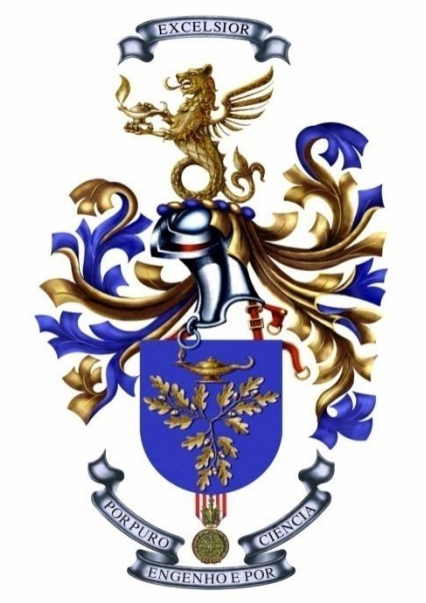
INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE ESTADO MAIOR CONJUNTO
2016/2017

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

ANÁLISE DE VULNERABILIDADE EM INFRAESTRUTURAS CRÍTICAS

MAJ ENG António Carlos dos Santos Ferreira



INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

ANÁLISE DE VULNERABILIDADE EM INFRAESTRUTURAS CRÍTICAS

MAJ ENG António Carlos dos Santos Ferreira

Trabalho de Investigação Individual do CEMC 2016/17

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

ANÁLISE DE VULNERABILIDADE EM INFRAESTRUTURAS CRÍTICAS

MAJ ENG António Carlos dos Santos Ferreira

Trabalho de Investigação Individual do CEMC 2016/17

Orientador: CFr Luís Jimenez

Pedrouços 2017

Declaração de compromisso Anti Plágio

Eu, **António Carlos dos Santos Ferreira**, declaro por minha honra que o documento intitulado **Análise de Vulnerabilidade em Infraestruturas Críticas**, corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Estado-Maior Conjunto 2016/17** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Temos consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 19 de junho de 2017

António Carlos dos Santos Ferreira

Agradecimentos

A todos os que me acompanharam nesta epopeia… o meu obrigado!...

… em particular, ao meu amigo Gabriel Gomes, pela sua ajuda e orientação…

… em especial, à minha família pela paciência e coragem que tiveram e pelo amor que partilhamos!

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

A análise de vulnerabilidade é um aspeto fulcral para o desenvolvimento de metodologias que permitam a definição de níveis de proteção em infraestruturas críticas. Ao longo da investigação procurou-se discutir o conceito de vulnerabilidade e as metodologias e processos para a sua avaliação em infraestruturas críticas face à ameaça terrorista, com particular foco no desenvolvimento de um modelo de análise, explorando um método de apoio à decisão multicritério, de forma a ser possível limitar os riscos na máxima extensão possível.

Através de uma metodologia de investigação qualitativa, na qual se aplicou um modelo de análise assente nas dimensões Ameaça e Infraestrutura e nos seus respetivos fatores, verifica-se que a vulnerabilidade de uma infraestrutura crítica consiste na probabilidade de sucesso de um ataque, por parte de uma ameaça - devidamente identificada, caraterizada, analisada e categorizada – contra uma infraestrutura com determinadas caraterísticas, as quais definem o seu valor para o utilizador e para o agressor

A criação de um modelo algorítmico de análise da vulnerabilidade, complementado por ferramentas de registo e de cálculo, permite, através de um processo racional, científico e algébrico, transformar uma análise qualitativa de fatores, em valores mensuráveis, quantificáveis e cuja operação algébrica os integra num resultado final que expressa, em valor de percentagem, o grau de vulnerabilidade de uma infraestrutura crítica perante uma ameaça terrorista.

Palavras-chave

Vulnerabilidade, infraestrutura crítica, ameaça terrorista, modelo de análise, Macbeth

Abstract

Vulnerability assessment is a crucial aspect for the development of methodologies to define the levels of protection in critical infrastructures.

Throughout the investigation, we discussed the concept of vulnerability and methodologies and processes for it assessment in critical infrastructures due to the terrorist threat. The investigation focused on developing an analysis model, exploring a multi-criteria decision method, in order to limit the risks to the maximum extent possible.

Through a qualitative research methodology, in which we applied an analysis model based on the dimensions Threat and Infrastructure and their respective factors, we verified that the vulnerability of a critical infrastructure consists in the probability of success of an attack, conducted by a threat - properly identified, characterized, analysed and categorized - against an infrastructure with certain characteristics, which value its defined by the user and aggressor point of view.

The construction of an algorithmic model for vulnerability assessment, complemented by tools to support the calculations and records, allows, through a rational, scientific and algebraic process, transform a qualitative analysis of factors into measurable and quantifiable values, whose algebraic operation integrates them into a final result that expresses, in percentage, the degree of vulnerability of a critical infrastructure to a terrorist threat.

Keywords

Vulnerability, critical infrastructure, terrorista threat, assessment model, Macbeth

Lista de abreviaturas, siglas e acrónimos

A

Ac Acessibilidade (fator de análise)

ANPC Autoridade Nacional de Proteção Civil

Ao Ambiente operacional (fator de análise)

At Atividade (fator de análise)

C

CE Conselho Europeu

CIDIUM Centro de Investigação e Desenvolvimento do IUM

CINAMIL Centro de Investigação da Academia Militar

CNPCE Conselho Nacional de Planeamento Civil de Emergência

Co Capacidade operacional (fator de análise)

Cr Criticidade (fator de análise)

D

DHS *Department of Homeland Security*

DL Decreto-Lei

Dn Dinâmica (fator de análise)

DoD *Department of Defense*

Ds Disponibilidade (fator de análise)

E

Es Esforço (fator de análise)

EUA Estados Unidos da América

F

FEMA *Federal Emergency Management Agency*

FND Forças Nacionais Destacadas

I

IC Infraestrutura Crítica

IESM Instituto de Estudos Superiores Militares

In Intenção (fator de análise)

Im Impacto (fator de análise)

Ip Importância pública (fator de análise)

IUM Instituto Universitário Militar

L

Lc Localização (fator de análise)

M

Ms Medidas de segurança (fator de análise)

N

NIPP *National Infrastructure Protection Plan*

O

OE Objetivos Específicos

OG Objetivo Geral

P

PrInSeF Proteção de Infraestruturas e Segurança Física

Ps Perceção de sucesso (fator de análise)

Pu Publicidade (fator de análise)

PVF Ponto de vista fundamental

Q

QC Questão Central

QD Questão Derivada

S

Sb Substituição/Recuperação (fator de análise)

T

TO Teatro de Operações

U

UE União Europeia

UNIFIL *United Nation Interim Force in Lebanon*

V

Vs Visibilidade (fator de análise)

Introdução

O funcionamento das infraestruturas críticas (IC) pode ser afetado de várias formas, quer de génese natural (e.g. inundação), quer antrópica (e.g. acidente, roubo, atentado terrorista), podendo os seus efeitos variar entre uma simples perturbação e a destruição total, quer apenas de uma infraestrutura ou, por efeito dominó, com implicações em outras ou em vários setores vitais (Segurança e Ciências Forenses, 2016).

A proteção de infraestruturas críticas é um tema que ganhou enorme preponderância a partir dos atentados terroristas de 11 de setembro de 2011 nos Estados Unidos da América (EUA), e que obrigou a repensar o seu posicionamento quanto à componente física da proteção de IC (Natário, 2014 cit. por Ferreira, 2016, p. 1).

A União Europeia (UE) apenas despertou para o tratamento desta temática em 2004, após os atentados de Madrid, tendo apenas, em 2007, sido aprovado pelo Conselho Europeu (CE) o Programa Europeu de Proteção das Infraestruturas Críticas e no qual está definido, como sendo responsabilidade dos Estados-Membros, assegurar a proteção de infraestruturas críticas nos respetivos territórios (Conselho Europeu, 2008). No seguimento, foi publicada, em 08 de dezembro de 2008, a Diretiva 2008/114/CE do Conselho, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (Segurança e Ciências Forenses, 2012).

Paralelamente às primeiras iniciativas da UE, foi também em 2004 que a proteção de IC começou a ser uma preocupação em Portugal. Na altura, fruto da multidisciplinaridade e transversalidade do assunto, foi criado um grupo de trabalho, coordenado pelo então Conselho Nacional de Planeamento Civil de Emergência (CNPCE)[1] e que envolveu representantes dos vários setores do Estado e da comunidade privada. Numa primeira fase dos trabalhos, procedeu-se à classificação das IC de acordo com critérios que traduzem a sua importância relativa para o país. Numa segunda fase, que ainda decorre e que se constitui como a etapa central da proteção de IC, procede-se à identificação das vulnerabilidades das IC face às ameaças que as poderão afetar, de forma a implementar medidas eficientes para a sua redução (ProCiv, 2016).

[1]O Decreto-Lei n.º 73/2012, de 26 de março, transferiu para a Autoridade Nacional de Proteção Civil (ANPC) as atribuições do Conselho Nacional de Planeamento Civil de Emergência, extinto nesse ano, tendo o Decreto-Lei n.º 163/2014, de 31 de outubro, atribuído à ANPC a missão de assegurar o planeamento e coordenação das necessidades nacionais na área do planeamento civil de emergência, com vista a fazer face a situações de crise ou de guerra. Tratou-se de um reforço substancial do âmbito de ação da ANPC, o qual passou a englobar as situações de crise e de guerra para além dos acidentes graves e catástrofes.

A avaliação da vulnerabilidade é, assim, um passo essencial para a definição do nível de proteção necessário para a infraestrutura, bem como o instrumento basilar para o desenho das medidas protetivas.

Apesar deste contributo mais orientado para questões de segurança interna, e numa ótica de duplo uso, surge também a necessidade de olhar para as IC em Teatros de Operações (TO) para onde as Forças Nacionais Destacadas (FND) são projetadas e cuja proteção é essencial para o cumprimento da missão e para a proteção da própria força. Assim, serve a presente investigação o propósito de fornecer uma ferramenta de planeamento que permita, a um comandante ou responsável por uma IC, determinar a sua suscetibilidade ao ataque de um agressor, identificando as caraterísticas físicas ou procedimentos que tornam determinada infraestrutura (e.g. aquartelamento militar), área, sistema ou evento, particularmente vulnerável a um espectro de possibilidades verosímeis de uma ameaça.

Associado ainda à temática da proteção de infraestruturas, decorre no Centro de Investigação e Desenvolvimento do Instituto Universitário Militar (CIDIUM) e no Centro de Investigação da Academia Militar (CINAMIL) um projeto de investigação denominado "Proteção de Infraestruturas e Segurança Física (PrInSeF)"[2]. Com o PrInSef, pretende-se obter "produtos que tenham aplicação direta no incremento da segurança das instalações militares contra a ameaça terrorista, seja em território nacional seja em Forças Nacionais destacadas e, de forma concorrente, contribuir para o desenvolvimento de recomendações de conceção ou reforço, para proteção de infraestruturas com interesse estratégico para o país (civis ou militares), as quais importa preservar, evitando interrupções graves ao funcionamento da sociedade" (Gomes, s.d.).

Sendo um dos objetivos específicos do PrInSef "estudar metodologias que permitam a definição de níveis de proteção em infraestruturas, baseadas no risco" (Gomes, s.d.), a análise de vulnerabilidade é um aspeto fulcral para o desenvolvimento desse estudo, para o qual podem contribuir os resultados obtidos pela presente investigação.

O presente trabalho de investigação, realizado no decurso do Curso de Estado-Maior Conjunto, enquadra-se no domínio das Ciências Militares, na área de investigação das

[2] O projeto de investigação PrInSef, decorre no IUM e na Academia Militar, entre 2014 e 2019, cujo diretor de projeto é o Major General Corte-Real Andrade e tem por investigador principal o Major Engenharia Gabriel Gomes. O objetivo global do projeto é a edificação de um corpo de conhecimentos concetuais e técnicos que permitam o incremento da segurança física e integridade estrutural de infraestruturas estratégicas, em território nacional ou edifícios governamentais e outras instalações em países estrangeiros, tais como embaixadas, aquartelamentos de FND, entre outros..

Técnicas e Tecnologias Militares, especificamente na sua subárea de Engenharias de Aplicação Militar.

A investigação, conforme o tema geral definido para o trabalho e de acordo com a delimitação estabelecida, teve por finalidade discutir o conceito de vulnerabilidade e as metodologias e processos para a sua avaliação em infraestruturas críticas (em território nacional ou expedicionárias) face à ameaça terrorista, com particular foco no desenvolvimento de uma metodologia de análise, explorando um modelo de apoio à decisão multicritério, de forma a ser possível limitar os riscos na máxima extensão possível.

Dada a diversidade de definições de IC e de modelos para as caraterizar surgiu a necessidade de limitar o estudo à análise da vulnerabilidade de IC nacionais, de acordo com a atual classificação da Autoridade Nacional de Proteção Civil (ANPC), e de aquartelamentos militares em TO fora do território nacional. Sendo a ameaça uma das dimensões a estudar, verificou-se que esta carateriza-se, atualmente, por um espetro bastante largo de ação, pelo que foi fundamental delimitar o estudo à ameaça terrorista com recurso a explosivos. Não foram estudados os riscos naturais ou riscos tecnológicos acidentais.

Para orientar o percurso de investigação em torno da finalidade apresentada, definiu-se como objetivo geral (OG) para o presente estudo "Desenvolver uma metodologia de análise da vulnerabilidade de infraestruturas críticas".

Para atingir este objetivo geral definiram-se três objetivos específicos (OE), os quais atingidos, permitem o seu cumprimento:

OE 1 - Classificar as ameaças passíveis de afetar a vulnerabilidade de uma IC;

OE 2 - Avaliar as caraterísticas de uma IC passíveis de afetar a sua vulnerabilidade;

OE 3 – Construir um método algorítmico de análise da vulnerabilidade de uma IC, integrando uma metodologia de apoio à decisão multicritério.

Dada a finalidade da investigação e os objetivos geral e específicos propostos, houve que concretizar a problemática da investigação através de uma questão central (QC), que concorreu diretamente para atingir o OG. Assim a QC é: "Como determinar a vulnerabilidade de uma IC, aplicando uma metodologia que permita limitar os riscos na máxima extensão possível?"

Para atingir os OE, decompôs-se a QC em três questões derivadas (QD), as quais, respondidas, permitiram responder à QC. As QD são:

QD 1 - Em que medida a ameaça terrorista afeta a vulnerabilidade de uma IC?

QD 2 - De que forma as caraterísticas de uma determinada IC afetam a sua vulnerabilidade?

QD 3 - Como aplicar as caraterísticas associadas à ameaça e à infraestrutura num método algorítmico que permita determinar a vulnerabilidade de uma IC, integrando um modelo de apoio à decisão multicritério?

A metodologia seguida na elaboração deste trabalho de investigação baseou-se num raciocínio indutivo (IESM, 2016, p.20) assente no conhecimento base existente sobre os conceitos e as dimensões em análise e das quais resultou, através de uma investigação qualitativa (IESM, 2016, p.27), a construção de um modelo de aplicação tendo em vista o apoio à decisão.

No sentido de dar corpo à investigação, o trabalho está organizado em quatro capítulos e conclusões. No primeiro capítulo é feito o enquadramento conceptual e metodológico da investigação, apresentando uma base teórica e conceptual relativa à proteção de infraestruturas críticas, à análise de vulnerabilidade e aos modelos teóricos existentes para a sua determinação. É ainda descrito o percurso metodológico e o modelo de análise utilizado e que sustenta a investigação, os argumentos e os resultados obtidos.

No segundo capítulo, carateriza-se a ameaça terrorista com recurso ao uso de explosivos e analisam-se os fatores que permitem categorizar a ameaça e determinar de que forma esta afeta a vulnerabilidade de uma IC.

No terceiro capítulo, analogamente ao anterior, identificam-se as caraterísticas de uma IC, analisam-se os fatores e as probabilidades associadas que contribuem para determinar o grau de vulnerabilidade de uma IC.

O quarto capítulo constitui-se como parte fulcral da nossa investigação. Com base na análise feita à ameaça e às caraterísticas de uma IC, constrói-se um método algorítmico para analisar a vulnerabilidade de uma IC, associando-lhe a aplicação de um método de análise multicritério que permita, ao decisor, maniatar os pesos dos critérios usados na análise da vulnerabilidade, de forma a aproximar a sua observação qualitativa do problema a uma solução quantitativa.

Por último, conclui-se a investigação demonstrando de que forma a avaliação da ameaça e das caraterísticas da infraestrutura afetam a vulnerabilidade de uma IC e que a existência de um método algorítmico, integrando um modelo de apoio à decisão multicritério, permite ao "dono" de uma IC determinar a sua vulnerabilidade e identificar os fatores, cujas alterações permitem um incremento da sua proteção.

1. A investigação e a metodologia

1.1. Revisão da literatura

O tema da proteção de IC tem vindo a ganhar relevância, quer no seio das Organizações Internacionais quer ao nível das Nações, nomeadamente na análise da gestão de riscos a que este tipo de infraestruturas está sujeito.

De acordo com o CNPCE, considera-se IC "aquela cuja destruição total ou parcial, disfunção ou utilização indevida possa afetar, direta ou indiretamente, de forma permanente ou prolongada: (i) O funcionamento do setor a que pertence, ou de outros setores; (ii) O funcionamento de Órgãos de Soberania; (iii) O funcionamento de Órgãos da Segurança Nacional; (iv) Os Valores Básicos, afetando, desta forma, gravemente, o Bem-Estar Social. A sua criticidade determinar-se-á pelo impacto que a sua destruição, disfunção ou utilização indevida possa determinar no conjunto dos critérios referidos" (Segurança e Ciências Forenses, 2012).

Decorrente do N.º2 do Art.º 2º do Decreto-lei n.º 62/2011, de 9 de Maio, do Ministério da Defesa Nacional[3], passou a estar preconizado na legislação portuguesa que IC é "a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções".

Contudo, de todas as definições, a que melhor complementa as anteriores está apresentada no Conceito Estratégico Militar: "Entende-se por IC, aquela cuja disrupção, é passível de causar perturbações ao funcionamento de bens de primeira necessidade, gerar insegurança ou provocar a perda de confiança nas instituições, afetando o normal funcionamento da sociedade e do Estado de Direito (…)." (Conselho de Chefes de Estado-Maior, 2014).

Quanto ao conceito de proteção, das inúmeras definições encontradas em bibliografia, consideram-se as seguintes como base para a presente investigação.

Pela Diretiva n.º 2008/114/CE, do Conselho, de 8 de dezembro, proteção consiste em "todas as actividades destinadas a assegurar a funcionalidade, continuidade e integridade de uma infra-estrutura crítica tendo em vista coarctar, atenuar e neutralizar uma ameaça, risco ou vulnerabilidade".

[3]O presente decreto-lei estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem estar económico e social da sociedade nos setores da energia e transportes, transpondo a Diretiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro.

Já o *National Infrastructure Protection Plan* (NIPP), dos EUA, define proteção como sendo as ações necessárias para deter uma ameaça, mitigar as vulnerabilidades, ou minimizar as consequências associadas a um ataque terrorista ou a um desastre natural ou tecnológico (US DHS, 2009).

Para a operacionalização deste conceito, existe bibliografia que apresenta modelos, os quais permitem a identificação das medidas de proteção e que visam, essencialmente, a avaliação da ameaça, a identificação das vulnerabilidades e a gestão do risco. Todos estes modelos têm também em atenção a relação custo/benefício, porque os aspetos financeiros são cada vez mais relevantes na tomada de decisão.

A *Federal Emergency Management Agency* (FEMA) norte-americana, através da sua publicação FEMA 426 - *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, de 2003, apresenta um processo de análise do risco (Figura 1) para identificação das melhores e mais viáveis medidas de mitigação a aplicar a edifícios face a um ataque terrorista. Neste processo pode-se identificar a inclusão da vulnerabilidade como fator diretamente concorrente para a análise do risco.

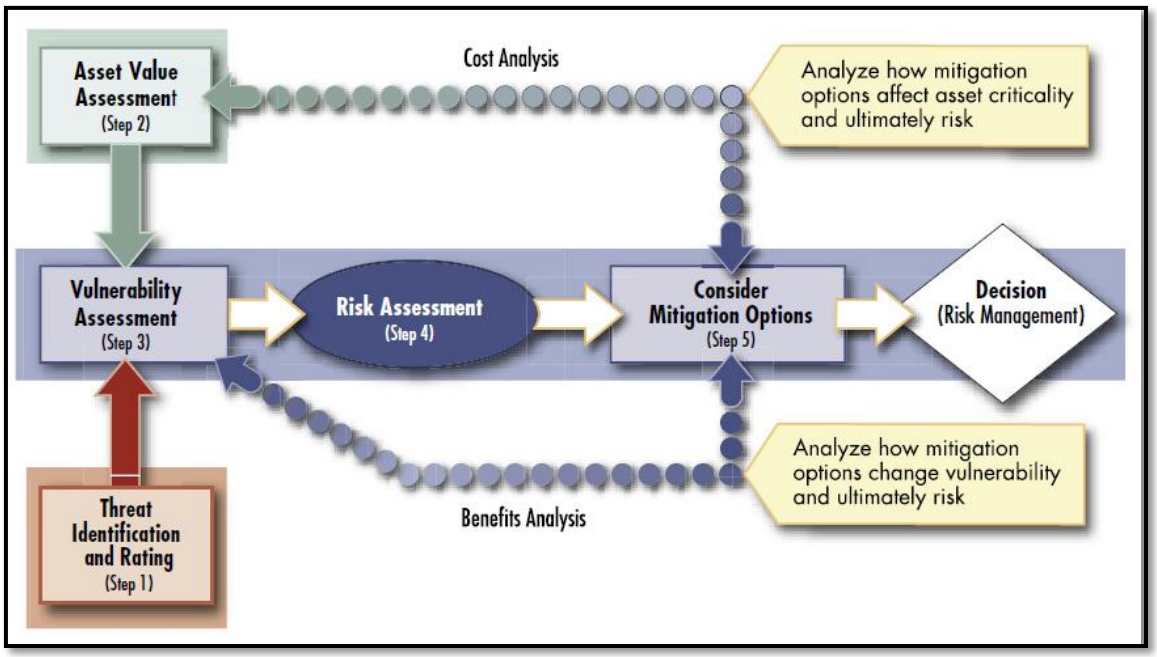


Figura 1 – Modelo de avaliação do risco

Fonte: (FEMA, 2003)

Na Figura 2 pode-se ver representado um modelo utilizado pelo exército britânico para determinar o nível de proteção da força em operações militares e as medidas a implementar para a sua adequação ao risco identificado (UK MoD, 2007, p. 2-2). Verifica-se também, neste processo, a preponderância da avaliação da vulnerabilidade como ferramenta para a gestão do risco operacional.

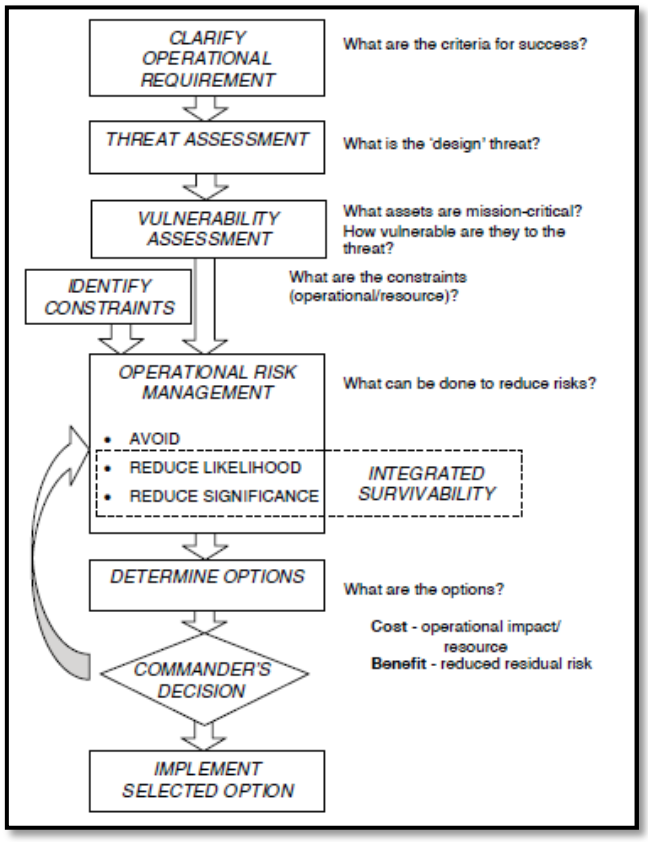


Figura 2 – Planning force protection engineering

Fonte: (UK MoD, 2007, p. 2-2)

Já Krauthammer (2008, pp. 10-11) apresenta um método de abordagem para a análise do risco no planeamento e execução de infraestruturas, identificando a vulnerabilidade como um fator multiplicativo na determinação do risco.

Risco = Ameaça x Impacto x Vulnerabilidade

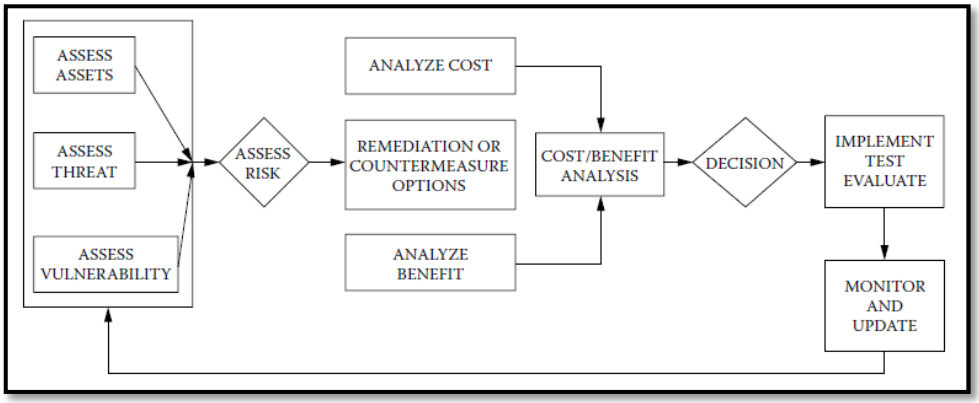


Figura 3 – Risk management approach

Fonte: (Krauthammer, 2008, p.10)

Em qualquer um dos modelos pode-se observar, que num determinado momento do processo, surge uma fase ou etapa na qual é efetuada a avaliação da vulnerabilidade, a qual irá contribuir diretamente para a avaliação do risco e, posteriormente, para a decisão sobre

que medidas implementar. Assim, associado à proteção está, indubitavelmente a vulnerabilidade, a qual, através da implementação de medidas de proteção, será mitigada de forma a minimizar as consequências resultantes de uma ação da ameaça.

Mas o que é a vulnerabilidade?

Vulnerabilidade consiste na combinação da atratividade de uma infraestrutura como alvo e o nível de dissuasão ou de proteção fornecido pelas contramedidas existentes[4] (Renfroe e Smith, 2016).

Já Almeida, citando Apostolakis and Lemon (2003:362), define vulnerabilidade como sendo a "manifestação de estados inerentes do sistema (quer sejam eles físicos, técnicos, organizacionais, culturais) que podem ser explorados por uma adversidade para danificar ou causar danos no sistema"(2011, p.15).

Das definições anteriores, verifica-se que existem duas interpretações quanto ao conceito de vulnerabilidade. Na primeira, a vulnerabilidade representa a probabilidade de sucesso de um ataque, resultante de uma determinada ameaça a uma infraestrutura com determinadas caraterísticas. Na segunda, a vulnerabilidade surge como sendo uma caraterística (física, procedimental, etc.) da infraestrutura suscetível de ser explorada pela ameaça, ou seja, uma fragilidade. Apesar de serem dois conceitos distintos, o primeiro geral e o segundo particular, eles complementam-se. No entanto, a presente investigação incidirá apenas sobre o primeiro conceito, definido por Renfroe e Smith.

A análise da vulnerabilidade é o processo que um comandante ou responsável por uma infraestrutura crítica emprega para determinar a suscetibilidade de uma infraestrutura ao ataque de um agressor, ou a probabilidade de sucesso de um ataque. Responde assim à questão, "a que tipo de ataque é a infraestrutura mais/menos vulnerável?".

O objetivo último do processo é a identificação das caraterísticas físicas ou procedimentos que tornam determinada infraestrutura, área, sistema ou evento, particularmente vulnerável a um espectro de possibilidades verosímeis de uma ameaça.

Existem, assim, duas dimensões que estão na base de qualquer processo de avaliação de vulnerabilidade de uma IC: a própria infraestrutura e a ameaça.

Da revisão literária efetuada, existe bastante bibliografia que aborda a análise de vulnerabilidade, seja como processo individual ou como parte integrante do processo de gestão de risco. No entanto, as abordagens que se encontram na maioria da bibliografia

[4] Tradução do autor: *"combination of the attractiveness of a facility as a target and the level of deterrence and/or defense provided by the existing countermeasures"*

analisada são meramente conceptuais ou teóricas. Relevam-se duas fontes que, de forma mais científica e pormenorizada, indicam o caminho a seguir para a construção de uma metodologia para a avaliação da vulnerabilidade de uma IC.

A FEMA faz a abordagem, desta temática, através de duas publicações: *FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (2011) e *FEMA 452 - Risk Assessment: a How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings* (2005).

Nestas publicações, a FEMA define um modelo assente em três etapas, cada uma com quatro passos, sendo as duas primeiras, a identificação e categorização da ameaça e a avaliação do valor da infraestrutura, fatores essenciais para avaliar a vulnerabilidade (FEMA, 2005, p. 1-1). Apesar da definição das etapas e dos respetivos passos, este modelo é bastante teórico e simplista, orientado para infraestruturas "civis".

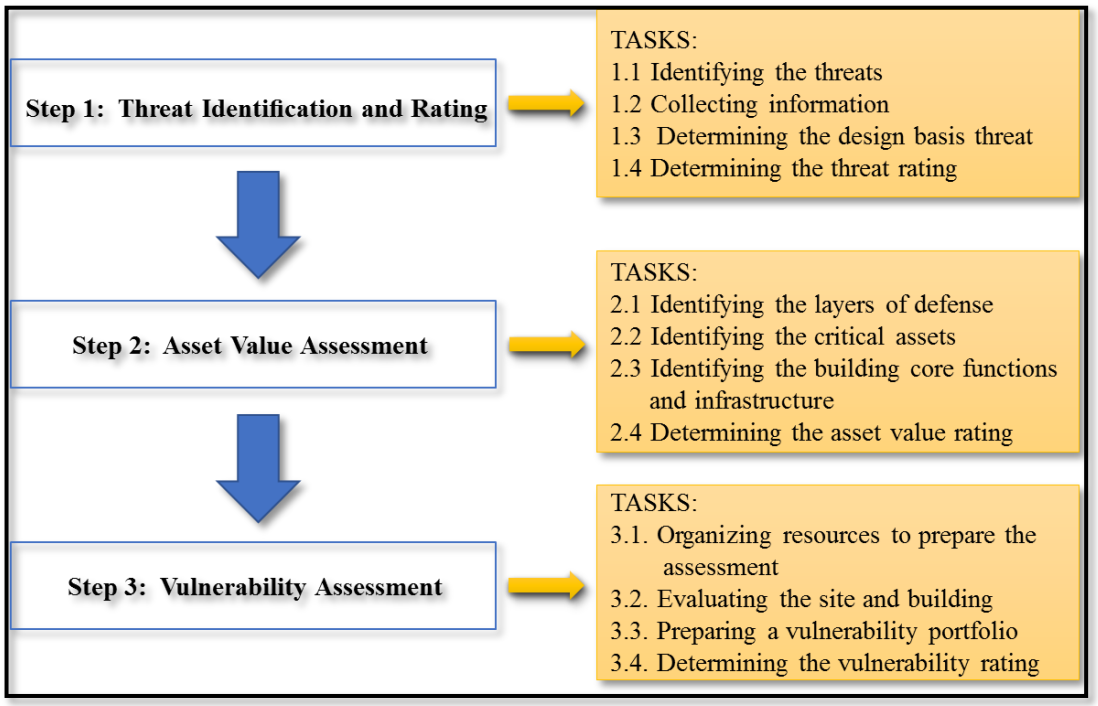


Figura 4 – Steps and tasks for Vulnerability Assessment

Fonte: (FEMA, 2005, p. 1-1)

O Departamento de Defesa (DoD) dos EUA, integrado na série de manuais *Unified Facilities Criteria*, apresenta nos *UFC 4-020-01 - DoD Security Engineering Facilities Planning Manual (2008)* e *UFC 4-010-01 - DoD Minimum Antiterrorism Standards for Buildings (2013)* um modelo de planeamento, para as suas instalações, que visa estabelecer os critérios e requisitos de projeto para o incremento da segurança e de medidas antiterroristas nos seus edifícios.

Os critérios e requisitos definidos incluem os ativos a proteger, as ameaças a esses ativos, os níveis de proteção que devem ter face à ameaça e as restrições impostas pela legislação ou pelos proprietários ou utilizadores das infraestruturas (US DoD, 2008, pp. 3-4 a 3-5).

Neste modelo, os primeiros sete passos permitem determinar o nível de proteção inicial e, de forma associada, a vulnerabilidade da infraestrutura.

Tal como no modelo apresentado pela FEMA, também este inclui a avaliação do valor da infraestrutura e a análise da ameaça como as dimensões principais para a avaliação da vulnerabilidade.

Este modelo é exclusivamente orientado para infraestruturas militares, em território nacional ou em TO.

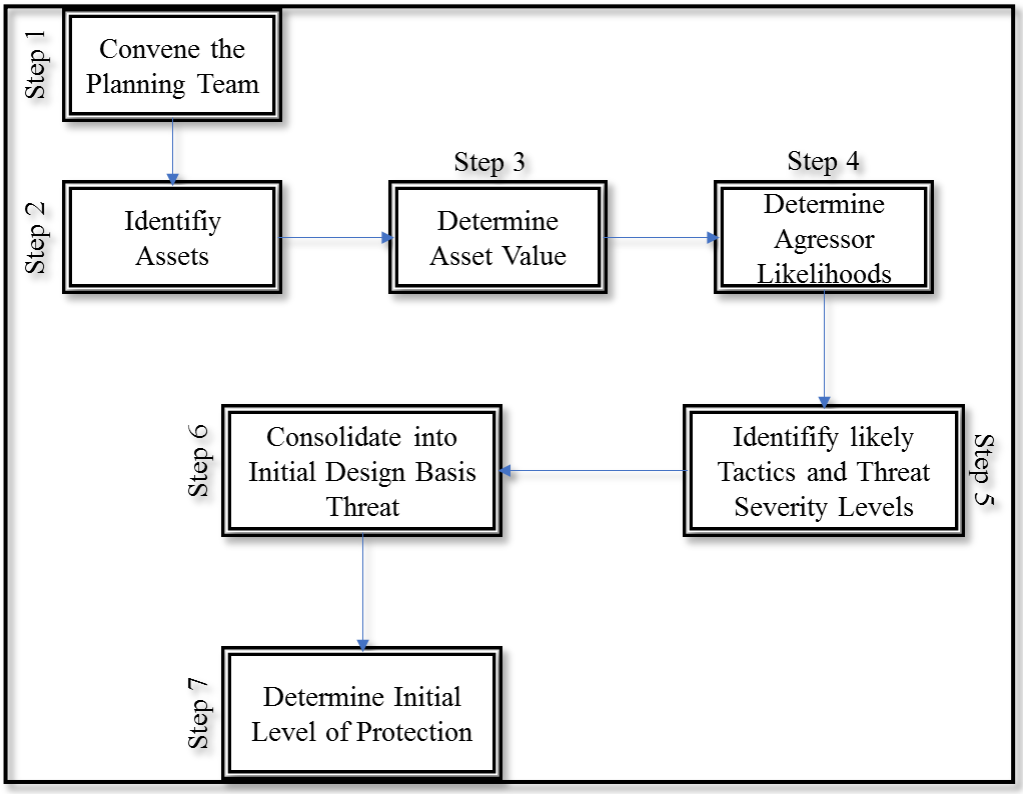


Figura 5 – The Design Criteria Development Procedure (the first seven steps)

Fonte: (US DoD, 2008, pp. 3-4 a 3-5)

Ambos os modelos são aproximações teóricas, ainda distantes de se constituírem como uma ferramenta prática para o apoio à decisão.

No entanto, apresentam informação que nos permite estruturar um modelo de análise a aplicar à investigação, nomeadamente na identificação das dimensões e das variáveis a analisar.

1.2. **Metodologia de investigação e modelo de análise**

Esta investigação seguiu uma estratégia Qualitativa segundo o percurso e instrumentos metodológicos a seguir descriminados. A opção por uma estratégia qualitativa justificou-se pelo facto se procurar compreender o "significado atribuído por um indivíduo" (investigador) "a um determinado problema" (como analisar a vulnerabilidade) (Creswell, 2013, p. 4 cit. por IESM, 2016, p. 29), "pretendendo-se desta forma, através da exploração do comportamento, das perspetivas e das experiências" (influência da ameaça e das caraterísticas da infraestrutura na vulnerabilidade) "alcançar uma interpretação da realidade social" (construção de um modelo) (Vilelas, 2009, p. 105 cit. por IESM, 2016, p. 29).

Sendo o objetivo geral da investigação criar um modelo, houve que adotar um raciocínio descritivo e Indutivo, na medida em que o investigador desenvolve conceitos, ideias e entendimentos a partir de padrões encontrados nos dados, em vez de recolher dados para comprovar modelos, teorias ou verificar hipóteses. Neste processo indutivo, procurou-se passar do particular para o geral, tendo como "ponto de partida a observação de factos particulares para, através da sua associação, estabelecer generalizações que permitam formular uma lei ou teoria" (IESM, 2016, p. 20).

Para trabalhar as variáveis e encontrar as premissas que levem à definição de uma metodologia para a análise da vulnerabilidade, começou-se por utilizar um desenho de pesquisa Transversal de forma a estudar a variação das variáveis nas dimensões subordinadas ao conceito e permitir, após esta análise, detetar padrões de associação, estabelecendo e modelando essa variação (Bryman, 2012, cit. por IESM, 2016, p. 35).

O percurso metodológico seguido pela investigação é o apresentado nas Orientações Metodológicas para a elaboração de Trabalhos de Investigação, compreendendo três fases. A fase exploratória, materializada pelo Projeto de Investigação, seguindo-se a fase analítica, orientada para a recolha, análise e apresentação de dados, terminando com a fase conclusiva, orientada para as conclusões e contributos para o conhecimento (IESM, 2016).

Na fase exploratória enquadrou-se o tema, estabeleceu-se o corpo de conceitos inicial e o enquadramento legal e doutrinário. Para tal efetuou-se uma entrevista exploratória e uma aprofundada revisão da literatura. Fruto destes instrumentos metodológicos foi possível determinar a metodologia mais adequada para atingir o objetivo desta investigação. Esta fase terminou com a apresentação e aprovação do Projeto de Investigação.

Na fase analítica, pretendeu-se discutir o conceito de vulnerabilidade e desenvolver uma metodologia para a sua avaliação em IC face à ameaça terrorista, explorando um modelo

de apoio à decisão multicritério. Esta fase teve como ponto de partida o modelo de análise apresentado no Apêndice 1. Começou-se por concetualizar a vulnerabilidade, após o que se passou a identificar, caraterizar e analisar as variáveis de forma a poder categorizar as dimensões Ameaça e Infraestrutura. Com base nas dimensões e variáveis analisadas, procedeu-se à modelação de um algoritmo e à criação de ferramentas que permitam transformar julgamentos qualitativos em avaliações quantitativas. De seguida, avaliou-se a aplicabilidade de um método de apoio à decisão multicritério em complemento ao modelo em construção, de forma a permitir uma maior interação deste com os utilizadores.

Antes de se propor a metodologia, foi necessário testar e validar o modelo. Assim, na fase conclusiva, o modelo foi submetido a uma situação (cenário) criada para o efeito - com aplicação da metodologia para resolver o problema associado à situação -, avaliado do ponto de vista dos resultados e dos processos e corrigido nas inconformidades. Acrescenta-se ainda, nesta fase, as conclusões e os resultados obtidos, os quais devem contribuir para o debate necessário sobre esta matéria.

Nesta investigação, a recolha de dados assentou exclusivamente na análise documental (IESM, 2016, pp. 25-26). Esta baseou-se na legislação europeia e nacional, em doutrina de referência e manuais técnicos subordinados ao objeto de estudo. A partir da análise documental, já iniciada na fase exploratória, pretendeu-se enquadrar o tema, compreender a aplicação de metodologias de análise da vulnerabilidade de IC usadas por outros países (com principal enfoque nos EUA) e compreender o funcionamento e aplicabilidade de um modelo de apoio à decisão multicritério. A utilização de um cenário aplicado a uma IC nacional permitiu testar a aplicabilidade do modelo de análise da vulnerabilidade criado e obter a sua validação.

2. Avaliação da Ameaça

Qualquer modelo de análise da vulnerabilidade de uma infraestrutura tem que começar por avaliar a ameaça com que essa infraestrutura se poderá deparar e para a qual apresenta vulnerabilidades.

Por definição, ameaça consiste em "Estados, organizações, pessoas, grupos ou condições com capacidade para danificar ou destruir vidas humanas, recursos vitais, ou instituições"(Exército Português, 2012).

Com especial interesse para a presente investigação, uma das formas de ameaça é o terrorismo, o qual pode ser definido "como a utilização ilegal, de forma efetiva ou potencial, da força ou violência contra pessoas ou bens, tentando coagir ou intimidar governos ou sociedades, para alcançar objetivos políticos, religiosos ou ideológicos" (Exército Português, 2012).

Para avaliar a ameaça é necessário: (i) identificar e caraterizar a sua tipologia, as táticas e técnicas e o tipo de armamento associado; (ii) analisar a ameaça de acordo com fatores internos e externos; e (iii) classificar a ameaça de acordo com a análise efetuada aos seus fatores.

2.1. Identificação e caraterização da ameaça

2.1.1. Tipologia de terroristas

Associando ao próprio conceito de terrorismo, o terrorista, enquanto agressor, individual ou coletivo, é aquele que tem intenção de causar danos materiais ou baixas humanas para atingir os seus objetivos (US Army, 2007, p. 1-7).

Existem várias formas de classificação do terrorismo, sendo que para a presente investigação optou-se pela preconizada pela FEMA (2012, p. 4-1):

(i) Terrorismo doméstico: tem origem interna e sem relação com entidades exteriores ao país, normalmente com motivações políticas extremistas, éticas ou separatistas. Geralmente apresenta efeitos menos severos que o terrorismo internacional;

(ii) Terrorismo internacional: os terroristas internacionais estão ligados a potências estrangeiras, numa rede de células operacionais e cujas atividades trespassam as fronteiras nacionais. Este tipo de terroristas são, normalmente, mais bem organizados e equipados, que os terroristas de nível doméstico, o que leva a que os seus ataques sejam mais frequentes e severos. Incluem-se nos terroristas internacionais extremistas políticos e grupos de orientação étnica e religiosa;

(iii) Terrorismo patrocinado por Estados: os terroristas patrocinados por Estados operam, geralmente, de forma independente, no entanto com apoio de um governo estrangeiro, incluindo a partilha de informações e o apoio à condução das operações. Estes grupos, possuem capacidades militares e utilizam um variado leque de armamento, desde armamento militar a armas improvisadas. Representam a maior percentagem dos ataques terroristas, principalmente através dos ataques suicidas. São grupos terroristas de orientação predominantemente étnica e/ou religiosa.

2.1.2. Táticas e técnicas – ataques com recurso a explosivos

Os explosivos podem ser utilizados de diversas formas em diferentes tipos de ataques. As diferenças nas táticas e técnicas usadas com recurso a explosivos assentam, essencialmente, nos seguintes fatores (FEMA, 2012, p. 4-4):

(i) Disponibilidade do material e as suas caraterísticas (uso militar ou improvisado);

(ii) Especialização do agressor no manuseamento de materiais explosivos;

(iii) Quantidade de explosivo usada face ao efeito pretendido;

(iv) Meios de lançamento (uso de viaturas ou emprego manual);

(v) Método de iniciação da explosão (por impacto; detonador pirotécnico; detonador elétrico acionado manual, remota ou temporalmente, ou a combinação de ambos).

As táticas e técnicas associadas ao uso de explosivos caraterizam-se, e distinguem-se de outras, pela sua forma de emprego, duração, extensão dos efeitos e pelas condições do local que mitigam ou ampliam a sua ação.

Tabela 1 – Principais caraterísticas de um ataque com IED

Tipo de ataque	Forma de emprego	Duração	Extensão dos efeitos	Condições do local
Ataque com explosivos	Detonação de um explosivo num determinado alvo ou na sua proximidade, colocado manualmente, por veículo ou projetado	Instantâneo; possibilidade de uso de um segundo ou mais IED, prolongando a duração da ameaça ou do perigo até o local ser declarado limpo	A extensão dos danos é determinada pelo tipo e quantidade de explosivos.	Terreno, vegetação e infraestruturas em redor do alvo mitigam os efeitos da explosão, absorvendo e/ou refletindo a energia libertada e fragmentos. Ao invés, os efeitos da explosão podem ser ampliados devido ao fácil acesso ao alvo, falta de barreiras de proteção, fraca construção e a facilidade de dissimulação do IED

Fonte: adaptado de (FEMA, 2005, p. 1-13)

O tipo de ataque com recurso a explosivos (militares ou de uso comercial), pode-se classificar de acordo com os métodos de lançamento (FEMA, 2012, p. 4-5):

(i) Explosivo enviado por correio;

(ii) Explosivo enviado por sistema distribuição de encomendas;

(iii) Explosivo deixado no local (mochila, mala, embalagem, tubo explosivos, etc);

(iv) Explosivo atirado para o local (seja de forma manual ou com recurso a meios de propulsão);

(v) Bombista suicida;

(vi) Veículo bomba (estacionado ou em movimento).

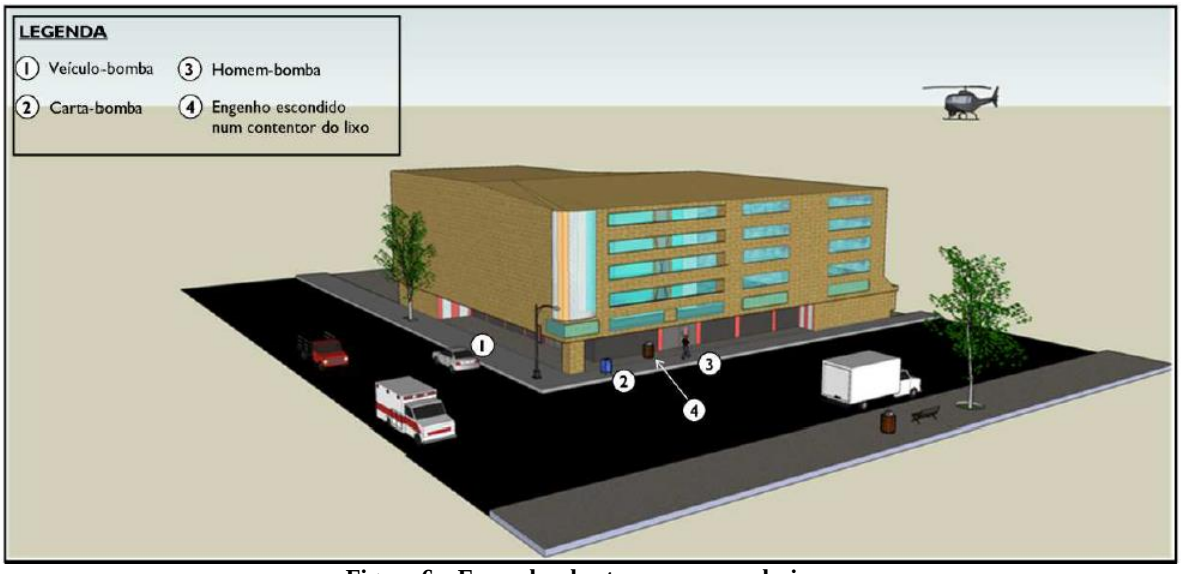


Figura 6 – Exemplos de ataques com explosivos

Fonte: (Conceição, 2008, p. 34)

Tendo em conta o efeito produzido, todos estes métodos podem-se agrupar nos seguintes (US DoD, 2008, p. 2-4):

(i) Explosivos lançados manualmente;

(ii) Veículo-bomba estacionado;

(iii) Veículo-bomba em movimento;

A estes métodos de lançamento correspondem o tipo de local em que se dá o ataque, ou mais propriamente, a explosão. Assim esta pode ocorrer no exterior ou no interior do edifício, causando efeitos distintos na infraestrutura e na área adjacente.

A ataques no interior do edifício estão, geralmente, associados os métodos em que os explosivos são lançados manualmente pois devido às suas dimensões mais reduzidas são mais facilmente dissimulados na passagem por quaisquer barreiras de segurança. No interior do edifício, os danos podem ser ampliados se os explosivos forem transportados até aos

pontos nevrálgicos da infraestrutura como locais com grande concentração de pessoas, fontes de energia, fragilidades infraestruturais. Apesar da possibilidade de entrada no edifício de um veículo-bomba, eventos recentes demonstram uma maior probabilidade da utilização de explosivos lançados manualmente (e.g. bombista suicida) no interior de edifícios (FEMA, 2005, p. 1-7).

Um ataque no exterior de um edifício é mais provável de acontecer que no seu interior devido às limitações de segurança impostas ao acesso e ao redor das infraestruturas.

Neste tipo de ataques é mais provável a utilização de veículos-bomba, seja em movimento ou estacionados, para que a quantidade de explosivos associada reduza a distância edifício-explosão imposta pelas barreiras de segurança. Assim, os locais estratégicos para a detonação de um veículo-bomba no exterior de um edifício serão sempre o mais próximo que o veículo consiga se aproximar: parque de estacionamento ou estrada junto à infraestrutura, portão de acesso ou nas zonas de carga e descarga.

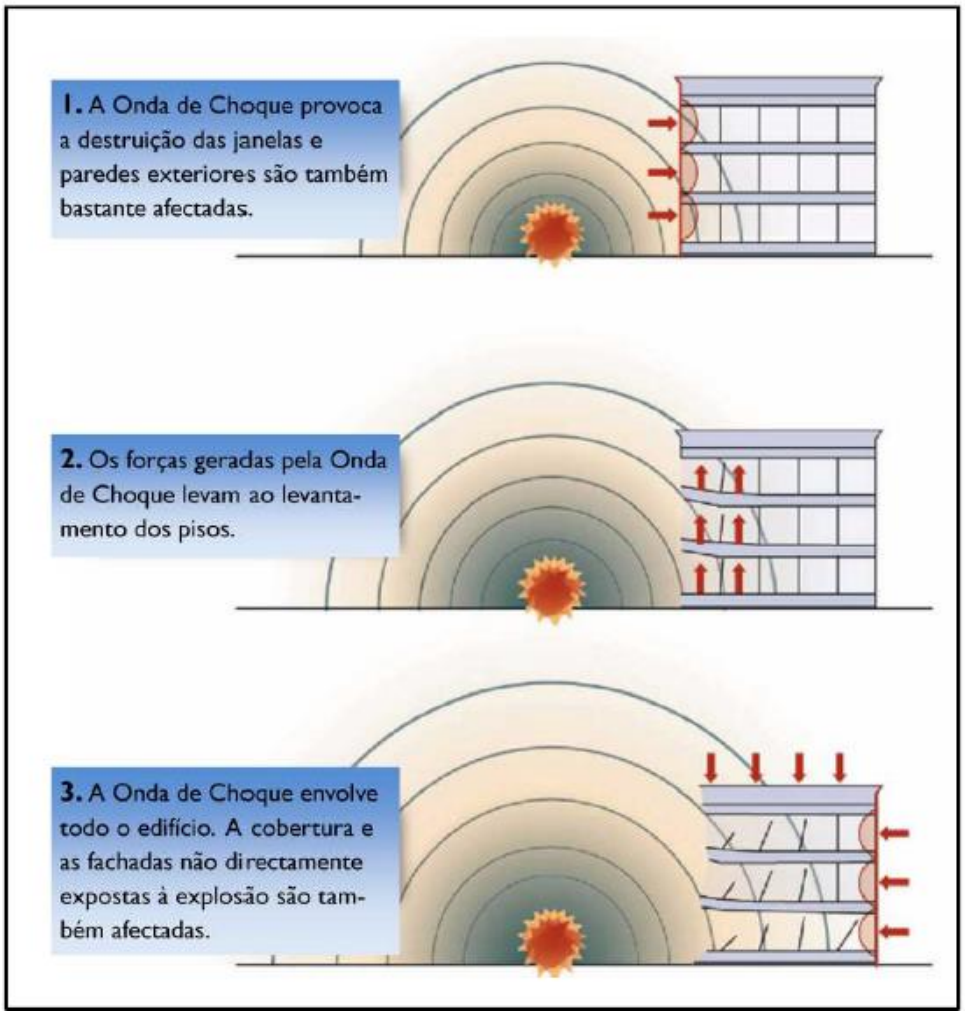


Figura 7 – Sequência dos efeitos, numa infraestrutura, resultante da explosão de um veículo-bomba no exterior.

Fonte: (Conceição, 2008, pág. 39, adaptado de FEMA, 2003, p. 34)

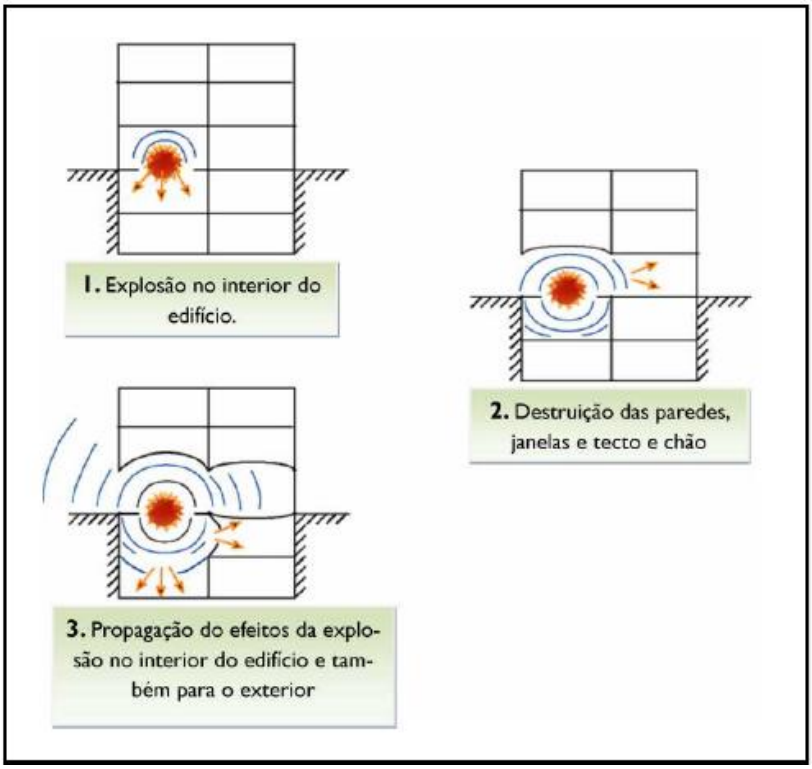


Figura 8 – Sequência dos efeitos numa infraestrutura resultante da explosão no interior.

Fonte: (Conceição, 2008, pág. 39, adaptado de FEMA, 2003, p. 34)

2.1.3. Armamento - explosivos

O uso de explosivos é bastante atrativo para um ataque terrorista, pois são fáceis e baratos de adquirir, provocam grandes danos e produzem um elevado efeito psicológico sobre a população e as instituições.

Independentemente do tipo de explosivo, este é medido equivalendo o seu peso à quantidade de TNT necessária para provocar o mesmo efeito.

Existem diversas formas de classificar os engenhos explosivos, sendo que nesta investigação, olhando para o engenho como uma arma e o seu emprego num ataque contra uma infraestrutura, segue-se a classificação adotada no UFC 4-020-01 (US DoD, 2008, pp. 2-9 a 2-10):

(i) *Improvised Explosive Device* (IED) – bombas de pequena dimensão, de fabrico caseiro, geralmente com explosivos plásticos ou TNT. Os explosivos plásticos são a preferência dos terroristas, pois são fáceis de adquirir, estáveis e difíceis de detetar;

(ii) Granadas de mão – de cariz militar, com pequena quantidade de explosivo, podendo ter associado material fragmentado. De menor probabilidade de utilização;

(iii) Veículos bomba – bombas com grandes quantidades de explosivos empregues em viaturas de diferentes dimensões. Devido à facilidade de transporte, podem ser usados outro tipo de material explosivo que não explosivo plástico ou TNT (e.g. nitrato de amónio, material gasoso pressurizado, etc).

Para melhor compreender os efeitos das diferentes quantidades de explosivo, é apresentada, na Tabela 2, a relação entre o tipo de contentor ou forma de transporte do explosivo, a sua quantidade, a distância de evacuação para os ocupantes de um determinado edifício convencional (sem qualquer tipo de reforço estrutural) e a distância de segurança para pessoas desprotegidas nas imediações da explosão.

Tabela 2 – Tipos de Ataques com Engenhos Explosivos e Distância de Segurança.

Ameaça explosiva		Quantidade Explosivos [kg]	Distância de segurança para um edifício [m]	Distância de segurança no exterior [m]
Tubo bomba		2,3	21	256
Cinto com explosivos		4,5	27	330
Colete com explosivos		9	34	415
Mala com explosivos		23	46	564
Veículo ligeiro (compacto) com explosivos		227	98	457
Veículo ligeiro (sedan) com explosivos		454	122	534
Veículo "*mini-van*" com explosivos		1814	195	838
Veículo ligeiro de transporte de carga com explosivos		4536	263	1143
Veículo pesado com explosivos		13608	375	1982
Veículo "*semi-trailer*" com explosivos		27216	475	2134

Fonte: adaptado de (FEMA, 2006, p. 1-7)

2.2. **Análise da ameaça**

Após a identificação e caraterização da ameaça há que categorizá-la de acordo com a análise de fatores associados ao nível da atividade terrorista. Esta análise assenta num processo de compilação e processamento da informação recolhida de forma a desenvolver indicadores que caraterizem uma possível atividade terrorista.

O Departamento de Defesa norte-americano, no *DoD Antiterrorism Handbook* (2004), define um grupo de fatores a usar numa metodologia de análise de uma ameaça terrorista: a capacidade operacional, a intenção, a atividade e o ambiente operacional.

2.2.1. Capacidade operacional (Co)

Este fator consiste no nível de capacidade operacional adquirida, avaliada e demonstrada para a condução de ataques terroristas (US DoD, 2004, p. 66).

Para categorizar a ameaça através deste fator deve-se utilizar a Tabela 5 (Apêndice B). Para tal devem-se recolher informações associadas às possibilidades dos grupos terroristas.

(i) Tipo de tática usada pelo grupo terrorista.

Que tipo de ataques tem o grupo terrorista conduzido no passado? Tem usado IED de pequena ou grande quantidade de explosivos? Existem indícios de que o grupo possui novas capacidades? Qual o grau de insucesso nos ataques anteriores? Mantém as mesmas táticas e técnicas usadas com sucesso no passado? O uso de diferentes táticas resulta em diferentes níveis de ameaça. Um grupo que conduza ataques contra propriedades apresenta menor nível de ameaça que um grupo que conduza ataques contra pessoas.

(ii) Capacidade/vontade de provocar "*mass casualties*".

O grupo possui capacidade ou intenção de conduzir ataques que provoquem grande quantidade de baixas? Já conduziu este tipo de ataques no passado?

(iii) *Targeting*

O grupo tem conduzido ataques em períodos de maior afluência ("hora de ponta")? Costuma utilizar um IED secundário para atingir as equipas de primeira intervenção? Procura limitar os efeitos do ataque aos danos em propriedade, colocando os IED em períodos e locais de menor afluência?

(iv) Patrocínio Estatal

O grupo possui apoio de um Estado? Se sim, qual(is)? Que tipo de apoio é fornecido (informações, logística, treino, financiamento)?

(v) Área de Operações

O grupo é interno do país ou transnacional? Pode o grupo operar regionalmente ou internacionalmente?

(vi) Acesso a tecnologia

O grupo tem acesso a tecnologia avançada? Usam computadores? Pode o grupo conduzir sofisticadas técnicas de vigilância ou empregar IED tecnologicamente mais avançados? Que tipo de equipamentos utilizam? Onde obtém o equipamento? Onde obtém o treino?

2.2.2. Intenção (In)

A intenção reflete o histórico ou a possibilidade, face a uma determinada situação recente, de um ataque terrorista contra os interesses nacionais (US DoD, 2004, p. 67).

Para categorizar a ameaça através do fator "*Intenção*" deve-se utilizar a Tabela 6 (Apêndice B). Para tal devem-se recolher informações associadas à intenção dos grupos terroristas.

(i) Ataques recentes

O grupo tem conduzido ataques recentemente? Que tipos de ataques? Que tipo de armamento usado? Foi identificado algum indicador pré-incidente? O grupo reclamou a autoria do ataque?

(ii) Ideologia anti-Portugal

O grupo terrorista possui uma ideologia política, religiosa ou cultural contra Portugal? Esta ideologia é pública? Quais os principais pontos de interesse nacionais para o grupo terrorista? Que eventos/acontecimentos se podem constituir como "gatilho" para uma ação terrorista?

(iii) Ataques noutros países

O grupo tem conduzido ataques terroristas em outros países? Onde? Que tipo de ataques? Que tipo de apoio logístico o grupo possui no local? Têm ameaçado interesses portugueses nesses países?

2.2.3. Atividade (At)

A atividade de um grupo terrorista num determinado país não tem que estar, obrigatoriamente, associada ao planeamento ou condução de ações, podendo mesmo não representarem uma ameaça direta aos interesses do país. Muitos grupos terroristas usam determinados países como bases de apoio (e.g. recrutamento, apoio logístico, treino), evitando aí conduzir atos terroristas para não afetar negativamente esta relação. É por isso

essencial determinar o tipo de atividade de um grupo terrorista analisando os elementos influenciadores na relação com o país onde opera ou se localiza (US DoD, 2004, p. 68).

Para categorizar a ameaça através do fator "*Atividade*" deve-se utilizar a Tabela 7 (Apêndice B). Alguns dos aspetos a considerar nesta análise são:

(i) Presença.

O grupo terrorista está presente no país? Apresenta algum tipo de atividade?

(ii) Angariação de financiamento e local seguro

O grupo terrorista usa o país para angariação de fundos financeiros? Que tipo de financiamentos? Qual a intenção para o uso desses financiamentos? O grupo usa o país como santuário ou local seguro?

(iii) Vigilância

O grupo terrorista tem conduzido ações de vigilância sobre possíveis alvos? O grupo é proficiente em ações de vigilância? Como tem conduzido as ações de vigilância? Qual a finalidade da informação obtida? O grupo tem ameaçado os interesses nacionais? Tem ocorrido eventos suspeitos que possam ser associados ao grupo terrorista?

(iv) Alterações à filosofia de escolha de alvos

O grupo terrorista tem demonstrado sinais de alteração à sua filosofia ou doutrina relativamente à seleção de alvos? Verificou-se alteração ao tipo de alvos selecionados?

(v) Envolvimento com células terroristas externas

Existem ligações do grupo terrorista com outras células? Qual a frequência do contacto com células externas? Como tem o líder do grupo interagido com as lideranças dessas células? Existe treino conjunto? Existe partilha de informação?

(vi) Movimentos de operacionais

Tem se verificado movimento dos elementos operacionais do grupo terrorista? Esses movimentos têm sido dissimulados? Qual o propósito desses movimentos?

(vii) Disrupção do grupo ou da rede

As forças de segurança têm interrompido atividades do grupo terrorista? Que causas levaram a essa interrupção? De que forma a interrupção da atividade influenciou a capacidade operacional do grupo?

(viii) Atividades em rede

Que tipo de atividades conduz o grupo no país? Operacionais? Logísticas? Qual o número de células a atuarem no país? E a dimensão dessas células?

(ix) Ataques a alvos nacionais

Existem indícios de possíveis ataques a alvos nacionais? Já foram reivindicados ataques por parte do grupo? O grupo tem alvos específicos identificados? Que tipo de alvos? Qual a localização dos alvos?

2.2.4. Ambiente Operacional (Ao)

A análise deste fator permite avaliar a forma como o ambiente social, político, económico e securitário, influenciam a capacidade e motivação de um indivíduo ou grupo conduzir um ataque terrorista (US DoD, 2004, p. 69).

Para categorizar a ameaça através do fator "*Ambiente operacional*" deve-se utilizar a Tabela 8 (Apêndice B). Para analisar este fator devem-se considerar os seguintes aspetos:

(i) Presença de forças de segurança ou de militares

Qual a presença de forças de segurança ou militares no país? E na região? Dimensão? Localização? Tempo de permanência? Qual a atividade das forças de segurança ou militares na região (treino, apoio, segurança, vigilância, etc)? Que perceção tem o grupo terrorista da presença das forças de segurança ou militares? O que pode atrair um grupo terrorista a conduzir um ataque contra as forças de segurança ou militares?

(ii) Influência de fatores externos

A nação hospedeira encontra-se em guerra? Pode este facto influenciar um ataque de um grupo terrorista? Existe um ambiente de insurreição? O grupo terrorista está envolvido em ações de insurgência?

(iii) Capacidades securitárias da nação hospedeira

As forças de segurança e militares da nação hospedeira conseguem manter a ordem social? Que nível de treino possuem para enfrentar ataques terroristas? Que tipo de equipamento possuem? Qual a sua dispersão territorial? Existem colaboração entre as forças da nação hospedeira e as forças nacionais? Existe partilha de informação entre as forças da nação hospedeira e as forças nacionais?

(iv) Influência política

Que influências políticas afetam as motivações do grupo terrorista para conduzirem um ataque? O sistema política, social e económico da nação hospedeira colapsou após atos terroristas?

2.3. **Classificação da ameaça**

Depois de identificadas, caraterizadas e analisadas as principais ameaças é necessário determinar a probabilidade de estas se efetivarem, permitindo assim classificar as ameaças em diferentes níveis. O nível de ameaça é parte integrante de qualquer processo de análise da vulnerabilidade e, consequentemente, da análise do risco e é utilizada para determinar, caraterizar e quantificar os danos causados por um terrorista (ou grupo terrorista) de acordo com as suas táticas e tipo de engenhos explosivos.

Existem vários tipos de escalas possíveis de serem usadas, variando a quantidade de níveis e a descrição dos indicadores que lhes estão associados. A escala por nós criada para classificar o nível de ameaça consiste na combinação de uma escala linguística de cinco estados e uma escala numérica de 20 níveis. Esta escala permite estabelecer uma relação entre os quatro fatores analisados, em função da sua probabilidade, credibilidade e dos efeitos das táticas, técnicas e do tipo de engenhos explosivos. A classificação pode ser obtida, através de uma avaliação qualitativa, associando a análise das caraterísticas da ameaça à perceção e ao julgamento subjetivo do decisor; ou através de uma avaliação quantitativa assente em métodos algébricos (capítulo quatro).

Tabela 3 – Classificação dos níveis de ameaça

Classificação dos níveis de ameaça		
Escala Qualitativa	**Escala Numérica**	**Descrição do nível de ameaça**
Elevado	17- 20	A ocorrência de um ataque é iminente. Células terroristas estão operacionalmente ativas. As forças de segurança, forças militares e serviços de informação confirmam a ameaça. O ambiente operacional favorece o terrorista.
Alto	13 - 16	A ocorrência de um ataque é provável. As forças de segurança, forças militares e serviços de informação confirmam a credibilidade da ameaça. O ambiente operacional favorece o terrorista.
Moderado	8 - 12	A ocorrência de um ataque é possível. As forças de segurança, forças militares e serviços de informação confirmam a existência de ameaça, mas não foi verificada a sua credibilidade. O ambiente operacional é neutro.
Baixo	4 - 7	A ocorrência de um ataque é pouco provável. As forças de segurança, forças militares e serviços de informação confirmam a existência de ameaça, mas não a probabilidade de que a mesma se materialize é reduzida. O ambiente operacional favorece o país ou a nação hospedeira.
Muito Baixo	2 - 3	A probabilidade de ocorrência de um ataque é negligenciável. De acordo com as forças de segurança e serviços de informação a ameaça não existe ou é praticamente inexistente. O ambiente operacional favorece o país ou a nação hospedeira.

Fonte: Adaptado de (FEMA, 2005, p. 1-25) e de (US DoD, 2004, p. 70)

2.4. **Síntese conclusiva**

Neste capítulo demonstrou-se em que medida a ameaça terrorista afeta a vulnerabilidade de uma IC e assim responder à QD1.

O ataque com recurso a engenhos explosivos têm sido a tática predileta dos grupos terroristas, prevendo-se a sua continuidade, nomeadamente na condução de ataques contra infraestruturas.

A vulnerabilidade de uma IC é afetada pela tipologia de terrorismo, variando este de acordo com as suas motivações étnicas, religiosas ou políticas, traduzindo-se em diferentes graus de probabilidade de ocorrência de um ataque terrorista contra essa mesma IC.

As táticas e técnicas usadas pelos terroristas, bem como os engenhos explosivos, são outro influenciador da vulnerabilidade de uma IC. Estas dependem da forma de emprego, da duração e extensão dos efeitos e das condições do local, sendo a dimensão da explosão causada e a associação carga-distância fatores determinantes para determinar a severidade dos efeitos e a correspondente, maior ou menor, probabilidade de sucesso do ataque terrorista.

A identificação e caraterização da ameaça é o ponto de partida para a sua categorização, analisando-a à luz de quatro fatores: a capacidade operacional para a condução de um ataque terrorista, a intenção de o perpetuar, as atividades desenvolvidas em torno de um ataque, nomeadamente atividades de planeamento e de apoio logístico, e o ambiente operacional que envolve o planeamento, preparação e execução do ataque.

Esta análise permite transformar julgamentos qualitativos em valores quantitativos, através de uma escala criada para o efeito, expressando a probabilidade e a credibilidade da ameaça na probabilidade de sucesso de um ataque terrorista contra uma IC.

3. Avaliação da Infraestrutura

Após a avaliação da ameaça é necessário efetuar a avaliação da infraestrutura, em particular do edificado. Uma infraestrutura constitui-se como um ativo, pelo que é necessário determinar em que medida se constitui um alvo perante um ataque terrorista.

Determinar o valor de uma infraestrutura como alvo permite aferir a suscetibilidade deste ser atacado ou não, em função, tanto de fatores tangíveis como de fatores intangíveis, influenciando o nível de proteção a adotar (Renfroe e Smith, 2016, p. 2).

O processo para a avaliação da infraestrutura deve compreender as seguintes fases (FEMA, 2005, p. 2-1):

(i) Identificação e caraterização dos perímetros de segurança da infraestrutura;

(ii) Identificação dos ativos críticos e das funções nucleares da infraestrutura;

(iii) Identificar os fatores de análise do valor de uma infraestrutura.

3.1. Identificação e caraterização dos perímetros de segurança

A definição de perímetros de segurança tem por objetivo criar diferentes perímetros defensivos, do exterior próximo em direção ao edifício.

O conceito de perímetro de segurança traduz, logo à partida, uma filosofia de segurança, independentemente do resultado da avaliação das vulnerabilidades e do risco e, consequentemente, da escolha das medidas de proteção a implementar.

3.1.1. Linhas de segurança

Os perímetros de segurança estão associados ao conceito de linha de segurança (FEMA, 2005, p. 2-1).

As linhas de segurança consistem em linhas concêntricas relativamente a uma infraestrutura, limitando os diversos perímetros de segurança, os quais estabelecem o aumento das medidas de controlo de acesso à infraestrutura, providenciam tempo de alerta e resposta e permitem aos ocupantes ou utilizadores da infraestrutura um maior grau de proteção física (Atlas, 2008, p. 147).

Aos diversos perímetros, limitados pelas linhas de segurança, corresponde zonas às quais estão associadas diferentes estratégias de segurança e proteção.

A FEMA (2005, p. 2-2) define três tipos de linhas de segurança:

(i) Primeira linha de segurança (zona afastada);

(ii) Segunda linha de segurança (zona intermédia);

(iii) Terceira linha de segurança (limites físicos do edificado da infraestrutura).

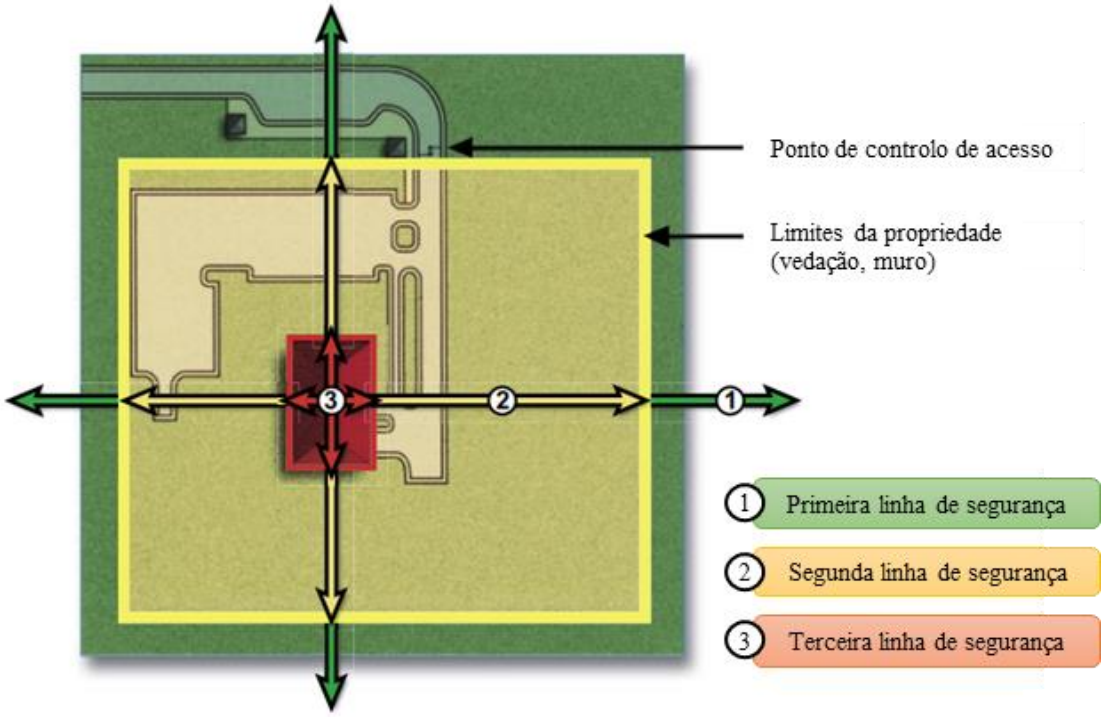


Figura 9 – Esquema, em planta, da localização das linhas de segurança.

Fonte: adaptado de (FEMA, 2005, p. 2-3)

A primeira linha de segurança engloba a área envolvente do edifício (edifícios e ruas). Tem em consideração o tipo de construções, densidade de ocupação e a natureza e intensidade das atividades que aí se desenvolvem.

Compreende todo o espaço para além do perímetro imposto por barreiras, mais ou menos físicas, e que limitam a propriedade da infraestrutura (FEMA, 2005, p. 2-2).

A segunda linha de segurança compreende o espaço entre o limite da propriedade onde se encontra o edifício e o próprio edifício.

Nesta zona as preocupações de segurança centram-se, por exemplo, nos pontos de acessos ao edifício (pessoas e veículos), nas zonas de estacionamento, na iluminação exterior e vigilância do espaço.

Em zonas urbanas, devido à proximidade dos edifícios, pode ir para além dos limites da propriedade onde está o edifício (FEMA, 2005, p. 2-2).

A terceira linha de segurança abrange os limites do edificado da própria infraestrutura, sendo a linha definida pela sua geometria. Nesta zona são analisados, do ponto de vista da segurança, os vários sistemas do edificado (FEMA, 2005, p. 2-2).

3.1.2. Estruturas, equipamentos e medidas que afetam a segurança da infraestrutura

Analisando os perímetros de segurança existem um conjunto de caraterísticas que afetam a segurança da infraestrutura, quer minimizando ou exponenciando os efeitos de um ataque terrorista. Estas caraterísticas, que se podem constituir como um *enabler* ou como um obstáculo à ação de um terrorista, estão associadas a cada uma das linhas de segurança.

(i) Primeira linha de segurança: nesta zona importa analisar a interação da infraestrutura com a sua envolvente, compreendendo até que ponto, certos fatores, como o tipo de construção, os níveis de ocupação ou o tipo de atividades existentes na envolvente, potenciam a ameaça ou se, pelo contrário, conferem maior proteção. Nesta zona podem existir outras infraestruturas, que se constituam como alvo de um ataque terrorista, e que causem danos colaterais na infraestrutura em análise, tais como:

- Monumentos relevantes ou edifícios icónicos;
- Unidades de forças de segurança, bombeiros ou hospitais;
- Edifícios governamentais;
- Embaixadas;
- Atividades comerciais relevantes;
- Armazéns de matérias perigosas;
- Infraestruturas de transporte (estradas, pontes, terminais de transporte, portos, aeroportos, tuneis);
- Traçado das ruas;
- Organização espacial.

(ii) Segunda linha de segurança: nesta zona importa perceber como proteger a infraestrutura, as pessoas e as atividades desenvolvidas, identificando acima de medidas ou obstáculos que impeçam o acesso à infraestrutura por parte de um atacante ou que absorvam/refratem os efeitos de um ataque terrorista com recurso a explosivos. Neste sentido surgem um conjunto de questões cuja resposta é o ponto de partida para a segurança:

- Existem vedações ou outro tipo de barreiras físicas;
- Qual a distância entre as barreiras físicas e a infraestrutura;
- Quantos e quais os pontos de acesso à infraestrutura;
- Existe controlo de acesso para pessoas ou veículos;
- Iluminação exterior;

- As zonas de acesso à infraestrutura permitem uma aproximação a velocidades elevadas.

(iii) Terceira linha de segurança: nesta ultima linha de segurança, que corresponde ao próprio edificado da infraestrutura, importa analisar os sistemas estruturais e não estruturais, bem como outras caraterísticas inerentes à construção e à segurança da infraestrutura e de que forma mitigam ou aumentam as consequências de um ataque. Existem, assim, um conjunto de parâmetros que devem ser considerados nesta análise:

- Qual a capacidade resistente da estrutura do edifício;
- Qual a capacidade resistente dos paramentos exteriores face a uma explosão;
- Qual a área de envidraçados; o vidro utilizado nas fachadas tem uma resistência superior;
- As redes prediais de abastecimento de águas, gás e energia são seguras;
- Existem no edifício materiais perigosos; quantidades e tipologia;
- O acesso a telhados e coberturas é restrito;

Uma boa caraterização da IC e da sua envolvente, assente nestes indicadores, é a base para a análise da infraestrutura do ponto de vista do seu valor para o utilizador e para o agressor.

3.2. **Identificação das funções nucleares e dos ativos críticos**

A identificação das funções nucleares e dos ativos críticos é um passo fundamental na avaliação de uma determinada infraestrutura e, consequentemente, para determinar o seu grau de vulnerabilidade.

3.2.1. Identificação das funções nucleares

Tendo em consideração os potenciais efeitos de um ataque terrorista, é fundamental determinar o conjunto de funções, com ligação direta à construção, operação e manutenção de uma infraestrutura, necessário para funcionamento da mesma após o ataque. Para esse efeito, devem-se analisar os seguintes parâmetros (FEM, 2005, p. 2-17):

(i) Quais os principais serviços existentes na infraestrutura;

(ii) Quais as atividades críticas desenvolvidas na infraestrutura;

(iii) Quem são os ocupantes, utilizadores e visitantes da infraestrutura;

(iv) Qual o grau de dependência de agentes externos, para as atividades desenvolvidas na infraestrutura;

	Setor	Subsetor
1	Órgãos de Soberania	Presidência da República
		Assembleia da República
		Governo
		Tribunais
2	Ministérios	Ministérios
3	Administração Pública	Administração Pública
4	Segurança	Serviços de Segurança
		Forças de Segurança
		Polícia Judiciária
		Serviços de Informações
5	Defesa	Forças Armadas
6	Proteção Civil	Proteção Civil
7	Comércio	Comércio
8	Comunicações	Comunicações de Dados e Internet
		Comunicações Móveis
		Rede Fixa de Comunicações
		Comunicações Satélites
		Serviços Postais
9	Media	Media
10	Energia	Combustíveis
		Energia Elétrica
		Gás Natural
11	Indústria	Indústria Alimentação Bebidas e Tabaco
		Indústria de Madeira, Cortiça e Mobiliário
		Indústria de Papel
		Indústria dos Minerais Não Metálicos
		Indústria e Comércio Automóvel
		Indústria Elétrica e Eletrónica
		Indústria Extrativa
		Indústria Farmacêutica
		Indústria Metalúrgica e Metalomecânica
		Indústria Química
		Indústria
12	Serviços Financeiros	Serviços Financeiros
13	Transportes	Transportes Aéreos
		Transportes Ferroviários
		Transportes Marítimos
		Transportes Fluviais
		Transportes Rodoviários
14	Água	Água
15	Alimentação	Alimentação
16	Ambiente	Ambiente
17	Saúde	Saúde

Figura 10 – Categorização das IC pela ANPC - Lista dos setores e subsetores.

Fonte: (Pais, 2015, cit. por Ferreira, 2016, p. 21)

As funções nucleares estão diretamente associadas à tipologia de IC. Para melhor identificação das funções nucleares recorreu-se à classificação das IC definida pela ANPC, a qual definiu 17 setores e 43 subsetores (Pais, 2015, cit. por Ferreira, 2016, pp. 20-21).

Na Tabela 9 (Apêndice C) propõe-se um conjunto de funções nucleares pré-definidas de acordo com as categorias de IC.

3.2.2. Ativos principais

Depois de identificadas as principais funções de uma infraestrutura segue-se, a identificação dos principais ativos. Os ativos de uma infraestrutura consistem em todas as suas componentes essenciais ao seu funcionamento, face às funções nucleares da mesma (Morgeson, J. et al, 2011, pp. 9-10).

Os ativos principais decorrem das funções nucleares da infraestrutura. A identificação dos ativos principais permite determinar quais os principais elementos de uma infraestrutura cuja proteção é essencial para o funcionamento da mesma após um ataque terrorista. Perante uma ameaça é mais fácil e menos oneroso adotar medidas para a proteção dos principais ativos de uma infraestrutura do que da própria infraestrutura como um todo. No entanto, a própria infraestrutura pode ser considerada um ativo cujo valor obriga a que se adotadas medidas de proteção como um todo.

A vulnerabilidade de uma infraestrutura assenta na avaliação de como as condições existentes afetam a proteção dos ativos identificados face a uma ameaça identificada.

Esta tarefa tem como premissa, o facto dos principais ativos de um edifício serem as pessoas.

Existe um numero ilimitado de diferentes tipos de ativos que se podem encontrar nas diversas tipologias de infraestruturas críticas. Esses ativos podem ser agrupados em categorias tendo em conta as suas funções principais.

Na Tabela 9 (Apêndice C) propõe-se um conjunto de ativos pré-definidos de acordo com as categorias de IC e as funções nucleares, no entanto, estas podem ser alteradas ou, introduzidas outras, tendo em consideração a especificidade de uma determinada IC.

3.3. **Fatores de análise da infraestrutura**

A análise de uma infraestrutura deve ser feita de dois pontos de vista: (i) do valor que esta ou os seus principais ativos têm para o utilizador e para o país; (ii) e do valor como alvo para o atacante.

Para cada um destes pontos de vista existem um conjunto de fatores de análise e que permitirão determinar a vulnerabilidade da infraestrutura.

3.3.1. Valor da infraestrutura ou dos ativos principais para o utilizador

Após a identificação da IC ou dos ativos é fundamental determinar o valor que representam para os seus utilizadores, ou seja, a consequência que terá se os ativos forem comprometidos pelo terrorista (US DoD, 2008, p. 3-9). O valor de um ativo ajuda o responsável pela infraestrutura a determinar o nível de proteção adequado. Quanto maior o seu valor, mais importante é para o utilizador, maior a necessidade de implementação de medidas de proteção para reduzir a vulnerabilidade.

Para determinar o valor de um ativo e consequentemente, da infraestrutura, para o utilizador, devem ser analisados quatro fatores (US DoD, 2008, pp. 3-9 a 3-15): (i) a criticidade da missão; (ii) o impacto; (iii) a substituição e (iv) importância pública.

(i) Criticidade para a missão (Cr)

A criticidade de uma infraestrutura ou de um ativo está relacionada com a capacidade requerida para o desempenho da função principal. A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 10 (Apêndice D).

(ii) Impacto (Im)

O impacto de uma infraestrutura ou de um ativo está relacionado com a criticidade destes para o funcionamento do sistema a que está associado, ao nível local, regional ou nacional e a influência que têm em outros sistemas como o económico, financeiro, político, etc. A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 11 (Apêndice D).

(iii) Substituição/recuperação (Sb)

Este factor representa a facilidade com que o ativo pode ser substituído ou a infraestrutura retomar a atividade. Para a análise deste fator deve ser feita a distinção entre o pessoal crítico à missão da infraestrutura e os restantes ativos. A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 12 (Apêndice D).

(iv) Importância pública (Ip)

Este fator foca-se nas repercussões públicas e políticas associadas à perda ou destruição da infraestrutura ou dos ativos e à consequente afetação da respetiva atividade. Associado a este fator estão considerações como a publicidade adversa, a perda de confiança e a perceção de insegurança. A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 13 – Importância pública (Apêndice D).

3.3.2. Valor da infraestrutura ou dos ativos principais para o agressor

A IC deve também ser analisada do ponto de vista de como se constitui um alvo remunerador para o alcançar dos objetivos do agressor. Quanto maior o valor da IC, mais remunerador é como alvo, logo maior a exposição a um ataque e maior a probabilidade de sucesso deste.

Para determinar o valor de um ativo e consequentemente, da infraestrutura, para o agressor, devem ser analisados nove fatores (US DoD, 2008, pp. 3-24 a 3-31): (i) a localização; (ii) publicidade; (iii) acessibilidade; (iv) disponibilidade; (v) dinâmica; (vi) visibilidade; (vii) esforço; (viii) medidas de segurança e (ix) perceção de sucesso pelo agressor.

(i) Localização (Lc)

Este fator reflete o pressuposto de que as infraestruturas no exterior do país apresentam maior probabilidade de se constituírem alvo de ataque que localizadas no interior das suas fronteiras, bem como é maior a ameaça próximo dos grandes aglomerados populacionais. A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 14 (Apêndice E).

(ii) Publicidade (Pu)

Este fator reflete o nível de publicidade associado à infraestrutura. Reflete o pressuposto de que as infraestruturas com maior publicidade estão mais expostas a ataques que as que são relativamente desconhecidas. A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 15 (Apêndice E).

(iii) Acessibilidade (Ac)

Este fator reflete o grau de dificuldade do acesso à infraestrutura ou aos ativos principais por parte de um atacante.

A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 16 (Apêndice E).

(iv) Disponibilidade (Ds)

Este fator analisa a quantidade de infraestruturas ou ativos principais, da mesma tipologia, na área envolvente. Reflete o pressuposto de que é menos provável o ataque a uma infraestrutura ou a um ativo principal se nas imediações existirem outros da mesma tipologia. A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 17 (Apêndice E).

(v) Dinâmica (Dn)

Este fator reflete o pressuposto de que é menos provável o ataque a um ativo principal que esteja frequentemente em movimento e de forma aleatória devido à imprevisibilidade da sua localização.

A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 18 (Apêndice E).

(vi) Visibilidade (Vs)

Este fator avalia a probabilidade de um atacante identificar uma infraestrutura ou ativo na sua localização. Este fator assenta na assinatura emitida pela infraestrutura ou pelo ativo e na necessidade do atacante possuir capacidades de recolha de informações.

A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 19 (Apêndice E).

(vii) Esforço (Es)

Este fator avalia a quantidade de recursos (e.g. know-how, capacidades, material, tempo, etc) necessários para danificar ou destruir uma infraestrutura ou um ativo principal de forma a que deixá-lo inoperacional. Reflete o grau de dificuldade necessário para neutralizar a infraestrutura ou os ativos principais.

A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 20 (Apêndice E).

(viii) Medidas de segurança (Ms)

Este fator avalia as medidas de segurança existentes para prevenir ou evitar o acesso à infraestrutura, detetar um acesso não autorizado e mitigar as ameaças. Reflete a percentagem de pessoal autorizado e de equipamento portátil e as formas de segurança da infraestrutura.

A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 21 (Apêndice E).

(ix) Perceção de sucesso pelo atacante (Ps)

Este fator avalia a probabilidade da perceção do atacante de comprometer com sucesso a operacionalidade da infraestrutura e conseguir escapar. Este critério serve de reforço ao anterior, acrescentando às medidas de segurança a perceção de sucesso por parte do atacante.

A análise deste fator e consequente categorização, deve ser enquadrada pelos indicadores descritos na Tabela 22 (Apêndice E).

3.4. **Síntese conclusiva**

Neste terceiro capítulo, analogamente ao anterior, demonstrou-se de que forma as caraterísticas de uma determinada IC afetam a sua vulnerabilidade, respondendo à QD2.

As caraterísticas da infraestrutura são, a par da ameaça, uma dimensão de análise da vulnerabilidade, sendo relevante avaliar a infraestrutura, como um todo ou olhando apenas para os seus ativos principais, do ponto de vista das condições físicas e funcionais que afetam a sua segurança e do ponto de vista do valor que esta tem para o seu utilizador e para o agressor.

Olhando para a infraestrutura do ponto de vista securitário, é importante analisá-la em três níveis, de acordo com os três perímetros de segurança. Para tal contribuem, entre outros, o tipo de construções, densidade de ocupação e a natureza e intensidade das atividades na área envolvente à infraestrutura (primeira linha de segurança – zona afastada), acessos à infraestrutura (pessoas e veículos), zonas de estacionamento, iluminação exterior e vigilância do espaço na segunda linha de segurança (zona intermédia) e os sistemas estruturais e não estruturais, bem como outras caraterísticas inerentes à construção da própria infraestrutura (terceira linha de segurança - zona próxima).

Para determinar o valor da IC para o utilizador, devem ser analisados os fatores da criticidade, do impacto, da substituição e da importância pública. Do ponto de vista do agressor, o valor da IC depende de fatores como a localização, publicidade, acessibilidade, disponibilidade, dinâmica, visibilidade, esforço, medidas de segurança e perceção de sucesso.

A análise de todos estes fatores permite, partindo de um julgamento qualitativo, quantificar o valor da IC para o utilizador e para o agressor e assim contribuir para determinar a probabilidade de sucesso do ataque terrorista.

4. Modelo de análise de vulnerabilidade de IC

Para se efetuar a análise da vulnerabilidade de uma IC é fundamental a existência de um modelo de análise e de uma equipa de trabalho para aplicação desse modelo, a qual deve ser constituída por analistas, conhecedores da infraestrutura e especialistas nas funções nucleares e áreas críticas do seu funcionamento, bem como conhecedores do modelo de análise a empregar.

O grau de vulnerabilidade de uma IC consiste numa expressão qualitativa ou quantitativa do nível a que uma determinada infraestrutura é suscetível a apresentar danos face a um determinado perigo (Morgeson et al, 2011, p. 24), sendo, como demonstrado nos capítulos anteriores, uma função dependente da ameaça e da infraestrutura.

Para além de determinar o grau de vulnerabilidade, todo o processo de análise da vulnerabilidade permite identificar formas de baixar a probabilidade de sucesso de um ataque terrorista contra uma IC. Esta análise é feita assente na expressão matemática geral (1), posteriormente decomposta em expressões matemáticas subsidiárias:

$$Vulnerabilidade = Probabilidade\ (Sucesso|Ataque)$$

$$V = P(S|A) \qquad (1)$$

4.1. Modelo algorítmico para análise da vulnerabilidade

Para analisar a vulnerabilidade de uma IC e dar corpo à expressão (1), construiu-se o modelo algorítmico ilustrado na Figura 11 e a seguir descrito, resultante de uma adaptação parcial dos modelos teóricos, apresentados pelo US DoD (2008), FEMA (2005) e Morgeson et al (2011), à análise e conclusões obtidas nos capítulos anteriores.

Este modelo consiste em seis passos, assente na análise da ameaça, apresentada no capítulo dois e na análise da infraestrutura, apresentada no capítulo três.

O modelo de análise construído é composto, para além do algoritmo, por um conjunto de folhas de trabalho com tabelas de apoio ao cálculo e ao registo de valores e que sustentarão o resultado final.

4.1.1. Passo 1 – Identificar o tipo de agressor, as táticas e técnicas e o tipo de engenhos explosivos a utilizar

O primeiro passo consiste em criar cenários tendo por base as várias tipologias de ameaça. Começa-se por identificar o(s) tipo(s) de agressor(es), o(s) tipo(s) de táticas e técnicas a utilizar e o(s) tipo(s) de engenhos explosivos, de acordo com o exposto no subcapítulo 2.1.

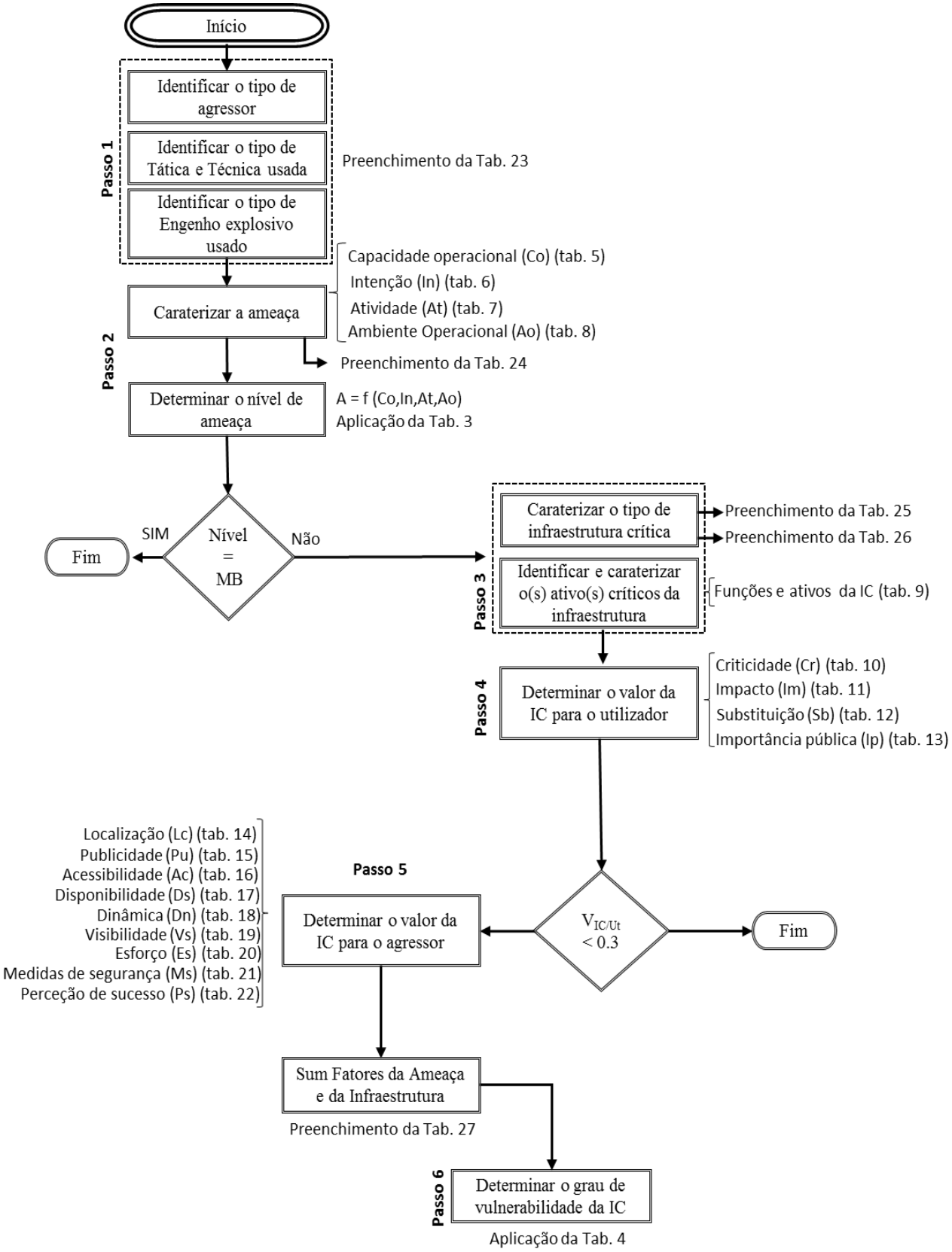


Figura 11 – Modelo algorítmico para análise da vulnerabilidade.

Fonte: (Autor, 2017)

Quanto melhor for a identificação da ameaça, maior será a sua caraterização e, consequentemente, a sua categorização e avaliação. Para resumir a identificação da tipologia de ameaças, deve-se preencher a Tabela 23.

4.1.2. Passo 2 – Caraterizar, analisar e avaliar o nível de ameaça

Feita a identificação da(s) tipologia(s) da ameaça, é necessário caraterizá-la, analisá-la e avaliá-la, de acordo com um conjunto de parâmetros, para determinar o seu nível.

A análise e avaliação da ameaça deve ter em consideração os quatro fatores (subcapítulo 2.2): (i) a capacidade operacional (Co); (ii) a intenção (In); (iii) a atividade (At) e (iv) o ambiente operacional (Ao).

Para a caraterização e análise, identificaram-se, no subcapítulo 2.2, um conjunto de questões e orientações, que permitem definir, para cada fator, o indicador que melhor define a ameaça e o valor a atribuir para a sua avaliação (Tabelas 5 a 8 – Apêndice B)

O nível de ameaça é, assim, uma função destes quatro fatores:

Ameaça = função (capacidade operacional, intenção, atividade, ambiente operacional)

$$A = f(Co,In,At,Ao) \quad (2)$$

Para determinar o nível da ameaça deve-se, então, somar os valores atribuídos a cada um dos quatro fatores.

$$A = \sum (Co,In,At,Ao) \quad (3)$$

Com o valor total do somatório deve-se fazer corresponder esse valor ao respetivo nível descrito na Tabela 3. Pode-se, em alternativa, através de uma análise qualitativa adotar o nível de ameaça tendo por base o descritivo correspondente.

Se para um determinado cenário o nível de ameaça for considerado "*MUITO BAIXO*" então, para esse cenário, deve ser considerado, à partida, um grau de vulnerabilidade "*MUITO BAIXO*".

4.1.3. Passo 3 – Caraterizar a infraestrutura

Após analisar a ameaça deve-se avançar para a caraterização da infraestrutura. Este passo comporta duas tarefas principais: (i) a identificação e caraterização dos perímetros de segurança da infraestrutura e (ii) a identificação das funções nucleares e dos ativos críticos da infraestrutura;

Após a identificação da infraestrutura a analisar, é necessário definir os perímetros de segurança, identificando as linhas de segurança (próxima, intermédia e afastada) e

caraterizando todas as estruturas, equipamentos e medidas localizadas nos seus limites e analisar a forma como afetam a segurança da infraestrutura (subcapítulo 3.2).

Para completar a caraterização da infraestrutura há que identificar as suas funções nucleares e os respetivos ativos críticos. Para tal devem-se analisar os principais serviços existentes, as atividades críticas e as componentes essenciais ao funcionamento da infraestrutura (subcapítulo 3.3). Na Tabela 9 (Apêndice C) é apresentada uma lista pré-definida com as categorias de ativos face ao tipo de infraestrutura e às suas funções primárias, devendo esta ser considerada como um ponto de partida e, sobre a qual, o analista pode ajustar face às caraterísticas específicas da infraestrutura em análise.

4.1.4. Passo 4 – Determinar o valor da IC para o utilizador

Caraterizada a infraestrutura está-se em condições de determinar o valor que esta tem para o utilizador, sendo uma função de quatro fatores:

Valor da IC para o utilizador = função (criticidade, impacto, substituição, importância pública)

$$V_{IC/Ut} = f\,(Cr,Im,Sb,Ip) \qquad (4)$$

Para determinar o valor da IC para o utilizador deve-se, então, somar os valores atribuídos a cada um dos quatro fatores e dividir pelo somatório dos seus valores máximos.

$$V_{IC/Ut} = \frac{\sum(Cr,Im,Sb,Ip)}{\sum Max(r,Im,Sb,Ip)} \qquad (5)$$

As IC com um $V_{IC/Ut}$ inferior a 0,3 podem ser consideradas de reduzido valor para o utilizador, permitindo-se dispensar a consequente análise de vulnerabilidade. No entanto, se o analista entender, pode continuar o processo e determinar a vulnerabilidade da IC.

4.1.5. Passo 5 – Determinar o valor da IC para o agressor

Para além do valor que tem para o utilizador, uma IC também tem um determinado valor para o agressor, calculado a partir de um conjunto de nove fatores.

Valor da IC para o agressor = função (localização,publicidade,acessibilidade, disponibilidade,dinâmica,visibilidade,esforço,medidas de segurança,perceção de sucesso)

$$V_{IC/Ag} = f\,(Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms,Ps) \qquad (6)$$

Para determinar o valor da IC para o agressor deve-se, então, somar os valores atribuídos a cada um dos nove fatores e dividir pelo somatório dos seus valores máximos.

$$V_{IC/Ag} = \frac{\sum(Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms,Ps)}{\sum Max\,(Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms,Ps)} \qquad (7)$$

4.1.6. Passo 6 – Determinar o grau de vulnerabilidade da IC

Sendo então a vulnerabilidade um valor em função da probabilidade de sucesso de um ataque, $V = P(S|A)$, o cálculo do seu valor está diretamente relacionado com o nível de ameaça, com o valor da IC para o utilizador e com o valor da IC para o agressor.

Ou seja, de forma algébrica:

$$V=P(S|A) \rightarrow V=f(A,V_{IC/Ut},V_{IC/Ag}) \rightarrow V=\sum(A,V_{IC/Ut},V_{IC/Ag}) \qquad (8)$$

Resumindo, o cálculo da probabilidade de sucesso de um ataque consiste no somatório dos 17 fatores determinados em função das caraterísticas da ameaça e da infraestrutura e dividir pelo somatório dos seus valores máximos:

$$V = \frac{\sum(Co,In,At,Ao,Cr,Im,Sb,Ip,Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms,Ps)}{\sum Max\ (Co,In,At,Ao,Cr,Im,Sb,Ip,Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms,Ps)} \qquad (9)$$

O preenchimento da Tabela 27 permite a obtenção, para uma determinada IC e mediante vários cenários, do valor da probabilidade de sucesso de um ataque.

O valor obtido através desta fórmula representa, para além da probabilidade de sucesso de um ataque terrorista, a percentagem de vulnerabilidade de uma IC.

Associado a um determinado intervalo de valores de probabilidade de sucesso de um ataque, ou de percentagem de vulnerabilidade, está um determinado grau de vulnerabilidade, o qual é determinado aplicando a Tabela 4.

Tabela 4 – Determinação do Grau de Vulnerabilidade

Grau de Vulnerabilidade	Probabilidade				
	<= 0,3	0,31 - 0,50	0,51 - 0,74	0,75 - 0,89	0,90 - 1
Elevado					X
Alto				X	
Médio			X		
Baixo		X			
Muito Baixo	X				

Fonte: Adaptado de (US DoD, 2008, p. 3-34)

4.2. **Integração do método Macbeth**

Numa tentativa de imaginar um modelo procedimental para a análise da vulnerabilidade, perspetiva-se ter que lidar com variados critérios, pelo que será necessário recorrer a ferramentas que permitam ou facilitem a conjugação desses critérios.

O método *MACBETH (Measuring Attractiveness by a Categorical Based Evaluation Technique)*, desenvolvido por Carlos Bana e Costa, Jean-Marie De Corte e Jean-Claude Vansnick, é um método de apoio à decisão que permite avaliar opções levando em conta

múltiplos critérios. Distingue-se de outros métodos multicritérios por basear a ponderação dos critérios e a avaliação das opções em julgamentos qualitativos sobre diferenças de atratividade (Bana e Costa e Oliveira, 2013).

A integração do método Macbeth no modelo de análise de vulnerabilidade construído, permite ao analista, com base nas perceções e preferências do decisor, fabricar os seus próprios pesos dos critérios, para depois voltar a integrá-los no modelo construído, substituindo os valores (ou pesos) pré-definidos nas tabelas 5 a 8 e 10 a 22.

4.2.1. Metodologia Macbeth

Esta metodologia envolve uma aprendizagem em grupo, a criação de uma interatividade entre atores, em particular entre analistas e decisores, a confrontação de preferências holísticas intuitivas com resultados dos métodos analíticos, o respeito do princípio de que o problema e a solução pertencem unicamente ao decisor e que o analista apenas tem responsabilidades na condução do processo e não no conteúdo da mesma (Bana e Costa et al., 2005).

Num processo de análise de vulnerabilidade de uma IC (em particular no modelo construído), o decisor pode, inicialmente, não ter a total compreensão do problema e/ou a perceção da importância a dar aos diversos critérios.

Sendo conhecedor do processo, o analista deve apoiar o decisor, ao longo do processo, de forma a que este vá construindo em si uma solução mais próxima da adequada ao problema.

No modelo construído, os valores dos pesos dados aos critérios são valores pré-definidos e propostos e com os quais o decisor pode não se sentir confortável dada a sua interpretação do problema ou a falta de clareza respeitante ao valor do peso de qualquer um dos critérios.

Com recurso ao método Macbeth, facilitado pela utilização do software com a mesma designação, o analista pode estruturar o modelo de análise da vulnerabilidade de acordo com as perceções e preferências do decisor, permitindo transformar os julgamentos qualitativos do decisor, e dos quais se obtém informações ordinais, em informação cardinal e valores quantitativos, adequando os pesos dos diversos critérios à solução pretendida pelo decisor.

Este processo de transformação de um julgamento qualitativo em informação quantitativa assenta no conceito de atratividade entre duas opções (Godinho, 2014, p. 44).

A aplicação do método Macbeth ao modelo de análise de vulnerabilidade de IC construído no subcapítulo anterior, assenta essencialmente na estruturação dos critérios e na avaliação dos pesos, permitindo, de forma interativa, manusear os pesos dos critérios, transformando julgamentos qualitativos em informação quantitativa assente no conceito de atratividade entre duas opções (Almeida, 2011, p. 55).

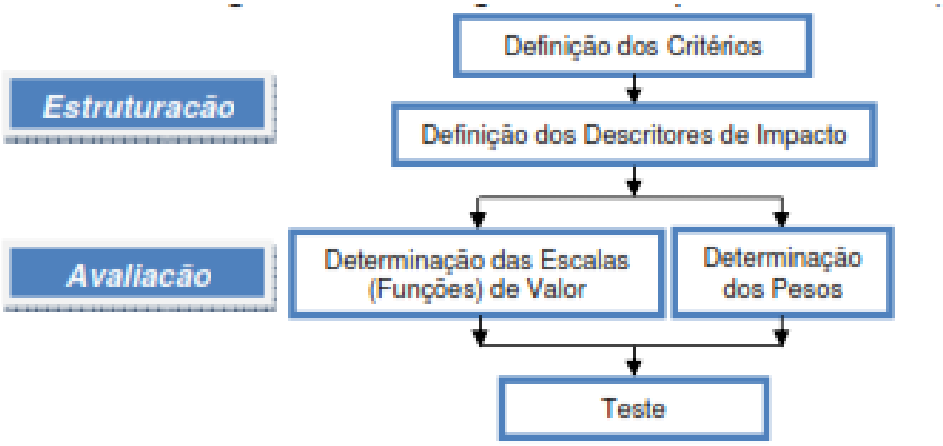


Figura 12 – Processo de estruturação e avaliação dos pesos dos critérios através do Macbeth.

Fonte: (Almeida, 2011, p. 56)

4.2.2. Conceito de atratividade

De acordo com Bana e Costa (1994, cit. por Godinho, 2014, p. 45), o conceito de atratividade consiste na forma de medir o valor das opções e, assim, quando o decisor for solicitado a emitir um determinado julgamento sobre uma opção ou conjunto de opções, deverá fazê-lo em termos de atratividade que "sente" por essa mesma opção. Bana e Costa e Vasnick (1995, cit. por Braz, 2011, p. 19) carateriza esta decisão como sendo a construção de uma função-critério *Vj*:

$$Vj : a \in A : Vj(a) \in \mathbb{R} \qquad (10)$$

tal que, o número real *Vj(a)* represente numericamente o valor de qualquer opção *a* pertencente a um conjunto de opções *A*, [$a \in A$], em termos de um determinado critério, no sentido em que:

$$\forall\, a, b \in A, v(a) > v(b), \text{ se e só se} \qquad (11)$$

- Para o decisor a opção a é mais atrativa ou preferível que b;
- Qualquer diferença positiva entre *v(a)* e *v(b)*, ou seja *v(a)* – *v(b)* > 0, represente numericamente a diferença de valor (atratividade) entre *a* e *b*, com *a* P (preferível a) *b*.

Assim, para $a, b, c, d \in A$ com *a* mais atrativa que *b*, e *c* mais atrativa que *d*, verifica-se que $v(a) - v(b) > v(c) - v(d)$ se, e somente se, a diferença de atratividade entre *a* e *b* é maior que a diferença de atratividade entre *c* e *d* (Braz, 2011, p.19).

Para que o decisor escolha entre as várias opções, a metodologia Macbeth introduz uma escala semântica formada por categorias de diferença de atratividade (*Sk*) com o objetivo de facilitar a interação entre o decisor e analista, sendo que a representação numérica destas categorias é feita através de um intervalo de números reais (S_k) tais que:

$$a\ P^k\ b,\ S_k < V(a) - V(b) < S_{k+1} \qquad (12)$$

Assim, o Macbeth exprime os julgamentos do decisor através de uma escala semântica formada por seis categorias de dimensão não necessariamente igual, delimitadas por limiares constantes $S_1, \ldots, S_6$, e que permite definir uma escala cardinal com base em informação ordinal (Braz, 2011, p. 20):

- C_1 – diferença de atratividade muito fraca: $C_1 = [S_1, S_2]$ *e* $S_1 = 0$;
- C_2 – diferença de atratividade muito fraca: $C_2 =]S_2, S_3]$;
- C_3 – diferença de atratividade muito fraca: $C_3 =]S_3, S_4]$;
- C_4 – diferença de atratividade muito fraca: $C_4 =]S_4, S_5]$;
- C_5 – diferença de atratividade muito fraca: $C_5 =]S_5, S_6]$;
- C_6 – diferença de atratividade muito fraca: $C_6 =]S_6, +++[$.

4.2.3. Estruturação

Nesta fase são atribuídos, para cada critério, um conjunto de descritores que procuram refletir todos os potenciais impactos associados às caraterísticas da ameaça e da própria infraestrutura (Godinho, 2014, p. 37). Estes descritores não são mais que as opções de escolha que o decisor tem associada à análise de cada um dos 17 critérios que concorrem para calcular a probabilidade de sucesso de um ataque e, consequentemente, determinar o grau de vulnerabilidade da IC.

Assim, os critérios de avaliação são estruturados, de acordo com o problema estudado e o modelo de análise da vulnerabilidade. Os critérios são agrupados em pontos de vista fundamentais[5] (PVF) de acordo com a forma de análise e as áreas de preocupação (Godinho, 2014, p. 38) para o analista e para o decisor: a ameaça, o valor da infraestrutura para o utilizador e o valor da infraestrutura para o agressor.

[5] Um PVF consiste na representação de um valor que, à luz dos atores, é considerado importante pelo que cabe explicitamente num processo de avaliação das ações ou alternativas pertencentes a um conjunto de soluções potenciais para o problema (Bana e Costa, 1992; Thomaz, 2005, cit. por Godinho, 2014, p. 39).

Após a identificação dos PVF, atribuem-se, a cada PVF, os respetivos critérios, permitindo, assim, a construção de uma Árvore de Valor para estruturação da base do problema (Thomaz, 2005, cit. por Godinho, 2014, p. 39).

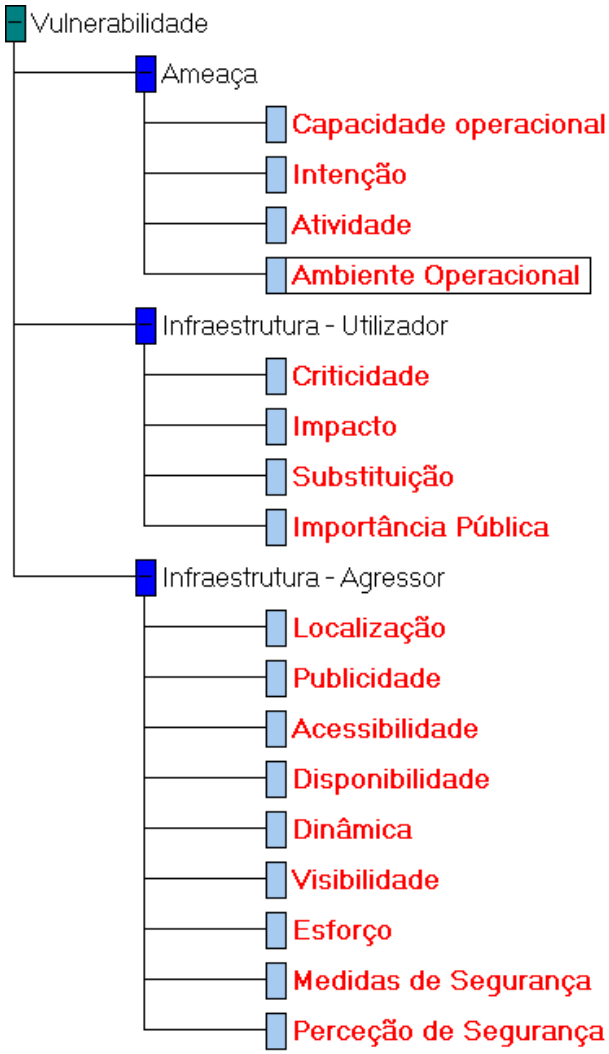


Figura 13 – Processo de estruturação e avaliação dos pesos dos critérios através do Macbeth.

Fonte: (Almeida, 2011, p. 56)

Organizados os PVF e os critérios, procede-se à definição, para cada critério, dos descritores de impacto ou dos níveis de performance, ou seja, das opções resultantes das caraterísticas de cada um dos critérios mediante a análise feita. Estes níveis de performance correspondem aos apresentados nas tabelas 5 a 8 e 10 a 22.

É na definição dos níveis de performance que se faz a diferenciação entre um julgamento qualitativo ou quantitativo

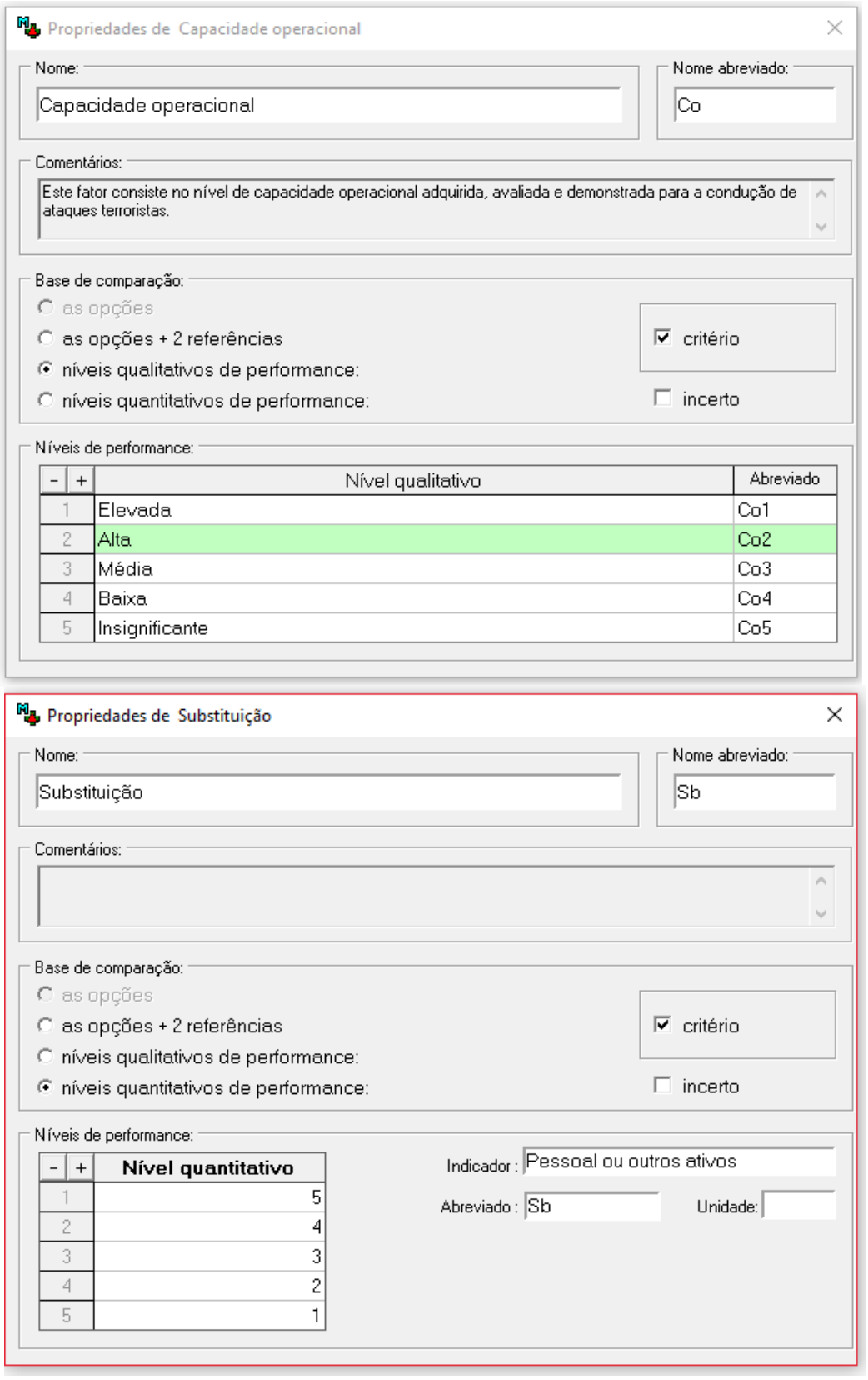


Figura 14 – Exemplo de dois critérios com a aplicação de níveis qualitativo e quantitativo de performance

Fonte: (Autor, 2017)

4.2.4. Avaliação

Nesta fase do processo são determinadas as funções de valor e os pesos.

A determinação de funções de valor, através do procedimento seguido pelo Macbeth, consiste na avaliação das diferenças de atratividade entre pares de níveis de performance em cada critério de avaliação (Almeida, 2011, p. 72). No caso de não haver diferença entre eles, a sua função de valor é "nula" (Bana e Costa et al., 2005). Nesta fase é pedido ao decisor que julgue qualitativamente as diferenças de atratividade, a partir das seis categorias semânticas apresentadas anteriormente: Muito Fraca, Fraca, Moderada, Forte, Muito Forte e Extrema.

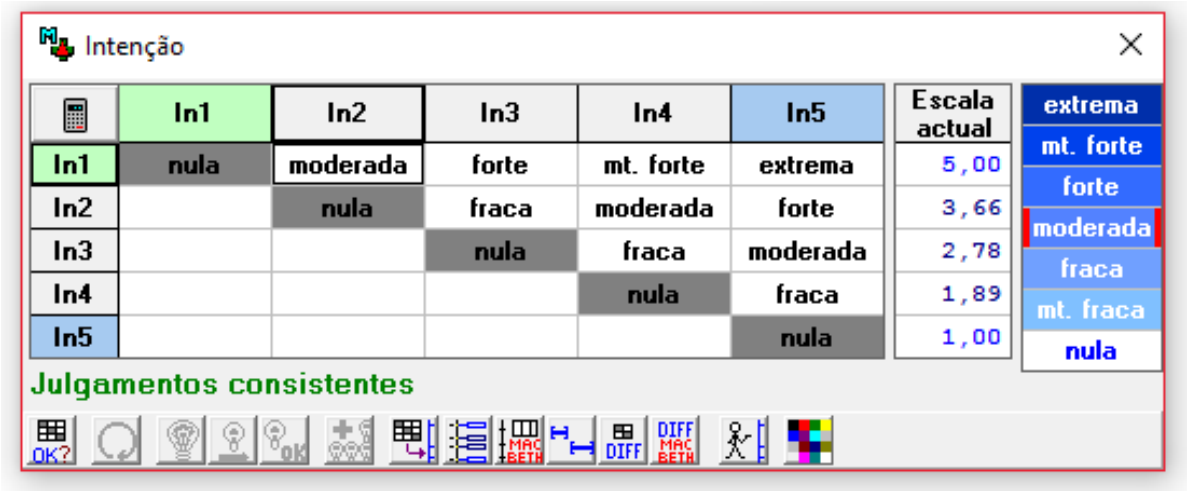


Figura 15 – Matriz triangular superior com diferenças de atratividade para o critério Intenção

Fonte: (Autor, 2017)

Após a matriz estar completa, consistente e validada pelo decisor, obtém-se as escalas termométricas (descritores qualitativos) e funções de valor (descritores quantitativos) para cada critério. A utilização destas escalas permite uma melhor perceção das pontuações obtidas nos diferentes níveis de performance (parâmetros) e das suas diferenças.

Com o software Macbeth é possível aos analistas e decisores ajustarem as proporções dos intervalos registados de cada escala de valor, no caso do decisor achar necessário, de acordo com a avaliação aos resultados obtidos (Bana e Costa et al., 2005 cit. por Almeida, 2011, p. 73).

A determinação dos pesos reflete a importância dos critérios de avaliação, sendo, para tal, necessário uma vez mais, a avaliação do valor dos julgamentos por parte do decisor. Os pesos dos critérios de avaliação são determinados através da avaliação que é feita à importância relativa que estes têm para o decisor (Bana e Costa et al., 2005 cit. por Almeida, 2011, p. 73).

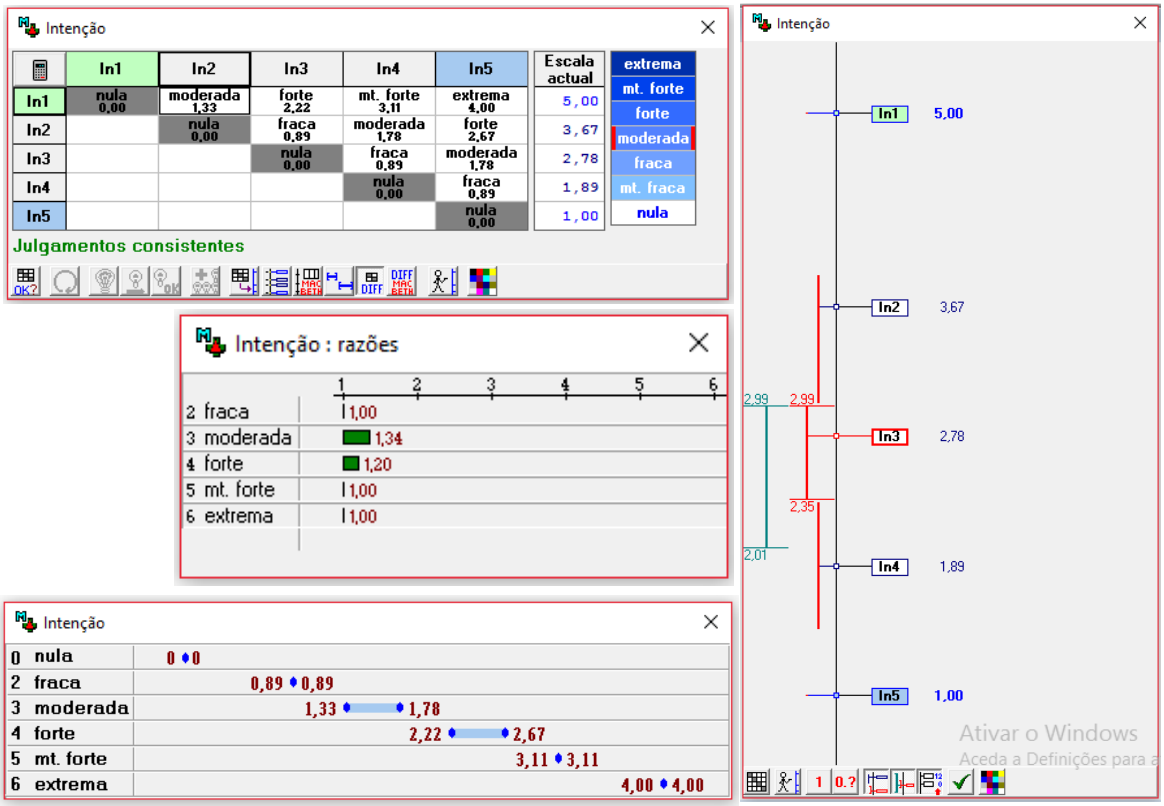


Figura 16 – Matriz de julgamento dos descritores de impacto para o critério Intenção, respetivas pontuações, escala termométrica e função de valor

Fonte: (Autor, 2017)

No final, os resultados obtidos a partir do software Macbeth, nomeadamente as funções de valor (descritivo quantitativo) e os pesos dos critérios, são introduzidos no modelo de análise da vulnerabilidade construído, substituindo os valores pré-definidos das tabelas 5 a 8 e 10 a 22 pelos novos valores.

4.3. Teste e validação do modelo

Qualquer metodologia, processo ou método, antes de ser proposto, deve ser testado e validado.

Para validar o modelo de análise da vulnerabilidade de uma IC descrito nos subcapítulos anteriores, aplicou-se o modelo a um cenário criado para o efeito, de forma a testar a aplicabilidade do processo e demostrar o seu funcionamento.

4.3.1. Cenário

Para a criação do cenário teve-se em consideração questões associadas à suscetibilidade e à confidencialidade do tema, das infraestruturas e dos resultados. Assim, para não colocar em causa estes dois fatores, optou-se por criar um cenário baseado numa realidade passada e cuja análise e respetivos resultados não terão qualquer relevância operacional, temporal ou espacial.

Efetuou-se a análise da vulnerabilidade do aquartelamento militar "UBIQUE CAMP", utilizado pela Unidade de Engenharia do Exército Português ao serviço da *United Nation Interim Force In Lebanon* (UNIFIL) entre 2006 e 2012.

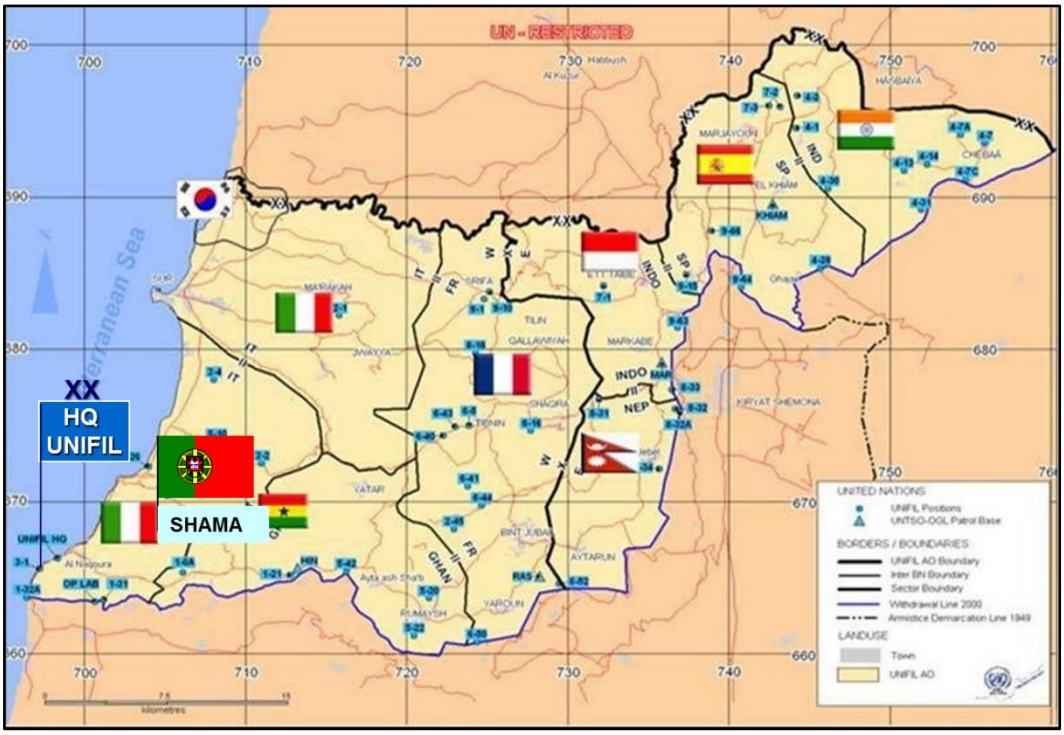


Figura 17 – Área de Operações UNIFIL – Localização do UBIQUE CAMP

Fonte: (EPE, 2012)

O UBIQUE CAMP é um aquartelamento, situado em Shama, Líbano, constituído por instalações permanentes, construídas em betão e alvenaria e semipermanentes, constituídas por estruturas contentorizadas tipo CO.RI.MEC, com uma área de 30.000 m2 (EPE, 2012).

Para a caraterização do aquartelamento foram utilizados dados dos relatórios das missões das Unidades de Engenharia e do livro "Ao Serviço da Paz. A Engenharia Militar Portuguesa na UNIFIL" (EPE, 2012). No Apêndice G apresenta-se uma breve caraterização do aquartelamento.

A ameaça presente no teatro de operações está diretamente relacionada com o Hezbollah. O Hezbollah é uma organização política e militar dos muçulmanos xiitas do Líbano, criada em 1982 no contexto da invasão de Israel ao sul do Líbano. Devido aos seus ataques contra civis israelitas dentro e fora de Israel e do seu apoio ideológico a outras organizações terroristas como o Hamas, é considerado pelos Estados Unidos, Israel e alguns estados ocidentais como uma organização terrorista (CSMIE, 2011).

Para a caraterização da ameaça foram utilizados dados dos relatórios das missões das Unidades de Engenharia e dos brífingues de atualização das Informações fornecidos pelo

Centro de Segurança Militar e de Informações do Exército (CSMIE, 2011). No Apêndice H apresenta-se uma breve caraterização da ameaça.

4.3.2. Aplicação e resultados

Ao cenário descrito aplicou-se o modelo de análise de vulnerabilidade construído, assente num processo algorítmico e complementado por uma base teórica relativa à avaliação da ameaça e à avaliação da infraestrutura descrita nos capítulos 2. e 3. e pelas tabelas e folhas de cálculo auxiliares apresentadas nos apêndices B a F.

Para melhor demonstrar o teste ao processo, encontra-se, no Apêndice I, um resumo da aplicação do modelo de análise de Vulnerabilidade, com o preenchimento das tabelas auxiliares.

Com base no cenário, começou-se por identificar o(s) tipo(s) de agressor(es), o(s) tipo(s) de táticas e técnicas a utilizar e o(s) tipo(s) de engenhos explosivos. Da análise feita, considerou-se o Hezbollah um grupo terrorista patrocinado por um estado, com o passado a demonstrar a utilização de táticas assentes em explosivos lançados manualmente, principalmente usando o colete com explosivos, e em veículos-bomba em movimento, através de veículos *"minivan"* com explosivos. Com esta informação, preencheu-se a Tabela 23 (conforme apresentado no Apêndice I). Por limitação de espaço, fez-se apenas o estudo para a utilização de um veículo-bomba em movimento tipo "*minivan*".

Após a identificação, caraterizou-se e analisou-se o grupo Hezbollah de acordo com os fatores Capacidade Operacional, Intenção, Atividade e Ambiente operacional, preenchendo-se a Tabela 24 e cujo resumo se apresenta no Apêndice I.

Após a análise, fez-se a sua categorização, por fatores, aplicando os pesos definidos nas tabelas 5 a 8. Para refinar estes pesos avaliando as opções em julgamentos qualitativos sobre diferenças de atratividade entre os fatores, aplicou-se o método Macbeth, substituindo-se os pesos iniciais pelos pesos obtidos através deste método, conforme se demonstra no exemplo abaixo aplicado ao fator Capacidade Operacional.

Para classificar a ameaça, integraram-se estes novos pesos na expressão matemática (3) obtendo-se uma pontuação para A=14,05, a qual, pela Tabela 3, representa uma ameaça "ALTA".

Sendo a IC em estudo um aquartelamento militar num TO, considerou-se como função principal a atividade militar.

Tendo em conta a limitação de espaço, considerou-se, para análise, o paiol do aquartelamento, como ativo principal associado às armas, munições e explosivos.

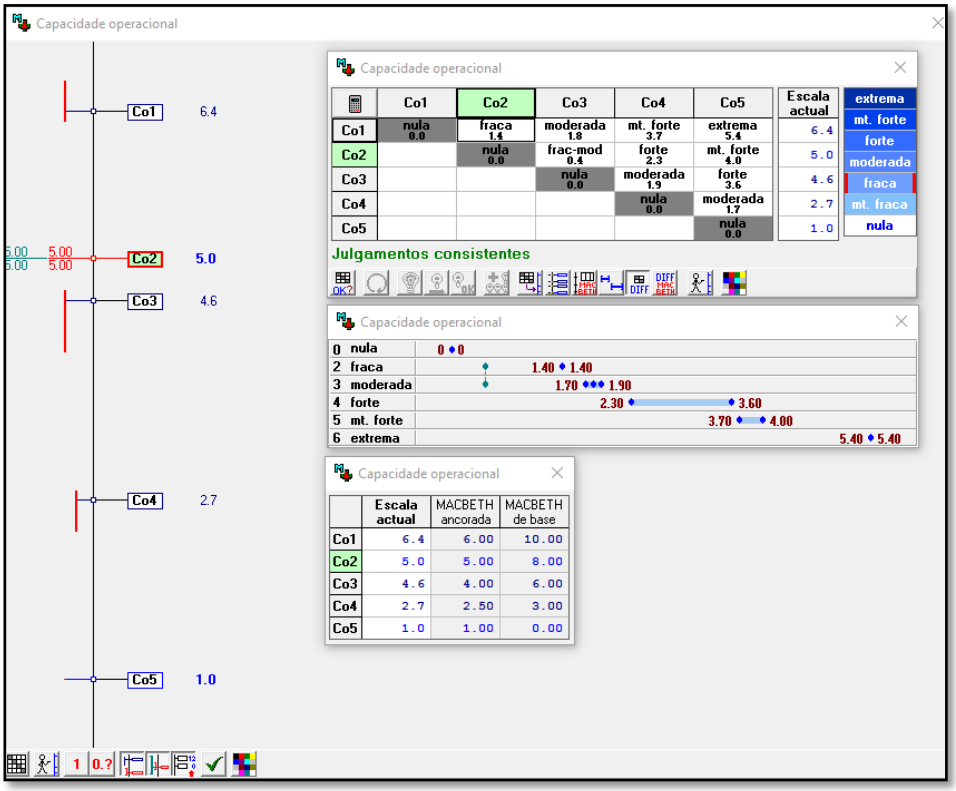


Figura 18 – Exemplo da aplicação do método Macbeth na ponderação dos pesos do fator Capacidade Operacional

Fonte: (Autor, 2017)

Procedeu-se, de seguida, à caraterização da IC, tendo presente exclusivamente a proteção do ativo principal, preenchendo-se a Tabela 25, cujo resumo se encontra no Apêndice I. Com base nesta caraterização, analisou-se a IC e o ativo principal, assente nos fatores associados ao valor da infraestrutura para o utilizador e para o agressor, preenchendo-se a Tabela 26, como demonstrado no Apêndice I.

Tal como se fez para a classificação da ameaça, também nesta fase se atribuíram os pesos para cada fator, tendo estes sido ajustados mediante aplicação do método Macbeth. Com estes pesos e aplicando as expressões matemáticas (5) e (7), obtiveram-se os valores da IC para o utilizador, $V_{IC/Ut}$ = 0,83, e da IC para o agressor, $V_{IC/Ag}$ = 0,52.

Por fim, aplicou-se a expressão matemática (9) para se obter o valor, em percentagem, da probabilidade de sucesso do ataque, face à ameaça contra o ativo principal: V = 0,59. Este valor, após aplicação da Tabela 4, permitiu determinar, para o ativo principal da IC, um nível de vulnerabilidade MÉDIO.

Para facilitar os cálculos acessórios foi-se preenchendo ao longo do processo, como demonstrado na Figura 19, a Tabela 27, a qual permitiu extrair os resultados parciais e final e converter os mesmos no respetivo grau de vulnerabilidade.

Tabela 27

Analista: António Ferreira

Data: 30 de maio de 2017

Designação da IC: Aquartelamento militar da UnEng/UNIFIL

Função nuclear da IC: Atividades militares

Ativo crítico da IC: Paiol (armas, munições e explosivos)

Agressor		Tática e técnica	Capacidade Operacional (Tab. 05)	Intenção (Tab. 06)	Atividade (Tab. 07)	Ambiente Operacional (Tab. 08)	Nível da Ameaça (A) (Tab. 03)	Criticidade (Tab. 10)	Impacto (Tab. 11)	Substituição (Tab. 12)	Importância Política (Tab. 13)	Valor da infraestrutura para o utilizador (VIC/Ut)	Localização (Tab. 14)	Publicidade (Tab. 15)	Acessibilidade (Tab. 16)	Disponibilidade (Tab. 17)	Dinâmica (Tab.18)	Visibilidade (Tab. 19)	Esforço (Tab. 20)	Medidas de segurança (Tab. 21)	Perceção de Sucesso (Tab. 22)	Valor da infraestrutura para o agressor (V IC/Ag)	Sum Fatores	Probabilidade de sucesso de um ataque
			Fatores																					
			Ameaça					Valor da IC para o utilizador					C para o agressor											
☐	Terrorista doméstico	Explosivos lançados manualmente																						
		Veículo-bomba estacionado																						
		Veículo-bomba em movimento																						
☐	Terrorista internacional	Explosivos lançados manualmente																						
		Veículo-bomba estacionado																						
		Veículo-bomba em movimento																						
X	Terrorista patrocinado por Estado	Explosivos lançados manualmente																						
		Veículo-bomba estacionado																						
		X Veículo-bomba em movimento	4,60	1,89	4,27	3,29	Alto	5,00	3,67	4,00	3,86	0,83	3,86	3,00	2,60	2,00	5,00	9,00	2,07	12,00	12,00	0,52	82,11	0,59

Passo 2

Se nível de ameaça for considerado "MUITO BAIXO" então, deve ser logo considerado, à partida, um grau de vulnerabilidade "MUITO BAIXO"

Passo 4

Se VIC/Ut for inferior a 0,3 a IC é considerada de reduzido valor para o utilizador, permitindo-se dispensar a consequente análise de vulnerabilidade

Passo 5

Passo 6

Tabela 4

Grau de Vulnerabilidade	Probabilidade				
	<= 0,3	0,31 - 0,50	0,51 - 0,74	0,75 - 0,89	0,90 - 1
Elevado					X
Alto				X	
Médio			X		
Baixo		X			
Muito Baixo	X				

Figura 19 – Preenchimento da Tabela 27 e aplicação da Tabela 4 para obtenção do grau de Vulnerabilidade

Fonte: (Autor, 2017)

4.3.3. Correção e validação

Os resultados obtidos permitem demonstrar a funcionalidade e aplicabilidade do modelo de análise da vulnerabilidade construído. Mais importante que os resultados obtidos, está o processo, ao qual, após ter sido aplicado a um cenário criado para o efeito, se identificaram inconformidades e lacunas, e se procederam às correções necessárias para tornar o modelo aplicável e funcional.

Durante o teste foram-se integrando e ajustando as ferramentas de apoio às várias etapas do processo, nomeadamente, através da criação de tabelas padronizadas e pré-orientadas para as ações de caraterização e de análise, cuja informação aí reunida sustenta a classificação obtida para as dimensões de análise Ameaça e Infraestrutura.

Um problema que se verificou durante o teste está relacionado com a articulação do modelo de análise com o método Macbeth. Se o modelo de análise da vulnerabilidade é intuitivo e facilmente aplicado, o método Macbeth, mesmo com a utilização do seu software, acarreta a necessidade de um grande conhecimento do seu funcionamento e da sua aplicação, bem como a necessidade de transpor dados entre eles, o que se verificou moroso. Ainda assim, os resultados obtidos demonstram que esta é uma ferramenta viável para visualizar o impacto que têm os pesos atribuídos aos fatores e ajustá-los aos objetivos pretendidos.

O modelo de análise da vulnerabilidade construído pode-se considerar parcialmente validado. Validado porque demonstrou-se aplicável e funcional, parcialmente porque o teste foi efetuado pelo próprio investigador perante um cenário criado para o efeito.

4.4. **Síntese conclusiva**

Este ultimo capítulo constitui a parte fulcral da nossa investigação e no qual se procurou uma forma de aplicação das caraterísticas associadas à ameaça e à própria infraestrutura, num método algorítmico, que permita determinar a vulnerabilidade de uma IC, integrando um modelo de apoio à decisão multicritério, respondendo assim à QD3.

Após o estudo das duas dimensões que compõem o conceito de vulnerabilidade, definiu-se um modelo, assente num processo algorítmico, que transforma julgamentos qualitativos, associados às caraterísticas da ameaça e da infraestrutura, num valor, numérico e quantificável, representativo do grau de vulnerabilidade da IC.

Este processo assenta em três tarefas primárias: caraterizar, analisar e avaliar.

Caraterizar, olhando para as dimensões ameaça e infraestrutura e identificar nelas os aspetos e caraterísticas que contribuem para determinar a vulnerabilidade; analisar essas

caraterísticas, mediante um conjunto de fatores; e por fim, avaliar a vulnerabilidade através da integração dos fatores analisados mediante a aplicação de fórmulas matemáticas.

Como qualquer processo de apoio à tomada de decisão, também um modelo de análise da vulnerabilidade de uma IC deve ter em conta fatores intrínsecos à experiência, ao conhecimento e à perceção do decisor, de forma a que este possa manusear o processo para ir de encontro às suas necessidades e exigências. No entanto, este manuseamento deve ser controlado de forma a não desvirtuar o processo. Surgiu assim a necessidade de integrar no processo algorítmico, um método de apoio à decisão multicritério, tendo-se verificado que o método Macbeth é um excelente auxiliar para adequar os pesos de ponderação a atribuir aos fatores de análise.

Por fim, demonstrou-se a aplicabilidade e funcionalidade do modelo criado, testando-o num cenário criado para o efeito, validando a sua aplicabilidade e funcionalidade como ferramenta de análise e de apoio à decisão.

Conclusões

As conclusões são o culminar, não só de um trabalho escrito, mas de uma investigação longa no tempo e nos objetivos.

A presente investigação teve por finalidade discutir o conceito de vulnerabilidade e as metodologias e processos para a sua análise em infraestruturas críticas (em território nacional ou expedicionárias) face à ameaça terrorista, com particular foco no desenvolvimento de uma metodologia de análise, explorando um modelo de apoio à decisão multicritério, de forma a ser possível limitar os riscos na máxima extensão possível. Perante esta finalidade, definiu-se como objetivo geral da investigação desenvolver uma metodologia de análise da vulnerabilidade de infraestruturas críticas.

As grandes linhas do procedimento metodológico de investigação assentaram na análise documental da legislação europeia e nacional relativa à proteção de IC, da doutrina de referência e, com grande enfoque, de manuais técnicos de instituições norte-americanas alusivos à temática em estudo. Os resultados foram obtidos através do modelo de análise que foi desenvolvido, assente no conceito de vulnerabilidade e nas suas dimensões Ameaça e Infraestrutura, as quais foram categorizadas e avaliadas, partindo da caraterização e análise das suas variáveis. Com estas, procurou-se transformar o conceito teórico de vulnerabilidade numa expressão algébrica, através da modelação de um algoritmo, no qual se integrou um método de apoio à decisão multicritério. Ao longo do modelo de análise e dos capítulos do presente trabalho foram-se respondendo às QD e, por fim, à QC.

A proteção das IC é um tema cada vez mais relevante, sendo o seu maior objetivo identificar e implementar as medidas necessárias para reduzir a sua vulnerabilidade e, consequentemente, diminuir os riscos associados.

O grau de vulnerabilidade de uma IC consiste na combinação da sua atratividade como alvo face a um ataque terrorista e o nível de dissuasão ou de defesa garantido pelas contramedidas ou medidas de proteção existentes.

O nível de ameaça é parte integrante de qualquer processo de análise da vulnerabilidade e, consequentemente, da análise do risco e é utilizada para determinar, caraterizar e quantificar os danos causados por um terrorista (ou grupo terrorista) de acordo com as suas táticas e tipo de engenhos explosivos.

A caraterização da ameaça tem como ponto de partida a identificação do tipo de agressor, podendo este estar associado ao terrorismo doméstico, ao terrorismo internacional ou ao terrorismo patrocinado por estados. O tipo de terrorismo poderá indiciar um conjunto

de caraterísticas relacionadas com as táticas e técnicas usadas e o tipo de engenho explosivo a empregar, contribuindo assim para tornar uma infraestrutura mais ou menos vulnerável.

As táticas e técnicas usadas por um terrorista ou grupo terroristas no ataque a uma IC podem consistir em engenhos explosivos lançados manualmente, o uso de veículos-bomba em movimento contra uma infraestrutura ou o uso de veículos-bomba estacionados junto a esta. A escolha de uma determinada tática resulta de dois fatores: das próprias caraterísticas e capacidades do agressor e da tipologia e caraterísticas da IC.

Quanto ao tipo de engenho explosivo empregue, este está diretamente relacionado com a tática usada, afetando o grau de vulnerabilidade pela maior ou menor probabilidade de provocar danos na IC, ou seja, quanto maior for a quantidade de explosivo, maior a probabilidade de causar danos.

Tendo por base a caraterização do tipo de agressor, das táticas e técnicas usadas e dos engenhos empregues, a ameaça terrorista afeta o grau de vulnerabilidade considerando a probabilidade de ocorrência de um ataque terrorista associada à capacidade operacional adquirida, avaliada e demonstrada, à intenção, à atividade desenvolvida e ao ambiente operacional.

A análise destes fatores permite categorizar a ameaça terrorista, de muito baixa a elevada, afetando o grau de vulnerabilidade, pois quanto maior for o nível de ameaça maior o grau de vulnerabilidade da IC.

O capítulo dois demonstra, assim, em que medida a ameaça terrorista afeta a vulnerabilidade de uma IC, respondendo à QD1.

Para além da ameaça terrorista, o grau de vulnerabilidade está diretamente associado às caraterísticas de uma IC.

Primeiro importa identificar e caraterizar os perímetros de segurança, os quais possuem um conjunto de caraterísticas que afetam a segurança da infraestrutura, quer minimizando ou exponenciando os efeitos de um ataque terrorista, podendo-se constituírem como *enablers* ou como obstáculos à ação de um terrorista.

É também fundamental identificar as funções nucleares da infraestrutura e como estas são importantes para o seu funcionamento, para o utilizador e para o agressor. Dadas as caraterísticas funcionais ou a dimensão da infraestrutura, pode-se verificar que a vulnerabilidade de uma IC está unicamente relacionada, não com a infraestrutura como um todo, mas com os ativos críticos. Assim a análise da vulnerabilidade da IC recairá apenas na identificação, caraterização e análise desses mesmos ativos.

Mas, acima de tudo, importa identificar e analisar os fatores que permitem compreender o valor que a infraestrutura ou um determinado ativo crítico têm para o utilizador, ou seja, a consequência que terá se os ativos forem comprometidos pelo terrorista, e o valor que tem como alvo para o agressor.

Com base nas caraterísticas da IC devem-se analisar a criticidade para a missão, o impacto, a facilidade com que o ativo pode ser substituído ou a infraestrutura retomar a atividade, a importância pública, localização, a publicidade, a acessibilidade, disponibilidade, dinâmica, visibilidade, esforço, medidas de segurança e a perceção de sucesso por parte do agressor.

Demonstrou-se, no capítulo três, que todos estes fatores e as probabilidades associadas contribuem para determinar o grau de vulnerabilidade de uma IC e identificar em quais se pode intervir, através de medidas de mitigação, para reduzir esse mesmo grau de vulnerabilidade. Responde-se, assim, à QD2.

No quarto capítulo procurou-se uma forma de aplicação das caraterísticas associadas à ameaça e à própria infraestrutura num método algorítmico que permita determinar a vulnerabilidade de uma IC, integrando um modelo de apoio à decisão multicritério.

Revisitando o conceito de vulnerabilidade e as suas dimensões, verifica-se que a vulnerabilidade de uma IC consiste na probabilidade de sucesso de um ataque, por parte de uma ameaça - devidamente identificada, caraterizada, analisada e categorizada – contra uma infraestrutura com determinadas caraterísticas que definem o seu valor para o utilizador e para o agressor. Posto isto, conclui-se que a análise da vulnerabilidade consiste na medição da probabilidade de sucesso do ataque através da integração de todos os fatores associados à ameaça e às caraterísticas da infraestrutura: capacidade operacional, intenção, atividade, ambiente operacional, criticidade, impacto, substituição, importância política, localização, publicidade, acessibilidade, disponibilidade, dinâmica, visibilidade, esforço, medidas de segurança e perceção de sucesso.

A criação de um modelo algorítmico, complementado por ferramentas de registo e de cálculo, permite, através de um processo racional, científico e algébrico, transformar uma análise qualitativa de fatores, em valores mensuráveis, quantificáveis e cuja operação algébrica os integra num resultado final que expressa, em valor de percentagem, a probabilidade de sucesso do ataque, ou seja, o grau de vulnerabilidade de uma IC perante uma ameaça terrorista.

Como qualquer processo de análise e, consequentemente, de tomada de decisão, o fator humano é preponderante para a aplicação de qualquer modelo algorítmico, principalmente quando surgem, neste processo, julgamentos subjetivos e dependentes das aptidões intelectuais e emocionais do analista e do decisor. A aplicação de um modelo de apoio à decisão multicritério, que permita ao decisor maniatar os pesos dos critérios usados na avaliação da vulnerabilidade, de forma a aproximar a sua observação qualitativa do problema a uma solução quantitativa, é, sem qualquer dúvida, uma mais-valia para este processo.

Com o método algorítmico de análise da vulnerabilidade de uma IC, no qual se integrou uma metodologia de apoio à decisão multicritério, atingiu-se o OE3, respondendo à QD3.

Dada as respostas às QD, estamos em condições de materializar o fim da investigação, respondendo à QC: como determinar a vulnerabilidade de uma IC, aplicando uma metodologia que permita limitar os riscos na máxima extensão possível?

A resposta a esta questão é materializada propondo o modelo de análise de vulnerabilidade, construído, testado e validado no capítulo quatro. Para determinar a vulnerabilidade de uma IC é necessário aplicar uma metodologia, assente num algoritmo, sequencial, interativo, analítico e algébrico, que permita transformar julgamentos qualitativos em valores quantitativos passíveis de serem utilizados, matematicamente, para determinar, em percentagem, a probabilidade de sucesso de um ataque terrorista com recurso a engenhos explosivos contra uma IC.

O processo algorítmico deve ser sequencial, quer em termos das dimensões e das variáveis quer em termos de tarefas. Ou seja, trabalhar primeiro a dimensão ameaça e, só depois, a infraestrutura (pois o estudo desta é feito tendo em consideração os efeitos que a ameaça produz) e para cada uma delas deve ser feita a identificação, caraterização, análise e classificação ou categorização, por esta ordem. O processo deve ser interativo, de forma a permitir que o analista possa adaptar a análise dos fatores às perceções e preferências do decisor, para o qual contribui a integração, nesta metodologia, do método de apoio à decisão multicritério Macbeth. O processo deve ser analítico, assente em fatores de análise pré-definidos e num padrão comum. O processo deve ser algébrico, de forma a permitir quantificar numericamente a análise e sustentar numa base realista e objetiva, não subjetiva, a decisão a tomar sobre as medidas a adotar para redução da vulnerabilidade de uma IC.

Por limitação de tempo e de considerandos relativos à confidencialidade do estudo, não foi possível testar o modelo proposto através da sua aplicação real numa IC nacional.

Propõe-se, em futuras investigações, seja no âmbito do CEMC ou, preferencialmente, do mestrado em Ciências Militares – Segurança e Defesa, validar a aplicação do modelo proposto a uma IC nacional.

A análise da vulnerabilidade é um dos passos iniciais no processo de proteção de IC, ao qual se segue a análise de risco. Para dar sequência a este processo é importante criar também uma metodologia que permita efetuar a análise de risco de uma IC face a um ataque terrorista, incorporando custos e restrições. Face a isto propõe-se uma nova linha de investigação com a finalidade discutir o conceito de risco e as metodologias e processos para a sua avaliação em infraestruturas críticas (em território nacional ou expedicionárias) face à ameaça terrorista, com particular foco no desenvolvimento de uma metodologia de análise, de forma a ser possível limitar os mesmos na máxima extensão possível.

Bibliografia

Almeida, A., 2011. *Metodologia Multicritério de Identificação e Priorização de Infra-Estruturas Críticas*. Dissertação para a atribuição do Grau de Mestre em Engenharia e Gestão Industrial. Instituto Superior Técnico.

Atlas, R.I., 2008. *21st Century Security and CPTED - Designing for Critical Infrastructure Protection and Crime Prevention*. Florida: CRC Press.

Bana e Costa, C.A., De Corte, J. M., Vasnick, J.C., 2005. *On the mathematical foundations of MACBETH. Multiple Criteria Decision Analysis: The State of Art Surveys*. Springer, pp.409-442.

Bana e Costa, C., Angulo-Meza, L., Oliveira, M., 2013. *O método MACBETH e aplicação no Brasil*. Engevista, 15(1), abril, pp.3–27.

Bennett, B., 2007. *Understanding, Assessing and Responding to Terrorism. Protecting Critical Infrastructure and personnel*. New Jersey: John Wiley & Sons, Inc.

Braz, J., 2011. *O MacBeth como ferramenta MCDA para o Benchmarking de Aeroportos*. Dissertação para a obtenção do Grau de Mestre em Engenharia Aeronáutica. Universidade da Beira Interior.

Conceição, L., 2008. *Proteção e segurança de edifícios face a ataques terroristas*. Dissertação para a obtenção do Grau de Mestre em Engenharia Militar. Instituto Superior Técnico.

Conselho de Chefes de Estado-Maior, 2014. *Conceito Estratégico Militar*. Lisboa: Ministério da Defesa Nacional.

Conselho Europeu, 2008. Identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção (Diretiva 2008/114/CE de 8 de dezembro de 2008), Bruxelas: Jornal Oficial da União Europeia.

CSMIE, 2011. Caraterização do Teatro de Operações do Líbano. In *Brífingue de atualização das Informações no TO do Líbano*. Centro de Segurança Militar e de Informações do Exército. 10 e 11 de novembro de 2011. Lisboa: CSMIE.

EUROPOL, 2016. *European Union Terrorism Situation and Trend Report (TE-SAT) 2016*. The Hague: European Police Office.

EPE, 2012. Ao Serviço da Paz. A Engenharia Militar Portuguesa na UNIFIL. Tancos: Escola Prática de Engenharia

Exército Português, 2012. *PDE 3-00 Operações*. Lisboa.

FEMA, 2003. *FEMA 427 – Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks. Risk Management Series*. EUA: FEMA.

FEMA, 2005. *FEMA 452 - Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings. Risk Management Series*. EUA: FEMA.

FEMA, 2006. *FEMA 453 – Design Guidance for Shelters and Safe Rooms. Risk Management Series*. EUA: FEMA.

FEMA, 2011. *FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings. Buildings and Infrastructure Protection Series*. EUA: FEMA.

FEMA, 2012. *FEMA 428 Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings. Buildings and Infrastructure Protection Series*. EUA: FEMA.

Ferreira, H., 2016. *Identificação e Caraterização de Infraestruturas Críticas - uma metodologia*. Trabalho de Investigação Individual. Instituto Universitário Militar.

Godinho, J., 2014. *Avaliação do desempenho de pessoas numa IPSS: Desenvolvimento de um modelo funcional*. Dissertação para a atribuição do Grau de Mestre em Gestão de Recursos Humanos. Instituto Superior de Línguas e Administração de Leiria.

Gomes, G., s.d.. *Proteção de Infraestruturas e Segurança Física - PrInSeF. Minuta do Projeto de Investigação (documento de trabalho)*. s.l..

Grohoski, D., 1996. *A Systems Approach to Assessing the Vulnerabilities of the U.S. Domestic Sea Ports to Acts of Sabotage and Terrorism*. Paper submitted to the Department of Advanced Research Programs. Naval War College.

IESM, 2016. *Orientações Metodológicas para a elaboração de Trabalhos de Investigação*. 1.a ed. Lisboa: IESM.

Krauthammer, T., 2008. *Modern Protective Structures*. Florida: CRC Press.

Ministério da Defesa Nacional, 2011. Procedimentos de identificação e de protecção das infra -estruturas (DL n.º 62/2011), Lisboa: Diário da República.

Morgeson, J. et al, 2011. *Doctrinal Guidelines for Quantitative Vulnerability Assessments of Infrastructure – Related Risks*. Vol.1. Virginia: Institute for Defense Analyses.

Murray, A., Grubesic, T., 2007. Critical Infrastructure. Reliability and Vulnerability. Heidelberg: Springer.

NATO, 2007. *AJP 3-14. Allied Joint Doctrine for Force Protection*. Brussels: NSA

Oliveira, M., 2015. *A segurança das Infraestrututas Críticas em Portugal*. Dissertação com vista à obtenção do grau de Mestre em Direito e Segurança. Universidade Nova de Lisboa.

Pais, I. e Mendes, C., 2012. *Proteção de infraestruturas críticas: Reduzir vulnerabilidades, aumentar a resiliência*. PROCIV, (51), Jun.

ProCiv, 2016. [em linha] Disponível em: http://www.prociv.pt/pt-pt/riscosprev/infraestruturascriticas/Paginas/default.aspx [Acedido 9 Dez. 2016].

Renfroe, N.A. e Smith, J.L., 2016. *Threat / Vulnerability Assessments and Risk Analysis*. [em linha] WBDG Whole Building Design Guide. Disponível em: https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis?r=riskmanage [Acedido 9 Dez. 2016].

Segurança e Ciências Forenses, 2012. Protecção de Infra-Estruturas Críticas. [em linha] Segurança e Ciências Forenses. Disponível em: https://segurancaecienciasforenses.com/2012/03/04/proteccao-de-infra-estruturas-criticas-2/ [Acedido 9 Dez. 2016].

UK MoD, 2007. *Military Engineering. Volume IX. Force Protection Engineering*. Part 1. London: MoD.

US Army, 2007. *A Military Guide to Terrorism in the Twenty-First Century*. Fort Leavenworth: US Army TRADOC

US Army, 2009. *FM 3-37. Protection*. Washington D.C.: Headquarters Department of the Army.

US Army, 2012. *ADP 3-37. Protection*. Washington D.C.: Headquarters Department of the Army.

US DHS, 2009. *National Infrastructure Protection Plan*. EUA: DHS.

US DoD, 2004. *DoD Antiterrorism Handbook*. EUA: DoD

US DoD, 2008. *UFC 4-020-01 DoD Security Engineering Facilities Planning Manual*. EUA: DoD.

US DoD, 2012. *UFC 4-010-02 DoD Minimum Antiterrorism Standoff Distances for Buildings*. EUA: DoD.

US DoD, 2013. *UFC 4-010-01 DoD DoD Minimum Antiterrorism Standards For Buildings*. EUA: DoD.

US DoD, 2016. *UFC 4-023-03 Design of Buildings to resist progressive collapse*. 3ª Ed. EUA: DoD.

Apêndice A — Modelo de análise

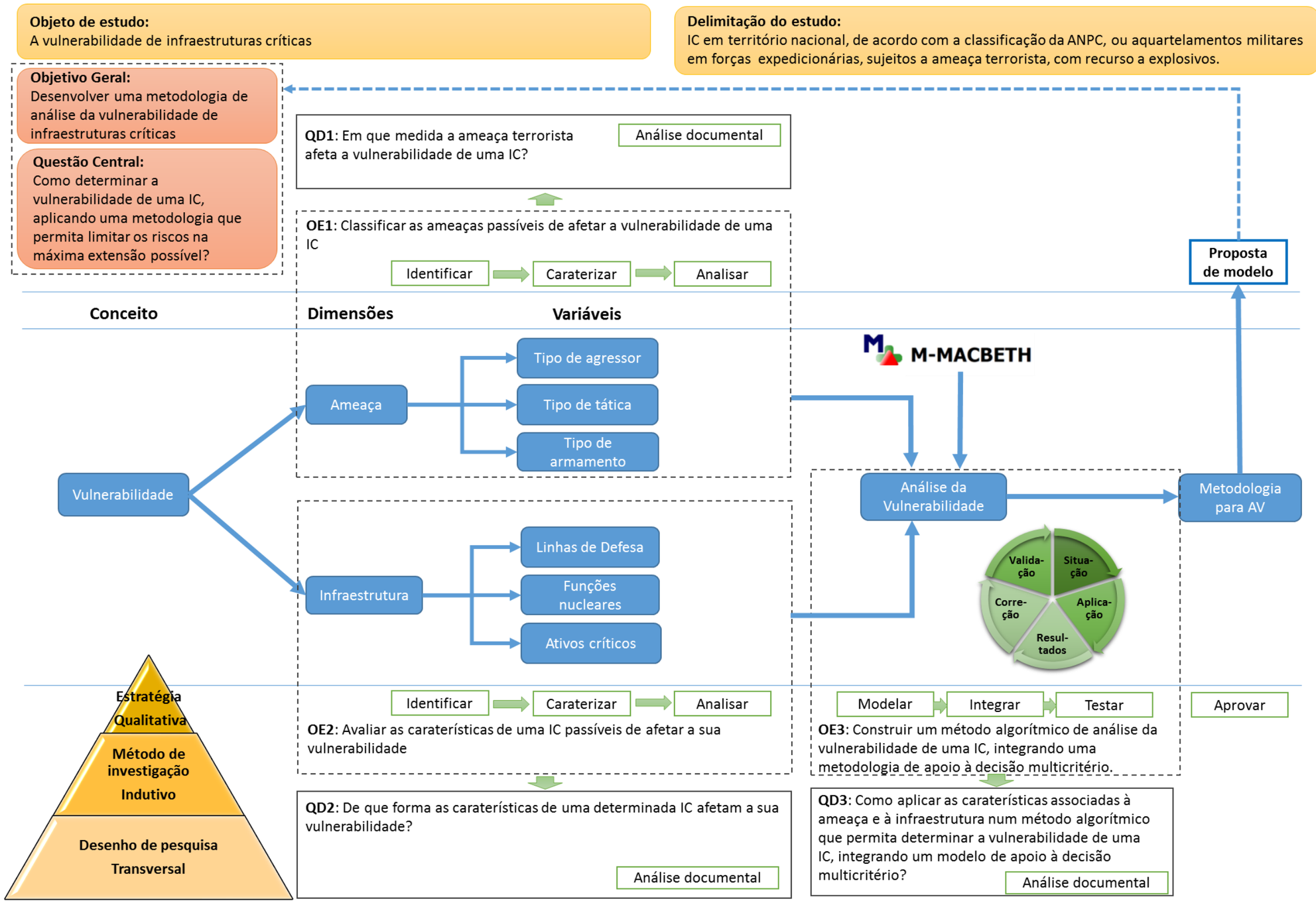


Figura 20 – Modelo de análise.

Fonte: (Autor, 2017)

Apêndice B — Tabelas para categorização da ameaça

Tabela 5 – Capacidade operacional

Capacidade operacional	Peso
Inexistente	0
Insignificante	1
Mínima	2
Média	3
Alta	4
Extrema	5

Fonte: Adaptado de (US DoD, 2008, p. 3-33)

Tabela 6 – Intenção

Intenção	Peso
Histórico inexistente	1
Ideologia anti-Portugal, mas sem histórico de ataques diretos	2
Ideologia anti-Portugal, com histórico de ataques fora do país	3
Ataques recentes contra interesses portugueses, no exterior	4
Ataques recentes contra interesses portugueses, em território nacional	5

Fonte: Adaptado de (US DoD, 2008, p. 3-33)

Tabela 7 – Atividade

Atividade	Peso
Inexistente	0
Presente mas inativo	1
Atividades de recrutamento e de angariação de fundos	2
Incidentes suspeitos ou suspeita de atividades de vigilância	3
Atividades identificadas (operacionais ou logísticas)	4
Ataque a alvos do país	5

Fonte: Adaptado de (US DoD, 2008, p. 3-34)

Tabela 8 – Ambiente operacional

Ambiente operacional	Peso
Favorece o país ou nação hospedeira	1
Neutro	3
Favorece o terrorista ou grupo terrorista	5

Fonte: Adaptado de (US DoD, 2008, p. 3-34)

Apêndice C — Tabela para identificação das funções e ativos principais de uma IC

Tabela 9 – Funções e ativos principais de uma IC

Infraestrutura Crítica		Funções																					Ativos													
Setor	Subsetor	Política	Administrativa	Económica	Financeira	Jurídica	Sociais	Segurança	Militares	Proteção e Socorro	Comerciais	Energia	Produção	Extração	Armazenamento	Distribuição	Educação, Formação e Treino	Investigação	Gestão da Informação	Comunicação	Trasnportes	Saúde	(...)	Pessoas	Aeronaves	Embarcações	Viaturas	Combustíveis e Lubrificantes	Armas, munições e explosivos	Equipamentos e material médico, medicamentos	Equipamentos industriais	Sistemas/redes energéticas	Sistemas de comunicação, computadores e redes	Informação	Bens de elevado valor financeiro	(...)
Órgãos de Soberania	Presidência da República	X	X				X																	X										X		
	Assembleia da República	X																	X					X										X		
	Governo	X	X				X												X					X										X		
	Tribunais		X			X													X					X										X		
Ministérios	Ministérios	X	X	X	X	X	X										X		X					X										X		
Administração Pública	Administração Pública	X	X	X	X	X	X										X		X					X										X	X	
Segurança	Serviços de Segurança		X					X		X									X					X										X		
	Forças de Segurança		X				X	X											X					X										X		
	Polícia Judiciária							X											X					X										X		
	Serviços de Informções							X											X					X										X		
Defesa	Forças Armadas								X	X									X					X	X	X	X	X	X					X		
Proteção Civil	Proteção Civil									X														X												
Comércio	Comércio										X				X	X								X											X	
Comunicações	Comunicações de Dados e Internet																		X	X												X	X		
	Comunicações Móveis																			X												X			
	Rede Fixa de Comunicações																			X												X			
	Comunicações Satélite																			X												X			
	Serviços Postais																			X												X			
Media	Media																		X	X												X	X		
Energia	Combustíveis											X	X	X	X	X											X	X				X			
	Energia elétrica											X	X	X	X	X												X				X			
	Gás natural											X	X	X	X	X											X	X				X			
Indústria	Indústria Alimentação, Bebidas e Tabaco												X		X	X															X				
	Indústria Madeira, Cortiça e Mobiliário													X	X	X															X				
	Indústria de Papel												X		X	X															X				
	Indústria dos Minerais não Metálicos													X	X	X															X				
	Indústria e Comércio de Automóvel												X		X	X															X				
	Indústria Elétrica e Eletrónica												X		X	X															X				
	Indústria Extrativa													X															X		X				
	Indústria Farmacêutica												X		X	X														X	X				
	Indústria Metalúrgica e Metalomecânica												X		X	X															X				
	Indústria Química												X		X	X															X				
	Indústria												X	X	X	X															X				
Serviços Financeiros	Serviços Financeiros	X		X	X														X													X	X	X	X	
Transportes	Transportes Aéreos																			X	X				X				X							
	Transportes Ferroviários																			X								X	X							
	Transportes Marítimos																			X						X			X							
	Transportes Fluviais																			X						X			X							
	Transportes Rodoviários																			X								X	X							
Água	Água												X		X	X															X	X				
Alimentação	Alimentação												X		X	X												X				X				
Ambiente	Ambiente						X																													
Saúde	Saúde						X															X								X		X	X	X		

Fonte: (Autor, 2017)

Apêndice D — Tabelas para cálculo do valor da IC para o utilizador

Tabela 10 – Criticidade

Criticidade	Peso
A perda, destruição ou uso indevido da infraestrutura ou do ativo não terá efeitos significantes na sua capacidade operacional, produtos ou serviços	0
A perda, destruição ou uso indevido da infraestrutura ou do ativo resultará na interrupção da sua capacidade operacional ao fim de um mês ou na redução de 10% dos seus produtos ou serviços	1
A perda, destruição ou uso indevido da infraestrutura ou do ativo resultará na interrupção da sua capacidade operacional ao fim de duas semanas ou na redução de 25% dos seus produtos ou serviços	2
A perda, destruição ou uso indevido da infraestrutura ou do ativo resultará na interrupção da sua capacidade operacional ao fim de uma semana ou na redução de 50% dos seus produtos ou serviços	3
A perda, destruição ou uso indevido da infraestrutura ou do ativo resultará na interrupção da sua capacidade operacional ao fim de um dia ou na redução de 75% dos seus produtos ou serviços	4
A perda, destruição ou uso indevido da infraestrutura ou do ativo resultará na interrupção imediata da sua capacidade operacional. A infraestrutura não cumpre a sua função	5

Fonte: Adaptado de (US DoD, 2008, p. 3-13))

Tabela 11 – Impacto

Impacto	Peso
A perda, destruição ou uso indevido da infraestrutura ou do ativo não terá impacto nacional ou regional	1
A perda, destruição ou uso indevido da infraestrutura ou do ativo terá impacto local, afetando apenas o normal funcionamento da infraestrutura	2
A perda, destruição ou uso indevido da infraestrutura ou do ativo terá impacto regional, afetando o sistema associado à infraestrutura	3
A perda, destruição ou uso indevido da infraestrutura ou do ativo terá impacto nacional, afetando o sistema associado à infraestrutura	4
A perda, destruição ou uso indevido da infraestrutura ou do ativo terá impacto nacional, afetando outros sistemas para além do sistema associado à infraestrutura (sistema económico, financeiro, político, etc)	5

Fonte: Adaptado de (US DoD, 2008, p. 3-14))

Tabela 12 – Substituição

	Substituição	Peso
Pessoal crítico para a missão	Existe pessoal imediatamente disponível no local para assumir as funções das baixas resultantes do ataque	1
	Pessoal transferido de outras componentes na infraestrutura para assumir as funções das baixas resultantes do ataque	2
	Pessoal transferido de outra infraestrutura para assumir as funções das baixas resultantes do ataque	3
	Necessidade de dotar o pessoal de preparação durante um período de tempo para assumir as funções das baixas resultantes do ataque	4
	Substituição irrealista devido à elevada especificidade e especialização das funções a assumir	5
Outros ativos	O ativo pode ser substituído ou a infraestrutura retomar a operação em menos de 24 horas	0
	O ativo pode ser substituído ou a infraestrutura retomar a operação entre 24 horas e 72 horas	1
	O ativo pode ser substituído ou a infraestrutura retomar a operação entre 72 horas e uma semana	2
	O ativo pode ser substituído ou a infraestrutura retomar a operação entre uma semana e um mês	3
	O ativo pode ser substituído ou a infraestrutura retomar a operação entre um e seis meses	4
	A substituição do ativo ou o retomar da operação requer mais de seis meses	5

Fonte: Adaptado de (US DoD, 2008, p. 3-15))

Tabela 13 – Importância pública

Importância Pública	Peso
Negligenciável: não é espectável a atenção por parte dos OCS	1
Mínima: a atenção dos OCS limita-se aos OCS locais	3
Moderada: a atenção dos OCS estende-se aos OCS nacionais	4
Alta: a atenção dos OCS estende-se aos OCS internacionais	5

Fonte: Adaptado de (US DoD, 2008, p. 3-15))

Apêndice E — Tabelas para categorização da ameaça

Tabela 14 – Localização da infraestrutura

Localização	Peso
Localizada no país fora das grandes áreas urbanas	1
Localizada no país próxima das grandes áreas urbanas	2
Localizada no exterior do país fora das grandes áreas urbanas	4
Localizada no exterior do país próxima das grandes áreas urbanas	5

Fonte: Adaptado de (US DoD, 2008, p. 3-24))

Tabela 15 – Nível de Publicidade da infraestrutura

Publicidade	Peso
A infraestrutura é relativamente desconhecida local e regionalmente	1
A infraestrutura é conhecida localmente mas relativamente desconhecida regionalmente	2
A infraestrutura é conhecida local e regionalmente mas relativamente desconhecida nacionalmente	3
A infraestrutura é conhecida a nível local, regional e nacional mas relativamente desconhecida internacionalmente	4
A infraestrutura é conhecida a nível local, regional, nacional e internacional	5

Fonte: Adaptado de (US DoD, 2008, p. 3-24))

Tabela 16 – Acessibilidade

Acessibilidade	Peso
Acesso extremamente difícil de obter; existência de numerosos obstáculos naturais ou artificiais; elevado nível de segurança física, com guardas armados; elevado nível de controlo de acessos	0
Acesso não disponível por terra, ar ou mar; obter acesso obriga a planeamento e recursos; existência de numerosos obstáculos; nível de segurança médio-alto (e.g. patrulhas, iluminação, dispositivos de alarme e anti-intrusão); localização dos ativos principais é difícil de atingir	2
Poucas rotas ou itinerários para aceder à infraestrutura ou ao ativo; existência de numerosos obstáculos; nível de segurança médio (e.g. patrulhas, iluminação, algumas medidas eletrónicas); localização dos ativos é difícil de atingir	4
Acesso disponível por terra, ar ou mar com adequado planeamento (existência de várias rotas e itinerários); existência de obstáculos; medidas de segurança limitadas (e.g. patrulhas, iluminação, sem medidas eletrónicas); Os ativos principais encontram-se no interior da infraestrutura	6
Acesso disponível por terra, ar ou mar (existência de várias rotas e itinerários); existência de poucos obstáculos (e.g. vedações); medidas de segurança mínimas; os ativos principais encontram-se no exterior	8
Acesso fácil por terra, ar ou mar (existência de várias rotas e itinerários); inexistência de obstáculos; sem medidas de segurança; os ativos principais são alcançados sem necessidade de aceder à infraestrutura, podem ser atingidos de um local afastado	10

Fonte: Adaptado de (Grohoski, 1996, p. 56))

Tabela 17 – Disponibilidade

Disponilidade	Peso
Estão disponíveis em grande quantidade, na zona imediatamente envolvente, outras infraestruturas ou ativos principais semelhantes	1
Estão disponíveis em pequena quantidade, na zona imediatamente envolvente, outras infraestruturas ou ativos principais semelhantes, mas existem em quantidade noutras localizações mais afastadas	2
Não existem, na zona imediatamente envolvente, outras infraestruturas ou ativos principais semelhantes, mas existem em quantidade noutras localizações mais afastadas	3
Não existem, na zona imediatamente envolvente, outras infraestruturas ou ativos principais semelhantes, mas existem em pequena quantidade noutras localizações mais afastadas	4
Não existem outras infraestruturas ou ativos principais semelhantes	5

Fonte: Adaptado de (US DoD, 2008, p. 3-25))

Tabela 18 – Dinâmica

Dinâmica	Peso
Ativo movimenta-se fequentemente de forma aleatória	1
Ativo movimenta-se fequentemente de forma previsível	2
Ativo movimenta-se periodicamente de forma aleatória	3
Ativo movimenta-se preiodicamente de forma previsivel	4
O ativo não se movimenta	5

Fonte: Adaptado de (US DoD, 2008, p. 3-25))

Tabela 19 – Visibilidade

Visibilidade	Peso
A infraestrutura ou o ativo apenas é identificada por atacantes com experiência ou apoio especializado na recolha de informações; não emite assinatura; identificado apenas durante o dia; localizado em local remoto.	6
A infraestrutura ou o ativo apenas é identificada por atacantes com significante nível de treino ou de apoio na recolha de informações; emite fraca assinatura (e.g. baixos níveis de luz ou ruído), facilmente identificado de dia mas apenas identificado de noite a uma distância de 100 metros; localizado numa área rural.	9
A infraestrutura ou o ativo apenas é identificada por atacantes com moderado nível de treino ou de apoio na recolha de informações; emite uma assinatura de nível médio (e.g. luzes e ruídos); facilmente identificado de dia mas apenas identificado de noite a uma distância de 500 metros; localizado numa área urbana de pequena dimensão.	12
A infraestrutura ou o ativo apenas é identificada por atacantes com fraco nível de treino ou de apoio na recolha de informações; emite uma grande assinatura (e.g. luzes e ruídos); facilmente identificado de dia e de noite, e a longas distâncias; localizado numa área urbana de média dimensão.	15

A infraestrutura ou o ativo é facilmente identificada por atacantes, com pouco ou nenhum nível de treino ou de apoio na recolha de informações; emite uma grande assinatura (e.g. luzes, ruídos e odores); facilmente identificado de dia e de noite,sob quaisquer condições atmosféricas e a longas distâncias; localizado numa área urbana de grande dimensão.	15

Fonte: Adaptado de (US DoD, 2008, p. 3-25) e de (Grohoski, 1996, p. 57))

Tabela 20 – Esforço

Esforço	Peso
Infraestrutura difícil de danificar; reforçada para evitar danos; impenetrável.	0
Infraestrutura reforçada para evitar danos; requer extenso *know-how* e capacidades para destruir ou danificar a infraestrutura; contramedidas difíceis de ultrapassar	3
Requer *know-how*, capacidades, quantidade significante de tempo e recursos para destruir ou danificar a infraestrutura; algumas contramedidas exigem tempo para serem ultrapassadas	6
Requer algum *know-how*, treino e limitadas quantidades de tempo e recursos para destruir ou danificar a infraestrutura; as contramedidas existentes podem ser facilmente ultrapassadas	9
Requer limitado *know-how*, capacidades e pequenas quantidades de tempo e recursos para destruir ou danificar a infraestrutura; não existem contramedidas	12
Requer pouco *know-how*, poucos recursos e tempo para destruir ou danificar a infraestrutura; não existem contramedidas	15

Fonte: Adaptado de (Grohoski, 1996, p. 57))

Tabela 21 – Medidas de segurança

Medidas de segurança	Peso
Forças de segurança equipadas e armadas (100% do pessoal e equipamento autorizado). Vigilância eletrónica, sistemas de alarme e anti-intrusão; guarnecimento físico da infraestrutura.	0
Forças de segurança equipadas e armadas (100% do pessoal e equipamento autorizado). Vigilância eletrónica, sistemas de alarme e anti-intrusão; verificação física da infraestrutura de hora a hora.	6
Forças de segurança equipadas e armadas (<95% do pessoal e equipamento autorizado). Sem vigilância eletrónica ou alarmes; patrulhamento de rotina e verificação física	12
Forças de segurança equipadas e armadas (<80% do pessoal e equipamento autorizado). Sem vigilância eletrónica ou alarmes; patrulhamento de rotina e observação visual	18
Elementos de segurança não-armados; patrulhamento de rotina e observação visual	24
Medidas de segurança inexistentes	30

Fonte: Adaptado de (Grohoski, 1996, p. 58))

Tabela 22 – Perceção de sucesso pelo atacante

Perceção de sucesso	Peso
Face às medidas de segurança existentes, o atacante perceciona possuir reduzida possibilidade de obter sucesso na destruição ou danificação da infraestrutura e escapar	6
Face às medidas de segurança existentes, o atacante perceciona possuir baixa possibilidade de obter sucesso na destruição ou danificação da infraestrutura e escapar	12
Face às medidas de segurança existentes, o atacante perceciona possuir moderada possibilidade de obter sucesso na destruição ou danificação da infraestrutura e escapar	18
Face às medidas de segurança existentes, o atacante perceciona possuir grande possibilidade de obter sucesso na destruição ou danificação da infraestrutura e escapar	24
Face às medidas de segurança existentes, o atacante perceciona possuir elevada possibilidade de obter sucesso na destruição ou danificação da infraestrutura e escapar	30

Fonte: Adaptado de (US DoD, 2008, p. 3-31))

Apêndice F — Folhas de cálculo e de registo

Tabela 23 – Tipo de agressor / Tática e Técnica usada / Tipo de engenho empregue

Tipo de tática e técnica / Tipo de engenhos explosivos / Tipo de agressor	Explosivos lançados manualmente					Veículo-bomba estacionado						Veículo-bomba em movimento					
	Granada de mão	Tubo bomba	Cinto com explosivos	Colete com explosivos	Mala com explosivos	Veículo ligeiro (compacto) com explosivos	Veículo ligeiro (sedan) com explosivos	Veículo "mini-van" com explosivos	Veículo ligeiro de transporte de carga com explosivos	Veículo pesado com explosivos	Veículo "semi-trailer" com explosivos	Veículo ligeiro (compacto) com explosivos	Veículo ligeiro (sedan) com explosivos	Veículo "mini-van" com explosivos	Veículo ligeiro de transporte de carga com explosivos	Veículo pesado com explosivos	Veículo "semi-trailer" com explosivos
Terrorista doméstico																	
Terrorista internacional																	
Terrorista patrocinio Estado																	

Fonte: (Autor, 2017)

Tabela 24 – Caraterização e avaliação da ameaça

Fatores	Indicadores	Caraterização	Avaliação
Capacidade operacional	Tipo de tática usada pelo grupo terrorista	*(Que tipo de ataques tem o grupo terrorista conduzido no passado? Tem usado IED de pequena ou grande quantidade de explosivos? Existem indícios de que o grupo possui novas capacidades? Qual o grau de insucesso nos ataques anteriores? Mantém as mesmas táticas e técnicas usadas com sucesso no passado?)*	*Tabela 5 (incluir peso inicial e peso após Macbeth)*
	Capacidade/vontade de provocar "mass casualties"	*O grupo possui capacidade ou intenção de conduzir ataques que provoquem grande quantidade de baixas? Já conduziu este tipo de ataques no passado?*	
	Targeting	*O grupo tem conduzido ataques em períodos de maior afluência ("hora de ponta")? Costuma utilizar um IED secundário para atingir as equipas de primeira intervenção? Procura limitar os efeitos do ataque aos danos em propriedade, colocando os IED em períodos e locais de menor afluência?*	
	Patrocínio Estatal	*O grupo possui apoio de um Estado? Se sim, qual(is)? Que tipo de apoio é fornecido (informações, logística, treino, financiamento)?*	
	Área de Operações	*O grupo é interno do país ou transnacional? Pode o grupo operar regionalmente ou internacionalmente?*	
	Acesso a tecnologia	*O grupo tem acesso a tecnologia avançada? Usam computadores? Pode o grupo conduzir sofisticadas técnicas de vigilância ou empregar IED tecnologicamente mais avançados? Que tipo de equipamentos utilizam? Onde obtém o equipamento? Onde obtém o treino?*	
Intenção	Ataques recentes	*O grupo tem conduzido ataques recentemente? Que tipos de ataques? Que tipo de armamento usado? Foi identificado algum indicador pré-incidente? O grupo reclamou a autoria do ataque?*	*Tabela 6 (incluir peso inicial e peso após Macbeth)*
	Ideologia anti-Portugal	*O grupo terrorista possui uma ideologia política, religiosa ou cultural contra Portugal? Esta ideologia é pública? Quais os principais pontos de interesse nacionais para o grupo terrorista? Que eventos/acontecimentos se podem constituir como um "gatilho" para uma ação terrorista?*	
	Ataques noutros países	*O grupo tem conduzido ataques terroristas em outros países? Onde? Que tipo de ataques? Que tipo de apoio logístico o grupo possui no local? Têm ameaçado interesses portugueses nesses países?*	
Atividade	Presença	*O grupo terrorista está presente no país? Apresenta algum tipo de atividade?*	*Tabela 7 (incluir peso inicial e peso após Macbeth)*
	Angariação de financiamento e local seguro	*O grupo terrorista usa o país para angariação de fundos financeiros? Que tipo de financiamentos? Qual a intenção para o uso desses financiamentos? O grupo usa o país como santuário ou local seguro?*	
	Vigilância	*O grupo terrorista tem conduzido ações de vigilância sobre possíveis alvos? O grupo é proficiente em ações de vigilância? Como tem conduzido as ações de vigilância? Qual a finalidade da informação obtida? O grupo tem ameaçado os interesses nacionais? Tem ocorrido eventos suspeitos que possam ser associados ao grupo terrorista?*	
	Alterações à filosofia de escolha de alvos	*O grupo terrorista tem demonstrado sinais de alteração à sua filosofia ou doutrina relativamente à seleção de alvos? Verificou-se alteração ao tipo de alvos selecionados?*	
	Envolvimento com células terroristas externas	*Existem ligações do grupo terrorista com outras células? Qual a frequência do contacto com células externas? Como tem o líder do grupo interagido com as lideranças dessas células? Existe treino conjunto? Existe partilha de informação?*	
	Movimentos de operacionais	*Tem se verificado movimento dos elementos operacionais do grupo terrorista? Esses movimentos têm sido dissimulados? Qual o propósito desses movimentos?*	

	Disrupção do grupo ou da rede	*As forças de segurança têm interrompido atividades do grupo terrorista? Que causas levaram a essa interrupção? De que forma a interrupção da atividade influenciou a capacidade operacional do grupo?*	
	Atividades em rede	*Que tipo de atividades conduz o grupo no país? Operacionais? Logísticas? Qual o número de células a atuarem no país? E a dimensão dessas células?*	
	Ataques a alvos nacionais	*Existem indícios de possíveis ataques a alvos nacionais? Já foram reivindicados ataques por parte do grupo? O grupo tem alvos específicos identificados? Que tipo de alvos? Qual a localização dos alvos?*	
Ambiente Operacional	Presença de forças de segurança ou de militares	*Qual a presença de forças de segurança ou militares no país? E na região? Dimensão? Localização? Tempo de permanência? Qual a atividade das forças de segurança ou militares na região (treino, apoio, segurança, vigilância, etc)? Que perceção tem o grupo terrorista da presença das forças de segurança ou militares? O que pode atrair um grupo terrorista a conduzir um ataque contra as forças de segurança ou militares?*	*Tabela 8 (incluir peso inicial e peso após Macbeth)*
	Influência de fatores externos	*A nação hospedeira encontra-se em guerra? Pode este facto influenciar um ataque de um grupo terrorista? Existe um ambiente de insurreição? O grupo terrorista está envolvido em ações de insurgência?*	
	Capacidades securitárias da nação hospedeira	*As forças de segurança e militares da nação hospedeira conseguem manter a ordem social? Que nível de treino possuem para enfrentar ataques terroristas? Que tipo de equipamento possuem? Qual a sua dispersão territorial? Existem colaboração entre as forças da nação hospedeira e as forças nacionais? Existe partilha de informação entre as forças da nação hospedeira e as forças nacionais?*	
	Influência política	*(Que influências políticas afetam as motivações do grupo terrorista para conduzirem um ataque? O sistema política, social e económico da nação hospedeira colapsou após atos terroristas?)*	

Fonte: (Autor, 2017)

Tabela 25 – Caraterização de uma Infraestrutura

Fatores	Indicadores	Caraterização	F	D
1ª Perímetro de Segurança ***(Compreende todo o espaço para além do perímetro imposto por barreiras, mais ou menos físicas, e que limitam a propriedade da infraestrutura)***	Monumentos relevantes ou edifícios icónicos	*Existem monumentos relevantes ou edifícios icónicos que se possam constituir alvos principais para um ataque terrorista? Distância à IC? A IC pode-se tornar um alvo secundário?*		
	Forças de Segurança, bombeiros ou hospitais	*Existem Forças de Segurança na proximidade da IC? Quais? Capacidades? Constituem-se elementos de dissuasão? Qual a capacidade de resposta? Existem bombeiros ou hospitais na proximidade das IC? Representam capacidade de primeira intervenção?*		
	Edifícios governamentais	*Existem monumentos relevantes ou edifícios icónicos que se possam constituir alvos principais para um ataque terrorista? Distância à IC? A IC pode-se tornar um alvo secundário?*		
	Atividades comerciais, industriais, ou outras, relevantes	*Quais as atividades relevantes na proximidade das IC? Qual a relação dessas atividades com a IC? Tornam a IC mais visível e mais exposta a um ataque terrorista?*		
	Armazéns de matérias perigosas	*Existem locais com matérias perigosas armazenadas? Que tipo de matérias perigosas? Distâncias de segurança associadas a essas matérias?*		
	Infraestruturas de transporte	*Existem infraestruturas de transporte que facilitem a acessibilidade à IC? Que a tornem mais visível? Que permita uma mais fácil primeira intervenção de socorro?*		
	Traçado das ruas	*Tipologia do traçado? Proximidade à IC? Tráfego? Limites à velocidade) Limitações ao tipo de veículos? Permite visibilidade à IC?*		
	Organização espacial/envolvente	*Tipologia de terreno envolvente? Existem edifícios ou terreno com altura que permita observação direta sobre a IC? Existe vegetação? A área envolvente garante distância de segurança entre a IC e as restantes infraestruturas mais próximas? Parqueamento perto dos limites da IC?*		
2ª Perímetro de Segurança ***(compreende o espaço entre o limite da propriedade onde se encontra o edifício e o próprio edifício)***	Vedações ou outro tipo de barreiras físicas	*A IC possui vedações ou outro tipo de barreiras físicas? Caraterísticas? Qual a sua capacidade resistente? Que grau de segurança garante à IC?*		
	Distância entre as barreiras físicas e a infraestrutura	*Qual a distância entre as barreiras físicas e a IC?*		
	Pontos de acesso à IC	*Quantos acessos existem à IC? Quais? Caraterísticas das medidas físicas utilizadas nos pontos de acesso?*		
	Controlo de acesso para pessoas ou veículos	*Como é feito o controlo de acessos? Que medidas de segurança existem no controlo de acessos? Existe histórico de falhas no controlo de acessos? Parqueamento?*		
	Iluminação exterior	*Existe iluminação exterior? Que tipo de iluminação? Existem zonas "mortas" fora do alcance da iluminação?*		

	Medidas de segurança	*Existem medidas que limitem a velocidade de viaturas na aproximação à IC? Existem forças ou serviços de segurança? Que tipo e quais as competências dessas forças? Patrulhamentos? Pessoal armado?*		
3º Perímetro de Segurança ***(abrange os limites do edificado da própria infraestrutura, sendo a linha definida pela sua geometria)***	Configuração	*Arquitetura da edificado? Disposição dos principais ativos? Medidas de segurança previstas na disposição do edificado?*		
	Estrutura do edifício	*Tipologia da estrutura do edifício (betão armado, alvenaria, madeira, metálica), capacidade resistente? Resistência a explosões? E a incêndios? Diferentes zonas com diferentes capacidades resistentes de acordo com a disposição dos principais ativos?*		
	Paramentos exteriores	*Tipologia dos paramentos exteriores (betão armado, alvenaria, madeira, etc)? Espessura?*		
	Envidraçados	*Dimensões dos envidraçados? Tipo de envidraçados? Capacidade resistente dos envidraçados? Existem elementos de proteção aos envidraçados?*		
	Redes prediais	*Quais as redes prediais existentes? Traçados das redes prediais? Caraterísticas das redes prediais?*		
	Existência de materiais perigosos	*Existem materiais perigosos na IC? Quais? Quantidades? Perigos associados? Medidas de proteção?*		
	Acesso ao interior da IC	*Quantos acessos existem ao interior da IC? Quais? Caraterísticas das medidas físicas utilizadas nos pontos de acesso?*		
	Acesso a telhados e coberturas	*Existem acessos ao telhado e coberturas? Quantos? Localização? Existem medidas de segurança associadas?*		
	Medidas de segurança	*Para além das já mencionadas, que medidas de segurança existem na IC? Sistema de alarmes, pessoal armado, patrulhamentos, etc?*		
F- Favorável	D- Desfavorável			

Fonte: (Autor, 2017)

Tabela 26 – Aplicação dos fatores de avaliação de uma infraestrutura

Fator	Avaliação	Peso
Criticidade	*Tabela 10*	*(incluir peso inicial e peso após Macbeth)*
Impacto	*Tabela 11*	*(incluir peso inicial e peso após Macbeth)*
Substituição	*Tabela 12*	*(incluir peso inicial e peso após Macbeth)*
Importância pública	*Tabela 13*	*(incluir peso inicial e peso após Macbeth)*
Localização	*Tabela 14*	*(incluir peso inicial e peso após Macbeth)*
Publicidade	*Tabela 15*	*(incluir peso inicial e peso após Macbeth)*
Acessibilidade	*Tabela 16*	*(incluir peso inicial e peso após Macbeth)*
Disponibilidade	*Tabela 17*	*(incluir peso inicial e peso após Macbeth)*
Dinâmica	*Tabela 18*	*(incluir peso inicial e peso após Macbeth)*
Visibilidade	*Tabela 19*	*(incluir peso inicial e peso após Macbeth)*
Esforço	*Tabela 20*	*(incluir peso inicial e peso após Macbeth)*
Medidas de segurança	*Tabela 21*	*(incluir peso inicial e peso após Macbeth)*
Perceção de sucesso pelo atacante	*Tabela 22*	*(incluir peso inicial e peso após Macbeth)*

Fonte: (Autor, 2017)

Tabela 27 – Cálculo da probabilidade de sucesso de um ataque – percentagem de vulnerabilidade

Analista:

Data:

Designação da IC:

Função nuclear da IC:

Ativo crítico da IC:

Agressor	Tática e técnica	Fatores: Ameaça – Capacidade Operacional (Tab. 05)	Ameaça – Intenção (Tab. 06)	Ameaça – Atividade (Tab. 07)	Ameaça – Ambiente Operacional (Tab. 08)	Ameaça – Nível da Ameaça (A) (Tab. 03)	Valor da IC para o utilizador – Criticidade (Tab. 10)	Valor da IC para o utilizador – Impacto (Tab. 11)	Valor da IC para o utilizador – Substituição (Tab. 12)	Valor da IC para o utilizador – Importância Política (Tab. 13)	Valor da IC para o utilizador – Valor da infraestrutura para o utilizador (VIC/Ut)	Valor da IC para o agressor – Localização (Tab. 14)	Valor da IC para o agressor – Publicidade (Tab. 15)	Valor da IC para o agressor – Acessibilidade (Tab. 16)	Valor da IC para o agressor – Disponibilidade (Tab. 17)	Valor da IC para o agressor – Dinâmica (Tab.18)	Valor da IC para o agressor – Visibilidade (Tab. 19)	Valor da IC para o agressor – Esforço (Tab. 20)	Valor da IC para o agressor – Medidas de segurança (Tab. 21)	Valor da IC para o agressor – Perceção de Sucesso (Tab. 22)	Sum Fatores	Probabilidade de sucesso de um ataque
☐ Terrorista doméstico	Explosivos lançados manualmente																					
	Veículo-bomba estacionado																					
	Veículo-bomba em movimento																					
☐ Terrorista internacional	Explosivos lançados manualmente																					
	Veículo-bomba estacionado																					
	Veículo-bomba em movimento																					
☐ Terrorista patrocinado por Estado	Explosivos lançados manualmente																					
	Veículo-bomba estacionado																					
	Veículo-bomba em movimento																					

Passo 2 **Passo 4** **Passo 5** **Passo 6**

Se nível de ameaça for considerado "MUITO BAIXO" então, deve ser logo considerado, à partida, um grau de vulnerabilidade "MUITO BAIXO"

Se VIC/Ut for inferior a 0,3 a IC é considerada de reduzido valor para o utilizador, permitindo-se dispensar a consequente análise de vulnerabilidade

Fonte: (Autor, 2017)

Apêndice G — Aquartelamento UBIQUE CAMP

Alojamentos

\

Proteção em muros de Hesco Bastion e T-Wall

Alimentação

Comando

Oficinas

Lazer

Enfermaria e Capela

Paióis

Torres de observação, Posições de tiro, bunkers (Hesco Bastion)

Porta de Armas

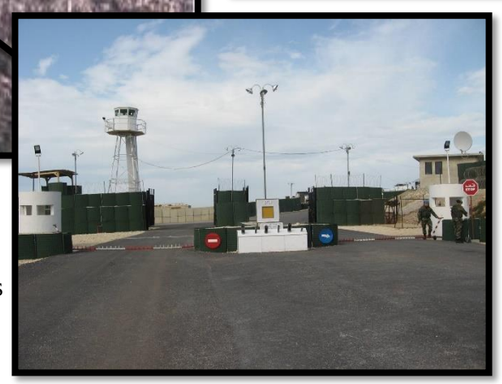


Figura 21 – Aquartelamento UBIQUE CAMP

Fonte: adaptado de (EPE, 2012, pp. 88 – 89)

Apêndice H — Caraterização da ameaça HEZBOLLAH

HEZBOLLAH - PARTIDO DE DEUS

O Hezbollah é uma organização política e militar dos muçulmanos xiitas do Líbano, criada em 1982 no contexto da invasão de Israel ao sul do Líbano. desde 2005 o Hezbolah conta com catorze deputados na assembleia nacional do Líbano. o secretário-geral da organização é o xeque Hassan Nasrallah, que ocupa este cargo desde 1992.

Organização e efetivos

- Estrutura hierárquica;
- Células com estrutura operacional;
- Direção Estatal;
- 1000 membros armados ativos + População
- Bases de formação/ treino: Vale do Bekka sul do Líbano, resistências nos subúrbios, a sul e oeste de Beirute

Motivação: nacionalista ou territorialista

Objetivos de curto prazo

- Obter o apoio em massa da população libanesa para a causa em questão;
- Aumentar as capacidades a nível de recursos humanos e materiais da organização

Objectivos de longo prazo

- Conquistar o poder político através de uma maior representação parlamentar;
- Destruir Israel como Estado;
- Criar um Estado Islâmico sobre Jerusalém.

Orientação política, religiosa e a raiz étnica

Métodos e alvos de recrutamento:

- Reuniões na escola, palestras, encenações teatrais onde incutem e publicitam os seus ideais
- Para controlo da população, usa a componente de redes de apoio social para garantir o apoio à população através de actos de doação, servindo-se dos apoios da Síria e do Irão. Facilmente poderá instigar a população a executar protestos e manifestações contra uma eventual mudança de postura da UNIFIL, interferindo na sua acção ou potenciando uma aproximação excessiva à população que comprometa a sua segurança e controlo;

Tácticas e Operações Predilectas:

- Atentados Bombistas (em 83` o atentado contra a embaixada americana matou 350 pessoas).
- O Hezbollah está muito bem treinado e organizado e em áreas específicas, como ataques terroristas fazendo recurso aos VBIED (*Vehicle Borne Improvised Explosive Devices*), IED (*Improvised Explosive Devices*), uso de minas, execução de emboscadas e técnicas de guerrilha
- Raptos: na década de 90 várias pessoas foram raptadas incluindo William Buckley, chefe do CIA.
- A propensão para matar está bem patente nos inúmeros ataques desenvolvidos contra: alvos Israelitas (patrulhas e controlos fronteiriços), alvos Norte Americanos e Franceses (a embaixadas e a altos representantes).

Capacidade Técnica:

- De ordem ofensiva, pela capacidade de conduzir uma campanha sustentada contra Israel infringindo massivos e contínuos danos militares e civis, na zona fronteiriça Israelita.
- De ordem defensiva, pela capacidade de operar coordenadamente acções defensivas, contra as forças de assalto Israelitas, conservando a sua sobrevivência, poder e organização.
- Células terroristas a operar no Sul do Líbano são mencionadas em relatórios, pelo que, acções contra a UNIFIL não são de excluir. De acordo com uma avaliação realizada por fontes seguras, não mais de 200 terroristas estarão infiltrados nos campos de refugiados palestinianos. Estes grupos constituem-se na principal ameaça às Forças da UNIFIL

Informações:

- O Hezbollah possui três unidades de recolha e processamento de Informação. Uma unidade é responsável por atividades de "*Intelligence*" contra Israel, no intuito de reunir informações sobre bases, instalações Israelitas e outros potenciais alvos.
- Os operacionais do Hezbollah conduzem operações de SIGINT. contra as comunicacões Israelitas.

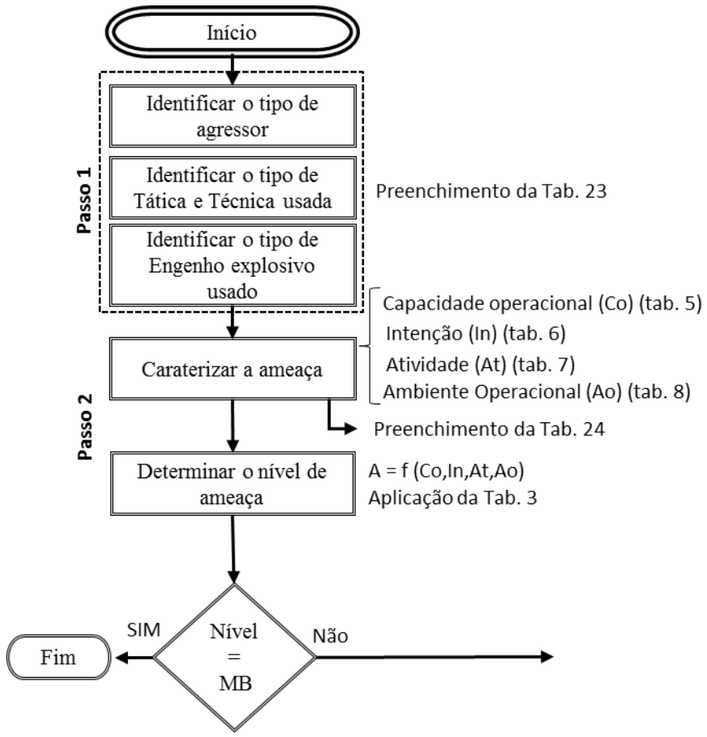
Armamento e Equipamento:

- Devido ao facto de o Hezbollah ter características de milícia não é obrigado a manifestar a aquisição, ou intenção de aquisição do armamento listado, ou seja, a informação não é possível de qualquer confirmação independente.
- O principal armamento utilizado pelo grupo Hezbollah é a base de mísseis de variados alcances e para diferentes fins, tais como, terra – terra, terra -mar e terra – ar .

Capacidade de Transporte:

- A capacidade de transporte do Hezbollah é pouco adequada, dado que a maioria das viaturas são civis e pouco apropriadas para transporte de algum tipo de equipamento bélico.
- As estradas principalmente em Beirute e sul do Líbano normalmente são controladas pelo exército libanês reforçado pelas forças da UNIFIL e utilizadas para mobilização de pessoal.

Apêndice I — Aplicação do modelo ao Cenário



Tipo de tática e técnica / Tipo de engenhos explosivos / Tipo de agressor	Explosivos lançados manualmente					Veículo-bomba estacionado						Veículo-bomba em movimento					
	Granada de mão	Tubo bomba	Cinto com explosivos	Colete com explosivos	Mala com explosivos	Veículo ligeiro (compacto) com explosivos	Veículo ligeiro (sedan) com explosivos	Veículo "mini-van" com explosivos	Veículo ligeiro de transporte de carga com explosivos	Veículo pesado com explosivos	Veículo "semi-trailer" com explosivos	Veículo ligeiro (compacto) com explosivos	Veículo ligeiro (sedan) com explosivos	Veículo "mini-van" com explosivos	Veículo ligeiro de transporte de carga com explosivos	Veículo pesado com explosivos	Veículo "semi-trailer" com explosivos
Terrorista doméstico																	
Terrorista internacional																	
Terrorista patrocinio Estado				X										X			

Figura 22 – Preenchimento da Tabela 23

Fonte: (Autor, 2017)

Fatores	Indicadores	Caraterização	Avaliação	
			Peso inicial	Peso após Macbeth
Capacidade operacional	Tipo de tática usada pelo grupo terrorista	O Hezbollah tem conduzido, desde a sua criação (1981), ações terroristas com recurso ao uso de explosivos, seja em eventos de grande dimensão com viaturas pesadas carregadas com explosivos (atentado em 1983) ou com homens-bomba em eventos de menor dimensão	4	4,6
	Capacidade/vontade de provocar "mass casualties"	O grupo possui capacidade de conduzir atentados causadores de grandes baixas, tendo o já feito no passado.		
	Targeting	Os ataques costumam ser cirurgicos,atingindo os efeitos pretendidos		
	Patrocínio Estatal	Possui apoio do Irão, financeiramente e através da disponibilização de locais de treino, armamento e operacionais		
	Área de Operações	O grupo é interno, libanês, mas atua em vários países da região.		
	Acesso a tecnologia	O grupo possui equipamento de ponta, moderno, sendo apoiado pelo Irão. Para além da capacidade terrorista possui uma grande capacidade militar convencional		
Intenção	Ataques recentes	O grupo tem conduzido ataques recentemente, maioritariamente contra a população cristã do Líbano ou contra personalidades governamentais mais liberais. Conduziu um ataque contra o contingente espanhol da UNIFIL.	2	1,89
	Ideologia anti-Portugal	Apesar de possuir uma ideologia política e religiosa contrária a Portugal, não existe conflito de interesses entre o Hezbollah e o contingente nacional. No entanto, não é favorável à presença da UNIFIL no sul do Líbano		
	Ataques noutros países	O Hezbollah tem conduzido ataques em territórios estrangeiros, principalmente nos anos 80 e 90. Mais recentemente tem participado em ações na Síria		
Atividade	Presença	O grupo tem uma forte presença no país, desenvolvendo uma grande atividade	4	4,27
	Angariação de financiamento e local seguro	O grupo angaria os seus recursos financeiros maioritariamente no exterior. Quanto ao recrutamento, este é feito maioritariamente na populatção de etnia xiita.		
	Vigilância	•O Hezbollah possui três unidades de recolha e processamento de Informação. Uma unidade é responsável por atividades de "Intelligence" contra Israel, no intuito de reunir informações sobre bases, instalações Israelitas e outros potenciais alv. Não existe preocupação de vigilância sobre alvos portugueses		
	Alterações à filosofia de escolha de alvos	Nada a referir		
	Envolvimento com células terroristas externas	O Hezbollah não mantém ligações a células terroristas externas.		
	Movimentos de operacionais	Existe grande atividade de vigilância junto à fronteira com Israel, bem como atividades de recrutamento junto à população xiita.		
	Disrupção do grupo ou da rede	As forças de segurança libanesas controlam as atividades, mas não possuem capacidade de disromper as ligações internas e externas do grupo		
	Atividades em rede	Mantém uma forte ligação em rede dentro do Líbano e com o Irão		
	Ataques a alvos nacionais	Não existem indicios de possíveis ataques contra os interesses nacionais ou contra a força portuguesa		
Ambiente Operacional	Presença de forças de segurança ou de militares	As forças de segurança libanesas têm pouca expressão no sul do Líbano, estandoa segurança desta região praticamente entregue ao Exército libanês. A presença do exército é forte, conduzindo principalmente ações de vigilância das atividades do Hezbollah e controlo de movimentos. Nesta região estão presentes cerca de 12000 militares da UNIFIL com o objetivo de impedir o confronto entre o Hezbollah e forças armadas libanesas e Israel.	3	3,29
	Influência de fatores externos	O Líbano encontra-se em conflito com Israel, sendo o Hezbollah um dos seus grandes instigadores.		
	Capacidades securitárias da nação hospedeira	As forças de segurança e militares da nação hospedeira conseguem manter a ordem social?. No entanto possuem pouca formação e treino para enfrentar ataques terroristas. Eixstem colaboração entre as forças da nação hospedeira e as forças nacionais. Existe partilha de informação entre as forças da nação hospedeira e as forças nacionais.		
	Influência política	O Hezbollah é uma organização política.		

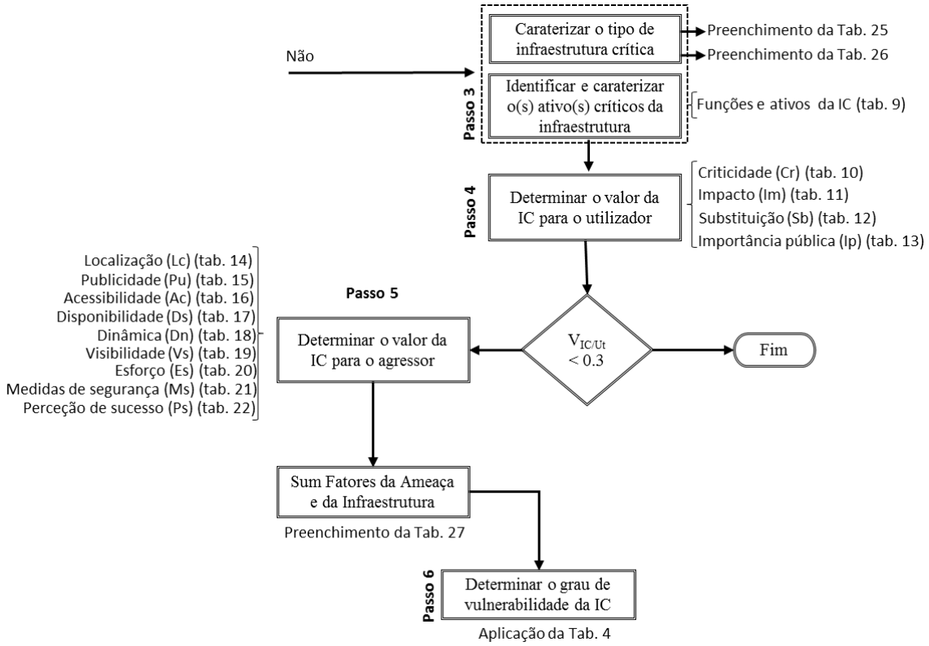
Figura 23 – Preenchimento da Tabela 24

Fonte: (Autor, 2017)

Fatores	Indicadores	Caraterização	F	D
1ª Perímetro de Segurança *(Compreende todo o espaço para além do perímetro imposto por barreiras, mais ou menos físicas, e que limitam a propriedade da infraestrutura)*	Monumentos relevantes ou edifícios icónicos	*Não existem monumentos relevantes ou edifícios icónicos*	X	
	Forças de Segurança, bombeiros ou hospitais	*Próximo da IC existe uma unidade do Exército libanês e uma unidade da UNIFIL*	X	
	Edifícios governamentais	*Não existe edifícios governamentais*	X	
	Atividades comerciais, industriais, ou outras, relevantes	*Não existem atividades relevantes*	X	
	Armazéns de matérias perigosas	*Não existem armazéns de matérias perigosas*	X	
	Infraestruturas de transporte	*Apenas existe uma estrada que passa junto à IC*		X
	Traçado das ruas	*Passa uma estrada junto ao limite sul do aquartelamento. Esta estrada, pavimentada em alcatrão, de boa acessibilidade, faz a ligação entre a povoação de Shama e outras no interior da região com a estrada costeira que liga Naqoura a Tyre e ao norte do Líbano. Tem um tráfego de nível médio, à base de viaturas ligeiras e médias de transporte de pessoal e de mercadorias.A estrada passa junto ao aquartelamento permitindo visibilidade à IC.*		X
	Organização espacial/envolvente	*A área envolvente ao aquartelamento , à exceção do lado sul onde passa a estrada, consiste num terreno baldio, bastante rochoso, com vegetação rasteira e espinhosa., dificultando a aproximação à IC a pessoas e impossibilitando a veículos. É um terreno aberto que permite boa visibilidade às médias e longas distâncias permitindo uma fácil deteção de possíveis aproximações à IC. Não existem edifíciosou terreno em alturana envolvente que permita observação para o interior da IC.*	X	
2ª Perímetro de Segurança *(compreende o espaço entre o limite da propriedade onde se encontra o edifício e o próprio edifício)*	Vedações ou outro tipo de barreiras físicas	*O perímetro do aquartelamento carateriza-se por uma forte barreira física, composta por muros de Hesco Bastion, com uma altura média de 4 metros e uma esssura média de 3 metros., com elevada resistência a explosões. Na parte do perímetro paralela à estrada, a barreira consiste num muro de betão armado (T-Wall), pré-fabricado, com uma altura de 6 metros e espessura de 40 centímetros., com elevada resistência ao embate de viaturas e a explosões. O topo dos muros é ainda reforçado por concertinas de arame farpado, dificultando a transposição dos mesmos.*	X	
	Distância entre as barreiras físicas e a infraestrutura ou o ativo	*O paiol (ativo principal em estudo) encontra-se no interior da IC, a uma distância de aprox. 150m do principal acesso à IC e a 200m dos limites da IC com a estrada. A distância mais curta ao limite da IC é de aprox. 30m.*	X	
	Pontos de acesso à IC	*Existem dois acessos ao aquartelamento. Um usado apenas para emergência, constítuido por altos portões metálicos,, opacos, com estrutura reforçada e postos de vigia junto. O acesso principal consiste em duas zonas distintas de acesso, uma para peões outra para pessoas. Nestas zonas os portões são metálicos, gradeados mas com menor grau de segurança que o acesso secundário, no entanto mantem segurança em permanência.*	X	
	Controlo de acesso para pessoas ou veículos	*Existem dois tipos de controlo de acessos. Um físico, constituído à base de barreiras físicas, criando uma "gincana", controlando a velocidade e o tipo de viaturas que acedem à IC.Outro procedimental, composto por um conjunto de medidas de segurança, como vigilância, cartões de acesso, revista a pessoal e viaturas, etc.*		X
	Iluminação exterior	*A iluminação exterior permite evitar , às curtas distâncias, zonas mortas à observação visual durante a noite*	X	
	Medidas de segurança	*A segurança é garantida por militares, armados, em permanência, em postos de vigia, junto ao ponto de acesso à IC e em patrulhas de rotina no interior da IC. Não existe sistema de alarme nem sistemas de vigilância eletrónicos*	X	
3º Perímetro de Segurança *(abrange os limites do edificado da própria infraestrutura, sendo a linha definida pela sua geometria)*	Configuração	*O paiol (ativo principal em estudo) consiste em três armazéns, com dimensões equivalentes a um contentor de 20 pés cúbicosde volume, dispostos paralelamente, com uma área de acesso comum aos mesmos. Não possui uma disposição que pemita interdependência entre os compartimentos*		X
	Estrutura do edifício	*O paiol tem um estrutura metálica, composta por contentores metálicos*		X
	Paramentos exteriores	*Os contentores metálicos são revestidoc por paramentos exteriores em Hesco Bastions, na totalidade da sua altura e com uma espessura de 1m. A parte superior dos contentores é revestida por uma camada de 60cm de brita e areia. Estes paramentos garantem resistência a explosões de pequenas dimensões*	X	
	Envidraçados	*Não possui envidraçados*	X	
	Redes prediais	*Apenas possui rede elétric. Não possui rede de abastecimento de água, o que dificulta as operações de mitigação dos efeitos de uma explosão.*		X
	Existência de materiais perigosos	*O paiol possui no seu interior uma grande quantidade de explosivos. Munições, cargas explosivas TNT, lança-foguetes LAW, etc. O perigo associado a este material é a explosão. Tendo em consideração a quantidade de explosivo armazenada os efeitos da explosão serão enormes*		X
	Acesso ao interior da IC	*Existe apenas um acesso ao paiol, através de um portão gradeado, devidamente fechado. Todos os contentores que compõem o paio estão devidamente fechados.*	X	
	Acesso a telhados e coberturas	*O acesso à cobertura do paiol é facilitado devi à organização espacial, ao desnívelamento do aquartelamento e à proximidade de outras instalações no interior da IC*		X
	Medidas de segurança	*As unicas medidas de segurança são as barreiras física, muro em Hesco Bastion, existente em torno do paiol. Existem patrulhas de rotina no aquartelamento com passagem pelo paiol. Não existem alarmes nem sistemas de vigilância eletrónicos.*		X

Figura 24 – Preenchimento da Tabela 25

Fonte: (Autor, 2017)



Fator	Avaliação	Peso inicial	Peso ponderado após Macbeth
Criticidade	A perda, destruição ou uso indevido da infraestrutura ou do ativo resultará na interrupção imediata da sua capacidade operacional. A infraestrutura não cumpre a sua função	5	5
Impacto	A perda, destruição ou uso indevido da infraestrutura ou do ativo terá impacto nacional, afetando o sistema associado à infraestrutura	4	3,67
Substituição	O ativo pode ser substituído ou a infraestrutura retomar a operação entre um e seis meses	4	4
Importância pública	Moderada: a atenção dos OCS estende-se aos OCS nacionais	3	3,86
Localização	Localizada no exterior do país fora das grandes áreas urbanas	4	3,86
Publicidade	A infraestrutura é conhecida local e regionalmente mas relativamente desconhecida nacionalmente	3	3
Acessibilidade	Poucas rotas ou itinerários para aceder à infraestrutura ou ao ativo; existência de numerosos obstáculos; nível de segurança médio (e.g. patrulhas, iluminação, algumas medidas eletrónicas); localização dos ativos é difícil de atingir	4	2,6
Disponibilidade	Estão disponíveis em pequena quantidade, na zona imediatamente envolvente, outras infraestruturas ou ativos principais semelhantes, mas existem em quantidade noutras localizações mais afastadas	2	2
Dinâmica	O ativo não se movimenta	5	5
Visibilidade	A infraestrutura ou o ativo apenas é identificada por atacantes com experiência ou apoio especializado na recolha de informações; não emite assinatura; identificado apenas durante o dia; localizado em local remoto.	9	9
Esforço	Infraestrutura reforçada para evitar danos; requer extenso know-how e capacidades para destruir ou danificar a infraestrutura; contramedidas difíceis de ultrapassar	3	2,07
Medidas de seguraça	Forças de segurança equipadas e armadas (<95% do pessoal e equipamento autorizado). Sem vigilância eletrónica ou alarmes; patrulhamento de rotina e verificação física	12	12
Peceção de sucesso pelo atacante	Face às medidas de segurança existentes, o atacante perceciona possuir baixa possibilidade de obter sucesso na destruição ou danificação da infraestrutura e escapar	12	12

Figura 25 – Preenchimento da Tabela 26

Fonte: (Autor, 2017)