respondendo à seguinte pergunta: "- *Qual a importância do atributo* "feeling em segurança" *(ou* capacitação *ou* experiência em segurança*) para a formação do peso de percepção relativo do especialistas, quando comparado com o atributo* capacitação *(ou* experiência*)*?". Com este mesmo modelo de pergunta e as devidas substituições, são obtidas as demais comparações relativas dos demais atributos. As respostas devem pertencer ao seguinte conjunto de valores lingüísticos:

Conjunto-resposta = {**igual, moderadamente superior, superior, fortemente superior, extremamente superior**}.

Após todos os especialistas terem construído suas matrizes de valores lingüísticos, procede-se à conversão dos valores lingüísticos das células dessas matrizes

em valores "crisp" da escala fundamental de Saaty, com a mesma correspondência em números fuzzy das expressões lingüísticas {TIQ, MMIQ, BMIQ, FMIQ, EMIQ}, mostrada na figura 6. Depois dessa conversão, completa-se a parte de baixo da diagonal principal das matrizes, fazendo $a_{ij} = 1/a_{ji}$.

De posse dessas matrizes recíprocas, computa-se uma matriz média, fazendo cada célula da matriz média igual à soma das células correspondentes das matrizes dos especialistas dividida pelo número de especialistas. Em seguida, calcula-se o *autovetor normalizado* (***D***) desta matriz média, determinando, assim, as importâncias relativas de cada atributo para a formação do índice em avaliação. Após este passo, pode-se verificar a consistência dos julgamentos, calculando-se a Razão de Consistência (RC) da matriz de julgamentos. O próximo passo consiste da construção das matrizes de comparações entre pares de especialistas em relação a cada um dos atributos do 2º nível da hierarquia. Comecemos pela determinação do "feeling" relativo dos especialistas.

"Feeling" Relativo dos Especialistas

O "*feeling*" relativo dos especialistas é obtido com a partir das matrizes de comparações aos pares dos especialistas em relação ao "feeling", segundo o julgamento de cada especialista. As linhas sólidas da figura 9 destacam o *locii* dessas comparações.

Figura 9: Estrutura Hierárquica para o Problema da Avaliação do "Feeling" Relativo dos Especialistas em Segurança

Sendo *m* o número de especialistas, *m* matrizes *m* x *m* de comparação relativa do "*feeling*" são construídas, com cada elemento das matrizes resultando da resposta de cada especialista à seguinte pergunta-modelo: - *Como você avalia o "feeling" sobre segurança contra ameaças intencionais do especialista i em relação ao especialista j?* As respostas fornecidas pelos especialistas devem pertencer ao mesmo conjunto de valores lingüísticos utilizados nas comparações relativas do passo anterior.

A conversão desses valores lingüísticos em valores numéricos adotará a escala fundamental de correspondência numérica "*crisp*" do Saaty, de 1 a 9, tendo em vista a necessidade de agregar os outros valores relativos, também "*crisp*", obtidos para os dois outros fatores de diferenciação da percepção. Veremos, pela forma de apropriar a informação relativa a esses dois outros fatores, que a manipulação com números "crisp" nesta etapa do modelo é praticamente compulsória.

Após todos os especialistas terem construído suas matrizes, uma matriz média é obtida, com o valor de cada célula sendo a média aritmética simples[6] dos valores das células correspondentes de cada matriz construída.

[6] Neste ponto do modelo, não faz sentido ter ainda uma média aritmética ponderada. A explicitação das diferenças de percepção dos especialistas ou, em outras palavras, do índice relativo de conhecimento e experiência em segurança de cada especialista, só é obtido com a agregação dos valores do "*feeling*" aos valores dos demais fatores de diferenciação.

De posse dessa matriz média, computamos o autovetor (*eigenvector*) normalizado ($\boldsymbol{F_g}$), determinando o *"feeling" relativo dos especialistas*. Tal como no passo anterior, após encontrar esse autovetor, é conveniente verificar a consistência dos julgamentos dos especialistas, calculando ao razão de consistência (***RC***) dos julgamentos da matriz.

Em termos formais, temos que cada especialista gera uma matriz de valores lingüísticos (Tabela 8, a seguir), que é convertida em uma matriz de valores numéricos (Tabela 9), segundo a escala fundamental de Saaty.

Tabela 8 - Matriz de Comparação Relativa do "Feeling" dos Especialistas.
(em Valores Lingüísticos)

"FEELING"	$\mathbf{E_1}$	$\mathbf{E_2}$	**...**	$\mathbf{E_n}$
$\mathbf{E_1}$	TIQ	BMIQ	...	MMIQ
$\mathbf{E_2}$	-	TIQ	...	EMIQ
...	...	...	TIQ	...
$\mathbf{E_m}$	-	-	...	TIQ

Tabela 9 – Matriz de Comparação Relativa do "Feeling" dos Especialistas.
(em Números *Fuzzy*)

"FEELING"	$\mathbf{E_1}$	$\mathbf{E_2}$	**...**	$\mathbf{E_n}$
$\mathbf{E_1}$	1	f_{12}	...	f_{1m}
$\mathbf{E_2}$	-	1	...	f_{2m}
...	...	...	1	...
$\mathbf{E_m}$	-	-	...	1

onde: $f_{ji} = 1 / f_{ij}$, $\quad i,j = 1,...,m$

f_{ij} = número "crisp" da escala fundamental do Saaty.

Após essa conversão, uma matriz média é obtida, fazendo cada nova célula f_{ij} igual à média aritmética simples dos valores das células correspondentes das matrizes geradas. Assim:

$$f_{ij} = (\sum f_{ij}) / m \qquad \text{(XIV)}$$

Em seguida, completa-se a matriz média, atribuindo a cada célula abaixo da diagonal principal um valor igual ao recíproco do valor da célula diametralmente oposta a esta, localizada correspondentemente acima dessa diagonal, e computa-se o autovetor normalizado $\boldsymbol{F_g}$ **,** cujas componentes f_g (g=1,..., m) representam os índices relativos do "feeling" dos especialistas.

Capacitação Relativa e Experiência Relativa

O processo para determinar a **capacitação relativa** e a **experiência relativa** dos **especialistas** é mais simples, envolvendo uma pontuação desses fatores, de acordo com critérios empíricos apresentados nas tabelas 10 e 11, a seguir. Nessas tabelas, a capacitação e a experiência em segurança contra ameaças intencionais são apropriados por meio da pontuação de 12 subfatores (seis por fator):

1) **capacitação** - formação em segurança nos níveis *técnico*, *graduação*, *especialização*, *atualização*, *mestrado* e *doutorado*; e

2) **experiência** – (a) cargos e funções exercidas (*agente de segurança*, *supervisor de segurança*, *gerente de segurança*, *auditor de segurança*); e (b) *participação em emergências* e *participação em investigações*.

No campo da segurança contra ameaças intencionais, os profissionais são normalmente avaliados, para fins de promoção a postos de maior relevância no órgão ou empresa, por meio de tais critérios.

Tabela 10 – Critérios para Pontuação em Capacitação Profissional em Segurança Contra Ameaças Intencionais.

FATOR	SUBFATOR	CRITÉRIO (pontos = pts.)
CAPACITAÇÃO	**Curso Técnico ou 2º Grau**	Sim = 3 pts Não = 0 pts.
	Curso de Graduação	Sim (voltado para a segurança) = 8 pts. Sim (voltado pra outra área) = 5 pts. Não = 0 pts.
	Especialização em Segurança	Sim = 4 pts. Não = 0 pts.
	Atualização em Segurança	Sim = 3 pts Não = 0 pts.
	Mestrado	Sim. (voltado para a segurança) = 10 pts.; Sim. (voltado para outra área) = 7 pts. Não = 0 pts.
	Doutorado	Sim. (voltado para a segurança) = 20 pts. Sim. (voltado para outra área) = 15 pts. Não = 0 pts.

Tabela 11 – Critérios para Pontuação em Experiência Profissional em Segurança Contra Ameaças Intencionais.

FATOR	SUBFATOR	CRITÉRIO (pontos = pts.)
EXPERIÊNCIA	**Agente de Segurança**	1 ponto para cada ano no cargo ou função
	Supervisor de Segurança	2 pts. para cada ano no cargo ou função
	Gerente de Segurança	3 pts. para cada ano no cargo ou função
	Auditor de Segurança	4 pts. para cada ano no cargo ou função
	Participação em Emergência	5 pts para cada participação
	Participação em Investigação	10 pts. para cada participação

Para fins de generalização e apresentação matemática do modelo, os especialistas serão denotados por E_g, (g = 1,..., m). Com base nesses critérios de pontuação, cada especialista E_g é avaliado, quanto a seu perfil de **capacitação** e de **experiência**, resultando respectivamente nos totais de pontos por especialista por fator, K_g e X_g. Esses totais por especialista são somados, resultando nos totais gerais, K e X, por fator. O total por especialista por fator, K_g ou X_g, é, então, dividido pelo total geral por fator, K *ou* X, resultando nos valores normalizados, k_g e x_g, representativos,

respectivamente, do *índice relativo de capacitação* e do *índice relativo de experiência* de cada especialista do grupo de avaliação.

Formalizando matematicamente, temos:

$K_{\mathbf{g}}$ = ($\sum$pontos de $E_{\mathbf{g}}$ em *capacitação*), (XV)

$X_{\mathbf{g}}$ = ($\sum$pontos de $E_{\mathbf{g}}$ em *experiência*), (XVI)

$K = (\sum K_{\mathbf{g}}), \quad g = 1,..., m$ (XVII)

$X = (\sum X_{\mathbf{g}})\ g = 1,..., m$ (XVIII)

$k_{\mathbf{g}} = K_{\mathbf{g}} / K, \quad g = 1,..., m$ (XIX)

$x_{\mathbf{g}} = X_{\mathbf{g}} / X, g = 1,..., m$ (XX)

Quer dizer, neste estágio do algoritmo, temos três autovetores normalizados, que determinam respectivamente os "feelings" relativos ($\boldsymbol{F}_{\mathbf{g}}$), as capacitações relativas ($\boldsymbol{K}_{\mathbf{g}}$) e as experiências relativas ($\boldsymbol{X}_{\mathbf{g}}$) dos especialistas, e um autovetor de importância relativas ($\boldsymbol{D}$) destes atributos para a formação do índice agregado desses fatores. Fazendo a síntese desses julgamentos, mediante a multiplicação da matriz formada pelos autovetores do "feeling" relativo, capacitação relativa e experiência relativa dos especialistas pelo autovetor das importâncias relativas, determina-se um vetor de pesos $\boldsymbol{W}_{\mathbf{g}}$, no qual cada componente w_{g} é o **índice agregado de "feeling", capacitação e experiência** ou ***"peso de percepção"*** do especialista g (g = 1,..., m). Assim:

$$W_{\boldsymbol{g}} = \left[K_{\boldsymbol{g}} \quad X_{\boldsymbol{g}} \quad F_{\boldsymbol{g}}\right]_{\mathbf{3\ x\ m}} \bullet \left[D\right]_{\mathbf{1\ x\ 3}}, \qquad g = 1,..., m \qquad \text{(XXI)}$$

Os componentes $\boldsymbol{w}_{g}$, do autovetor $\boldsymbol{W}_{\mathrm{g}}$, serão utilizados como pesos para os julgamentos ou avaliações que cada especialista $E_{\boldsymbol{g}}$, (g = 1,..., m) fizer durante todo o

processo de atribuição de valores comparativos na construção das matrizes de comparação do modelo.

4.3 ESTABELECIMENTO E DESCRIÇÃO DA ESTRUTURA HIERÁRQUICA DO PROBLEMA

A segunda etapa do modelo consiste do estabelecimento de uma estrutura hierárquica para o problema. Já apresentada na figura 7, essa estrutura contém cinco níveis hierárquicos. O primeiro nível é o próprio objetivo do problema, isto é, a grandeza *Nível de Ameaça Intencional ao Sistema de Transporte (NAI)* que se quer determinar.

O segundo nível hierárquico contém o problema da avaliação dos potenciais das ameaças intencionais, cuja determinação é feita pela agregação por multiplicação dos valores relativos dos atributos do terceiro nível.

O terceiro nível hierárquico é composto pelos atributos identificados como relevantes para a determinação desses potenciais, os quais são avaliados pelo processo *fuzzy*-hierárquico. Estes atributos, conforme já mencionado nesta tese, são: a *impactabilidade adversa da ameaça sobre o sistema,* a *perpetrabilidade da ameaça* e a *probabilidade de perpetração da ameaça.*

O quarto nível hierárquico é composto pelos *fatores e/ou condições* (*subatributos*) que concorrem, contribuem ou têm afetação na formação desses atributos. Para o atributo *impactabilidade adversa*, identificamos a *criticalidade dos alvos para o funcionamento do sistema,* o *potencial de interferência da ameaça em outros componentes ou funções* e a *letalidade da ameaça.* Para a *perpetrabilidade*, identificamos a *capacidade de liderança e de organização do perpetrador,* as *necessidades de ordem técnica e logística para perpetração da ameaça* e a *facilidade de obtenção de meios técnicos e materiais para perpetração da ameaça.* Para a

probabilidade de perpetração, identificamos o *status de implementação e controle das medidas de segurança* e as *conjunturas política, social, econômica e de segurança doméstica* e *internacional.*

Note-se que tais subatributos não esgotam os fatores e condições capazes de afetar os atributos relevantes das ameaças intencionais. Outros fatores e condições, se considerados igualmente relevantes pelo grupo de *experts*, podem ser incluídos na estrutura. Para fins de generalização, denotaremos esses fatores e/ou condições de *subatributos* C_k (k = 1,..., p).

Finalmente, o quinto nível é composto pelas ameaças intencionais identificadas como capazes de serem perpetradas contra o sistema de transporte, as quais, também para fins de generalização do problema, são denotadas por A_i (i = 1,..., n).

Completando o conjunto de variáveis do problema, temos os *índices de capacitação, experiência e feeling* (ou *pesos de percepção)* dos *m* especialistas designados para as avaliações, que denotamos por $\boldsymbol{w}_g$ (g = 1,..., m).

Por meio dessa estrutura, ao final da aplicação do processo, as ameaças intencionais ficam ordenadas em *valores relativos* de *impactabilidade adversa*, *perpetrabilidade* e *probabilidade de perpetração*, que são os três atributos relevantes cujos produtos determinam os potenciais relativos de cada uma das ameaças intencionais ao sistema de transporte.

Na prática, conforme já adiantamos, nosso modelo fica reduzido a três subproblemas de hierarquia analítica *fuzzy* bem definidos, todos com estrutura hierárquica de três níveis. Esta redução deve-se ao fato de que, o ***potencial de uma ameaça intencional ao sistema de transporte*** é definido como o produto daqueles três atributos relevantes, sem consideração de qualquer importância relativa desses três atributos para a obtenção do resultado final.

Em outras palavras, o ***potencial de ameaça intencional*** é o simples agregado por multiplicação dos valores relativos obtidos para esses atributos, com a aplicação do processo *fuzzy-AHP*. Assim, comparações relativas da importância destes atributos para os potenciais relativos de cada ameaça intencional não são computadas.

Neste ponto do modelo, as computações do AHP terminam, dando vez à determinação dos potenciais de ameaça e à determinação do nível de ameaça intencional ao sistema, conforme definições propostas nesta tese.

4.4 AVALIAÇÃO DAS IMPORTÂNCIAS E DOMINÂNCIAS RELATIVAS *FUZZY*

Esta terceira etapa do modelo começa com a construção das matrizes de importâncias relativas *fuzzy* e de seus respectivos autovetores normalizados *fuzzy*. Com a simplificação do problema, a construção dessas matrizes inicia-se pelos atributos do 3º nível hierárquico. Teremos, na prática, três subproblemas a resolver, cada um dos quais com seguinte estrutura hierárquica genérica de três níveis, mostrada na Figura 10, a seguir.

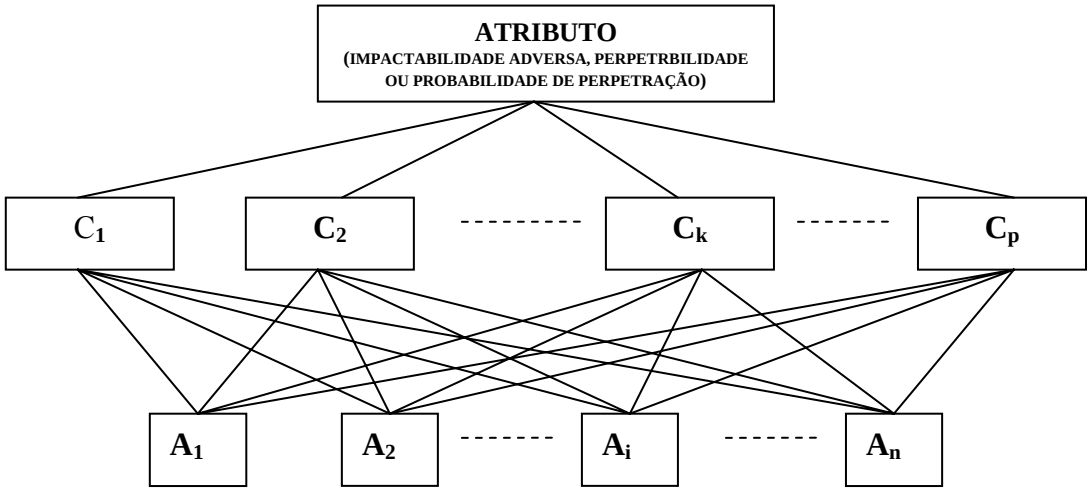

Figura 10 – Estrutura Hierárquica Genérica para a Avaliação dos Valores Relativos dos Atributos *Impactabilidade Adversa, Perpetrabilidade e Probabilidade de Perpetração.*

Neste passo, cada especialista $\boldsymbol{E_g}$ (g = 1,..., m) faz avaliações comparativas, baseados em sua percepção, entre pares dos subatributos C_k (k = 1,..., p), expressando, em termos lingüísticos, a importância relativa desses subatributos para a formação dos atributos do 3º nível da hierarquia, isto é, para a *impactabilidade adversa,* a *perpetrabilidade* ou a *probabilidade de perpetração*.

A questão-modelo que os especialistas devem responder neste passo é a seguinte: "*- Quão importante é o subatributo* C_k *para a formação do atributo impactabilidade adversa (ou* perpetrabilidade *ou* probabilidade de perpetração*,* conforme o que estiver em avaliação*), quando comparado ao subatributo* C_j?". As respostas para esta questão devem ser uma das seguintes "expressões ou valores lingüísticos": *tão importante quanto (TIQ), moderadamente mais importante que (MMIQ), bem mais importante que (BMIQ), fortemente mais importante que (FMIQ)* e *extremamente mais importante que (EMIQ).* A matriz de importância relativa em valores lingüísticos, de acordo com cada especialista, ficaria, por exemplo, como a mostrada na Tabela 12, a seguir.

Tabela 12: Matriz de Importância Relativa em Valores Lingüísticos de acordo com o Especialista g

IMPACTABILIDADE	C_1	C_2	**...**	C_p
C_1	***TIQ***	***MMIQ***	...	***BMIQ***
C_2	-	***TIQ***	...	***FMIQ***
...	...	...	***TIQ***	...
C_p	-	-	...	***TIQ***

Onde os valores lingüísticos TIQ, MMIQ, BMIQ, FMIQ e EMIQ correspondem ao julgamento que cada especialista atribuir à comparação entre os dois subatributos.

Depois que essas *m* matrizes de expressões lingüísticas são obtidas, cada uma dessas expressões é convertida em números *fuzzy* triangulares a_{kjg} **,** conforme escala modificada de Saaty. Devido à ordem das comparações, até este ponto dos

procedimentos, essas matrizes só têm valores nas células acima da diagonal principal. A matriz apresentada na Tabela 13 a seguir dá um exemplo de como ficam essas matrizes após essa conversão.

Tabela 13: Matriz de Importância Relativa em Números *Fuzzy* Triangulares de acordo com o Especialista *g*

ESPECIALISTA *g*	C_1	C_2	...	C_p
C_1	a_{11g}	a_{12g}	...	a_{1pg}
C_2	-	a_{22g}	...	a_{2pg}
...	...	...	...	...
C_p	-	-	...	a_{ppg}

Em seguida, determinam-se as médias ponderadas desses números, utilizando como pesos os índices agregados de capacitação, experiência e "feeling" (w_g) dos especialistas. Completa-se a construção da matriz, atribuindo às células de baixo da diagonal o inverso dos valores das células simétricas de cima da diagonal. O resultado é uma matriz *fuzzy* $\tilde{A}$ recíproca, cujos elementos são comparações relativas médias a_{kj} (k,j = 1,..., p) dos pares de subatributos (Tabela 14 a seguir).

Tabela 14: Matriz *Fuzzy* $\tilde{A}$ de Comparações Relativas Médias

ESPECIALISTA *g*	C_1	C_2	...	C_p
C_1	a_{11}	a_{12}	...	a_{1p}
C_2	a_{21}	a_{22}	...	a_{2p}
...	...	...	...	...
C_p	a_{p1}	a_{p2}	...	a_{pp}

Em termos formais, temos:

$$a_{kj} = (1/m) \sum\nolimits_{\oplus} w_g \cdot a_{kjg}, \qquad g = 1,.., m; \qquad k,j = 1,.., p \qquad \text{(XXII)}$$

onde: a_{kjg} = número fuzzy triangular, correspondente à expressão lingüística atribuída à importância de C_k em relação a C_j para o atributo do 3º nível da

hierarquia, diretamente a ele conectado (digamos, a impactabilidade adversa), pelo especialista E_g;

w_g = índice agregado de capacitação, experiência e *feeling* de E_g;

$a_{11} = a_{22} = ... = a_{pp} = (1, 1, 1)$; e

$a_{jk} = 1 / a_{kj}$

De posse da matriz *fuzzy* $\tilde{A}$ de comparações relativas médias a_{kj} ($k,j = 1,..., p$), o modelo prossegue com a rotina de computações do AHP para determinar o correspondente autovetor normalizado principal *fuzzy* (*fuzzy eigenvector*) $\boldsymbol{R}$ dessa matriz, cujas componentes expressam a importância relativa dos subatributos C_k para o atributo do 3º nível da hierarquia diretamente a eles conectados.

Formalmente, a determinação do autovetor $\boldsymbol{R}$ da matriz *fuzzy* $\tilde{\boldsymbol{A}}$ envolve a solução da seguinte equação:

$$\tilde{\boldsymbol{A}} \bullet \boldsymbol{R} = \lambda_{máx} \bullet \boldsymbol{R} \qquad \text{(XXIII)}$$

Conforme já explicado anteriormente, a solução desta equação pode envolver dificuldades se a ordem da matriz for superior a três. Por esse motivo, o AHP adota um algoritmo simples e prático para determinar esse autovetor principal normalizado *fuzzy* da matriz *fuzzy* $\tilde{A}$. Esse algoritmo consiste dos seguintes passos:

(1º) - determina-se a soma dos valores das células de cada coluna da matriz *fuzzy* $\tilde{A}$;

(2º) - divide-se o valor de cada célula de cada coluna pela soma dessa coluna, obtendo-se uma nova matriz *fuzzy* $\tilde{A}$ normalizada; e

(3º) - computa-se a média dos valores das células de cada fileira da nova matriz *fuzzy* $\tilde{\boldsymbol{A}}$ normalizada, gerando os valores $\boldsymbol{r_k}$ das componentes de $\boldsymbol{R}$.

O vetor formado por esses valores médios é o autovetor principal normalizado *fuzzy* $\boldsymbol{R}$, da matriz *fuzzy* $\tilde{\boldsymbol{A}}$. As componentes r_k desse autovetor representam as *importâncias relativas fuzzy* de cada uma das variáveis C_k para a formação do atributo relevante do nível de ameaça intencional ao sistema, diretamente conectados a estas no 3º nível da hierarquia.

Neste ponto, é possível verificar a consistência dos julgamentos, bastando para isso calcular a razão de consistência (RC).

Teremos, portanto, três vetores $\boldsymbol{R}$, um para cada atributo relevante do 3º nível da hierarquia ($\boldsymbol{R}_{\text{IMPAC}}$, $\boldsymbol{R}_{\text{PERPE}}$ e $\boldsymbol{R}_{\text{PROBA}}$).

O mesmo raciocínio e a mesma rotina de computações são aplicados para o terceiro nível da hierarquia, obtendo-se os autovetores principais normalizados *fuzzy* $\boldsymbol{S_{ki}}$, das ameaças intencionais para cada um dos subatributos C_k. Tais autovetores, a exemplo do nível anterior, representam as *dominâncias relativas fuzzy* ou os *pesos fuzzy* das ameaças por subatributos C_k. As componentes $\boldsymbol{s_{ki}}$ desses autovetores representam as dominâncias relativas de cada ameaça A_i por subatributo C_k.

Teremos, obviamente, tantos autovetores $\boldsymbol{S_{ki}}$ quantos sejam os subatributos do 4º nível da hierarquia.

4.5 AVALIAÇÃO DOS ATRIBUTOS RELEVANTES: SÍNTESE DAS IMPORTÂNCIAS E DOMINÂNCIAS RELATIVAS

Nesta etapa, as importâncias relativas e as dominâncias relativas locais são sintetizadas, determinando valores relativos por ameaça de cada um dos atributos relevante. Isto é realizado mediante a multiplicação da matriz formada pelos autovetores *fuzzy* de dominâncias relativas das ameaças por subatributo pelo autovetor *fuzzy* das importâncias relativas dos subatributos para cada atributo do 3º nível a eles diretamente conectados na hierarquia. O vetor resultante dessa multiplicação determina, para o 3º

nível da hierarquia, respectivamente as *impactabilidades relativas,* as *perpetrabilidades relativas* e as *probabilidades relativas* de todas as ameaças consideradas no problema.

Em termos formais, temos:

$$\boldsymbol{IMPAC} = (\text{Matriz formada pelos vetores } \boldsymbol{S_{ki}}) \otimes \boldsymbol{R}_{\text{IMPAC}}\,, \qquad \text{(XXIV)}$$

$$\boldsymbol{PERPE} = (\text{Matriz formada pelos vetores } \boldsymbol{S_{ki}}) \otimes \boldsymbol{R}_{\text{PERPE}}\,, \qquad \text{(XXV)}$$

$$\boldsymbol{PROBA} = (\text{Matriz formada pelos vetores } \boldsymbol{S_{ki}}) \otimes \boldsymbol{R}_{\text{PROBA}}\,, \qquad \text{(XXVI)}$$

onde: $i = 1,..., n$; $k = 1,..., p$ (p podendo ser diferente para cada atributo);

$\boldsymbol{R}_{\text{IMPAC}}$ = autovetor normalizado R da importância relativa dos subatributos C_k para a *impactabilidade adversa;*

$\boldsymbol{R}_{\text{PERPE}}$ = autovetor normalizado R da importância relativa dos subatributos C_k para a *perpetrabilidade;*

$\boldsymbol{R}_{\text{PROBA}}$ = autovetor normalizado R da importância relativa dos subatributos C_k para a *probabilidade de perpetração*; e

$\otimes$ = agregador por multiplicação de números *fuzzy*

IMPAC = vetor das impactabilidades relativas das ameaças;

PERPE = vetor das perpetrabilidades relativas das ameaças; e

PROBA = vetor das probabilidades relativas de perpetração das ameaças.

4.6 AVALIAÇÃO DOS POTENCIAIS DAS AMEAÇAS INTENCIONAIS ESPECÍFICAS E NÍVEL DE AMEAÇA INTENCIONAL AO SISTEMA DE TRANSPORTE

O potencial de uma ameaça intencional específica ($\boldsymbol{POTA_i}$) ao sistema de transporte considerado, de conformidade com a definição adotada, é determinado pelo

produto das respectivas impactabilidades relativas, perpetrabilidades relativas e probabilidades relativas das ameaças intencionais consideradas, ou seja, por:

$$\boldsymbol{POTA_i} = \boldsymbol{IMPAC_i} \otimes \boldsymbol{PERPE_i} \otimes \boldsymbol{PROBA_i}\ , \quad i = 1,..., n \qquad \text{(XXVII)}$$

onde: $\boldsymbol{IMPAC_i}$ = impactabilidade relativa da ameaça *i*;

$\boldsymbol{PERPE_i}$ = perpetrabilidade relativa da ameaça *i*; e

$\boldsymbol{PROBA_i}$ = probabilidade relativa da ameaça *i*.

É preciso esclarecer que o potencial de ameaça assim computado é também um valor relativo que expressa uma priorização relativa das ameaças por potencial.

4.7 AVALIAÇÃO DO NÍVEL DE AMEAÇA INTENCIONAL AO SISTEMA DE TRANSPORTE

E, finalmente, o nível de ameaça intencional ao sistema de transporte é determinado, encontrando o maior destes potenciais específicos avaliados para as ameaças intencionais identificadas como possíveis de serem perpetradas contra o sistema de transporte, isto é:

$$\boldsymbol{NAI} = \text{máx}\ \boldsymbol{POTA_i}\ , \qquad i = 1,..., n \qquad \text{(XXVIII)}$$

Tendo em vista que os potenciais de ameaça ($\boldsymbol{POTA_i}$) são números *fuzzy* triangulares, a determinação do maior entre eles envolve o uso de um método conhecido como *Método dos Conjuntos Maximizantes e Minimizantes Fuzzy* (Chen, 1985). Bastante simples e intuitivo, o método de Chen supera com facilidade os outros cinco métodos por lê mencionados em seu artigo.

No caso particular do problema de determinação do máximo potencial de ameaça aqui tratado, poderíamos facilmente utilizar o método de Jain (1976, 1977), que utiliza apenas o lado direito das funções de pertinência para encontrar o maior dos

números fuzzy, entretanto, achamos que o uso de Chen (1985) é mais racional e intuitivo.

No próximo capítulo, apresentamos um exemplo ilustrativo para o sistema de aviação civil, utilizando três especialistas, três ameaças intencionais e os subatributos mostrados na estrutura hierárquica mostrada na figura 7. Ao final do exemplo, mostramos uma ilustração com o conjunto maximizante de Chen como critério para obter a função utilidade total, a partir da qual os números fuzzy são ordenados em valor.

Capítulo 5

EXEMPLO ILUSTRATIVO:
AVALIAÇÃO DO NÍVEL DE AMEAÇA INTENCIONAL À AVIAÇÃO CIVIL

Neste capítulo, um exemplo ilustrativo de avaliação do nível de ameaça intencional ao sistema de aviação civil de um país hipotético é apresentado, com o objetivo de explicitar as etapas e passos do modelo *fuzzy*-hierárquico proposto.

5.1 CARACTERIZAÇÃO E DADOS DO EXEMPLO

Neste exemplo ilustrativo, são utilizados três especialistas em segurança da aviação civil contra atos de interferência ilícita (E_1, E_2, E_3), com os seguintes e respectivos perfis de capacitação e experiência profissional, apresentados nas tabelas 15, 16 e 17 a seguir.

As tabelas 18, 19 e 20 contêm as comparações relativas feitas por esses especialistas entre si, quanto ao "feeling" em segurança da aviação civil, em valores lingüísticos.

As tabelas 21, 22 e 23 contêm as comparações de cada um desses especialistas, quanto à importância relativa de cada um dos três fatores para a formação do *índice agregado de capacitação,experiência e "feeling"* .

Tabela 15: Perfil de Capacitação e Experiência Profissional do Especialista E_1

FATOR	SUBFATOR	CRITÉRIO	Pontos
CAPACITAÇÃO	**Curso Técnico**	Sim	3
	Curso de Graduação	Sim	5
	Especialização em Segurança	Sim	4
	Mestrado	Sim. (voltado para a segurança)	10
		TOTAL	**22**
EXPERIÊNCIA	**Agente de Segurança**	15 anos	15
	Supervisor de Segurança	10 anos	20
	Gerente de Segurança	5 anos	15
		TOTAL	**45**

Tabela 16: Perfil de Capacitação e Experiência Profissional do Especialista E_2

FATOR	SUBFATOR	CRITÉRIO	Pontos
CAPACITAÇÃO	**Curso Técnico**	Sim	3
	Curso de Graduação	Sim (voltado para a segurança)	8
	Especialização em Segurança	Sim	4
		TOTAL	**15**
EXPERIÊNCIA	**Agente de Segurança**	15 anos	15
	Supervisor de Segurança	10 anos	20
	Participação em Emergência	3	15
		TOTAL	**50**

Tabela 17: Perfil de Capacitação e Experiência Profissional do Especialista E_3

FATOR	SUBFATOR	CRITÉRIO	Pontos
CAPACITAÇÃO	**Curso Técnico**	Sim	3
	Curso de Graduação	Sim (voltado para a segurança)	8
	Especialização em Segurança	Sim	4
	Mestrado	Sim. (voltado para a segurança)	10
		TOTAL	**25**
EXPERIÊNCIA	**Gerente de Segurança**	10 anos	30
	Auditor de Segurança	5 anos	20
	Participação em Emergência	1	5
	Participação em Investigação	1	10
		TOTAL	**65**

Tabela 18 – Matriz de Comparação Relativa do "Feeling" dos Especialistas, em Valores Lingüísticos, conforme E_1.

"FEELING"	E_1	E_2	E_3
E_1	TIQ	BMIQ	MMIQ
E_2	-	TIQ	EMIQ
E_3	-	-	TIQ

Tabela 19 – Matriz de Comparação Relativa do "Feeling" dos Especialistas, em Valores Lingüísticos, conforme E_2.

"FEELING"	E_1	E_2	E_3
E_1	TIQ	MMIQ	BMIQ
E_2	-	TIQ	FMIQ
E_3	-	-	TIQ

Tabela 20 – Matriz de Comparação Relativa do "Feeling" dos Especialistas, em Valores Lingüísticos, conforme E_3.

"FEELING"	E_1	E_2	E_3
E_1	TIQ	MMIQ	BMIQ
E_2	-	TIQ	FMIQ
E_3	-	-	TIQ

Tabela 21 – Matriz de Comparações dos Fatores quanto à Importância na Formação do Índice Agregado dos Especialistas, conforme $E1$, em Valores Lingüísticos.

IMPORTÂNCIA	"Feeling"	Capacitação	Experiência
"Feeling"	TIQ	BMIQ	MMIQ
Capacitação	-	TIQ	BMIQ
Experiência	-	-	TIQ

Tabela 22 – Matriz de Comparações dos Fatores quanto à Importância na Formação do Índice Agregado dos Especialistas, conforme $E1$, em Valores Lingüísticos.

IMPORTÂNCIA	"Feeling"	Capacitação	Experiência
"Feeling"	TIQ	FMIQ	MMIQ
Capacitação	-	TIQ	FMIQ
Experiência	-	-	TIQ

Tabela 23 – Matriz de Comparações dos Fatores quanto à Importância na Formação do Índice Agregado dos Especialistas, conforme $E1$, em Valores Lingüísticos.

IMPORTÂNCIA	"Feeling"	Capacitação	Experiência
"Feeling"	TIQ	FMIQ	BMIQ
Capacitação	-	TIQ	MMIQ
Experiência	-	-	TIQ

As demais variáveis do problema são aquelas constantes da figura 7. Para facilidade de referência, denotaremos os atributos relevantes da ameaça (3º nível da hierarquia) por B_1 (*impactabilidade adversa*), B_2 (*perpetrabilidade*) e B_3 (*probabilidade de perpetração*). Os *fatores e condições* (ou subatributos) serão denotados por C_k (k = 1,..., 9), já que cada um dos três atributos relevantes se conecta a três subatributos do 4º nível hierárquico. As ameaças são denotadas por A_1, A_2, A_3.

As tabelas 24, 25 e 26 contêm respectivamente os julgamentos, em valores lingüísticos, de cada um dos três especialistas (E_1, E_2, E_3), para as comparações entre si dos três subatributos do 4º nível hierárquico (ou seja, a *criticalidade do alvo para o funcionamento do sistema* (C_1), o *potencial de interferência adversa em outros*

componentes e/ou funções do sistema (C_2) e o *potencial para causar vítimas fatais ou ferimentos graves* (C_3)), quanto à importância relativa destes para a formação do atributo relevante *impactabilidade adversa* do 3º nível da hierarquia. Com esses julgamentos e os pesos dos especialistas, são avaliadas as importâncias relativas desses subatributos para a *impactabilidade adversa*. Para evitar repetição desnecessária de procedimentos computacionais, os valores das importâncias relativas dos subatributos conectados aos dois outros atributos relevantes para a formação destes serão admitidos como já avaliados, sendo seus valores providos no devido momento de sua utilização no modelo.

As tabelas 27, 28 e 29 contêm também respectivamente os julgamentos, em valores lingüísticos, de cada um dos três especialistas (E_1, E_2, E_3), para as comparações entre si das três ameaças do 5º nível hierárquico, em relação ao subatributo C_1 (*criticalidade do alvo para o funcionamento do sistema*). Com essas matrizes de comparações relativas e os pesos dos especialistas, são computadas as dominâncias relativas locais dessas três ameaças para esse subatributo. Da mesma forma que na avaliação anterior, para evitar repetição desnecessária de procedimentos computacionais, os valores das dominâncias relativas dessas três ameaças para os demais subatributos serão admitidos como já avaliados, sendo seus valores igualmente providos no devido momento de sua utilização no modelo.

A seguir, são fornecidas as tabelas 24 a 29.

Tabela 24 – Matriz de Comparações Relativas da Importância dos Subatributos C_1, C_2 e C_3 para a Impactabilidade Adversa, conforme E_1, em Valores Lingüísticos.

IMPACTABILIDADE ADVERSA	**C_1**	**C_2**	**C_3**
C_1	TIQ	BMIQ	1/FMIQ
C_2	-	TIQ	1/BMIQ
C_3	-	-	TIQ

Tabela 25 – Matriz de Comparações Relativas da Importância dos Subatributos C_1, C_2 e C_3 para a Impactabilidade Adversa, conforme E_2, em Valores Lingüísticos.

IMPACTABILIDADE ADVERSA	C_1	C_2	C_3
C_1	TIQ	MMIQ	1/BMIQ
C_2	-	TIQ	1/BMIQ
C_3	-	-	TIQ

Tabela 26 – Matriz de Comparações Relativas da Importância dos Subatributos C_1, C_2 e C_3 para a Impactabilidade Adversa, conforme E_3, em Valores Lingüísticos.

IMPACTABILIDADE ADVERSA	C_1	C_2	C_3
C_1	TIQ	FMIQ	1/EMIQ
C_2	-	TIQ	1/BMIQ
C_3	-	-	TIQ

Tabela 27 – Matriz de Comparações Relativas das Dominâncias das Ameaças A_1, A_2 e A_3 para o Subatributo C_1, conforme E_1, em Valores Lingüísticos.

E1	A_1	A_2	A_3
A_1	TIQ	MMIQ	MMIQ
A_2	-	TIQ	BMIQ
A_3	-	-	TIQ

Tabela 28 – Matriz de Comparações Relativas das Dominâncias das Ameaças para o Subatributo C_1, conforme E_2, em Valores Lingüísticos.

E2	A_1	A_2	A_3
A_1	TIQ	MMIQ	BMIQ
A_2	-	TIQ	MMIQ
A_3	-	-	TIQ

Tabela 29 – Matriz de Comparações Relativas das Dominâncias das Ameaças para o Subatributo C_1, conforme E_3, em Valores Lingüísticos.

E3	A_1	A_2	A_3
A_1	TIQ	BMIQ	MMIQ
A_2	-	TIQ	BMIQ
A_3	-	-	TIQ

5.2 AVALIAÇÃO DOS "PESOS DE PERCEPÇÃO" EM SEGURANÇA CONTRA ATOS DE INTERFERÊNCIA ILÍCITA DOS ESPECIALISTAS.

Para a avaliação dos "pesos" dos especialistas, isto é, do *índice agregado de capacitação, experiência e "feeling"* em segurança contra atos de interferência ilícita de cada especialista, inicia-se convertendo os valores lingüísticos das tabelas 18, 19 e 20 em valores numéricos, de acordo com a escala fundamental de Saaty. Essas matrizes, após conversão, ficam assim:

Tabela 30 – Matriz de Comparação Relativa do "Feeling" dos Especialistas, conforme E_1, em Valores Numéricos.

"FEELING" (segundo E1)	**E_1**	**E_2**	**E_3**
E_1	1	5	3
E_2	-	1	9
E_3	-	-	1

Tabela 31 – Matriz de Comparação Relativa do "Feeling" dos Especialistas, conforme E_2, em Valores Numéricos.

"FEELING" (segundo E2)	**E_1**	**E_2**	**E_3**
E_1	1	3	5
E_2	-	1	7
E_3	-	-	1

Tabela 32 – Matriz de Comparação Relativa do "Feeling" dos Especialistas, conforme E_3, em Valores Numéricos.

"FEELING" (segundo E3)	**E_1**	**E_2**	**E_3**
E_1	1	3	5
E_2	-	1	7
E_3	-	-	1

Em seguida, calcula-se a matriz de comparações médias, fazendo cada célula desta matriz igual à soma das células das três matrizes anteriores dividida por três.

Tabela 33 – Matriz de Comparações Médias do "Feeling" dos Especialistas, em Valores Numéricos.

"FEELING" (médio)	**E_1**	**E_2**	**E_3**
E_1	1	11/3	13/3
E_2	-	1	23/3
E_3	-	-	1

Completa-se a parte de baixo da diagonal principal, fazendo cada célula abaixo da diagonal igual ao inverso da célula diametralmente oposta, em relação à diagonal. Assim:

Tabela 34 – Matriz de Comparações Médias do "Feeling" dos Especialistas, em Valores Numéricos.

"FEELING" (médio)	**E_1**	**E_2**	**E_3**
E_1	1	11/3	13/3
E_2	3/11	1	23/3
E_3	3/13	3/23	1

Calcula-se o autovetor normalizado $\boldsymbol{F_g}$ dessa matriz, segundo o algoritmo simplificado do AHP, obtendo:

Tabela 35 – Autovetor Normalizado da Matriz de Comparações Médias do "Feeling" dos Especialistas.

Autovetor F_g	
f_1	0,587
f_2	0,317
f_3	0,095

O autovetor $\boldsymbol{F_g}$ determina o "***feeling***" relativo dos especialistas, segundo a própria avaliação destes. De acordo com esse vetor, o Especialista 1 tem o maior "***feeling***" entre os três. Passemos agora ao cômputo dos outros dois fatores, ***capacitação profissional*** e ***experiência profissional***.

Das tabelas 15, 16 e 17, obtemos: $k_1 = 22$, $k_2 = 15$, $k_3 = 25$, $x_1 = 45$, $x_2 = 50$ e $x_3 = 65$, onde K_g e X_g correspondem ao número de pontos do Especialista E_g (g=1,..,3), em capacitação e experiência, respectivamente.

A partir desses valores, pode-se facilmente obter os vetores $\boldsymbol{K}_g$ e $\boldsymbol{X}_g$ de capacitação relativa e de experiência relativa dos especialistas. Assim:

$$K = \sum K_{\mathbf{g}} = K_1 + K_2 + K_3 = 22 + 15 + 25 = 62$$

$$X = \sum X_{\mathbf{g}} = X_1 + X_2 + X_3 = 45 + 50 + 65 = 160$$

Agora, fazendo $k_g = K_g / K$ e $x_g = X_g / X$, obtemos:

$k_1 = 0{,}355$ $k_2 = 0{,}242$ $k_3 = 0{,}403$ e

$x_1 = 0{,}281$ $x_2 = 0{,}313$ $x_3 = 0{,}406$

Temos, então:

Tabela 36 – Vetor Normalizado da Capacitação Relativa dos Especialistas.

Vetor K_g	
$\boldsymbol{k_1}$	0,355
$\boldsymbol{k_2}$	0,242
$\boldsymbol{k_3}$	0,403

e

Tabela 37 – Vetor Normalizado da Experiência Relativa dos Especialistas.

Vetor X_g	
$\boldsymbol{x_1}$	0,281
$\boldsymbol{x_2}$	0,313
$\boldsymbol{x_3}$	0,406

Convertendo as tabelas 21, 22 e 23 em valores numéricos, fazendo a média desses valores e completando a parte de baixo da diagonal da matriz resultante, com os recíprocos dos valores da parte de cima da diagonal, obtemos a matriz de comparações médias da importância relativa dos fatores para a formação do índice agregado (“peso”) dos especialistas. Essa matriz é mostrada a seguir na tabela 38.

Tabela 38 – Matriz de Comparações Médias da Importância Relativa dos Fatores para a Formação do Índice Agregado dos Especialistas, em Valores Numéricos.

Importância Relativa dos Fatores	"Feeling"	Capacitação	Experiência
"Feeling"	1	19/3	3
Capacitação	3/19	1	17/3
Experiência	1/3	3/17	1

Computando o autovetor normalizado ***D*** dessa matriz, obtemos:

Tabela 39 – Vetor Normalizado ***D*** da Importância Relativa dos Fatores para a Formação do Índice Agregado dos Especialistas.

Vetor *D*	
d_1	0,608
d_2	0,275
d_3	0,118

Agora, substituindo os respectivos valores desses vetores na fórmula a seguir e efetuando o produto, determinamos o vetor dos "pesos" relativos dos especialistas em segurança da aviação civil contra atos de interferência ilícita. Assim,

$$W_g = \left[K_g \quad X_g \quad F_g\right]_{3\,x\,3} \bullet \left[D\right]_{1\,x\,3}, \qquad g = 1,..., 3, \qquad \text{(XXIX)}$$

obtemos:

Tabela 40 – Vetor Normalizado W_g Representativo do Índice Agregado de Capacitação, Experiência e "Feeling" dos Especialistas.

Vetor W_g	
w_1	0,362
w_2	0,270
w_3	0,368

5.3 AVALIAÇÃO DAS IMPORTÂNCIAS E DOMINÂNCIAS RELATIVAS DOS SUBATRIBUTOS PARA A FORMAÇÃO DOS ATRIBUTOS RELEVANTES.

As tabelas 24, 25 e 26 mostram matrizes contendo as avaliações, em termos lingüísticos, dos especialistas E_1, E_2 e E_3, quanto à importância relativa dos subatributos C_1, C_2 e C_3 para a formação do atributo relevante *impactabilidade adversa*. Convertendo essas matrizes de expressões lingüísticas nas respectivas matrizes de números *fuzzy* triangulares, por meio da correspondência numérico-conceitual da escala fundamental de Saaty, modificada para números *fuzzy*, e computando a média ponderada dos valores das células dessas matrizes, com os índices agregados dos especialistas como pesos, obtemos a matriz *fuzzy* de comparações relativas médias (Ã), cujos elementos $\boldsymbol{a}_{ij}$ médios são dados pela seguinte expressão:

$$\boldsymbol{a}_{ij} = (\sum a_{ijg} \cdot w_g) / 3. \qquad \text{(XXX)}$$

A matriz fuzzy de comparações relativas médias (**Ã**) obtida dessa forma, já completada em seus valores recíprocos em relação à diagonal principal, é mostrada na tabela 41, a seguir.

Tabela 41 – Matriz de Comparações Médias da Importância Relativa dos Subatributos para a Impactabilidade Adversa, em Números *Fuzzy*.

IMPACTABILIDADE ADVERSA	C1	C2	C3
Criticalidade do Alvo para o Func. do Sistema (C1)	**(1, 1, 1)**	**(1.425, 2.092, 2.759)**	**(.755, 1.421, 2.088)**
Potencial de Interfer. da Ameaça em Outros Componentes ou Funções do Sistema (C2)	**(.362, .478, .702)**	**(1, 1, 1)**	**(.513, 1.180, 1.847)**
Letalidade da Ameaça (C3)	**(.479, .704, 1.325)**	**(.541, .847, 1.949)**	**(1, 1, 1)**

Computando o autovetor normalizado *fuzzy* $\boldsymbol{R}_{\mathbf{IMPAC}}$ dessa matriz, obtemos:

Tabela 42 – Autovetor Normalizado *Fuzzy* $\boldsymbol{R}_{\mathbf{IMPAC}}$ Representativo da Importância Relativa dos Subatributos C1, C2 e C3 para a Impactabilidade Adversa.

Autovetor $\boldsymbol{R}_{\mathbf{IMPAC}}$	
$\boldsymbol{r_1}$	(.244, .461, .798)
$\boldsymbol{r_2}$	(.133, .267, .511)
$\boldsymbol{r_3}$	(.152, .272, .606)

Para verificar a consistência dos julgamentos convertidos em números *fuzzy* no processo, precisamos calcular a Razão de Consistência (RC) da matriz fuzzy de julgamentos. Para isso, é necessário determinar o autovalor máximo dessa matriz ($\lambda_{máx}$), utilizando os valores-suporte de maior pertinência das componentes do autovetor *fuzzy* normalizado $\boldsymbol{R}_{\mathbf{IMPAC}}$ e da soma das colunas da matriz *fuzzy* $\tilde{\boldsymbol{A}}$. Assim:

$\lambda_{máx} = 0{,}461 \cdot 2{,}182 + 0{,}267 \cdot 3{,}939 + 0{,}272 \cdot 3{,}601 = 3{,}038$

$IC = (\lambda_{máx} - n)/ (n-1) = (3{,}038 - 3) / (3-1) = 0{,}038 / 2 = 0{,}019$

$RC = IC / IR = 0{,}038 / 0{,}52 = 0{,}073$ (< 10% → julgamentos consistentes (Saaty, 1980)), onde IR = 0,52 é o índice randômico para uma matriz 3x3).

Os autovetores normalizados das importâncias relativas dos subatributos para os atributos *perpetrabilidade* e *probabilidade de perpetração*, os outros dois subproblemas deste mesmo nível (3º nível) da hierarquia são resolvidos, seguindo estes mesmos procedimentos. Conforme adiantamos, seria enfadonho repetir os mesmos procedimentos computacionais para determinar esses vetores, de forma que vamos fornecer dois autovetores com valores hipotéticos próximos aos valores obtidos no anterior, conforme mostrado nas tabelas 43 e 44, a seguir.

Tabela 43 – Autovetor Normalizado *Fuzzy* $\boldsymbol{R_{PERPE}}$ Representativo da Importância Relativa dos Subatributos para a Perpetrabilidade.

Autovetor $\boldsymbol{R_{PERPE}}$	
$\boldsymbol{r_1}$	(.234, .401, .792)
$\boldsymbol{r_2}$	(.143, .287, .551)
$\boldsymbol{r_3}$	(.182, .312, .636)

Tabela 44 – Autovetor Normalizado *Fuzzy* $\boldsymbol{R_{PROBA}}$ Representativo da Importância Relativa dos Subatributos para a Probabilidade de Perpetração.

Autovetor $\boldsymbol{R_{PROBA}}$	
$\boldsymbol{r_1}$	(.183, .374, .714)
$\boldsymbol{r_2}$	(.153, .315, .565)
$\boldsymbol{r_3}$	(.152, .311, .606)

Nosso próximo passo consiste da avaliação das dominâncias relativas das ameaças em relação aos subatributos. Como neste exemplo temos três ameaças para serem comparadas aos pares por cada um dos subatributos, os procedimentos computacionais são os mesmos. Quer dizer, uma vez de posse das matrizes de julgamentos dos especialistas, contidas nas tabelas 27, 28 e 29, é feita a conversão em números *fuzzy*. Após essa conversão, multiplicam-se os valores pelos "pesos" dos especialistas, obtendo as matrizes *fuzzy* ponderadas. Em seguida, essas matrizes são somadas e divididas por três (o número de especialistas avaliadores), resultando na matriz fuzzy de comparações médias (Ã) mostrada na tabela 45, a seguir.

Tabela 45 – Matriz de Comparações Médias das Ameaças em Relação ao Subatributo C_1 da Impactabilidade Adversa, em Números *Fuzzy*.

CRITICALIDADE DO ALVO P/ FUNCIONAMENTO DO SISTEMA	**A1**	**A2**	**A3**
Explosão de Bomba em Terminal de Transporte (A1)	**(1, 1, 1)**	**(.579, 1.245, 1.912)**	**(.513, 1.180, 1.847)**
Seqüestro de Veículo de Transporte (A2)	**(.523, .803, 1.728)**	**(1, 1, 1)**	**(.820, 1.487, 2.153)**
Sabotagem em Controle de Tráfego (A3)	**(.542, .847, 1.948)**	**(.464, .673, 1.220)**	**(1, 1, 1)**

Computando o autovetor normalizado *fuzzy* $\boldsymbol{S_1}$ dessa matriz, obtemos:

Tabela 46 – Autovetor Normalizado *Fuzzy* $\boldsymbol{S_1}$ da Dominância Relativa das Ameaças A1, A2 e A3 para a Criticalidade do Alvo.

Autovetor S_1	
s_{11}	(**.152, .375, .737**)
s_{11}	(**.173, .350, .750**)
s_{11}	(**.143, .275, .594**)

Calculando a Razão de Consistência para verificação da consistência dos julgamentos.

$\lambda_{máx} = 0{,}375 \cdot 2{,}651 + 0{,}350 \cdot 2.917 + 0{,}275 \cdot 3{,}667 = 3{,}024$

$IC = (\lambda_{máx} - n)/ (n-1) = (3{,}024 - 3) / (3-1) = 0{,}024 / 2 = 0{,}012$

$RC = IC / IR = 0{,}012 / 0{,}52 = 0{,}023$ (< 10% → julgamentos consistentes).

Os demais autovetores normalizados das matrizes de comparações relativas das ameaças para os outros oito atributos restantes seriam determinados da mesma forma, a partir das matrizes de julgamentos dos especialistas. Como não é propósito deste exemplo repetir desnecessariamente procedimentos computacionais já explicados, limitar-nos-emos a fornecer oito autovetores finais, hipoteticamente obtidos dessas comparações. As tabelas 47 a 55 mostram esses vetores.

Tabela 47 – Autovetor Normalizado *Fuzzy* $\boldsymbol{S_2}$ de Dominância Relativa das Ameaças A1, A2 e A3 para o Potencial de Interferência em outros Componentes.

Autovetor S_2	
S_{21}	(**.182, .376, .823**)
S_{21}	(**.163, .355, .767**)
S_{21}	(**.147, .269, .604**)

Tabela 48 – Autovetor Normalizado *Fuzzy* S_3 de Dominância Relativa das Ameaças A1, A2 e A3 para seu Potencial de Letalidade.

Autovetor S_3	
S_{31}	(**.142, .395, .787**)
S_{31}	(**.153, .340, .756**)
S_{31}	(**.145, .265, .584**)

Tabela 49 – Autovetor Normalizado *Fuzzy* S_4 de Dominância Relativa das Ameaças A1, A2 e A3 para a Capacidade de Liderança e Organização do Perpetrador.

Autovetor S_4	
S_{41}	(**.131, .356, .776**)
S_{41}	(**.193, .385, .780**)
S_{41}	(**.133, .259, .561**)

Tabela 50 – Autovetor Normalizado *Fuzzy* S_5 de Dominância Relativa das Ameaças A1, A2 e A3 para as Demandas de Ordem Técnica e Logística.

Autovetor S_5	
S_{51}	(**.141, .272, .658**)
S_{51}	(**.153, .455, .850**)
S_{51}	(**.132, .273, .584**)

Tabela 51 – Autovetor Normalizado *Fuzzy* S_6 de Dominância Relativa das Ameaças A1, A2 e A3 para a Facilidade de Obtenção de Meios Técnicos e Materiais.

Autovetor S_6	
S_{61}	(**.163, .365, .737**)
S_{61}	(**.172, .387, .791**)
S_{61}	(**.141, .248, .535**)

Tabela 52 – Autovetor Normalizado *Fuzzy* S_7 de Dominância Relativa das Ameaças A1, A2 e A3 para o Status de Implementação da Regulamentação de Segurança.

Autovetor S_7	
s_{71}	(**.172, .386, .777**)
s_{72}	(**.163, .323, .735**)
s_{73}	(**.123, 291, .548**)

Tabela 53 – Autovetor Normalizado *Fuzzy* S_8 de Dominância Relativa das Ameaças A1, A2 e A3 para a Conjuntura Doméstica.

Autovetor S_8	
s_{81}	(**.147, .379, .739**)
s_{82}	(**.167, .349, .752**)
s_{83}	(**.142, .272, .564**)

Tabela 54 – Autovetor Normalizado *Fuzzy* S_9 de Dominância Relativa das Ameaças A1, A2 e A3 para a Conjuntura Internacional.

Autovetor S_9	
s_{91}	(**.163, .395, .767**)
s_{92}	(**.213, .331, .832**)
s_{93}	(**.123, .274, .574**)

5.4 AVALIAÇÃO DOS ATRIBUTOS RELEVANTES: SÍNTESE DAS IMPORTÂNCIAS RELATIVAS COM AS DOMINÂNCIAS RELATIVAS.

Neste passo, procede-se à síntese das *importâncias relativas dos subatributos para a formação dos atributos* com as *dominâncias relativas das ameaças por subatributo* para obter os *valores relativos* de cada *atributo relevante*, isto é, a *impactabilidade adversa relativa*, a *perpetrabilidade relativa* e a *probabilidade de perpetração relativa* de *cada ameaça*. Essa síntese é feita, portanto, por atributo relevante. O procedimento computacional dessa síntese é a multiplicação da *matriz formada pelos três autovetores de dominâncias relativas das ameaças*, associados ao subatributos conectados ao atributo, pelo *autovetor de importâncias relativas desses subatributos*. Essencialmente, essa síntese significa uma *transição* das *dominâncias relativas das ameaças por subatributo* para *dominâncias relativas das ameaças por*

atributo, explicitando, no nível hierárquico desses atributos, os valores relativos destes por ameaça. Assim, em termos formais, temos:

$$\boldsymbol{IMPAC} = \left[\boldsymbol{S_1} \quad \boldsymbol{S_2} \quad \boldsymbol{S_3}\right]_{3 \times 3} \bullet \left[\boldsymbol{R}_{IMPAC}\right]_{3 \times 1} \qquad \text{(XXXI)}$$

$$\boldsymbol{PERPE} = \left[\boldsymbol{S_4} \quad \boldsymbol{S_5} \quad \boldsymbol{S_6}\right]_{3 \times 3} \bullet \left[\boldsymbol{R}_{PERPE}\right]_{3 \times 1} \qquad \text{(XXXII)}$$

$$\boldsymbol{PROBA} = \left[\boldsymbol{S_7} \quad \boldsymbol{S_8} \quad \boldsymbol{S_9}\right]_{3 \times 3} \bullet \left[\boldsymbol{R}_{PROBA}\right]_{3 \times 1} \qquad \text{(XXXIII)}$$

Após as devidas operações matriciais com aritmética *fuzzy*, obtêm-se:

$$\boldsymbol{IMPAC} = \begin{matrix} \boldsymbol{IMPAC_1} = (0{,}083;\ 0{,}381;\ 1{,}486) \\ \boldsymbol{IMPAC_2} = (0{,}087;\ 0{,}349;\ 1{,}449) \\ \boldsymbol{IMPAC_3} = (0{,}076;\ 0{,}270;\ 1{,}137) \end{matrix}$$

$$\boldsymbol{PERPE} = \begin{matrix} \boldsymbol{PERPE_1} = (0{,}080;\ 0{,}334;\ 1{,}446) \\ \boldsymbol{PERPE_2} = (0{,}055;\ 0{,}406;\ 1{,}589) \\ \boldsymbol{PERPE_3} = (0{,}050;\ 0{,}260;\ 1{,}106) \end{matrix}$$

$$\boldsymbol{PROBA} = \begin{matrix} \boldsymbol{PROBA_1} = (0{,}079;\ 0{,}386;\ 1{,}437) \\ \boldsymbol{PROBA_2} = (0{,}088;\ 0{,}334;\ 0{,}871) \\ \boldsymbol{PROBA_3} = (0{,}063;\ 0{,}280;\ 1{,}058) \end{matrix}$$

5.5 DETERMINAÇÃO DOS POTENCIAIS DAS AMEAÇAS INTENCIONAIS À AVIAÇÃO CIVIL

Os potenciais das ameaças intencionais específicas à aviação civil são determinados, conforme definição proposta, pelos produtos desses atributos por ameaça. Assim:

$$\boldsymbol{POTA_i} = \boldsymbol{IMPAC_i} \otimes \boldsymbol{PERPE_i} \otimes \boldsymbol{PROBA_i}\ , \quad i = 1,..., n \qquad \text{(XXXIV)}$$

Efetuando esses produtos, obtemos:

$$POTA = \begin{matrix} POTA_1 = (0{,}001;\ 0{,}049;\ 3{,}087) \\ POTA_2 = (0{,}000;\ 0{,}047;\ 2{,}005) \\ POTA_3 = (0{,}000;\ 0{,}020;\ 1{,}330) \end{matrix}$$

5.6 AVALIAÇÃO DO NÍVEL DE AMEAÇA INTENCIONAL À AVIAÇÃO CIVIL

Aplicando o Método dos Conjuntos Maximizantes e Minimizantes (Chen, 1985) a esses potenciais, encontramos $POTA_1$ como o maior desses potenciais de ameaça, de forma que o nível de ameaça intencional à aviação civil é dado por esse potencial. Isto é:

$$NAI = POTA_1 = (0{,}001;\ 0{,}049;\ 3{,}087)$$

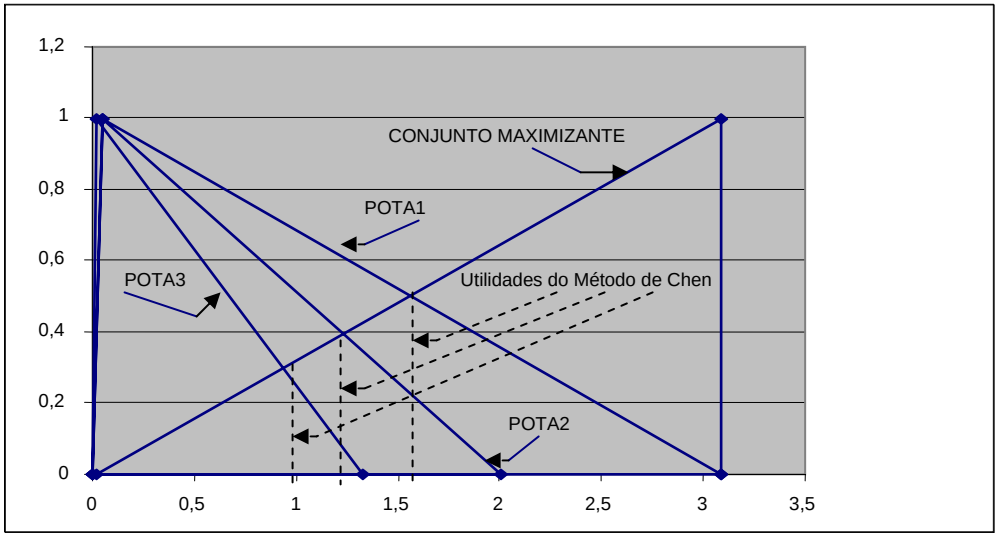

Figura 11: Método de Chen para Ordenar Números Fuzzy

Em outras palavras, isto quer dizer que a explosão de bomba em terminal de transporte aéreo civil, ou antes, em um aeroporto, é a ameaça que deve nortear a programação de segurança, enquanto uma nova avaliação do nível de ameaça não indicar outra coisa.

Capítulo 6

CONCLUSÃO

6.1 SÍNTESE DOS RESULTADOS DA PESQUISA

Após os atentados de 11 de setembro de 2001, envolvendo a aviação comercial dos EUA, o alto custo de implementação dos novos padrões de segurança, destinados a melhorar a prevenção e a proteção dos sistemas de transporte contra ameaças intencionais, acabou ressaltando a questão da compatibilidade e da proporcionalidade das medidas de segurança ao nível de ameaça intencional a esses sistemas.

Após exaustivas discussões nos fóruns internacionais do setor, o gerenciamento de risco da segurança contra ameaças intencionais foi globalmente reconhecido e recomendado como processo de gestão importante e necessário para provisão dos serviços de segurança em tais sistemas. Atrelada à recomendação do gerenciamento de risco da segurança como prática para a gestão dessa atividade no setor, veio também a abordagem sistêmica como metodologia de análise da segurança contra ameaças intencionais e destas em seus aspectos relacionados com a perpetrabilidade, impactabilidade, além da probabilidade de perpetração.

A avaliação do nível de ameaça intencional aos ativos físicos e operacionais desses sistemas, um agregado intuitivamente denominado no setor de *nível de ameaça ao sistema*, tornou-se uma atividade crítica do gerenciamento de risco da segurança, já que o risco associado a tais ameaças é admitido como uma função desse nível. Com a determinação desse nível e conseqüente definição dos riscos associados às ameaças intencionais, a provisão da segurança pode ser realizada de forma proporcional aos níveis de ameaça avaliados, permitindo uma alocação mais racional dos recursos humanos e materiais disponíveis no setor para essa atividade.

Acima de tudo, esse agregado pode ser utilizado diretamente pelas autoridades governamentais para reavaliar os alertas de segurança nacionais contra ameaças intencionais, normalmente utilizados para estabelecer medidas preventivas e de contingência para esses sistemas.

O nível de ameaça a um sistema de transporte, contudo, não é um conceito simples e claro, capaz de permitir avaliações simples e imediatas. Entretanto, o potencial de uma ameaça específica a um sistema de transporte pode admitir um conceito razoável, que, na definição proposta nesta tese, envolve uma agregação conjuntural de atributos relevantes associados às ameaças intencionais, conforme afetados por fatores e condições internos e externos ao sistema de transporte.

Por analogia à energia potencial de um corpo em um campo gravitacional, essa agregação conjuntural foi definida como o produto de três atributos relevantes associados às ameaças intencionais: a impactabilidade adversa da ameaça, a perpetrabilidade da ameaça e a probabilidade de perpetração da ameaça. Essa definição criou as condições necessárias para definir o **nível de ameaça intencional a um sistema de transporte** como o ***maior dos potenciais de ameaça*** assim avaliados.

Potenciais de ameaça assim determinados podem variar com a forma e intensidade das interações entre esses atributos, bem como com o *status* e a evolução dos fatores e condições com afetação sobre estes. A avaliação de potenciais de ameaças específicas mostra-se, portanto, uma atividade vital para o processo de gerenciamento de risco da segurança, já que provê elementos de informação cruciais para este processo.

Devido às características vagas e ambíguas, os atributos relevantes das ameaças intencionais e as condições e fatores do ambiente em que o sistema opera são em geral difíceis de avaliar quantitativamente em *termos absolutos*. Seus valores, geralmente

expressões em linguagem natural avaliadas por percepção, são naturalmente *imprecisos* e difíceis de manipular formalmente por métodos quantitativos clássicos.

Para superar essa dificuldade, nosso modelo introduz uma associação do *Processo de Hierarquia Analítica* com a *Teoria dos Conjuntos "Fuzzy"*. Esta associação possibilita estruturar o problema em uma hierarquia de subproblemas de menor complexidade, na qual aqueles atributos são avaliados *em termos relativos fuzzy*.

Essa avaliação em termos relativos fuzzy é obtida mediante a substituição dos números "crisp" da escala fundamental do AHP (Saaty, 1980) por números fuzzy triangulares. Com esta substituição, os números intermediários "crisp" 2, 4, 6 e 8, previstos nessa escala para representar situações de compromisso entre dois julgamentos já são modelados matematicamente nas funções de pertinência dos números fuzzy triangulares adotados em substituição aos números "crisp" impares. Dessa maneira, o modelo provê um formalismo matemático adequado à resolução do problema, reduzindo a *imprecisão* inerente aos resultados.

Os resultados são coerentes e apresentam elementos de informação com um razoável grau de confiabilidade para o processo de tomada de decisão do gerenciamento do risco da segurança dos transportes contra ameaças intencionais. Uma eventual comparação do nível de ameaça intencional assim computado com representações em números fuzzy triangulares dos níveis de ameaça adotados no país para definir o alerta de segurança nos sistemas de transporte pode ser feito a posteriori, produzindo a informação necessária para atualizar tal alerta.

6.2 RECOMENDAÇÕES PARA PESQUISA FUTURA

Durante a pesquisa, observou-se que inconsistências de julgamento podem ocorrer com relativa facilidade na construção das matrizes de importâncias relativas, se

não forem tomadas certas precauções na escolha e caracterização das *condições e fatores* (*subatributos*) que concorrem, contribuem ou afetam os atributos relevantes das ameaças intencionais. Parte dessas inconsistências parece derivar do fato desses fatores e condições apresentarem algum grau de colinearidade de percepção por parte dos especialistas, por mais que estes apresentem diferenças em seus ”pesos de percepção”. Outras inconsistências parecem derivar da falta de entendimento dos especialistas quanto ao significado e forma de afetação de tais subatributos na formação dos respectivos atributos do nível hierárquico superior da estrutura. De forma similar, podem surgir inconsistências nos julgamentos das dominâncias relativas das ameaças com respeito a esses fatores e condições.

O aparecimento de tais inconsistências é em geral difícil de evitar no processo de avaliação, mas alguma coisa pode ser feita quando sua ocorrência é constatada. Naturalmente, esta constatação só é possível mediante o cômputo da razão de consistência (CR) da matriz de julgamentos comparativos. Sua detecção também é possível de realizar na fase de construção das matrizes de comparação, mediante uma análise criteriosa das transitividades dos julgamentos. Aliás, um expediente utilizado no AHP para levantar as intransitividades decorrentes nos julgamentos em razão das inconsistências é a elevação das matrizes de comparações relativas ao quadrado sucessivamente, até obter diferenças menores que um determinado grau de precisão ε (por exemplo ε = 0,001) entre os valores das componentes sucessivas dos autovetores normalizados computados.

Uma outra forma de evitar esses problemas pode ser mediante uma pesquisa mais específica dos fatores e condições que entram na formação dos atributos relevantes. A inclusão de fatores mais pertinentes e não colineares em sua concorrência, contribuição ou afetação para a determinação dos valores dos atributos relevantes das

ameaças poderá resultar em potenciais mais consistentes e compatíveis com a percepção geral que os especialistas formam a respeito do ambiente de ameaça a que os sistemas de transporte podem ficar submetidos. Uma pesquisa que envolva o refinamento da escolha de tais subatributos pode dar uma significativa contribuição para precisão dos resultados.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDREWS, J.D. e MOSS, T.R. (1993). *Reliability and Risk Assessment*. 1st Ed. Longman Group, UK.

AVEN, T. (1992) *Reliability and Risk Analysis*. 1st Ed. Elsevier Applied Science.

BERGER, J. (1985) *Statistical Decision theory and Bayesian Analysis*. Second Edition. Springer-Verlag. New York.

BEDFORD, T. e COOKE, R. (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, UK, 414 págs.

BOUTI, A. and KADI, D.A. (1994) "A state-of-the-art review of FMEA/FMECA". *International Journal of Reliability, Quality and Safety Engineering*. Vol 1, No. 4, pg 515-543.

BOX, G.E.P., and TIAO, G.C. (1973). *Bayesian Inference in Statistical Analysis*. Addison - Wesley.

BRASILIANO, A. C. R. (2003). "Métodos para Análise de Risco na Segurança Patrimonial". *Revista Proteger*. Brasil.

BROOKE, Paul. (2000). "Risk Assessment Strategies". *Network Computing Magazine*. USA, October.

BUCKLEY J. J. (1985). "Fuzzy hierarchical analysis". *Fuzzy Sets and Systems*, Volume 17, Issue 3, December, pp. 233-247.

CHEN, S. H. (1985). "Ranking Fuzzy Numbers with Maximizing Sets and Minimizing Sets". *Fuzzy Sets and Systems,* 17, 113-129.

CHILDS, David. (2002). "Information Technology Security System Engineering Methodology". *SANS GSEC Practical Assignment* v.1.3. USA, Abril.

CHEN, S. M., (1996). "Evaluating weapon systems using fuzzy arithmetic operations," *Fuzzy Sets and Systems*, 77, 265-276.

CHENG, C. H., (1996). "Evaluating naval tactical missile systems by fuzzy-AHP based on the grade value of membership function," *European Journal of Operational Research*, 96, 343-350.

COOPER, D. R.; SCHINDLER, P. S. (2003). *Métodos de pesquisa em administração*. 7. ed. Editora Bookman. Porto Alegre.

COSENZA, C. A. N. (2005). Apostila do Curso "Introdução à Lógica Fuzzy". Programa de Engenharia da Produção. COPPE/UFRJ.

DHILLON, B.S. e SINGH, C.H. (1981). *Engineering Reliability: New Techniques and Applications.* Wiley, USA.

DOBSON, J.E. e RANDELL, B. (1986). “Building reliable secure computing ystems out of unreliable insecure components”. In: *Proc. of the 1986 IEEE Symp. Security and Privacy*, pp. 187-193, April 1986.

FEIN, Robert A. et alii. (1995). “Threat Assessment: An Approach to Prevent Targeted Violence”. *National Institute of Justice*. USA, July, 1995.

____. (1998). “Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials”. *National Institute of Justice*. USA, July 1998.

FILEV, D. e YAGER, R.R. (1994). *Essentials of Fuzzy Modeling and Control*, Wiley-Interscience.

FRAY, J.-M., DESWARTE, Y., POWELL, D. (1986) “Intrusion tolerance using fine-grain fragmentation-scattering”, In: *Proc. 1986 IEEE Symp. on Security and Privacy*, Oakland, April 1986, pp. 194-201.

FULLWOOD, R. R. e HALL, R. E. (1988). *Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications*. Pergamon Press, Oxford.

GAO - U.S. GENERAL ACCOUNTING OFFICE, (1996). *Terrorismo e Tráfico de Drogas: As Ameaças e o Papel da Tecnologia de Detecção de Explosivos e Narcóticos*. In: Relatório nº GAO/NSIAD/RCED, p. 96-76 BR, USA, Março.

____, (1998). *Combating Terrorism: Threat and Risk Assessment Can Help Prioritize and Target Program Investments*. In: Report nº GAO/NSIAD/98-74, USA.

____, (2000) *Information Security Risk Assessment, GAO Practices of Leading Organizations*. Special publication GAO/AIMD-00-33. USA.

____, (2001) *Terrorist Acts Illustrate Severe Weaknesses in Aviation Security*. In: Relatório n.º GAO-01-1166T, USA. Setembro.

____, (2002) *Aviation Security: Transportation Security Administration Faces Long Term Challenges*. In: Relatório n.º GAO-02-971T, USA. July.

____, (2005). *Risk Management: Further Refinements Needed to Assess Risksand Prioritize Protective Measures at Ports and Other Critical Infrastructure*. In: Report to Congressional Requesters GAO-06-91, USA, December.

____, (2006). *AVIATION SECURITY: TSA Has Strengthened Efforts to Plan for the Optimal Deployment of Checked Baggage Screening Systems, but Funding Uncertainties Remain*. In: Testimony GAO-06-875T- before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives.

____, (2007). *Cost Estimates Related to TSA Funding of Checked Baggage Screening at Los Angeles and Ontario Airports*. In: Report to Congressional Committees GAO-07-445, USA, March.

GIL, A. C. (2002). *Como elaborar projetos de pesquisa*. 4. ed. Editora Atlas. São Paulo.

GULL, S. F. (1988) "Bayesian inductive inference and maximum entropy". In: *Maximum Entropy and Bayesian Methods in Science and Engineering*, *vol. 1: Foundations*, ed. by G. Erickson and C. Smith, pp. 53-74. Kluwer.

HAIMES, Y. Y. (1998). *Risk Modeling, Assessment, and Management*. John Wiley & Sons, Inc. New York, USA.

HAIMES Y. Y. (2004). *Risk Modeling, Assessment, and Management*. 2nd ed. John Wiley & Sons, Inc. Hoboken, New Jersey, USA.

HENLEY, E. J. e KUMAMOTO, H. (1981). *Reliability Engineering and Risk Assessment*. Prentice-Hall, US.

JAIN, R. (1976). "Decision-Making in the Presence of Fuzzy Variables". *IEEE Trans. Systems Man. And Cybernetics,* 6. pp. 698-703.

JAIN, R. (1977). "A Procedure for Multi-Aspect Decision-Making Using Fuzzy Sets". *International Journal of Systems Sciences*, 8, pp 1-7.

JAYNES, E. T. (1983). "Bayesian intervals versus confidence intervals". In: *E.T. Jaynes. Papers on Probability, Statistics and Statistical Physics*, ed. by R. D. Rosenkrantz, p. 151. Kluwer.

JOSEPH, M.K. e AVIZIENIS, A. (1988). "A fault tolerance approach to computer viruses", in *Proc. of the 1988 IEEE Symposium on Security and Privacy*, pp 52-58, April 1988.

KARA-ZAITRI, C., KELLER, A.Z., BARODY, I. and FLEMING P.V. (1991). "An Improved FMEA methodology". In: *Proceedings Annual Reliability and Maintainability Symposium*, pp 248-252.

KARA-ZAITRI, C., KELLER, A.Z., and FLEMING P.V. (1992). "A Smart Failure Mode and Effect Analysis Package". In: *Proceedings Annual Reliability and Maintainability Symposium*, pg 414-421,.

KATO, H., DE RU W.G., ELOFF, J.H.P (1996). "Risk Analysis Modeling with the Use of Fuzzy Logic". *Computers and Security*, Volume 15, Number 3, pp. 239-248 (10). Elsevier

KARSAK, E. E. and KUZGUNKAYA, O., (2002). "A fuzzy multiple objective programming approach for the selection of a flexible manufacturing system," *International Journal of Production Economics*, 79, 101-111.

KUO, R. J., CHI, S. C., and KAO, S. S., (1999). "A decision support system for locating convenience store through fuzzy AHP," *Computers & Industrial Engineering*, 37, 323-326.

LAPRIE, J.-C. et al., (1995). *Guide de la sûreté de fonctionnement*. 324p., ISBN 2-85428-382-1, Cépaduès-Editions, Toulouse, France.

LAPRIE, J.-C. (1992) *Dependability: Basic Concepts and Terminology*. Springer-Verlag.

LAPRIE, J. C. (1990) *Dependability Concepts and Terminology*. In: First Year Report, Task A, Vol 1 of 3 LAAS. Toulouse, France.

LAPRIE, J. C. (1998). "Dependability: from concepts to limits". In: *Proceedings of the IFIP International Workshop on Dependable Computing and its Applications*. DCIA 98, Johannesburg, South Africa, January 12-14, 1998.

LAAZARICK, R. (2000) "Sistematic Assessment of Airport Risk (SAAR)". In: *Proceedings of NDIA 16th Annual Security Technology Symposium*. New Jersey, USA. CRAMM, UK.

LIANG, , G-S. Et Al. (1991). "A Fuzzy Multi-Criteria Decision Method for Facility Site Location". *International Journal of Production Research*, Vol. 29, Nº 11, pp. 2313-2330.

MASLOW, A. (1954) *Motivation and Personality*, NY: Harper, Contents. Second Ed. NY: Harper, 1970. Contents. Third Ed. NY: Addison-Wesley, 1987.

McCORMICK, R. (1981). *Reliability and Risk Analysis: Methods and Nuclear Power Applications*. Academic Press, USA.

MIKHAILOV L. (2003) "Deriving priorities from fuzzy pairwise comparison judgements". *Fuzzy Sets and Systems*, Volume 134, Issue 3, Pages 365-385.

MON, D. L., C. H. CHENG, and LIN, J. C., (1994). "Evaluating weapon system using fuzzy analytical hierarchy process based on entropy weight," *Fuzzy Sets and Systems*, 62, 127-134.

MOSCATO, D. R. (1998). "Database gateway processor risk analysis using fuzzy logic". *Information Management & Computer Security*, 6/3, pp. 138–144. Elsevier.

NIPC-NATIONAL INFRASTRUCTURE PROTECTION CENTER (2002). *Risk Management: An Essential Guide to Protecting Critical Assets*. Wahington DC, EUA. Nov 2002.

OACI – Organização de Aviação Civil Internacional (2001). *Resolutions Adopted at the 33rd Session of the Assembly*. Montreal, Canada. http://www.icao.int/icao/en/assembl/a33/resolutions_a33.pdf.

____. (2002). Convenção de Chicago, Anexo 17, Montreal: 4 ed.

____. Doc 8.973, Security Manual, Set. 2002, Montreal: 6 ed.

O'HAGAN, A. (1994) *Bayesian Inference*, volume 2B of *Kendall's Advanced Theory of Statistics*. Edward Arnold. New York.

O'HAGAN, A. e FORSTER, J. (2003) *Kendall's Advanced Theory of Statistics, Volume B: Bayesian Inference*. Edward Arnold, New York.

OMI - International Maritime Organization (2002). Proceedings of the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974: 9 - 13 December 2002. London, Great Britain.

PELAEZ, C.E. e BOWLES, J.B. (1995) "Applying Fuzzy Cognitive-Maps Knowledge-Representation to Failure Modes Effects Analysis". Proceedings Annual Reliability and Maintainability Symposium, pg 450-459.

PEDRYCZ, W. e GOMIDE, F. (1998) Introduction to Fuzzy Sets, Cambridge, MA: MIT Press.

PEREIRA, A. L. (2003) Apostila da Disciplina Análise de Confiabilidade e Segurança de Sistemas de Transportes. Programa de Engenharia de Transportes PET / COPPE / UFRJ. Rio de Janeiro, Brasil.

PEREIRA, A. L. (2006) Apostila da Disciplina Teoria Geral dos Sistemas. Programa de Engenharia de Transportes PET / COPPE / UFRJ. Rio de Janeiro, Brasil.

RASCHE, Tilman. (2001). Risk Analysis Methods: A Brief Review. The University of Queensland, USA, June 2001.

ROLAND, H.E. e MORIATY, B. (1990). System Safety Engineering and Management. 2nd Ed. John Wiley & Sons, Inc.

REASON, J. (1990). Human Error. Cambridge University Press, UK.

ROBINSON, K. (2001). Flexible Approach to Implementing Security Measures. ICAO Journal, Montreal: v. 56, n 5.

ROSS, T.J. (2004). Fuzzy Logic with Engineering Applications, 2nd Edition, Wiley.

SAATY, T.L., (1979). "Exploring the Interface Between Hierarchies, Multiple Objectives and Fuzzy Sets," Fuzzy Sets and Systems, pp. 57-68.

SHIMONSKI, R. J. (2002). Risk Assesment and threat Identification. Security+ Study Guide and DVD Training System. Amazon.com. EUA.

STAMATELATOS, M., VESELY, W. e DUGAN, J., (2002). Fault Tree Handbook with Aerospace Applications, Version 1.1. NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC.

STAMATIS, D.H. (1995) *Failure Mode and Effect Analysis - FMEA from Theory to Execution.* ASQC Quality press.

SUTTON, I.S., (1992) *Process Reliability and Risk Management*. 1st Ed. Van Nostrand Reinhold.

UITP (2004). Press Release: UITP and UIC sign declaration on terrorism at international conference on personal security in public transport. Proceedings of the Conference on Personal Security in Public Transport. Genebra, Suiça.

US Congress (2001). Public Law 107–71(107th Congress). ‘‘Aviation and Transportation Security Act’’. Washington, DC, USA.

VAN LAARHOVEN P.J.M. and PEDRYCZ W. (1983) A fuzzy extension of Saaty's priority theory. *Fuzzy Sets and Systems, Volume 11, Issues 1-3,, Pages 199-227.*

VROOM, V. (1964). *Work and Motivation*. John Wiley, New York, USA.

YEN, J. e LANGARI, R. (1998). Fuzzy Logic: Intelligence, Control and Information, Prentice Hall, 1st edition.

YU, C. S., (2002). “A GP-AHP method for solving group decision-making fuzzy AHP problems,” *Computers & Operations Research*, 29, 1969-2001.

WECK, M., KLOCKE, F., SCHELL, H. and RUENAUVER, E. (1997). “Evaluating alternative production cycles using the extended fuzzy AHP method,” *European Journal of Operational Research*, 100(2), 351-366.

WILLIS, H. H., Morral, A. R., Kelly, T. K., Medby, J. J. (2005). Estimatig Terrorism Risk. Publicado pela RAND Corporation, Santa Monica, CA, USA. (disponível no site http://www.rand.org/)

ZADEH, L. A. (1965), Fuzzy Sets. *Information and Control*, 8, 338-353.

ZADEH, L. A. (1975-1976), The Concept of a Linguistic Variable and its Application to Approximate Reasoning. Part 1, 2 and 3, Information Science, 8, 199-249, 301-357; 9, 43-58.nformation and Control, 8, 338-353.

ZADEH, L.A., (1983). A computational approach to fuzzy quantifyers in natural languages. *Comput. Math*. 9, 149–184.

ZADEH, L.A., (2000). Outline of a computational theory of perceptions based on computing with words. In: Sinha, N.K., Gupta, M.M. (Eds.), *Soft Computing and Intelligent Systems: Theory and Applications*. Academic Press, London, pp. 3–22.

ZADEH, L.A., (2002). Towards a Perception Based Theory of Probabilistic Reasoning. In: *Journal of Statistical Planning and Inference* 105 (2002) 233–264 www.elsevier.com/locate/jspi

ZADEH, L.A. (1973) *Outline of a new approach to the analysis of complex systems and decision processes*, IEEE Trans. on Systems, Man and Cybernetics SMC-3, 28-44.

ZADEH, L.A. (1979). Fuzzy sets and information granularity, *Advances in Fuzzy Set Theory and Applications*, M. Gupta, R. Ragade and R. Yager (eds.), 3-18. Amsterdam: North-Holland Publishing Co.

ZADEH, L.A. (1997). Toward a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic, *Fuzzy Sets and Systems* 90, 111-127.

BIBLIOGRAFIA

ARMSTRONG, David. (2001). Flight Risks: Nation's Airlines Adopt Aggressive Measures for Passenger Profiling. Wall Street Journal, NY, USA, 25 October 2001.

BEKEN, T. Vander. (2002). Crime Proofing and Crime Assessment. Apresentação no Institute for International Research on Criminal Policy. Bruxelas, Outubro de 2002.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado, 1988.

BRASIL. Código Brasileiro de Aeronáutica, Lei nº 7.565 de 19 de dezembro de 1986, Brasília.

CASADA, M.L., SCHOOLCRAFT, S.G. e WALKER, D.A. (2001) Enterprise Risk Management: A Key for Optimizing the Cost-benefit Balance of Process Safety. Center for Chemical Process Safety Conference, Toronto, Ontario, Canada, October 2001.

DAC – Departamento de Aviação Civil (1997). PDSAC IV: Quarto Plano de Desenvolvimento do Sistema de Aviação Civil, Rio de Janeiro, Brasil.

DAC – Departamento de Aviação Civil (1997). PNAVSEC – Plano de Segurança da Aviação Civil, 3. ed. Rio de Janeiro, 2000.

FAA, FEDERAL AVIATION ADMINISTRATION (2001). Civil Aviation Security Strategic Plan 2001-2004. FAA Aviation Security Research and Development Technical Center. USA.

GUTHRIE, V.H., et Alii. (2000). Risk-based Decision Making: Do You Have the Right Stuff? 18th International System Safety Society Conference, Forth Worth, TX, USA, September 2000.

OACI – Organización de Aviación Civil Internacional (1980). Facilitation, Anexo 9, Jul. 1980, Montreal: 8 ed.

____. Doc 9.137, Servicios Operacionales de Aeropuerto, Parte 8, Montreal: 1ed.,1983.

____ .Doc 9.137, Planificatión de Emergencia en los Aeropuertos, Parte 7, Montreal: 2 ed. 1991.

____ Doc 8.364, Convention on offences and certain other acts committed on board aircraft. Signed at Tokio on 14 September 1963.

____ Doc 8.920, Convention for the suppression of unlawful seizure of aircraft. Signed at the Hague on 16 December 1970.

_____ Doc 8.966. Convention for the suppression of unlawful acts against the safety of civil aviation. Signed at Montreal on 23 September 1971.

____ Doc 9.518, Protocol for the suppression of unlawful acts of violence at airports serving international civil aviation. Done at Montreal on 23 September 1971.

____ Doc 9.571. Convention on the marking of plastic explosives for the purpose of detection. Done at Montreal on 1 March 1991.

____ Doc 7.100. Tariffs for airports and air navigation services. Montreal, 2002.

____. Boletins AVSEC, Montreal, Canadá, 2000.

RUSSOMANO, D.J., BONNELL, R.D. e BOWLES, J.B. (1992) "A Blackboard Model of an Expert System for Failure Mode and Effects Analysis". *Proceedings Annual Reliabilty and Maintainability Symposium*, pg 483-489.

SODYIA A.S., ANASHOGA S.A., OLADUNJOYE B.A. (2007). "Threat Modeling Using Fuzzy Logic Paradigm", *Issues in Informing Science and Information Technology*, Vol. 4, pp. 53-61. (disponível em http://proceedings.informingscience.org/InSITE2007/IISITv4p053-061Sodi261.pdf) (acessado em outubro 2007)

SPRUSTON, Donald. (2002). "General Aviation – Matching Security to the Threat". *AVSEC World 2002 Conference,* Roma , Itália, 29-31de Outubro.

STUNGIS, George E., Ph.D. and SCHORI, Thomas R., Ph.D. (2003), "A Terrorist Target Selection and Priorization Model", *Journal of Homeland Security*. USA, Março.

SUOKAS, J. and ROUHIAINEN, V. (1993) *Quality Management of Safety and Risk Analysis*. Elsevier Science Publishers B.V.

TUCKER, Jonathan B. (2003). "Strategies for Countering Terrorism: Lessons from the Israeli Experience". *Journal of Homeland Security*. USA, Março .

WALKER, D.A. et Alii. (1998). "The Status of Risk and Reliability Management Programs in Industry". *Process Plant Safety Symposium*, Houston, TX, USA, October.

WALKER, D.A. e GUTHRIE, V.H. (1999). "Enterprise Risk Management". *17th International System Safety Society Conference*, Orlando, FL, USA, August.

WALKER, D.A., SCHOOLCRAFT, S.G. et Alii. (2001). "Quick-reference Guide to Risk-based Decision Making (RBDM): A Step-by-step Example of the RBDM Process in the Field". *19th International System Safety Society Conference*, Huntsville, AL, USA, September.

ZAKARIA, Fareed. (2002). "Freedom vs. Security: The Case for 'Smart Profiling' as a Weapon in the War on Terror". *Newsweek*, Vol. CXL, No. 2 (8 July 2002), p. 31.USA.

Anexo 1

INTELLIGENCE GOV UK

(http://www.intelligence.gov.uk/threat_levels.aspx, acessado em setembro 2007)

Threat Levels: The System to Assess the Threat from International Terrorism

What are Threat Levels

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. This information may well be incomplete and decisions about the appropriate security response are made with this in mind.

Together with the detailed assessments behind them, this analysis informs security practitioners in key sectors and the police of the potential threat of terrorist attack. Threat assessments are also produced as necessary for individuals and events. There are five threat levels which inform decisions about the levels of security needed to protect our Critical National Infrastructure (CNI).

- **Low** - an attack is unlikely
- **Moderate** - an attack is possible, but not likely
- **Substantial** - an attack is a strong possibility
- **Severe** - an attack is highly likely
- **Critical** - an attack is expected imminently

How do we decide Threat Levels

In reaching a judgement on the appropriate threat level in any given circumstance several factors need to be taken into account, these include:

Available intelligence: It is rare that specific threat information is available and can be relied upon. More often, judgements about the threat will be based on a wide range of information, which is often fragmentary, including the level and nature of current terrorist activity, comparison with events in other countries and previous attacks. Intelligence is only ever likely to reveal part of the picture.

Terrorist capability: An examination of what is known about the capabilities of the terrorists in question and the method they may use based on previous attacks or from intelligence. This would also analyse the potential scale of the attack.

Terrorist intentions: Using intelligence and publicly available informaton to examine the overall aims of the terrorists and the ways they may achieve them including what sort of targets they would consider attacking.

Timescale: The threat level expresses the likelihood of an attack in the near term. We know from past incidents that some attacks take years to plan, while others are put together more quickly. In the absence of specific intelligence, a judgement will need to be made about how close an attack might be to fruition. Threat levels do not have any set expiry date, but are regularly subject to review in order to ensure that they remain current.

Who decides Threat Levels

The Joint Terrorism Analysis Centre (JTAC) was created in 2003 as the UK's centre for the analysis and assessment of international terrorism. JTAC is responsible for setting international terrorism threat levels and Ministers are informed of its decision. It also issues warnings of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies, as well as producing more in-depth reports on trends, terrorist networks and capabilities.

The Security Service is responsible for assessing the level and nature of the threat arising from domestic terrorism, principally the Irish related terrorist threat.

Where can I find out what the current National Threat Level is

National threat levels are continually monitored and are altered as required. We cannot anticipate how frequently they may be amended as this is dependent on available intelligence at any one time.

Information about the national threat level will be available on this website as well as the Security Service and Home Office websites.

Information on the risks of terrorism for British nationals overseas can be found on the Foreign and Commonwealth Forum website.

What are Response Levels and how do they relate to Threat Levels

Response levels provide a broad indication of the protective security measures that should be applied at any particular moment. They are set by security practitioners in Government and in some Critical National Infrastructure sectors. They are informed by the threat level but also take into account specific assessments of vulnerability and risk.

Response levels tend to relate to sites, whereas threat levels usually relate to broad areas of activity.

Within response levels, there is a variety of security measures that can be applied as appropriate - the response level will not produce the same measures at every location. Many of the measures will not be obvious or visible to the public.

There are three levels of response which broadly equate to threat levels as shown below:

Response Levels and how they relate to Threat Levels

Response Level	Description	Related Threat Levels
Normal	Routine protective security measures appropriate to the business concerned	Low and Moderate
Heightened	Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk	Substantial and Severe
Exceptional	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk	Critical

The security measures taken to protect people and Critical National Infrastructure will not be announced publicly, to avoid informing terrorists about what we know and what we are doing about it. Because response levels are the result of detailed assessments of risk to specific elements of the Critical National Infrastructure, changes in the national threat level will not necessarily produce changes to the sector-specific response levels.

How the Public should respond to different National Threat Levels

Public vigilance is always important regardless of the current national threat level, but it is especially important given the current national threat. Sharing national threat levels with the general public keeps everyone informed and explains the context for the various security measures (for example airport security or bag searches) we may encounter as we go about our daily lives.

--x--

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo