INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE ESTADO-MAIOR CONJUNTO

2010 - 2011

TII

PROTECÇÃO PORTUÁRIA,

EM AMBIENTE DE ANTI-TERRORISMO

DOCUMENTO DE TRABALHO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DA MARINHA PORTUGUESA / DO EXÉRCITO PORTUGUÊS / DA FORÇA AÉREA PORTUGUESA/ DA GUARDA NACIONAL REPUBLICANA.

Paulo Alexandre Rafael da Silva
Capitão-de-fragata

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

PROTECÇÃO PORTUÁRIA,

EM AMBIENTE DE ANTI-TERRORISMO

Capitão-tenente Paulo Alexandre Rafael da Silva

Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto

Lisboa – 2011

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

PROTECÇÃO PORTUÁRIA,

EM AMBIENTE DE ANTI-TERRORISMO

Capitão-tenente Paulo Alexandre Rafael da Silva

Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto

Orientador:

Capitão-tenente António Jacinto Coelho Gomes

Lisboa – 2011

Agradecimentos

O presente trabalho constitui o quinhão mais visível do esforço desenvolvido no decurso da frequência do Curso de Estado-Maior Conjunto, é por isso inteiramente justo, realmente incontornável, o reconhecimento público àqueles que contribuíram para o tornar possível.

Plasmo assim nestas linhas o meu profundo agradecimento…

Ao CTEN Coelho Gomes, pela sua disponibilidade, apoio e orientação inestimável, sobretudo na fase mais crítica do trabalho.

Ao CFR Neves Correia e ao CFR Neves Rodrigues pelo prestimoso contributo na clarificação de aspectos legais e legislativos.

Ao Eng. Seixas da Fonseca (Director de Serviços de Actividades Sectoriais do IPTM) e ao Cte. Taveira Rodrigues (Oficial de Protecção do Porto de Lisboa), que nas entrevistas concedidas me proporcionaram o entendimento desta problemática do ponto de vista da autoridade portuária.

Ao Cte. Mário Oliveira (EMSA), cuja troca de correspondência permitiu perceber o relacionamento inter-departamental na Europa.

A S.Exa. o VALM Cunha Lopes (Director-Geral da Autoridade Marítima e Comandante-Geral da Polícia Marítima), ao CMG Matos Nogueira (Oficial de Ligação entre o Comando Naval e a Direcção Geral da Autoridade Marítima) e ao CMG Salvado de Figueiredo (Comandante do N.R.P. "D. Francisco de Almeida"), que nas entrevistas concedidas contribuíram em muito para a percepção da matéria em estudo, sob o ponto de vista militar e policial, mas também inter-departamental.

Aos camaradas do CEMC, pelo apoio, pelo conhecimento partilhado, mas sobretudo pela amizade e pelo meu enriquecimento enquanto pessoa.

Um agradecimento muito especial à amiga, à critica, à companheira e à mulher, à Rosário que, a 800 milhas ou mais, foi sempre quem esteve mais próxima, motivando e incentivando, fazendo-me tentar ser sempre um pouco melhor… OBRIGADO.

Índice

Índice de figuras

Índice de tabelas

Resumo

O presente trabalho tem por objecto de estudo a implementação de medidas de protecção portuária em ambiente anti-terrorista.

Desenvolve-se inicialmente através da caracterização da ameaça terrorista naquele ambiente específico e prossegue com a verificação das medidas de protecção já existentes tentando enquadrar o desenvolvimento de projectos de novas medidas de protecção como o *Defense Against Terrorism – Program of Work* (DAT – POW), na iniciativa *Protection of Harbors and Ports* (PHP).

A metodologia de investigação escolhida foi a do método científico, recorrendo-se essencialmente a fontes primárias, a documentação enquadrante no domínio do direito internacional, a documentos doutrinários nacionais, fazendo a sua transposição para um contexto multi-nacional, e a documentos oficiais que, no âmbito operacional, estabeleceram directrizes para a protecção de Força em ambiente portuário.

Foram igualmente utilizados trabalhos publicados que abordam diferentes vertentes do objecto de estudo e procedeu-se à recolha de informação através de entrevistas a alguns membros de organizações nacionais e europeias, militares e civis.

A leitura do trabalho permitirá constatar que em ambiente portuário um ataque terrorista pode ter múltiplas formas e o número de alvos apetecíveis é elevado.

Irá ainda verificar-se que a preocupação global com este fenómeno levou à implementação de várias medidas de protecção aplicáveis ao ambiente portuário, de carácter multi-disciplinar, tanto unilaterais como no âmbito de organizações internacionais e até inter-organizacionais.

Ainda assim foi possível verificar a existência de lacunas que podem ser colmatadas ou mitigadas por novos projectos de implementação de medidas de protecção, sendo que para a sua efectiva operacionalização se sugere uma abordagem à cúpula da organização que superintenda os diversos departamentos competentes na área portuária.

Finalmente verificou-se que para tirar partido da potencial utilidade dos produtos ou capacidades desenvolvidos no âmbito da iniciativa DAT – POW PHP da OTAN poderá ser necessário atender a diversas questões formais, fazendo-se assim um conjunto de recomendações quando à adopção de linhas de actuação que podem dar continuidade à iniciativa.

Abstract

This project aims to study the implementation of harbour protection measures in an anti-terrorist environment.

It has been initially developed by characterizing the terrorist threat in that specific environment, then verifying the existing measures already in place, aiming to frame further developments of new measures, such as those under NATO program *Defence Against Terrorism – Program of Work* (DAT – POW), specifically under the *Protection of Harbors and Ports* (PHP) initiative.

The chosen methodology of investigation was the scientific method for social sciences, following primary sources such as framing international law documentation, as well as Portuguese doctrinaire documents. Some operational doctrinaire documents addressing in harbour force protection were also consulted.

A number of freely available documents were regarding the object of study were also approached and a number of interviews were conducted in order to collect relevant information and points of view from member of Portuguese and international organizations, both military and civilian.

By reading this project it will be possible to verify that a terrorist attack in a harbour environment may occur in many ways and that the number of likely targets is quite high.

It will also be possible to verify that a general concern with this phenomenon led to the implementation of several protective measures in the harbour environment, which have a multi-disciplinary character, and have been in place through national, international organizations and inter-organization initiatives.

It was also possible to verify the existence of security breaches which may be coped with or mitigated by implementing of complementary protecting measures projects, such as NATO's DAT – POW PHP. However, it is suggested that its effective implementation requires a top – down approach, addressing a higher organization which should superintend the largest number of agencies with responsibilities in harbours and ports.

Finally, it has been verified that in order to take full advantage of the potential utility of any product or capability developed under NATO's DAT – POW PHP initiative it may be necessary to address a number of formal matters. Thus, a number of recommendations are made in the end, pointing to a number of possible courses of action that may aid in the continuity of that initiative.

Palavras-chave

Análise de risco

Anti-terrorista

Código ISPS

Defence against terrorism

Infra-estruturas críticas

Medidas de protecção

Protecção

Protecção portuária

Terrorismo

Vulnerabilidades

Lista de abreviaturas, siglas e acrónimos

A

ADM — Armas de Destruição em Massa

AIS — *Automatic Identification System*

AMN — Autoridade Marítima Nacional

C

CCOPP — Centro Coordenador de Operações de Protecção do Porto

CIP — Certificado Internacional de Protecção

CSR — *Continuous Synopsis Record*

D

DAT — *Defense Against Terrorism*

DNV — *Det Norske Veritas*

E

EMSA — *European Maritime Safety Agency*

EUA — Estados Unidos da América

I

ILO — *International Labour Organization* – Organização Internacional do Trabalho

IMO — *International Maritime Organization* – Organização Marítima Internacional

IPTM — Instituto Portuário e dos Transporte Marítimos

ISPS — *International Ship and Port Facility Security Code* – Código Internacional para a Protecção dos Navios e das Instalações Portuárias

L

LRIT — *Long Range Identification and Tracking*

M

M _____ Milhas Náuticas (1 M = 1852 metros)

M/V_____ *Merchant vessel* (Navio mercante)

MTSA_____ *Maritime Transportation Security Act*

N

NATO _____*North Atlantic Treaty Organization*

O

ONU _____Organização das Nações Unidas

OTAN _____Organização do Tratado do Atlântico Norte

P

PHP _____ *Protection of Harbors and Ports*

POW _____*Program Of Work*

PPP _____Plano de Protecção do Porto

PSI _____ *Proliferation Security Initiative*

R

RAND_____ *Research And Development Corporation*

S

SOLAS____ *International Convention for the Safety of Life at Sea* – Convenção Internacional para a Salvaguarda da Vida Humana no Mar de 1974

U

UE _____ União Europeia

USCG_____ *United States Coast Guard*

USS _____*United States Ship*

Introdução

> "Todas as iniciativas que aportem um reforço de segurança devem ser apadrinhadas".
>
> VALM Cunha Lopes

a. Justificação do Tema

Na sequência dos atentados terroristas à bomba em Madrid, a 11 de Março de 2004, que se saldaram em 171 mortos e um número de feridos superior a 1700, a Conferência dos Directores de Armamento Nacional (CNAD - Conference *of National Armament Directors*[1]), propôs o *Defense Against Terrorism- Programme of Work* (DAT - POW), visando providenciar um mecanismo para a identificação, desenvolvimento e disponibilização de contra-medidas, como parte da resposta da Aliança ao terrorismo e a outras ameaças. Este programa foi apoiado pelos Chefes de Estado e Governos na Cimeira de Istambul, em Junho de 2004.

O programa teve como prioridade inicial a luta contra o terrorismo e encontra-se nesta altura focalizado na protecção contra ameaças assimétricas, abordando esta problemática com a promoção do desenvolvimento de capacidades que apoiem operações expedicionárias, mas acrescendo a dificuldade de ser operacionalizadas num contexto que não é puramente militar, pelo contrário será necessário contar com a colaboração e até apoio das autoridades civis locais.

De entre as dez iniciativas de maior significado dentro do programa enquadra-se no contexto do presente trabalho aquela que respeita à Protecção Portuária (*PHP – Protection of Harbour & Ports*). Esta iniciativa foi inicialmente liderada pela Itália, tendo procedido à determinação da tecnologia existente e à investigação e desenvolvimento de sensores adequados para a detecção da ameaça, assim como a sua integração. Assumiu-se, após a

[1] CNAD é o comité da OTAN responsável por reunir consenso entre as nações membro no que respeita a cooperação no campo do armamento, padronização do material e satisfação de necessidades na área da defesa.

realização de testes em diversos cenários que os sensores electromagnéticos, acústicos e ópticos atingiram o grau de eficiência suficiente para proporcionar uma vigilância adequada no ambiente pretendido.

O DAT – POW PHP reveste-se de particular importância em termos nacionais atendendo a que Portugal assumiu a liderança da iniciativa em Setembro de 2010, sendo que a Marinha Portuguesa lidera actualmente o processo de desenvolvimento dum Sistema de Apoio à Decisão (SAD) baseado num simulador dotado de Inteligência Computacional, o qual deverá ser capaz de analisar os mais diversos cenários, os quais devem conter, entre outros, elementos como: equipamentos, pessoal necessário e/ou disponível, grau de risco assumido, dispositivo no terreno, centros de controlo existentes e localização. Esse SAD deverá fornecer uma solução para cada um dos cenários, contemplando a organização da Força, os seus métodos e procedimentos, bem como o desenvolvimento de tecnologias que permitam maior eficácia e eficiência do dispositivo.

Tendo-se desenvolvido um conjunto de sensores julgados adequados à detecção atempada de ataques em ambiente portuário, caracterizando-se esse ataque por ter origem numa ameaça assimétrica, logo que esteja disponível o já referido SAD que indicará qual a postura mais adequada a ter, ficará ainda por ser resolvido o complexo problema de implementar no terreno as soluções preconizadas.

A maior dificuldade da real implementação de medidas de protecção, quer sejam passivas quer sejam activas, deriva da multiplicidade de cenários em que tal pode vir a ser necessário, uma vez que a Força poderá vir a encontrar-se num porto dum país pertencente à Aliança, dum outro onde decorra efectivamente uma operação, ou noutro país amigo visitado pela Força apenas por razões logísticas no decurso dessa mesma operação.

Dando continuidade ao desenvolvimento tecnológico no âmbito do DAT-POW, o presente trabalho pretende enquadrar aquele projecto nas iniciativas existentes e identificar eventuais obstáculos à efectiva implementação no terreno das soluções gizadas para uma eficaz protecção portuária em ambiente de anti-terrorismo, sendo portanto relevante quer no âmbito nacional quer no âmbito da Aliança, sobretudo ao considerar que a Marinha Portuguesa lidera presentemente a iniciativa PHP.

b. Enunciado do tema, contexto e base conceptual

Pretendeu-se abordar a temática da protecção portuária em ambiente anti-terrorista, caracterizando a ameaça e verificando as medidas técnicas e formais já existentes de

maneira a enquadrar o DAT-POW PHP apontando possíveis linhas de actuação operacional que permitam a efectiva utilização das capacidades já desenvolvidas ou em desenvolvimento.

c. Objecto da Investigação e sua Delimitação

O objecto da presente investigação centra-se na implementação de medidas de protecção portuária em ambiente anti-terrorista. Para tal foi necessário caracterizar essa ameaça naquele ambiente específico, determinar a natureza das medidas de protecção existentes e tentar enquadrar projectos de medidas de protecção adicionais como o DAT-POW PHP da OTAN.

As conclusões do presente trabalho de investigação poderão ser utilizadas no destacamento de qualquer Força, não se restringindo à sua componente naval, uma vez que o projecto em desenvolvimento se torna relevante sempre que uma área portuária esteja a ser usada ou careça de ser protegida, podendo essa área ser vasta ou contemplar apenas infra-estruturas críticas, tratando-se em todo o caso dum ambiente complexo.

d. Objectivos da Investigação

Este trabalho incide na implementação eficaz de medidas de defesa portuária, as quais incluem, sem ser de carácter restrito, as capacidades desenvolvidas no âmbito do DAT-POW PHP.

Pretendeu-se igualmente determinar se existem obstáculos à implementação no terreno das capacidades que eventualmente venham a ser desenvolvidas no âmbito do DAT – POW PHP.

e. Metodologia

A metodologia de investigação escolhida para a elaboração do presente Trabalho de Investigação Individual foi a do método científico, com recurso ao modelo hipotético-dedutivo, conforme determinado na NEP DE 218 do Instituto de Estudos Superiores Militares (IESM).

Assim, para a presente investigação foi adoptada a seguinte Pergunta de Partida:

Como pode concretizar-se eficientemente uma protecção portuária?

No seguimento desta Pergunta de Partida foram levantadas quatro Questões Derivadas (QD), que de seguida se apresentam:

- QD1: Como se caracteriza a ameaça portuária em ambiente terrorista?

- QD2: Qual a natureza das medidas existentes para fazer face à ameaça terrorista em ambiente portuário?

- QD3: Como pode o DAT – POW PHP enquadrar-se no contexto actual da protecção portuária?

- QD4: Que questões, no relacionamento inter-departamental, devem ser consideradas na implementação eficaz de medidas de protecção portuária em ambiente anti-terrorista utilizando capacidades próprias da Força?

No seguimento do anteriormente exposto, procurando dar resposta às QD colocadas, definiram-se para orientar o estudo as seguintes hipóteses:

- H1: Em ambiente portuário um ataque terrorista pode ser perpetrado de múltiplas formas e o número de alvos apetecíveis é elevado.

- H2: As medidas de protecção existentes têm por base regulamentação internacional e têm surgido como resultado do esforço consertado, multi-disciplinar, de diversas organizações.

- H3: As medidas de protecção existentes podem apresentar lacunas que o O DAT – POW PHP, em desenvolvimento, pode auxiliar a mitigar.

- H4: O carácter multidisciplinar da protecção portuária envolve um leque alargado de entidades pelo que se deve promover o conhecimento mútuo das capacidades e requisitos através duma abordagem à cúpula das organizações.

Para levar a cabo a investigação recorreu-se essencialmente a fontes primárias, a documentação enquadrante no domínio do direito internacional, a documentos doutrinários nacionais, fazendo a sua transposição para um contexto multi-nacional, e a documentos

oficiais que, no âmbito operacional, estabeleceram directrizes para a protecção de Força em ambiente portuário.

Foram igualmente utilizados trabalhos publicados que abordam diferentes vertentes do objecto de estudo, designadamente na caracterização da ameaça assimétrica e na problemática do relacionamento inter-departamentos.

Procedeu-se também à recolha de informação através de entrevistas a alguns membros de organizações nacionais e europeias, militares e civis, designadamente junto da Autoridade Marítima e de autoridades portuárias.

De forma a evitar, tanto quanto possível, eventuais conflitos com o âmbito do termo segurança e dos termos em língua inglesa *"safety"* e *"security"*, adoptou-se o termo **protecção** para fazer referência a matérias atinentes com a prevenção de actos violentos contra instalações portuárias e navios.[2]

[2] A única excepção é a que consta na citação que abre esta introdução, por fidelização para com termos precisos empregues pela personalidade citada.

1. Terrorismo Marítimo

A expressão terrorismo marítimo designa:

> "… a execução de quaisquer actividades ou actos terroristas que tenham lugar no ambiente marítimo, fazendo uso ou tendo como alvo navios ou plataformas no mar ou em portos, ou contra um passageiro ou trabalhador, contra instalações costeiras, ou áreas ou populações portuárias." (Chalk, 2008: 3)[3]

O fenómeno em si é pouco relevante do ponto de vista histórico e estatístico conforme se deduz da base de dados sobre o terrorismo da RAND *Corporation*[4], onde apenas 2% dos actos terroristas ocorridos entre 1976 e 2006 podem ser considerados marítimos.[5] (Greenberg, 2006:9)

A natureza eminentemente conservadora dos grupos terroristas no que respeita à natureza da sua acção traduz-se no recurso a métodos de ataque já testados, afastando-os por isso do ambiente marítimo. Isto é atribuído ao facto de que a condução duma operação no mar requer competências específicas de complexidade crescente em função da complexidade do acto a perpetrar, além da necessidade de dispor de veículos adequados para o transporte e para o ataque. Portanto, a limitada disponibilidade de recursos financeiros e materiais, bem como a complexidade e morosidade do treino requerido para levar a cabo um acto terrorista marítimo relevante, podem ter dissuadido a migração do ambiente e modo normal de operação terrorista para um ambiente adverso e relativamente desconhecido.

Contudo, é imprudente menosprezar o estado actual da ameaça terrorista marítima com base em dados históricos, ainda que recentes, visto que no passado os alvos marítimos não se constituíam como efectivas oportunidades, muito se devendo à falta de capacidade ou de intenção.

---

[3] Citando Quentin, Sophia. Tradução da definição do Grupo de Trabalho sobre o Terrorismo Marítimo do Conselho para a Segurança e Cooperação na Ásia-Pacífico. *Council for Security Cooperation in the Asia Pacific*.

[4] *Research And Development Corporation*

[5] Algumas fontes consideram apenas 1%. *National Memorial Institute for the Prevention of Terrorism* (MIPT).

Ao longo dos últimos anos, desde o virar do século, tem-se assistido a um aumento significativo de ataques terroristas no mar, consequentemente o receio que redes de militantes islamitas Jihadistas estejam a desenvolver capacidades operacionais que extravasam os seus teatros de operação normais, alastrando para o mar, tem crescido entre os países ocidentalizados. De facto, crê-se que Abdel Rahim al-Nashiri[6], responsável pelo planeamento de acções terroristas marítimas da al Qaeda, nomeadamente dos ataques ao USS "Cole" e ao M/V "Limburg", estaria na fase final de planeamento de ataques à navegação mercante ocidental no Estreito de Gibraltar aquando da sua prisão. Na mesma linha, o sírio Lu'ai Sakra, que também se crê estivesse ligado à al Qaeda, estaria envolvido, aquando da sua captura em 2005, num plano que envolvia o uso de embarcações rápidas carregadas com explosivos para abalroar navios de passageiros que transportassem cidadãos israelitas em direcção à Turquia. Deve ainda ser incluída na lista de ataques terroristas marítimos significativos a tentativa falhada contra o USS "The Sullivans" em Janeiro de 2000. Paralelamente aos já referidos ataques e aos planos que, a existirem, dariam continuidade a uma linha de acção já consolidada, diferentes fontes internacionais alegaram que al Qaeda disporia de uma frota navios operando para diversas companhias e sob diversas bandeiras. Ainda que estas alegações nunca chegaram a ser confirmadas, a sua veracidade conferiria uma capacidade substancial para levar acabo um ataque terrorista, quer servindo-se de um dos navios como arma terminal, quer usando-os como veículo de transporte.

Este crescente receio é largamente alimentado pela proliferação da pirataria, ainda que os dois fenómenos sejam diferentes na sua essência, pois no que respeita à natureza mais elementar da sua natureza a pirataria tem como móbil o lucro, enquanto que o terrorismo visa a disrupção política e social. O racional que leva à comparação dos dois fenómenos é o de que as vulnerabilidades existentes e que têm possibilitado a continuidade e até o aumento do fenómeno da pirataria podem igualmente ser aproveitadas para a execução de ataques terroristas, sendo as mais relevantes as seguintes:

- O aumento do tráfego comercial marítimo que, juntamente com um grande número de portos, proporciona inúmeros alvos que apresentam elevado potencial lucrativo;

[66] Conhecido por Ameer al Baar ou Príncipe do Mar

- A maior densidade do tráfego marítimo implica naturalmente um maior número de navios que circula através de estreitos, a menor distância de terra e em pontos de confluência;
- As dificuldades económicas e financeiras de muitos Estados costeiros, as quais se repercutem primariamente sobre as populações, que são fortemente atraídas para o ilícito, e sobre a capacidade de actuação das forças de segurança, designadamente pela falta de investimento nas capacidades de monitorização, vigilância e policiamento da orla costeira;
- A falta de vigilância costeira e de medidas de protecção portuária que se verificam em vários países possibilita a concretização de actos de pequena criminalidade, como roubo ou vandalismo, que por si só não representam um perigo imediato, mas que deixam a nu vulnerabilidades e oportunidades para a concretização de actos terroristas;
- A proliferação do tráfego de armamento;
- A corrupção de alto nível tem facultado fugas de informação relativas a actividades de protecção, actividades comerciais lucrativas e tem permitido a concretização do fenómeno conhecido por "navio fantasma", valioso de *per se* e um potencial veículo de ataque.

Além das vulnerabilidades que se consideram ser catalisadores do fenómeno da pirataria e que podem igualmente ser favoráveis ao perpetrar de actos terroristas marítimos, há ainda a considerar outros fenómenos que podem privilegiar estes últimos, como por exemplo:

- O florescimento duma indústria desportiva e de entretenimento ligada ao mar é igualmente apontada como factor facilitador do acesso de grupos terroristas a recursos e treino necessários que podem conduzir ao desenvolvimento das necessárias competências para actuar em zonas molhadas;
- A disrupção económica provocada por um acto terrorista que consiga afectar, bloqueando ou fechando, uma via marítima crítica ou um porto importante, pondo em causa a actual lógica do transporte global marítimo do *"just in time, just enough"*, que representa cerca de 80% do comércio global, é tida como sendo um poderoso aliciante à acção terrorista.

a. Capacidades terroristas

Na secção anterior ficou clara a existência de oportunidades para concretizar actos terroristas marítimos que derivam duma relativa facilidade de concretização, ao longo dum largo espectro de cenários (conforme se verá em maior detalhe na próxima secção), da visibilidade pública e do potencial impacto político e económico, ou seja, existem condições que, no seu conjunto, tornam o terror marítimo atractivo a extremistas, encontrando-se assim o factor motivacional que poderá mover aqueles grupos.

Contudo, além das oportunidades e da motivação, uma acção terrorista, independentemente da sua natureza, carece que se reúnam capacidades, meios materiais e humanos. O ambiente marítimo, ainda que represente uma oportunidade tentadora, pela sua complexidade implica a aquisição de competências especiais, que podem efectivamente ser criadas ainda que de forma paulatina, o que se considera evidenciado pelo já referido incremento da actividade terrorista neste domínio.

Ainda assim, o número de organizações com reconhecidas capacidades para actuar no ambiente marítimo e que delas já deram provas é relativamente reduzido, havendo a destacar, as seguintes:

- O Exército Provisório da República da Irlanda (PIRA – *Provisional Irish Republican Army*), que tem explorado de forma conspícua as ligações marítimas para assegurar a a cadeia logística no que ao fornecimento de material de guerra geral diz respeito;
- Os separatistas Chechenos, que têm efectuado ataques esporádicos contra férris na vizinhança do Estreito do Bósforo;
- Al-Gama'a al-Islamiyya, que levou a cabo ataques contra paquetes na primeira metade da década dos anos 90 do século XX;
- Organizações palestinas, como o Hamas, a Jihad Islâmica Palestiniana, a Autoridade Palestiniana, o Comando Geral da Frente Popular para a Libertação da Palestina, a Frente Democrática para a Libertação da Palestina e a Frente de Libertação da Palestina, sendo que esta última foi responsável pelo rapto do paquete "Achille Lauro" em 1985;
- O Hezbollah do Líbano, de quem se sabe ter recebido treino marítimo, patrocinado pelo Irão, tendo sido capaz de tirar proveito destas competências adquiridas para movimentar carga e pessoal;

- O Grupo Abu Sayyaf ASG, responsável por inúmeros ataques marítimos a sul da Filipinas, incluindo o afundamento em 2004 do "Super-Ferry 14", que se saldou em 116 mortos;
- O Gerakan Aceh Merdeka, ou Movimento de Libertação de Aceh, que antes de fazer o acordo de paz com o governo indonésio em 2005, foi associado a um significativo número de raptos no Estreito de Malaca, incluindo rebocadores, barcos de pesca e outras embarcações de pequena dimensão;
- Os Tigres Tamil de Libertação, a quem, graças ao seu braço de Tigres Marítimos, se reconhece a maior capacidade de perpetrar ataquem terroristas marítimos, ainda que se julgue que a sua capacidade, quer por falecimento dos operacionais quer por destruição do material, tenha sido substancialmente reduzida como resultado do maremoto de Dezembro de 2004 no Oceano Índico;
- Jamaat al-Tawhid wa'l-Jihad, ou Grupo de Unidade da Jihad, a organização Sunita relacionada com a al Qaeda e que conduziu os anteriormente referidos ataques, ao USS "Cole" em 2000 e ao M/V "Limburg" em 2002.

b. Os cenários prováveis

Diversas são as audiências que têm analisado as possibilidades de um ataque terrorista, designadamente em ambiente marítimo, de onde acaba por ser possível deduzir-se a ameaça e, restringindo o âmbito, considerar um ambiente portuário. Importa pois perceber se existem pontos de concordância entre abordagens distintas abrangendo o sistema de alianças nacional, militar e político, bem como visitar a perspectiva nacional.

(1) Abordagem dos Estados Unidos da América (EUA)

O Serviço de Pesquisa do Congresso dos EUA[7] publicou em 2007 um relatório sobre protecção e terrorismo marítimos, no qual aborda a geração de cenários possíveis como uma conjugação de múltiplas variáveis, considerando diversas possibilidades para

[7] *Congressional Research Service* (CRS)

cada variável, organizadas sistematicamente em forma tabelar[8] (tabela 1) (Parfomak, 2007:7).

Tabela 1: Características dum ataque terrorista marítimo

VARIÁVEIS	POSSIBILIDADES
ACTOR	– Al Qaeda e/ou afiliados – Islamista não militante – Nacionalista estrangeiro – Funcionários portuários descontentes – Outros
OBJECTIVO	– Falecimentos em número significativo – Disrupção portuária – Disrupção do comércio – Desastre ambiental
LOCALIZAÇÃO	– Mais de 360 portos nos EUA – 165 parceiros comerciais dos EUA – 9 locais de compressão/engarrafamento marítimo
ALVO	– Navios militares – Navios de carga – Petroleiros – Paquetes ou férris – População na área portuária – Canais de navegação – Instalações fabris ou industriais portuárias – Plataformas marítimas
TÁCTICA	– Embarcações pequenas e rápidas com explosivos – Pequenas aeronaves com explosivos – Abalroamento com navios – Mísseis lançados a partir de navios – Minas – Ataque por mergulhadores – Ataque à bomba com recurso a veículos subaquáticos autónomos – Explosão de navio tanque – Explosivos em navios de carga – ADM em navios de carga

Sugerem então os autores (Parfomak, 2007:23-25), que os cenários possíveis para um ataque terrorista marítimo podem ser deduzidos seleccionando uma possibilidade para

[8] Adaptação do autor.

cada variável, combinando-as em seguida, obtendo-se assim um cenário lógico e sempre possível.

(2) Abordagem europeia

Em 2005 a empresa de consultoria Det Norske Veritas (DNV) produziu um relatório que apresentava à Comissão Europeia os seus achados sobre o impacto da legislação europeia na protecção dos transportes[9], ainda que o seu enfoque seja na necessidade de protecção do transporte modal terrestre, acaba por abordar também o transporte marítimo e as suas interfaces, o que é natural devido ao carácter intermodal de toda a actividade económica.

Tabela 2: Vulnerabilidades portuárias europeias

FONTES DE RISCO		**ELEMENTOS VULNERÁVEIS**
INFRA-ESTRUTURAS	Vias de ligação	Linhas de navegação Comportas
	Interfaces	Portos oceânicos Portos ou terminais interiores
ELEMENTOS OPERACIONAIS	Sistemas de controlo	*Vessel Traffic Services* (VTS) *Vessel Traffic Managements*
	Sistemas de comunicação	GPS VHF Rede AIS
	Pessoal	Mergulhadores Estivadores Manutenção Administração
	Unidades móveis	Navios Barcaças
CARGA		Não perigosa Explosiva Tóxica Inflamável

[9] DNV (26 October 2005), *Study on the impact of possible European legislation to improve transport security, Final report: Impact assessment*.

Nesse relatório identificam-se como elementos susceptíveis a um ataque terrorista, tanto no que respeita ao sistema de transporte como às cadeias logísticas, envolvendo a navegação, a área molhada e as interfaces com os transportes terrestres, aquelas que se resumem na tabela 2[10].

Na tabela 2 poderia incluir-se outros elementos vulneráveis, por exemplo ao nível das infra-estruturas que aquele estudo não identifica, de entre as fontes de risco com elementos mais vulneráveis a um ataque terrorista, as que respeitam às unidades móveis e à carga, isto devido ao grande número e variedade de operadores activos na cadeia logística, que na Europa podem atingir os 4,7 milhões de companhias, se incluirmos os modos de transporte rodoviários e ferroviários.

Prosseguindo uma sistematização própria a DNV divide os riscos e caracteriza-os em duas grandes categorias, riscos das infra-estruturas e riscos associados à cadeia logística.

Quanto aos riscos para as infra-estruturas, o propósito terrorista seria o de provocar danos sérios ou destruir elementos físicos da cadeia logística com impactos significativos na actividade económica, podendo associar-se a perda dum número significativo de vidas.

Quanto aos riscos da cadeia logística a DNV sugere que o propósito seria provocar danos, mas sobretudo baixas humanas. Neste caso são os elementos operacionais, a carga ou ambos que estão em causa, não se constituindo como alvo, mas como vector de ataque. O relatório subdivide-os ainda em duas subcategorias:

- O uso da cadeia logística como meio de transporte duma arma terminal, quer seja na unidade móvel (navio ou embarcação no caso marítimo), ou dissimulada na carga (engenho explosivo convencional ou nuclear, bem como biológico, químico ou radiológico) que é descarregada ou espoletada;
- O uso de elementos da cadeia logística como armas, sendo que neste caso:
    - A carga pode ser usada como arma, libertando carga perigosa, tóxica ou química ou fazendo explodir uma carga perigosa, preferencialmente em áreas densamente povoadas;
    - A própria unidade móvel pode ser usada como arma, de maneira directa fazendo-a por exemplo colidir e assim causando danos na infra-estrutura,

[10] Adaptação do autor a partir de DNV (2005), op.cit.

podendo implicar a perda de vidas humanas, ou ainda de forma indirecta colidindo com outra unidade móvel que transporte carga perigosa.

(3) Abordagem nacional

O universo de audiências que se tem dedicado a analisar a ameaça terrorista marítima, designadamente a Autoridade Marítima Nacional (AMN), cujas directivas serviram de base ao presente desenvolvimento[11], são em grande medida concordantes com as análises anteriormente abordadas, afirmando designadamente que qualquer navio se pode constituir como um meio de projecção de uma arma de destruição em massa, ou transportar, ainda que inconscientemente, um agente nocivo de largo espectro e capacidade. Além disso, reconhece-se ainda que um navio pode, numa perspectiva diametralmente oposta, ser alvo de ataques terroristas; afirma-se designadamente que os navios de guerra são alvos privilegiados pelo seu valor e pelo simbolismo com que representam o seu Estado, a par dos navios de passageiros, estes pelo elevado número de vidas ameaçadas, enquanto que:

> "os navios de carga podem mesmo ser utilizados como perigosos meios de projecção; a própria natureza de certas cargas de matérias perigosas, potencia a sua explosão provocada, por exemplo em **zonas portuárias**[12], com as consequências ambientais e humanas que facilmente se imaginam."

Ainda no âmbito nacional são consideradas como ameaças principais:

- Ataques a navios nas águas sob jurisdição nacional, quando a navegar, **fundeados ou atracados**, inclusive nas águas interiores;
- Manipulação ou apropriação ilícita da carga, dos equipamentos ou dos sistemas do navio para provocar incidentes de protecção;
- Acções ilícitas ou terroristas contra passageiros e tripulações a bordo de navios;
- Utilização por grupos terroristas, de qualquer tipo de navio, como meio de projecção, de forma a provocar danos a navios, plataformas ou **instalações**

[11] Autoridade Marítima Nacional. Directiva 001/2004, de 22 de Março de 2004, sobre Medidas especiais para reforçar a protecção dos navios que pratiquem portos nacionais
[12] Sublinhado e negrito da responsabilidade do autor.

portuárias, com consequências ambientais e humanas de grande visibilidade e dimensão;

- Danos causados a navios ou a **instalações portuárias**, com recurso ao emprego de engenhos explosivos, fogo posto, sabotagem ou vandalismo.

c. Provável em vez de Possível

De entre as abordagens explanadas anteriormente (EUA, europeia e nacional), é por força de evidência que o espectro de cenários considerado pelos EUA é o mais abrangente de todos. De facto, verificando todas as variáveis que podem caracterizar um ataque terrorista marítimo (ver tabela 1), sendo que qualquer cenário pode ser gerado usando apenas uma possibilidade de cada variável, combinando-a com uma única possibilidade da variável seguinte, mas cobrindo todas as variáveis identificadas, obtém-se um número de combinações muito elevado, sendo que qualquer delas corresponde a um cenário lógico.

Propõe-se, com base naquela tabela, uma simplificação que consiste em eliminar a variável localização, uma vez que cada porto representa uma realidade concreta e diferente, com desafios próprios, com regulamentação e jurisdição que variará igualmente entre países, sendo que o problema da ameaça consubstanciada pela combinação das demais varáveis será comum a todos.

Ainda assim, da análise resultam quatro variáveis com um número de possibilidades distinto, que quando combinadas resultam em 1600 cenários possíveis, mas este número reflecte apenas uma combinação simples, que se ousa chamar básica, uma vez que se pode ainda combinar mais do que uma possibilidade de cada variável, criando assim cenários que continuam a ser lógicos, mas que agora passaram a ser complexos, resultando ademais num número desmedido.

(1) Pragmatismo norte-americano

No relatório do CRS ressalva-se precisamente que o número de cenários possíveis é demasiado vasto para serem convenientemente abordados, sobretudo com constrangimentos ao nível dos recursos financeiros disponíveis, sendo por isso necessário ter uma abordagem extraordinariamente pragmática, avaliando quais serão os cenários mais prováveis e actuar sobre eles preventivamente. Assim, seguindo a lógica pragmática exposta, aquele relatório selecciona os cenários mais prováveis num futuro próximo, apontando para os seguintes:

- Usar um navio porta contentores para introduzir ilegalmente agentes químicos, biológicos ou radioactivos para perpetrar um ataque não convencional de larga escala em terra ou até num porto de grande importância como Roterdão, Singapura, Hong Kong, Dubai, Nova Iorque ou Los Angeles;
- Fazer uso dum navio de aspecto inócuo, por exemplo, de pesca, cabotagem costeira ou rebocador, para transportar armas ou material bélico;
- Sequestrar um navio exigindo resgate, o que, alem de servir como factor motivacional e angariador, poderia servir para financiar uma campanha de violência política de cariz étnico, ideológico, religioso ou separatista;
- Afundar um navio num estreito internacional para perturbar seriamente ou até bloquear o tráfego marítimo;
- Sequestrar um navio tanque de gás liquefeito (LNG) e detoná-lo ou usá-lo como se de um engenho com espoleta de impacto se tratasse, podendo também dar-se o caso de se fazer colidir o navio contra uma infra-estrutura ou contra outro navio;
- Fazer uso duma embarcação rápida para atacar um petroleiro ou uma unidade móvel de perfuração ao largo para afectar o preço do petróleo a nível mundial ou provocar um desastre ecológico de poluição de larga escala;
- Atingir directamente um paquete ou um ferry provocando um número muito elevado de baixas utilizando técnicas tais como: contaminação de água ou comida, detonação dum engenho explosivo improvisado ou através dum abalroamento por uma embarcação rápida.

(2) A visão europeia da ameaça

Os responsáveis pela elaboração do relatório da DNV identificaram um número de cenários que, sendo menos expressivo do que o relatório do CRS, é ainda considerável. Seguindo igualmente uma lógica pragmática, a margem oriental do Atlântico Norte identificou os métodos mais prováveis de intervenção terrorista, que pode ir desde a

tentativa de disrupção por via psicológica até à acção violenta de larga escala, e que se expõem na tabela 3[13].

Tabela 3: Métodos de intervenção terrorista nos transportes europeus

MÉTODOS DE INTERVENÇÃO	DESCRIÇÃO
Incendiário	(Auto explicativo)
Explosão (menos de 30 Kg TNT ou equivalente)	Cargas explosivas pequenas, transportáveis em sacos por uma só pessoa e que podem servir para iniciar uma explosão maior.
Explosão (30 Kg TNT ou equivalente)	Transportável em pequenos veículos
Explosão (3000 Kg TNT ou equivalente)	Transportável em grande veículos (por exemplo em rodovias com camiões)
Ataque com agentes biológicos, bioquímicos ou químicos	Libertação/dispersão
Ameaça terrorista	Ameaça de ataque, como por exemplo uma ameaça de bomba
Nuclear	Detonação duma arma nuclear
Contaminação radiológica	Detonação que resulta na libertação de radiação
Sequestro	Controlo pela força que pode envolver infiltração de agentes
Intervenção física ou mecânica	Sabotagem ou obstrução física
Ciber ataque	Disrupção de sistemas informáticos ou electrónicos

Considerando os 12 métodos de intervenção terrorista constantes da tabela 3, os autores identificam um total de 221 possíveis cenários para um ataque terrorista, considerando o transporte marítimo, rodoviário e ferroviário.

(3) Pragmatismo nacional

Ao pesarmos as análises norte-americana e europeia, acaba-se por encontrar similaridade tal na abordagem da AMN no que respeita aos prováveis cenários de ataque terrorista quando se considera a sua expressão mais básica e pragmática, que só não se pode falar em concordância plena devido a uma mera escolha de palavras.

Naturalmente que tal conformidade resulta da impossibilidade prática de considerar em profundidade todos os cenários, envolvendo alvos, propósitos e formas de ataque

[13] Adaptação pelo autor

terrorista, ainda que os recursos disponíveis e as capacidades existentes sejam substancialmente maiores do que as nacionais.

d. Síntese conclusiva do capítulo

O flagelo do terrorismo, perpetrado sob os mais diversos pretextos, tem-se alheado do ambiente marítimo. O número de ataques terroristas marítimos é de facto diminuto quando comparado com outras formas ou ambientes de actuação.

Contudo, as mais diversas análises apontam inúmeras vulnerabilidades, tanto ao nível das infra-estruturas portuárias como ao nível das unidades móveis (navios e embarcações), sobretudo em águas costeiras ou nos portos, e que tanto podem ser alvos como armas.

Terá sido o reconhecimento das vulnerabilidades, constituindo significativas oportunidades para encetar ataques de dimensão assinalável, com grande visibilidade e com efeitos perversos no normal desenrolar da actividade económica, que levou ao desenvolvimento, sobretudo por parte de grupos islamitas, de capacidades operacionais que permitissem ultrapassar a contento as dificuldades normalmente colocadas pela adversidade do meio marítimo, explorando-o e desviando-se de cenários de actuação consolidados onde, por força do conhecimento já adquirido, poderiam sentir-se mais confortáveis. Assim se explica que o início do século XXI tenha conhecido um incremento da actividade terrorista no mar.

As abordagens norte-americana e europeia admitem a existência dum significativo número de cenários possíveis para um ataque terrorista. A complexidade e custos da organização, recursos humanos e materiais e procedimentos, requerida para fazer face a todas as ameaças é de tal ordem que obriga a concentrar esforços para contrariar os cenários mais prováveis.

É assim que, numa aparente simplificação, encontramos também concordância com as ameaças identificadas pela AMN, reduzindo-as às seguintes:

- Ataques a navios fundeados ou atracados;
- Uso da carga ou dos sistemas dos navios;
- Ataques contra passageiros e tripulações;
- Uso de navios contra outros navios, plataformas ou instalações portuárias;
- Explosão, incêndio, e similares a navios ou a instalações portuárias.

Note-se então que, ainda que a formulação da ameaça não refira especificamente portos ou instalações portuárias, esta é de facto mais provável naquelas áreas ou na sua vizinhança, justificando-se assim uma particular atenção à protecção portuária.

Considera-se assim que se encontra respondida a QD1: *Como se caracteriza a ameaça portuária em ambiente terrorista?* Através da validação da H1: ***Em ambiente portuário um ataque terrorista pode ser perpetrado de múltiplas formas e o número de alvos apetecíveis é elevado.***

2. Protecção Portuária

Para contrariar uma ameaça, independentemente da sua natureza, é fundamental escalpelizar o seu processo. Tratando-se duma ameaça terrorista o exame do seu processo, ou cadeia de actividades dará sempre a sensação de ser generalista, pois as particularidades específicas dum atentado decorrerão das características peculiares dos seus perpetrantes.

Assim, a multiplicidade de potenciais actores e métodos terminais de ataque, em qualquer ambiente, sem que o marítimo ou portuário seja excepção, obriga a que as medidas de protecção adoptadas tenham uma natureza abrangente, tentando contrariar aquela ameaça tão cedo quanto possível e em qualquer fase do desenvolvimento da actividade, conforme pretende ilustrar a figura 1 (Jackson, 2007: 2 - 5).

Logo após os atentados de 11 de Setembro de 2001, as esmagadoras vulnerabilidades, por demais evidentes, a ataques inesperados e sem pré-aviso tornaram-se visíveis à generalidade da comunidade internacional, dando lugar a um largo número de reacções. Não se demorou a sentir o efeito da dedução de que os ataques então sofridos poderiam estender-se, ou ser reproduzidos, com outros vectores e em ambientes diferentes, incluindo o marítimo e dentro deste o ambiente portuário.

A necessidade de elevar o grau de protecção para fazer face a uma ameaça terrorista no mundo marítimo levou a que um alargado número de organizações, quer internacionais quer num âmbito mais restrito, mas com impacto ou influência transoceânica, implementassem medidas inovadoras, não só para a época, mas também actualmente, uma vez que, decorridos dez anos, a sua implementação ainda não pode ser considerada global.

Considerando que as medidas mais significativas já tomadas no âmbito da protecção portuária, têm um papel enquadrante das iniciativas emergentes, aquelas serão em seguida abordadas num quadro de referência das organizações que lhe dão génese:

a. No âmbito da Organização Marítima Internacional (IMO)

A IMO, ainda que condicionada pelo facto de ser um órgão regulador operante ao nível da ONU, implicando que as suas decisões e o seu grau vinculativo dependem de consensos políticos muitas vezes obtidos ao mais alto nível, terá sido das primeiras organizações internacionais a implementar medidas de prevenção contra ataques terroristas envolvendo o meio marítimo.

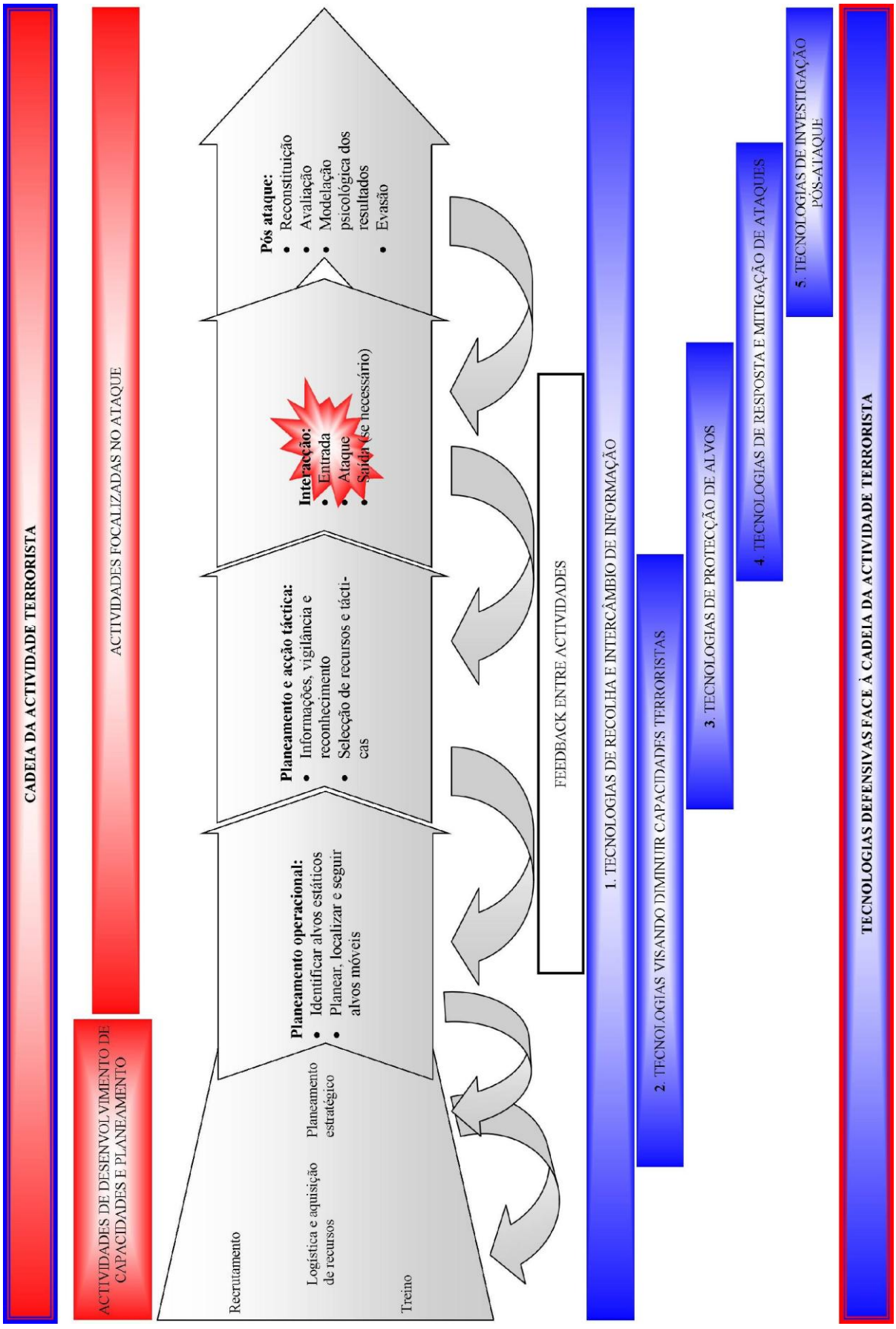

Figura 1: Cadeia das Actividades Terroristas face às Actividades de Contra-terrorismo

(1) Código Internacional para a Protecção dos Navios e das Instalações Portuárias

No capítulo das medidas de protecção física o Código Internacional para a Protecção dos Navios e das Instalações Portuárias (código ISPS[14]) constitui-se como o elemento que mais revolucionou o ambiente marítimo, quer pela sua abrangência global quer pela rapidez de implementação.

Os trabalhos desenvolveram-se entre Fevereiro e Dezembro de 2002 culminando numa conferência diplomática que adoptou uma alteração à Convenção Internacional para a Salvaguarda da Vida Humana no Mar [15]de 1974 (SOLAS) e também o Código ISPS.

Até aquela altura a Convenção SOLAS considerava apenas os aspectos relacionados com a segurança do transporte marítimo, tendo então passado a considerar igualmente as matérias relacionadas com a protecção do transporte marítimo, sendo que o Código ISPS teve e tem por objectivo estabelecer, ao nível da protecção, a ligação entre o transporte marítimo, os navios e as instalações portuárias, ou seja, a protecção global da actividade em conjunto com os meios e os terminais de interface, considerando estes últimos como essenciais para o desenvolvimento da actividade.

O Código ISPS tem por objectivo o estabelecimento duma moldura internacional para a cooperação interestadual, envolvendo os governos, órgãos administrativos e as indústrias portuárias e de navegação, de forma a identificar ameaças e tomar medidas preventivas contra incidentes ou quebras de protecção relacionadas com navios e instalações portuárias envolvidos no tráfego internacional, assegurando uma efectiva e atempada troca de informação de protecção e estabelecendo uma metodologia de efectuar auditorias de protecção, envolvendo metodologias e planos suficientemente flexíveis para se adequarem a diferentes tipos e níveis de ameaça; sendo tudo concorrencial para a edificação dum ambiente de confiança entre todos os actores no que respeita ao nível de protecção.

---

[14] International Ship and Port Facility Security Code
[15] *International Convention for the Safety of Life at Sea* (SOLAS)

O Código ISPS, dividido em duas partes, estabelece na sua Parte A requisitos obrigatórios para os navios e para as instalações portuárias e, na sua Parte B, directivas que devem ser implementadas pelos Estados contratantes. Em todo o caso, aquelas medidas aplicam-se a navios de passageiros, a navios de carga com 500 T de arqueação bruta[16] ou mais, a unidades móveis de perfuração ao largo e às instalações portuárias que recebem tráfego marítimo internacional.

Realçam-se, por se considerar relevantes e enquadrantes do tema, as medidas aplicáveis a navios que estão previstas no Código ISPS e que são as seguintes:

- A adopção dum seu número de identificação, consubstanciado fisicamente e de forma indelével;
- A instalação dum *Automatic Identification System* (AIS);
- A disponibilidade dum sistema de alerta que difunda um alarme caso ocorra uma acção hostil contra o navio;
- A concretização dum registo contínuo da actividade do navio, o *Continuous Synopsis Record* (CSR), que sob a forma de documento funciona como uma espécie de *curriculum vitae*;
- E dum Certificado Internacional de Protecção (CIP).

O Código ISPS prevê igualmente um conjunto de medidas, tanto activas como passivas, a implementar a bordo dos navios e nas instalações portuárias. Medidas essas que são adoptadas obedecendo a uma lógica de resposta em função do grau do grau de ameaça, correspondendo a três níveis diferentes:

- Nível 1: Rotina, as operações portuárias decorrem normalmente;
- Nível 2: Adopção de algumas medidas de protecção, restritivas quanto à operação normal, mas durante um período de tempo limitado;
- Nível 3: Elevada probabilidade de ocorrência dum incidente de protecção.

---

[16] Arqueação Bruta (GT) é uma medida do volume total dos espaços fechados do navio, reflecte por isso a dimensão do navio. É calculada pela expressão $GT = K_1 V$, em que:
V – volume total de todos os espaços fechados do navio [m^3]
$K_1 = 0.2 + 0.02\log_{10}V$

Uma das novidades introduzidas foi a de personalizar e personificar a protecção, ou seja, obrigar à nomeação de responsáveis pelas medidas de protecção; considerando, além dos navios e das instalações portuárias, os armadores; mandatando-se esses responsáveis para a elaboração de planos de protecção específicos e efectuando obrigatoriamente uma análise de risco, sendo que apenas então será emitido o CIP. O treino do pessoal e a execução de exercícios tampouco foram descurados.

O código ISPS prevê também a possibilidade de se redigir uma declaração de protecção, que é uma espécie de memorando de entendimento entre os responsáveis pelo navio e o porto que o recebe onde, em função do risco para as pessoas, para a propriedade e para o ambiente, se definem as responsabilidades recíprocas das partes. Desde a sua entrada em vigor, o código ISPS permitiu igualmente que, por razões de protecção, as autoridades competentes do Estado pudessem proceder a inspecções em navios, quer no porto quer na sua vizinhança, imediatamente antes da sua prática.

Seguindo a lógica reguladora já exposta, definiram-se igualmente as responsabilidades específicas dos actores presentes, designadamente:

- Estados aderentes;
- Companhias;
- Comandantes de navios;
- Portos ou autoridades portuárias.

A Parte B do código ISPS contém, de forma muito detalhada, um conjunto de recomendações, pretendendo-se que sirvam como uma espécie de guia para os diversos actores envolvidos na sua adopção e implementação operacional.

Aos Estados assinantes é requerida a nomeação de organizações de protecção, tanto para os navios como para as instalações portuárias, bem como o estabelecimento de pontos de contacto, nacionais ou regionais, para a efectiva gestão dos níveis de protecção e para o intercâmbio de informação relacionada com aspectos de protecção. Com o intuito de facilitar a sua implementação, o código ISPS apresenta ainda propostas detalhadas quanto à avaliação do risco e aos planos de protecção que devem ser preparados, quanto ao treino de pessoal e à realização de exercícios e, além disso, tipifica as situações e esclarece a

fórmula de redacção da já referida declaração de protecção (memorando de entendimento) entre os responsáveis pelo navio e o porto.

(2) Recolha e partilha de informação

A edificação dum panorama marítimo abrangente, com recurso a meios de vigilância, detecção e comunicações, frequentemente associada à obrigatoriedade de efectuar relatos por parte dos navios mercantes, é uma necessidade sentida e colocada em prática desde há largos anos por autoridades marítimas e até portuárias sob a forma de sistemas de controlo de tráfego marítimo[17], vulgarmente referidos pela abreviatura da designação em língua inglesa VTS, cuja tradução à letra é *Vessel Trafffic Service*.

A IMO é também a organização responsável pelo desenvolvimento da documentação de base que orienta o estabelecimento daqueles sistemas sendo em última instância o organismo que autoriza e oficialmente difunde o seu estabelecimento.

Uma das ferramentas tecnológicas que no início do século XXI foi colocada à disposição do mundo marítimo foi o já referido AIS, um sistema automático de transmissão e recepção de dados dos navios, relativos tanto a características estáticas como dinâmicas e considerando também a viagem específica que realiza. O AIS visava inicialmente proporcionar aos navios no mar um meio de detecção avançado que suprisse as lacunas do radar, contribuindo assim para a segurança da navegação.

Através duma alteração à convenção SOLAS, o AIS foi introduzido enquanto requisito obrigatório no ano 2000, tendo inicialmente como data limite para a sua implementação a bordo Julho de 2007; contudo, os acontecimentos de 11 de Setembro de 2001, e a percepção de que o AIS contribuiria significativamente para a edificação dum panorama marítimo levou a que se apressasse a sua implementação, tendo-se tornado obrigatória a sua implementação até 31 de Dezembro de 2004.

[17] Em Portugal, ainda que à data apenas exista cobertura do mar em do território continental até 50 M de costa, o Sistema Nacional de Controlo de Tráfego Marítimo entrou em funcionamento em 2008, tendo sido oficialmente inaugurado apenas em 2009

O alcance do AIS, consequentemente do panorama por ele proporcionado, é limitado às características da transmissão em VHF, ainda que em condições anormais de propagação se possam verificar alcances de algumas centenas de milhas náuticas.

Para fazer face a esta limitação, tendo presente as preocupações proteccionistas, associando-as a outras de natureza económica e de preservação do meio marinho, levantou-se a necessidade de localizar e seguir o percurso de navios mercantes a longas distâncias, desenvolvendo-se assim o sistema *Long Range Identification and Tracking* (LRIT) que permite monitorizar a navegação até 1000 M do Estado de bandeira do navio em questão. A obrigatoriedade da instalação dum equipamento LRIT foi vertida na Convenção SOLAS no ano de 2006, tornando-se efectiva no início de 2009.

b. No âmbito da Organização Internacional do Trabalho (ILO[18])

Os marítimos estão directamente envolvidos no transporte internacional de bens e de passageiros, incluindo o transporte de matérias perigosas. Além disso, os tripulantes têm normalmente acesso autorizado, ou pelo menos acesso facilitado, a todas as áreas portuárias, incluindo as de acesso restrito.

A natureza particular, até mesmo especial, das condições de vida e de trabalho das tripulações levou a que a ILO tivesse promovido adoptado um vasto número de Convenções e de Recomendações que se lhes aplicam de forma dedicada. Esta organização decidiu, em Janeiro de 2001, que realizaria uma "sessão marítima" em 2005 visando congregar num único instrumento, na medida do possível, os cerca de cinquenta documentos aplicáveis à área marítima.

Contudo, talvez sem surpresa, na primeira metade de 2002 surgiu um item urgente que passou a constar da agenda da 91ª sessão da ILO, que se realizou em Junho de 2003, e que teve por objecto a revisão da Convenção 158 sobre os Documentos de Identificação dos Marítimos (1958). De facto, a identificação dos marítimos, uma das grandes preocupações da IMO em termos de protecção, é uma competência que recai no âmbito da ILO; nomeadamente essa

[18] *International Labour Organization*

documentação de identificação carece de ser inequívoca e verificável numa fonte devidamente creditada.

c. No âmbito da Organização Mundial Aduaneira (WCO[19])

Em Junho de 2002 a WCO adoptou a Resolução sobre a Protecção e Facilitação da Cadeia Logística de Comércio Internacional. Organizou, na dependência directa do seu Secretariado-geral, um Grupo de Trabalho para definir medidas de protecção do comércio internacional contra ataques terroristas e de protecção da cadeia logística contra o seu uso indevido, designadamente no que respeita ao transporte de armas de destruição em massa (ADM) para fins terroristas, tendo desenvolvido a sua agenda em torno dos seguintes cinco tópicos prioritários:

- Questões legais e processuais;
- Assuntos comerciais e relacionamento com outras organizações;
- Desenvolvimento de capacidades;
- Implementação e informação;
- Promoção.

Espera-se que deste trabalho resulte um conjunto alargado de medidas:

- O desenvolvimento duma ferramenta de avaliação situacional que auxilie as autoridades aduaneiras no estabelecimento de regimes de protecção na cadeia logística;
- Acesso das autoridades aduaneiras a uma base de dados da WCO sobre verificações técnicas e equipamento de detecção;
- Revisão da Convenção de Contentores da WCO de 1972;

Logo a partir de Junho de 2003 começaram a vir a lume uma série de instrumentos, designadamente:

[19] *World Custom Organization*

- Revisão do modelo de dados da WCO, incluindo os principais elementos necessários às aduanas para a detecção de encomendas de elevado risco;
- Guia para os membros da WCO com vista a habilitá-los a adoptar uma base legal para a recolha, transmissão e troca de dados aduaneiros sem comprometer a necessária confidencialidade;
- Guia para a promoção da cooperação entre aduanas e indústria com vista a aumentar a protecção da cadeia logística e facilitar o fluxo de comércio internacional.

d. No âmbito do G8

O G8 também desde cedo, especificamente desde Junho de 2002 com a cimeira de Kananaskis, deu génese à abordagem da problemática do transporte em contentores e do seu impacto na protecção marítima.

Os membros do G8 encetaram um esforço concertado de cooperação com a IMO, na implementação das medidas geradas no seu seio, nomeadamente a alteração da Convenção SOLAS de forma a implementar a obrigatoriedade da instalação do AIS a bordo dos navios, a par da implementação do código ISPS. Além disso, firmou-se o compromisso de desenvolver e implementar um regime de protecção global ao transporte de carga em contentores, visando a detecção daqueles que são potencialmente perigosos e o estabelecimento de procedimentos para proceder ao exame, bem como o assegurar o seu transporte sem incidentes.

Foi desde então também iniciado um esforço de colaboração com a WCO para um melhor controlo de mercadorias e a partilha internacional de informação relevante para a protecção do transporte e comércio mundial.

Assim, pode-se afirmar que as principais economias mundiais têm vindo a actuar concertadamente com Organizações Internacionais no desenvolvimento e implementação das medidas de protecção que nos últimos anos passaram a dominar o espectro do transporte e comércio mundiais, com especial relevância para o transporte marítimo.

e. No âmbito da *International Organization for Standardization* (ISO)

A ISO tem vindo a desenvolver desde 2004 um conjunto de especificações, que com revisões regulares, visam a auxiliar a aplicação coerente de medidas de protecção da cadeia logística em geral e das instalações portuárias em particular, estabelecendo linhas de orientação para a operacionalização das medidas implementadas pelas organizações anteriormente referidas.

Destacam-se as especificações:

- ISO 28000:2007, que define os requisitos para um sistema de gestão da protecção, incluindo os aspectos críticos para garantir a protecção da cadeia logística.
- ISO 28001:2007, que estabelece os requisitos e fornece orientações para que as organizações que se relacionam com a cadeia logística internacional possam desenvolver e implementar procedimentos de protecção à cadeia logística e estabelecer e documentar um nível mínimo de protecção a uma cadeia logística ou a um dos seus segmentos.
- ISO 20858:2007, que cria o enquadramento para que as autoridades portuárias possam conduzir uma avaliação de protecção do porto, auxiliando na elaboração e dum plano de protecção portuário, tal como é exigido pelo código ISPS, e estabeleçam as competências dos seus funcionários na condução daquelas actividades.

f. As medidas de protecção tomadas pelos EUA

Após o ataque de 11 de Setembro de 2001 os EUA iniciaram a adopção unilateral dum conjunto de medidas de protecção que em larga escala se antecipavam àquelas que estavam a ser negociadas em *fora* internacionais. No contexto da protecção marítima, os EUA têm assumido que a matéria é de relevante interesse doméstico, sendo que, um pouco à semelhança do que já se verificava para a aviação civil, os operadores que desejam aceder àquele mercado não têm outra alternativa que não seja a de corresponder positivamente às medidas impostas.

Tabela 4: Âmbito do MTSA

Aplicação a	Navios dos EUA e de outros países
Com as seguintes características	• Trabalhe com explosivos, gás natural ou perigosos, outras cargas perigosas • Transfira produtos petrolíferos ou matérias perigosas • Abrangidos pelo capítulo XI da Convenção SOLAS • Transporte mais do que 150 passageiros em viagens domésticas • Transporte de passageiros em viagens internacionais • Transporte mais do que 12 passageiros de/para qualquer porto canadiano nos Grandes Lagos • Transporte carga e tenha enquanto registo mais do que 100 T de arqueação bruta • Barcaças transportando carga regulada
Requisitos MTSA	• Efectue uma avaliação de protecção de navio • Submeta à USCG[20] para aprovação um Plano de Protecção do Navio • Satisfaça outras medidas MTSA

Desde então que se sucedem as iniciativas parlamentares no âmbito da protecção, sendo que no caso marítimo há a destacar a aprovação pelo Congresso do *Maritime Transportation Security Act of 2002 (S.1214)* (MTSA), regulando a implementação de medidas de protecção, quer em navios quer em instalações portuárias, à semelhança do código ISPS, sendo de facto afirmado pelas autoridades norte-americanas que se trata do instrumento legal equivalente ao código ISPS da IMO[21], o que não é de estranhar atendendo a que o desenvolvimento de ambos decorreu em paralelo. A tabela 4 resume a abrangência do MTSA.

As instalações portuárias localizadas nos portos ou vias de comunicação dos EUA ou adjacentes, que lidem com os navios descritos na tabela 4 são igualmente abrangidas pelo MTSA.

A necessidade de coordenar e sincronizar a actuação dos departamentos do Estado com responsabilidades na matéria motivou a criação do *Department of Homeland Security*.

[20] *United States Coast Guard*

[21] http://homeport.uscg.mil/WebHelp/Guest/Content/About%20Homeport/Maritime%20Transportation%20Security%20Act.htm

Das medidas tomadas realçam-se três, nomeadamente:

- Regra das 24 horas; introduzida através de alterações à legislação aduaneira, obrigando a que o manifesto de carga dos navios que procedem para portos dos EUA chegue às autoridades aduaneiras 24 horas antes de serem efectivamente carregados nos portos de origem, se estes forem no estrangeiro. Esta regra entrou em vigor em 2003.
- *Container Security Initiative* (CSI); que resultou do facto de que cerca de 90% da carga transportada por via marítima segue dentro de contentores, sendo que os EUA recebem nos seus portos, provenientes de diferentes países, mais de 30.000 contentores por dia. A iniciativa teve início em 2002 sendo implementada com a participação directa de agentes aduaneiros e consiste em:
  - Estabelecer critérios de protecção visando a identificação de contentores com risco elevado;
  - Efectuar uma verificação prévia da carga dos contentores antes da sua chegada aos EUA;
  - Fazer uso de meios tecnológicos avançados para efectuar a verificação prévia de contentores com risco elevado;
  - Desenvolver e difundir o uso de "contentores inteligentes".

Esta iniciativa norte-americana teve inicialmente como alvo vinte portos europeus e asiáticos[22], mas alastrou rapidamente e actualmente são 58 os portos envolvidos na iniciativa[23], a qual reforça igualmente a regra das 24 horas, que foi na

[22] Algeciras, Antuérpia, Bremerhaven, Busan, Felixstowe, Génova, Hamburgo, Hong Kong, Kaohsiung, Kobe, La Spezia, Laem Chabang, Le Havre, Nagia, Roterdão, Xangai, Shenzhen, Singapura, Tóquio, Yokohama.

[23] http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/ports_in_csi.xml
America: Montreal, Vancouver e Halifax (Canada), Santos (Brasil), Buenos Aires (Argentina), Puerto Cortes (Honduras), Caucedo (República Dominicana), Kingston (Jamaica), Freeport (Bahamas), Balboa, Colón e Manzanillo (Panama), Cartagena (Colômbia); **Europa:** Roterdão (Holanda), Bremerhaven e Hamburgo (Alemanha), Antuérpia e Zeebrugge (Bélgica), Le Havre e Marselha (França), Gotemburgo (Suécia), La Spezia, Génova, Nápoles, Gioia Tauro e Livorno (Itália), Felixstowe, Liverpool, Thamesport, Tilbury, e Southampton (Reino Unido), Pireo (Grécia), Algeciras, Barcelona, e Valência (Espanha), Lisboa (Portugal); **Asia:** Singapura (Singapura), Yokohama, Tóquio, Nagoya e Kobe (Japão), Hong Kong, Shenzhen e Shanghai (China), Pusan (Coreia do Sul), Port Klang e Tanjung Pelepas (Malásia), Laem Chabang (Tailândia), Dubai,

verdade estendida ao restante tráfego marítimo geral (a granel e outro), uma vez que já era aplicada no transporte de carga em contentores.

A influência dos EUA e a percepção da necessidade de implementar medidas de protecção, que numa perspectiva de custo/eficácia fossem viáveis, levaram a que as autoridades portuárias da Europa acabassem por aderir à iniciativa sem que a União Europeia tivesse qualquer intervenção, pelo menos inicialmente.

– *Proliferation Security Initiative* (PSI); é uma iniciativa de "cooperação multinacional com o objectivo de desenvolver um esforço ao nível global de elaboração de normas contra a proliferação e o tráfico de armas de destruição em massa (ADM) – uma resposta global e continuada no tempo e no espaço é fundamental, para um problema também ele global e duradouro" (Barata, 2010), que surge na sequência da detecção de mísseis escondidos em sacos de cimento na carga do navio "So San" enquanto navegava no oceano Índico. A iniciativa procura o compromisso internacional com vista a:
  - Impedir a transferência de e para Estados e actores não estaduais de ADM e material relacionado, incluindo vectores de utilização;
  - Desenvolver procedimentos que facilitem a cooperação e a troca de informação entre Estados;
  - Contribuir para tornar as autoridades capazes de actuar de forma mais robusta na execução de tarefas de interdição.

g. A postura da União Europeia

A União Europeia também tem tido como uma das suas prioridades a protecção do transporte como um todo, numa abordagem holística da cadeia logística, incluindo naturalmente o transporte marítimo.

Contudo, a União Europeia tem privilegiado o desenvolvimento das medidas de protecção na concertação internacional que se vem desenvolvendo no âmbito da IMO, constituindo-se como órgão de cúpula dos Estados membros. Regista-se a preocupação entre as instituições europeias precisamente pelo facto

(Emiratos Árabes Unidos), Kaohsiung e Chi-Lung (Formosa), Colombo (Sri Lanka), Port Salalah (Oman), Port Qasim (Paquistão), Ashdod e Haifa (Israel); **África:** Durban (África do Sul) e Alexandria (Egipto).

de que a CSI foi implementada por alguns portos de Estados membros sem sua consulta ou regulação; não sendo claro se aquelas preocupações ou reservas derivam do receio de que as suas competências sejam contornadas unilateralmente pelos actores ou pelo receio de que, ao seguirem tal procedimento, os Estados membros possam afectar negativamente o comércio internacional ou sejam incompletas, na medida em que as acções de protecção carecem uma abordagem holística, portanto duma postura combinada e concertada no que respeita à implementação e monitorização de efeitos, que se tem verificado ao longo dos últimos anos. Além disso, existe a preocupação quanto à possibilidade de que a implementação de medidas de protecção de forma desregrada poderá promover a desigualdade competitiva entre portos, inclusive dentro da União Europeia, ferindo o princípio de reciprocidade entre parceiros comerciais.

A União Europeia tem participado activamente no desenvolvimento das iniciativas que têm surgido no seio das organizações internacionais antes referidas, bem como naquelas que são unilateralmente iniciadas pelos EUA, designadamente na transposição para a ordem europeia do código ISPS[24].

A atenção que estes assuntos têm merecido acabou por promover uma abordagem de protecção não só de estruturas e de meios de transporte, mas de toda a cadeia logística necessária às trocas comerciais e consequentemente ao desenvolvimento económico, considerando que uma cadeia de protecção é tão segura quanto o for o seu elo mais fraco.

A União Europeia tem estado na linha da frente em diversas vertentes ou abordagens à protecção portuária, como por exemplo, na uniformização da identificação individual que permite o acesso às instalações portuárias, que permite apesar do avultado investimento inicial, quer por parte das autoridades como dos agentes económicos, um controlo crescente no que respeita a

[24] Regulamento (CE) 725/2004, do Parlamento Europeu e do Conselho, de 31 de Março de 2004, relativo ao reforço da protecção dos navios e das instalações portuárias
Directiva 2005/65/EC, do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005, relativo à melhoria da protecção portuária

acessibilidades, uma caracterização de perfis individuais e corporativos facilitada e a troca de informação entre as autoridades de diferentes Estados membros.

Contudo, a implementação de medidas de protecção é potencialmente nefasta podendo inibir ou diminuir os fluxos comerciais, afectando a actividade económica; contudo, este é um aspecto que nunca deixou de ser considerado, promovendo-se mesmo estudos sectoriais e multi-disciplinares sobre o impacto da sua implementação.

O controlo das fronteiras da União tem sido também uma preocupação que tem merecido o desenvolvimento de programas específicos que incluem a transposição para o domínio marítimo de algumas dessas medidas, designadamente naquilo que respeita à troca de informação automatizada entre agentes aduaneiros. Essa preocupação consubstancia-se na conclusão nº 42 do Conselho Europeu de Laeken, de 14 e 15 de Dezembro de 2001[25]:

> "Melhor gestão dos controlos da fronteira externa da União ajudará no combate ao terrorismo, redes de imigração ilegal e de tráfego de seres humanos. O Conselho Europeu solicita ao Conselho e à Comissão que promova os ajustes necessários de cooperação entre os serviços responsáveis pelo controlo das fronteiras externas e examinar as condições em que se possa criar um mecanismo ou serviço comum responsável pelo controlo das fronteiras [...]."

A preocupação e empenho da União Europeia na luta contra a proliferação de ADM, indo ao encontro da PSI norte-americana, consubstancia-se no estabelecimento duma estratégia própria[26], que nasceu a partir do Conselho Europeu de Tessalónica, em 2003. A resolução dos órgãos europeus quanto este assunto está claramente expressa na seguinte afirmação:

---

[25] Tradução do autor. Citação retirada do Comunicado da Comissão ao Conselho e ao Parlamento Europeu *TOWARDS INTEGRATED MANAGEMENT OF THE EXTERNAL BORDERS OF THE MEMBER STATES OF THE EUROPEAN UNION*. COM(2002) 233

[26] *Strategy Against the Proliferation Weapons of Mass Destruction*

> "A União Europeia deve fazer uso de todos os seus instrumentos para prevenir, dissuadir, deter e, se possível, eliminar os actos de proliferação que causam preocupação ao nível global."[27]

Já no que se refere à edificação do panorama marítimo e da partilha de informação, onde se inclui a transposição para direito comunitário[28] das alterações à Convenção SOLAS que versam sobre a implementação do LRIT, a União Europeia tem sido particularmente activa. A afirmação anterior consubstancia-se na publicação do Roteiro para o estabelecimento dum "Ambiente Comum de Partilha de Informação" do domínio marítimo europeu[29], onde se lê:

> "A necessidade de partilhar informação, **em especial nos casos de ameaça iminente**, deve ser avaliada pelo seu detentor face ao risco de não a partilhar. Tal melhoria de panorama aumentará a eficiência das autoridades dos Estados membros e melhorará a relação custo – eficácia."[30]

Neste mesmo âmbito, a Agência Europeia de Segurança Marítima (EMSA[31]), desenvolve actualmente o *Integrated Maritime Data Environment* que acabará por ser uma plataforma informática que integrará outras redes de informação já existentes, como o SafeSeaNet, o CleanSeaNet, o LRIT e o "Thetis". Outro exemplo que ilustra a importância do panorama marítimo e da difusão da informação inter-agentes é o apoio que a EMSA presta à força naval que conduz a Operação "Atalanta"[32], fornecendo detalhes relativos à localização e características da navegação mercante esperada na área, contribuindo decisivamente para a *Maritime Situational Awareness*[33].

---

[27] Tradução do autor. Nota do Conselho da União Europeia 15708/03, de 10 de Dezembro
[28] Directiva 2009/17/EC do Parlamento Europeu e do Conselho, de 23 de Abril de 2009
[29] COM(2010) 584. Comunicado da Comissão ao Conselho e Parlamento Europeu, de 20 de Outubro de 2010
[30] Tradução do autor. Negrito da responsabilidade do autor
[31] *European Maritime Safety Agency* (EMSA)
[32] Conduzida pela União Europeia na região do Golfo de Aden com o objectivo principal de garantir a protecção aos navios do Programa Alimentar Mundial e complementarmente combater a pirataria naquelas águas.
[33] *Maritime Situational Awareness*: O conhecimento e compreensão efectivos de tudo quanto no domínio marítimo pode ter impacto na segurança e protecção.

h. Síntese conclusiva do capítulo

Ao verificar a complexidade da protecção portuária facilmente se conclui que a melhor forma de a conseguir plenamente seria a colocação duma barreira, tipo portão, de acesso absolutamente controlado, ou até, em abuso duma visão extraordinariamente proteccionista, vedar o porto em definitivo, o que naturalmente não é possível, até do ponto de vista do objecto, da função e da etimologia deixaríamos de falar em actividade portuária e portanto de protecção portuária.

Ao analisar as iniciativas que têm vindo a ser implementadas no plano internacional verifica-se uma substancial incidência nas tecnologias defensivas face à actividade terrorista do 1.º e 2.º escalão de acordo com a figura 1, nomeadamente a recolha e partilha de informação e a diminuição das capacidades terroristas, e ainda no 4.º escalão que corresponde à resposta e mitigação de ataques.

As medidas de protecção portuária são de carácter físico e organizacional e assentam no controlo do tráfego marítimo, no treino e certificação das tripulações e na monitorização estrita da carga transportada, mas também ao nível das infra-estruturas portuárias com o controlo de acessos, de pessoas e mercadorias, no treino para fazer face a situações de emergência e na gestão de todas as medidas implementadas, verificando e credibilizando a organização através dum sistema de auditorias.

Considera-se assim respondida a QD2: *Qual a natureza das medidas existentes para fazer face à ameaça terrorista em ambiente portuário?* Através da validação da H2: ***As medidas de protecção existentes têm por base regulamentação internacional e têm surgido como resultado do esforço consertado, multi-disciplinar, de diversas organizações.***

3. Transposição e aplicação das medidas de protecção portuária

Os Estados signatários da Convenção SOLAS verteram para o Direito interno as providências do código ISPS e operacionalizaram-no em maior ou menor medida, mas com natural preponderância para aqueles que desenvolvem um relacionamento comercial por via marítima com os EUA e desse universo com maior ênfase para os Estados membros da União Europeia, sendo este racional igualmente válido no que respeita à adesão à CSI para o caso dos portos com grande movimento de carga em contentores.

Para uma real efectivação das medidas referidas foi necessário legislar o relacionamento de múltiplas entidades que no capítulo interno, mas em áreas específicas, exerciam algum tipo de autoridade e funções de protecção, fossem elas preventivas ou reactivas, dando às medidas de protecção portuária o carácter multidisciplinar que, conforme se deduziu no capítulo anterior, é fundamental para contrariar com maior probabilidade de sucesso a ameaça terrorista às instalações portuárias. No caso português a matéria foi regulamentada inicialmente pelo despacho conjunto n.º 168/2004, de 8 de Março[34] e pelo Decreto-Lei n.º 226/2006, de 15 de Novembro, estabelecendo-se a Autoridade Competente para a Protecção do Transporte Marítimo e dos Portos, com um órgão consultivo próprio, o Conselho Consultivo para a Protecção do Transporte Marítimo e dos Portos, que congrega representantes de todos os organismos ou entidades com competências em matéria de protecção do transporte marítimo e dos portos, competências essas que foram também definidas no referido diploma.

Considera-se relevante a transposição para a ordem interna da evidência da complexidade da matéria da protecção do transporte marítimo e dos portos, a qual deriva da multidisciplinaridade que se vê reflectida no alargado número de departamentos considerados, nomeadamente:

- O Instituto Portuário e dos Transportes Marítimos;
- A Autoridade Marítima Nacional;
- As Capitanias dos Portos;
- As Administrações Portuárias;

[34] Publicado no Diário da República, 2.a série, n.o 72, de 25 de Março de 2004

- A Polícia Judiciária;
- O Serviço de Informações de Segurança;
- A Direcção-Geral das Alfândegas e dos Impostos Especiais sobre o Consumo;
- O Serviço de Estrangeiros e Fronteiras;
- A Autoridade Nacional de Saúde;
- A Polícia de Segurança Pública; e
- A Guarda Nacional Republicana.

O mesmo diploma determina ainda, ao nível da operacionalização da política de segurança e protecção, a constituição duma Comissão Consultiva de Protecção do Porto e dum Centro Coordenador de Operações de Protecção do Porto (CCOPP), funcionando este último em instalações da Autoridade Portuária ou da Capitania, cabendo ao Capitão do Porto coordenar a aplicação das medidas previstas no Plano de Protecção do Porto (PPP) sempre que seja requerido elevar o nível de segurança.

Ainda que pareça tratar-se duma organização complexa, o nível de coordenação e de cooperação institucional é satisfatório[35, 36], tal tem sido constatado não apenas com a realização de exercícios, mas também em situações que obrigaram à activação real do CCOPP do porto de Lisboa, que teria sido capaz de coordenar as respostas necessárias, ainda que se tenha verificado tratar-se de situações de falso alarme[37].

a. Infra-estruturas críticas e os limites do porto

Um dos aspectos fundamentais relativos à implementação de medidas de protecção é determinar concretamente o que há a proteger e de que forma ou até que extensão. Verifica-se, contudo, que mesmo para os portos certificados internacionalmente existem ainda duas grandes preocupações, nomeadamente a avaliação e classificação das infra-estruturas e a delimitação da área portuária; ou seja, do estabelecimento da fronteira,

---

[35] Opinião do Capitão-de-mar-e-guerra Matos Nogueira (Oficial de Ligação entre o Comando Naval e a Direcção Geral da Autoridade Marítima), veiculada em entrevista realizada em 16 de Fevereiro de 2011, corroborada pelo Comandante Miguel Ângelo Taveira Rodrigues (Oficial de Protecção do Porto de Lisboa), em entrevista realizada em 18 de Fevereiro de 2011 e pelo Engenheiro Carlos Seixas da Fonseca (Director de Serviços de Actividades Sectoriais do IPTM), em entrevista realizada em 18 de Março de 2011

36 Decreto Regulamentar n.º 86/2007, de 12 de Dezembro

[37] Afirmação do Capitão-de-mar-e-guerra Matos Nogueira (Oficial de Ligação entre o Comando Naval e a Direcção Geral da Autoridade Marítima), veiculada em entrevista realizada em 16 de Fevereiro de 2011

dependendo a primeira das preocupações da vulnerabilidade e do impacto que a indisponibilidade duma dada estrutura pode provocar e a segunda porque uma qualquer ameaça que possa afectar a actividade portuária poderá ter origem fora do entreposto ou local onde decorre a interface navio – terra.[38]

Numa abordagem que extravase os operadores portuários, mas de interesse para os departamentos competentes em matéria de protecção, Forças Armadas incluídas, o facto de a partir do porto (área molhada ou seca), poderem ser atingidas infra-estruturas críticas localizadas fora do perímetro da interface navio – terra, não deve ser descurado.

As preocupações referidas estão presentes apesar da razoável maturidade em termos da implementação do código ISPS, isto apesar de que estas preocupações foram explicitamente expressas em legislação comunitária, nomeadamente no Regulamento (CE) N.º 725/2004 do Parlamento Europeu e do Conselho, de 31 de Março de 2004, relativo ao reforço da protecção dos navios e das instalações portuárias:

> "15.5 A avaliação da protecção da instalação portuária deve incluir, pelo menos, os seguintes elementos:
>
> .1 identificação e avaliação dos bens e infra-estruturas que é importante proteger,
>
> […]
>
> .4 identificação dos pontos fracos, incluindo o factor humano, da infra-estrutura e das políticas e procedimentos aplicados."

– Na Directiva 2005/65/EC do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005, relativa à melhoria da protecção portuária:

> "Os Estados Membros devem definir para cada porto as fronteiras do porto…"

[38] De acordo com o Engenheiro Carlos Seixas da Fonseca (Director de Serviços de Actividades Sectoriais do IPTM), em entrevista realizada em 18 de Março de 2011

b. Análise de risco

A DNV, no já referido estudo por si realizado para a União Europeia[39], afirma a necessidade de efectuar uma análise de risco com o propósito de determinar a importância das infra-estruturas de transporte, onde incluímos as instalações portuárias.

Tabela 5: Matriz de Análise de Risco DNV para a cadeia logística europeia[40]

Consequências: Gravidade	Vítimas Mortais	Inactividade Indisponibilidade (dias)	A – Pouco possível	B – Difícil	C – Possível	D – Fácil
4	> 100	> 180				
3	20 a 100	15 a 180				
2	2 a 20	2 a 14				
1	< 2	< 2				

Vulnerabilidade

Possibilidade de proteger

A – Fácil; B – Possível; C – Difícil; D – Muito difícil

Para esse efeito a DNV sugere a utilização duma matriz de avaliação de risco (vide a tabela 5), considerando como factores para a determinação do risco os seguintes:

- Vulnerabilidade a um ataque: que reflecte a possibilidade de um ataque terrorista contra um elemento da cadeia logística ser bem sucedido, tendo em conta que as medidas de protecção normalmente aplicadas a essa instalação estão implementadas;
- Consequências dum ataque terrorista bem sucedido, as quais foram avaliadas tendo em conta dois factores:
  - O número de vítimas mortais;

[39] DNV (2005), op.cit.
[40] Tradução do autor a partir de DNV (2005), op.cit.

- O impacto económico, para o qual, por sua vez, se poderiam considerar como factores contributivos:
  - O custo de reconstrução dos elementos destruídos;
  - O volume de mercadoria afectado;
  - O tempo de inactividade ou indisponibilidade, que foi o único a ser considerado na matriz proposta.

Há ainda a realçar que os autores desta proposta clamam isenção quanto à localização específica do ataque, tendo uma abordagem genérica aos factores número de vítimas mortais e tempo de inactividade ou indisponibilidade.

c. A Vulnerabilidade

Ainda que os progressos no campo da protecção portuária tenham sido significativos, particularmente desde 2002, e ainda que seja notório um esforço continuado, existem vulnerabilidades, de alguma forma perceptíveis de forma intuitiva para quem lida de forma próxima com os portos, quer sejam marítimos quer sejam operadores em terra. Essas vulnerabilidades que podem ser deduzidas da análise da documentação reguladora, tanto do código ISPS como da legislação europeia, abandonando assim a subjectividade das percepções particulares.

Atente-se, por exemplo, ao articulado duma importante peça de regulamentação europeia[41]:

"14 PROTECÇÃO DA INSTALAÇÃO PORTUÁRIA

14.1 […]

14.2 Ao nível de segurança 1, serão executadas em todas as instalações portuárias, […], as seguintes actividades atinentes à identificação e prevenção de incidentes de protecção:

.1 execução de todas as tarefas relacionadas com a protecção da instalação portuária,

.2 controlo do acesso à instalação portuária,

[41] Regulamento (CE) Nº 725/2004 do Parlamento Europeu e do Conselho, de 31 de Março de 2004, relativo ao reforço da protecção dos navios e das instalações portuárias, secção 14

.3 vigilância da instalação portuária, incluindo os fundeadouros e cais,

.4 vigilância das zonas de acesso restrito a fim de assegurar que apenas pessoas autorizadas a elas podem aceder,

.5 supervisão da movimentação de carga,

.6 supervisão da movimentação das provisões dos navios, e

.7 pronta disponibilidade do sistema de comunicações de protecção."

A vulnerabilidade que se detecta é implícita, pois o que prende a atenção é a inexistência de qualquer referência a medidas de protecção na área molhada do porto, pelo menos no nível de segurança mais básico, sendo que a sua existência nos níveis superiores dependerá das medidas que estiverem previstas no PPP.

Considerando que a materialização das medidas previstas para as instalações portuárias no código ISPS o tornam mais seguro a acções provenientes de terra, este continua ainda vulnerável a um ataque conduzido a partir do espelho de água[42]. Esta realidade consubstancia-se também nas medidas previstas pela Autoridade Marítima Nacional[43], que consideram o patrulhamento, bem como o estabelecimento de zonas de interdição, da área molhada em torno dos navios, seguindo uma lógica crescente, quer em área coberta como de meios a utilizar, em função do tipo de navio a proteger e do grau de ameaça.

A permanente manutenção de medidas de protecção activa da área molhada não é viável; contudo, a vulnerabilidade a um ataque será reduzida através da redução da probabilidade de sucesso desse ataque, implementando aquelas medidas de protecção de forma reactiva, dando resposta a informação disponibilizada por departamentos estaduais competentes na área do combate ao terrorismo.[44]

---

[42] Opinião do Comandante Miguel Ângelo Taveira Rodrigues (Oficial de Protecção do Porto de Lisboa), em entrevista realizada em 18 de Fevereiro de 2011, corroborada pelo Engenheiro Carlos Seixas da Fonseca (Director de Serviços de Actividades Sectoriais do IPTM), em entrevista realizada em 18 de Março de 2011

[43] Directiva 001/2004, op. cit.

[44] Afirmação do Vice-almirante Álvaro José Cunha Lopes (Director-Geral da Autoridade Marítima e Comandante-Geral da Polícia Marítima), em entrevista realizada em 26 de Abril de 2011

d. Medidas adicionais ou novas medidas

Não podendo fechar-se um porto sob o pretexto da protecção porque tal paralisaria a actividade económica em larga escala, tem-se assistido, conforme documentado anteriormente, a um incremento da implementação de medidas de protecção. Ainda assim, a operacionalização da protecção portuária carece de análises de custo, de maneira a que não onere a actividade económica do porto ao ponto de a tornar deficitária.

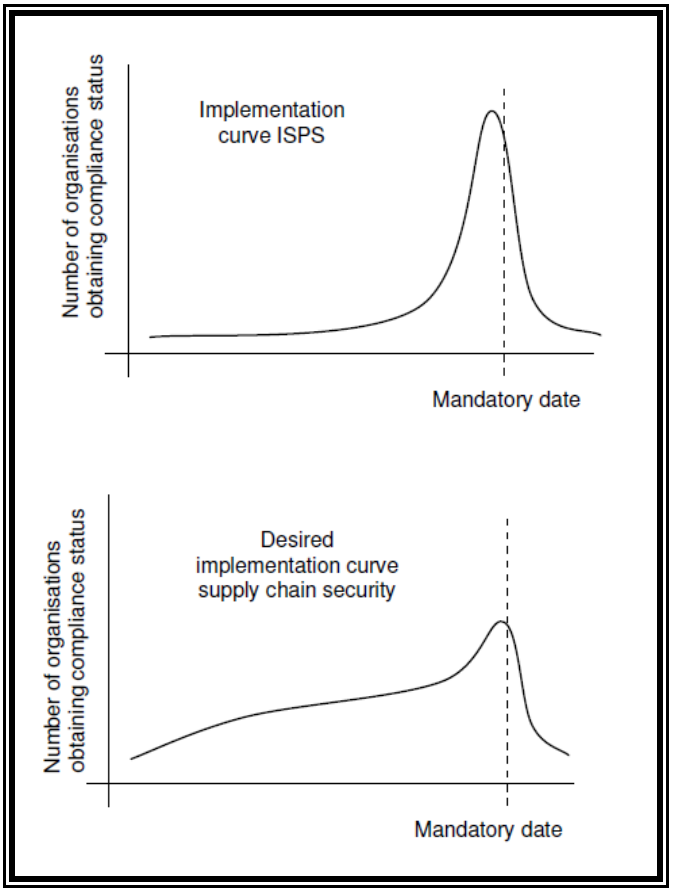

Figura 2: Curvas de adesão – código ISPS vs protecção da cadeia logística na EU

De facto, uma das preocupações das entidades responsáveis pela gestão dos transportes marítimos e dos portos são os encargos financeiros, não só com a implementação das medidas de protecção, mas também com a sua manutenção, que envolvem ainda as actividades de auditoria, de certificação e de manutenção, conforme fica claro no estudo realizado pela DNV[45].

[45] DNV (2005), op.cit.

A DNV dá conta duma preocupação com os encargos que envolvem a brusca implementação de medidas de protecção, sugerindo à União Europeia que, a verificar-se a sua aplicação a toda a cadeia logística, estas devem ser implementadas de forma mais equilibrada, em contraponto aos picos de despesa como aqueles que se verificaram aquando da implementação das medidas previstas no código ISPS, e que se reflectem directamente no número de organizações aderentes e que obtêm a certificação, conforme se ilustra na figura 2.

Pode-se afirmar que na generalidade da comunidade portuária existe um sentimento de alguma saturação e certamente de resistência à implementação de novas medidas, físicas ou processuais, que impliquem novas despesas[46], o que se atribui não só aos avultados montantes já dispendidos, mas também ao curto espaço de tempo em que tiveram que ocorrer e ao corrente clima recessivo.

Verifica-se assim que o clima portuário actual admite a necessidade de medidas suplementares para fazer face a lacunas de protecção contra ameaças terroristas, mas atendendo aos avultados investimentos já efectuados na área da protecção não existe vontade de efectuar novas despesas. Assim, iniciativas que aportem uma mais valia de protecção, sem custos para as administrações portuárias e sem impacto operacional e económico na actividade portuária, como pode ser o caso do DAT – POW PHP, serão potencialmente acolhidas de bom grado entre os departamentos competentes na área portuária.

e. Síntese conclusiva do capítulo

O número de departamentos concorrentes para a efectiva protecção portuária é bastante significativo, sendo fundamental a definição das competências específicas e o estabelecimento duma estrutura racional que permita a sua articulação ou coordenação.

Face à impossibilidade de defender no absoluto todas as ameaças em todas as alturas, existindo ademais limitação de recursos, a defesa portuária deve ter por base uma análise de risco.

[46] Opinião do Engenheiro Carlos Seixas da Fonseca (Director de Serviços de Actividades Sectoriais do IPTM), em entrevista realizada em 18 de Março de 2011

Os progressos efectuados em termos de medidas de protecção portuária são relevantes; contudo, existem lacunas por preencher, designadamente ao nível da identificação das infra-estruturas críticas e da prioritização na sua protecção. A protecção actualmente oferecida contra um ataque efectuado a partir da área molhada é muito reduzida.

As entidades responsáveis pela protecção portuária, administrações e operadores, não encaram de bom grado a implementação de novas medidas ou o robustecimento das existentes devido aos custos envolvidos, considerando que o esforço até ora desenvolvido foi bastante oneroso.

Ainda assim, o plano de protecção do porto pode não incluir infra-estruturas importantes para uma operação militar e as vulnerabilidades a ataques provenientes da zona molhada não são mitigadas de maneira fácil. O DAT – POW PHP deverá ser desenvolvido de maneira a enquadrar-se na realidade exposta, potenciando o mitigar das lacunas existentes.

Considera-se assim completamente respondida a QD3: *Como pode o DAT – POW PHP enquadrar-se no contexto actual da protecção portuária?* Através da validação da H3: ***As medidas de protecção existentes podem apresentar lacunas que o O DAT – POW PHP, em desenvolvimento, pode auxiliar a mitigar.***

4. Operacionalizar o programa DAT – POW PHP da OTAN

Havendo-se procedido à caracterização da ameaça terrorista em ambiente portuário, identificando-se as oportunidades, apontando-se os possíveis meios ou vectores de ataque, dando ênfase aos mais prováveis, e deduzindo-se a existência da vontade por parte de possíveis perpetrantes a partir de actuações relativamente recentes e da informação relativa ao desenvolvimento de capacidades, interessa agora tentar desenvolver uma maneira de integrar o DAT – POW PHP da OTAN com as medidas já existentes, tentar retirar possíveis ensinamentos do trabalho desenvolvido por outros departamentos e determinar a possibilidade duma efectiva operacionalização dos desenvolvimentos que venham a ser conseguidos.

a. Correlação com as medidas existentes

As medidas de protecção, físicas e organizacionais, que têm sido desenvolvidas sob a égide das organizações internacionais reduziram substancialmente a vulnerabilidade das instalações portuárias, mas esta afirmação é sobretudo válida para os portos ISPS e a adopção do respectivo código, com tudo o que de positivo lhe possa estar associado, ainda não é universal.

Além disso, conforme ficou demonstrado no capítulo 3, existem ainda lacunas em áreas fundamentais, nomeadamente no que respeita às infra-estruturas críticas e na prevenção de ataques efectuados a partir da zona molhada, pelo que se o DAT – POW PHP tiver em consideração a necessidade de lhes fazer face, contribuiria de forma significativa e visível para o incremento da protecção portuária.

Ao nível das infra-estruturas há ainda a acrescentar que a sua classificação como críticas pelas autoridades portuárias poderá não corresponder a uma eventual classificação por parte duma força OTAN, o que até se compreende pois os critérios de classificação empregues serão necessariamente diferentes para organizações com objectivos distintos, não esquecendo que, enquanto uma visa a manutenção e desenvolvimento da actividade económica a outra visa garantir a existência de condições para a condução de operações de forma segura.

Tomando por base a matriz de análise de risco proposta pela DNV para a caracterização das infra-estruturas da cadeia logística europeia (no capítulo 3 vide a tabela

5), propõe-se uma abordagem semelhante, mas com alterações nos factores considerados para a determinação do risco (vide a tabela 6), nomeadamente:

Tabela 6: Matriz de Análise de Risco proposta para o DAT – POW PHP

Consequências	Gravidade	Vítimas Mortais	Tipo de navio (se aplicável)	Impacto na operação (dias)	A Pouco possível	B Difícil	C Possível	D Fácil
	4	> 100	1	> 30				
	3	21 a 100	2	15 a 30				
	2	2 a 20	3	< 14				
	1	< 2	4	0				

Vulnerabilidade

Possibilidade de proteger

Fácil | Possível | Difícil | Muito difícil

- Vulnerabilidade a um ataque: que reflecte a possibilidade de um ataque terrorista contra uma infra-estrutura ser bem sucedido, tendo em conta que as medidas de protecção normalmente aplicadas a essa instalação estão implementadas, onde se incluem as normalmente praticadas pela autoridade portuária e as adicionais no âmbito da protecção de Força e do DAT – POW PHP;
- Consequências dum ataque terrorista bem sucedido, ou gravidade, tendo sido pesada tendo em conta três factores:
  - O número de vítimas mortais: sendo que as alterações propostas derivam da análise de ocorrências anteriores, nomeadamente do facto de que o ataque M/V "Limburg" em 2002 registou 1 vítima mortal[47] e aquele efectuado contra o USS "Cole" em 2000 saldou-se em 17 vítimas mortais, não

[47] Não são considerados os dois terroristas também falecidos no ataque

existindo na altura uma doutrina de protecção de força dentro da OTAN. Considerou-se ainda que um número maior de vítimas mortais ficaria a dever-se à existência de baixas civis;

- O tipo de navio a proteger[48], correspondendo a sua tipologia ao seguinte:
  - Tipo 1: Porta-aviões, navios de comando e controlo, navios reabastecedores, navios de assalto anfíbio; LPD[49] e submarinos;
  - Tipo 2: Contra-torpedeiros, fragatas e navios de contra-medidas de minas;
  - Tipo 3: Navios auxiliares, por exemplo rebocadores, balizadores, etc. ;
  - Tipo 4: Outros navios de risco, militares ou não.
- O impacto para a condução da operação, avaliado em termos de atraso e medido em dias, sendo que este factor reflecte o conhecimento de que o já mencionado ataque ao USS "Cole" não causou impacto na condução da operação.

Ainda que a matriz de avaliação de risco apresentada não venha a ter qualquer utilidade no desenvolvimento no DAT – POW PHP, esse tampouco era o seu propósito final. Aquilo para o que se pretende chamar a atenção é para a necessidade de efectuar uma análise de quais as estruturas que carecem de maior protecção e fazer com que o SAD incida sobre elas, reflectindo assim aquilo que está igualmente previsto na doutrina OTAN em termos de protecção de Força[50], conforme se verifica da leitura do ATP – 74:

> "A Protecção de Força deve basear-se na gestão do risco. Embora não seja possível proteger todos os elementos contra todas as ameaças a todo o momento, os elementos previamente considerados *críticos para a missão* devem ser protegidos. Como parte da Protecção de Força, uma avaliação integrada da ameaça, das vulnerabilidades e do risco é essencial para o processo de decisão…"[51]

[48] Adaptação do autor a partir da Directiva 001/2004 da AMN
[49] *Landing Platform Dock*
[50] ATP – 74 – Allied Maritime Force Protection Against Asymmetric Threats In Harbour And Anchorage
[51] ATP – 74, parágrafo 0201.3 – tradução do autor

Já no que diz respeito a qualquer acção conducente a mitigar a vulnerabilidade a um ataque proveniente da zona molhada, apenas fará sentido utilizar as capacidades da força para implementar medidas de protecção se estas não forem asseguradas pelas autoridades locais. Concretizando, referimo-nos por exemplo a:

- Vigiar com meios electromagnéticos e acústicos;
- Patrulhar a área molhada;
- Negar o acesso a áreas sensíveis.

Em termos absolutos, atendendo ao desenvolvimento das medidas de protecção de Força incidentes na componente naval, incluindo as orientações para a actuação táctica, seria de esperar que a robustez do que pode ser implementado apenas fosse deficitária caso o número de infra-estruturas e de navios a proteger obrigasse a uma dispersão de meios comprometedora.

b. Possíveis dificuldades de implementação no terreno

Existe uma noção generalizada no seio das Forças Armadas de que, uma vez autorizado o estacionamento duma Força, a nação hospedeira dispõe-se a apoiar os objectivos dessa Força contribuindo significativamente para proporcionar níveis de protecção significativos[52]. O ATP – 74, além de reflectir esta noção, deixa explícito que tal se deve ao interesse da nação hospedeira em impedir a ocorrência de ataques em portos sob sua jurisdição[53], facto que se entende se recordarmos que o ataque ao M/V "Limburg", além do efeito negativo na economia global consubstanciado no aumento imediato do preço do barril de crude em 0,48 dólares/barril, causou a ruptura económica do Iémen no médio prazo devido aos elevados prémios de risco exigidos para a navegação, que aumentaram 300 %, que viriam a resultar numa quebra de 93 % no tráfego de contentores, sendo que no conjunto o Iémen terá perdido 3,8 milhões de dólares ao mês em receitas portuárias (Greenberg, 2006: 16 - 17).

[52] Informação confirmada pelo Capitão-de-mar-e-guerra Salvado de Figueiredo (Comandante do N.R.P. "D. Francisco de Almeida"), em entrevista realizada em 11 de Fevereiro de 2011
[53] ATP – 74, parágrafo 0301.4

Contudo, a implementação de medidas de protecção de forma desregrada, em frenesim, pode levar ao crescimento dum sentimento de insegurança, resultando em efeitos económicos negativos, tal como os explicados no parágrafo anterior.[54]

Além disso, poderão existir obstáculos na aplicação táctica de algumas medidas, por exemplo, quando se trata da colocação de barreiras de protecção que, dependendo da localização e da facilidade da sua movimentação caso tal seja requerido, poderão levantar reservas aos operadores portuários.

No geral a colocação de sensores, ou outra afectação da área portuária para a colocação de elementos do DAT – POW PHP não deverá representar problema de maior para os operadores portuários, cifrando-se o tempo necessário para a sua concretização entre dois a cinco dias, isto para o caso de portos ISPS com elevados níveis organizacionais, como por exemplo o Porto de Lisboa[55]. Assim, ao nível táctico recomenda-se um contacto avançado com as autoridades portuárias e forças de protecção que tenham sido ou possam vir a estar envolvidos na implementação das medidas de protecção, verificando as medidas que estão previstas, reforçando-as quando requerido e clarificando quaisquer dúvidas sobre a resposta a dar a uma tentativa de ataque.

Já no plano operacional é necessário que se desenvolvam contactos de alto nível na fase de planeamento, clarificando a dimensão e o estatuto da Força, bem como as medidas de protecção requeridas, não só para a Força como um todo, mas também para a área portuária, clarificando quais os pontos de ligação para o escalão inferior. Existem mesmo questões relacionadas com a natureza dos meios a empregar, designadamente quanto à emissão de energia electromagnética e acústica no porto, ou o uso de meios electro-ópticos como câmaras de vigilância, pois em qualquer dos casos poderão existir disposições legais do país em questão que sejam impeditivas da sua utilização[56].

---

[54] Conforme fez notar o Vice-almirante Álvaro José Cunha Lopes (Director-Geral da Autoridade Marítima e Comandante-Geral da Polícia Marítima), em entrevista realizada em 26 de Abril de 2011

[55] No caso do Porto de Lisboa a diferença fica a dever-se à entidade que explora o terminal que se pretende ver afectado, Administração do Porto de Lisboa ou concessionário. A estimativa do Comandante Miguel Ângelo Taveira Rodrigues (Oficial de Protecção do Porto de Lisboa), em entrevista realizada em 18 de Fevereiro de 2011

[56] No caso de Portugal, de acordo com a Lei n.º 67/98, de 26 de Outubro, o uso de câmaras de vigilância teria que ser autorizado pela Comissão Nacional de Protecção de Dados. Tratando-se a referida Lei duma transposição da Directiva 95/46/CE do Parlamento e do Conselho Europeu poderão verificar-se restrições similares noutros Estados membros da União Europeia

Além dos eventuais obstáculos impostos pela legislação local, que se assume ser desconhecida à partida, existe a possibilidade de que a implementação de qualquer tipo de medidas de protecção seja entendida como uma espécie de ingerência ou de comprometimento da soberania, requerendo-se assim a realização de contactos ao mais alto nível, que assumiriam possivelmente a forma de autorização diplomática, mesmo quando as medidas são estáticas, ou não cinéticas, como é o caso da colocação de barreiras.

Relembrou, a este propósito, o Vice-almirante Álvaro José Cunha Lopes (Director-Geral da Autoridade Marítima e Comandante-Geral da Polícia Marítima) [57], que na única ocasião em que foi acordada a actuação da Aliança ao abrigo do art.º 5 º do Tratado da OTAN, intrinsecamente a situação que mais liberdade de actuação concede a uma Força militar, a condução das operações careceu ter em consideração a impossibilidade da livre utilização de território dum Estado soberano, ainda que se tratasse de comboios logísticos e que o Estado em questão fosse membro da Aliança.[58]

Muito mais delicada ainda se espera que seja a negociação que conduza ao emprego de meios cinéticos, sendo que dependendo da área em que a Força se encontre pode comprometer a própria proposta e aprovação de Regras de Empenhamento.

As dificuldades na implementação das medidas de protecção portuária serão de natureza diferente dependendo primeiramente do porto visitado e depois, se estiver em causa a condução duma operação, da natureza da operação e do estatuto do país com jurisdição sobre o porto, por exemplo:

- Se o porto em questão for uma instalação militar de um país da OTAN não são de esperar lacunas nas medidas de protecção, mas a eventual colocação de material ou o estabelecimento de patrulhas provenientes da Força, em terra ou no mar, poderá ainda não ser aceite pela nação hospedeira;
- Se estiver em causa uma operação no âmbito do art.º 5.º do Tratado do Atlântico Norte não deverá haver obstáculo à implementação de quaisquer medidas de protecção;
- Quando se tratar duma missão de gestão de crise será necessário negociar o estatuto da Força no território onde decorre a operação;

[57] Entrevista realizada em 26 de Abril de 2011
[58] Referência à impossibilidade de utilização do território da Turquia na guerra do Iraque em 2003

– No mesmo cenário que o da alínea anterior, mas num país próximo onde se estabeleça por exemplo uma base de apoio logístico, será necessário negociar, pelo menos, um memorando de entendimento.

Face ao que acima se expôs, a tabela 7 resume a natureza geral das actividades a desenvolver aos diversos níveis (estratégico, operacional e táctico), visando a implementação no terreno das medidas de protecção portuária.

Tabela 7: Actividades conducentes à implementação do DAT – POW PHP

NÍVEL	ACÇÃO
ESTRATÉGICO	– Autorização diplomática
OPERACIONAL	– Identificação de infra-estruturas críticas – Análise de risco – SAD do DAT – POW PHP – Estabelecimento de ligações em benefício do escalão táctico
TÁCTICO	– Acerto de pormenores com autoridades locais – Implementação no local – Implementação de medidas de protecção individual

c. Síntese conclusiva do capítulo

Considera-se que as hipóteses já validadas nos capítulos anteriores são indirectamente reforçadas com o exposto neste capítulo. Além disso, na sequência do capítulo anterior, laborando sobre a evidência do carácter multi-disciplinar da protecção portuária, verifica-se que os requisitos duma Força militar poderão encontrar lacunas nas medidas que se encontram implementadas pelas autoridades locais nas áreas portuárias.

Esse mesmo carácter multi-disciplinar obriga normalmente à tutela pela parte de vários departamentos, pelo que se torna evidente a conveniência de colocar as necessidades e pretensões da Força a uma entidade que tutele o maior número possível de departamentos locais com competências na área portuária. Sendo fundamental a conjunção de sinergias,

afigura-se que a abordagem individualizada poderá dificultar a coordenação das medidas de protecção.

Não de somenos importância é o facto de que a utilização de meios da OTAN, passivos ou activos, visando a implementação de medidas de segurança ou o reforço das que porventura existam, implica a aceitação por parte do Estado com soberania sobre a área de actuação, ou seja, a operacionalização do DAT – POW PHP obriga à obtenção de autorizações diplomáticas.

Considera-se assim que se encontra respondida a QD4: *Que questões, no relacionamento inter-departamental, devem ser consideradas na implementação eficaz de medidas de protecção portuária em ambiente anti-terrorista utilizando capacidades próprias da Força?* Através da validação da H4: ***O carácter multidisciplinar da protecção portuária envolve um leque alargado de entidades pelo que se deve promover o conhecimento mútuo das capacidades e requisitos através duma abordagem à cúpula da organização.***

Conclusão

Tendo por base os esforços desenvolvidos pela Aliança Atlântica para fazer face á ameaça terrorista, construiu-se a Pergunta de Partida de maneira a enquadrar a iniciativa respeitante à protecção portuária no contexto actual, sendo que as questões derivadas deduzidas visaram cobrir o vasto leque da problemática em estudo, caracterizando o objecto de estudo, determinando a real necessidade de prossecução da iniciativa e procurando determinar quais as questões que poderão carecer ser abordadas, ou até merecer particular atenção e cuidado, com vista à operacionalização dos desenvolvimentos resultantes.

Face ao escasso tratamento, ou caracterização específica, da ameaça terrorista em ambiente portuário, foi necessário consultar trabalhos de diversos departamentos versando sobre a ameaça terrorista marítima, começando ali a dedução das suas implicações num ambiente mais restrito, o portuário.

Em seguida abordaram-se as medidas de protecção que no meio marítimo e portuário foram desenvolvidas desde o ataque terrorista contra as torres gémeas do *World Trade Center* em 11 de Setembro de 2001, que não poderiam passar sem menção nem tampouco os sucessivos esforços para a sua refinação e actualização tecnológica, pois desta forma aprofundou-se a especificidade da ameaça terrorista em ambiente portuário. Foi possível, graças a esta abordagem, determinar a existência de alguns aspectos que, não sendo abordados no dia-a-dia das operações portuárias correntes, podem tornar-se críticos para uma Força militar.

Finalmente, á medida que a investigação documental prosseguia e parecia ganhar forma a validação das hipóteses, enunciadas como tentativas de resposta às questões derivadas, procurou-se a sua consolidação entrevistando diversas personalidades, civis e militares, que se destacam pelo conhecimento da problemática em estudo.

Assim, foi possível verificar que o número de atentados terroristas em ambiente marítimo é quase irrelevante quando comparado com o número de ataques levados a cabo noutros ambientes, o mesmo se verificando por força de razão quanto ao ambiente portuário.

Apesar disso, o sucesso obtido por dois atentados no início do século XXI revelou a existência de sérias vulnerabilidades. Igualmente, a reacção negativa dos mercados internacionais face ao atentado contra o M/V “Limburg”, com severas implicações

económicas, não só regionais, mas também globais, tornou evidente que o sucesso dum ataque neste ambiente tem um impacto significativo que não pode passar desapercebido a Estados de direito e a organizações internacionais, sendo impreterível tomar medidas para evitar que tal se repetisse. Além disso, esse mesmo efeito tampouco deverá ter passado desapercebido a organizações terroristas cujo fito seria precisamente a disrupção económica em larga escala.

Adicionalmente, o aumento registado nos últimos anos dos eventos de pirataria tem elevado o grau de preocupação quanto á possibilidade de ocorrência dum ataque terrorista marítimo ou portuário, não por qualquer similitude ideológica, mas porque o modo de operação que tem permitido esse incremento tem colocado a nu vulnerabilidades que podem ser também exploradas na execução de ataques terroristas.

Diversas autoridades, em ambas as margens do Atlântico Norte, conduziram estudos, tanto institucionais como independentes, com vista à identificação de possíveis cenários dum ataque terrorista em ambiente portuário. Os resultados obtidos são na essência concordantes, ainda que divirjam pontualmente, apontando para um vasto espectro de possibilidades que é impossível precaver na totalidade.

Fazer face a todos os cenários potenciais dum ataque terrorista obrigaria, em última instância, ao encerramento do porto, cessando a actividade económica, com os óbvios prejuízos que daí advêm, indo assim ao encontro preciso das pretensões das organizações terroristas.

Verificou-se a existência duma política de princípio de partilha de informação, inter-departamental, inter-organizacional e interestadual, antecipando qualquer tentativa de ataque terrorista; sendo que esta partilha se refere igualmente à disponibilização e validação do panorama marítimo e portuário.

As medidas de protecção portuária que visam a protecção directa de alvos, normalmente tratadas com maior detalhe por serem mais visíveis, são de carácter físico e organizacional, abrangendo os navios e as suas tripulações, a carga transportada e as infra-estruturas portuárias, com ênfase neste último ponto naquelas que servem de interface. Entre estas medidas destacam-se as previstas no código ISPS da IMO.

O incremento de protecção que iniciativas como as do código ISPS e outras similares aportaram nos últimos anos é bastante relevante. Ainda assim, conforme já se expôs, existe uma impossibilidade genética de anular todas as vulnerabilidades, ou de fazer face a todas as ameaças, pelo que qualquer acréscimo de protecção na área portuária será por princípio bem recebido, desde que não se crie um ambiente de temor ou sensação de

insegurança, pois os efeitos "psicológicos" podem ter efeitos económicos perniciosos, nem sejam necessários novos investimentos por parte de agentes económicos que tutelem a actividade portuária.

Assim, o SAD do DAT – POW PHP, bem como outros elementos desenvolvidos com esta iniciativa podem ser incorporados com sucesso, complementando as medidas existentes, sobretudo com o aporte duma optimização dos meios disponíveis recorrendo a uma análise de risco e eventualmente mitigando lacunas ao nível da protecção de infra-estruturas críticas para a condução duma operação militar, mas negligenciadas pelas autoridades portuárias.

Obtiveram-se também evidências de que a protecção portuária tem uma natureza multi-disciplinar, o que obriga, como no caso nacional, à existência de diversos departamentos, cada um com competências específicas. Assim, uma protecção portuária eficaz carece duma correcta articulação de diversas entidades. A implementação de medidas de protecção complementares, ainda que de natureza consultiva, como é o caso do SAD do DAT – POW PHP, resultará facilitada e provavelmente apenas será possível abordando uma estrutura de cúpula que superintenda todos os departamentos envolvidos.

A última e talvez mais relevante evidência obtida é a de que o acolhimento duma Força da OTAN, independentemente do seu estatuto, não lhe garante o imediato uso dos meios próprios no território em que se encontre ainda que se trate da implementação exclusiva de medidas de protecção, sejam eles passivos ou cinéticos. Este facto leva a concluir que a operacionalização de qualquer elemento do DAT – POW PHP careça de autorização diplomática, ou de outro tipo de acordo que dependendo da situação poderia assumir a forma de acordo quanto ao estatuto da Força ou de memorando de entendimento.

Na sequência das respostas às QD, apresentadas nas sínteses conclusivas de cada capítulo e revisitadas ao longo dos últimos parágrafos, julga-se ser possível agora responder à PP:

Como pode concretizar-se eficientemente uma protecção portuária?

Atendendo à multiplicidade de cenários possíveis, o esforço no estabelecimento de medidas de protecção portuária deverá centrar-se em fazer face aos mais prováveis, sendo que para esse efeito deverão identificar-se as infra-estruturas críticas e classificar os meios da Força que se pretendem proteger e em paralelo efectuar uma análise de risco com o fito de ajudar a determinar quais os meios ou medidas necessários ou adequados.

Será necessário verificar junto dos departamentos que tutelam essa área se todas as medidas preconizadas pela Força são consideradas, ou se existe necessidade de colaborar

com meios próprios, quer do tipo organizativo e de apoio à decisão, como o SAD do DAT – POW PHP, quer de outro tipo, para mitigar eventuais lacunas.

Revisitando a complexidade das áreas portuárias, é provável que o número de departamentos que tutelem ou contribuam nesta matéria seja elevado, pelo que se deverá tentar uma abordagem de cúpula que superintenda o maior número daqueles departamentos. Esta necessidade é ainda reforçada pela necessidade de obter autorização diplomática, ou de esclarecer qual a extensão de acção que é permitida.

Considerações de ordem prática e recomendações:

Os produtos ou capacidades desenvolvidos no âmbito da iniciativa DAT – POW PHP da OTAN têm, pela sua natureza, uma utilidade potencial. De maneira a possibilitar a sua efectiva exploração, entende-se que a adopção das linhas de actuação que a seguir se propõem poderá dar continuidade à iniciativa:

- O SAD do DAT – POW PHP é distribuído aos membros da Aliança;
- Os membros da Aliança testam o SAD do DAT – POW PHP e relatam a sua eficácia;
- Os membros da Aliança apresentam o SAD do DAT – POW PHP aos departamentos nacionais com competências sobre as zonas portuárias, recolhem e emitem parecer;
- O SAD do DAT – POW PHP poderá ser distribuído a países amigos, parceiros em coligações ou de outro tipo julgado conveniente;
- A considerar-se a distribuição sugerida na alínea anterior deverão ser privilegiados aqueles parceiros a que se reconheça maior dificuldade na implementação de medidas de protecção portuária, designadamente no que respeita ao código ISPS e outros similares;
- Pode dar-se início ao estabelecimento de contactos diplomáticos com vista a:
    - Determinar o grau de aceitação, tanto do SAD do DAT – POW PHP como de outros elementos desenvolvidos ao abrigo da iniciativa;
    - Estabelecer quais os canais e procedimentos administrativos que devem ser seguidos para a operacionalização no terreno;
    - Obter pré-acordos que permitam uma eventual implementação de elementos do DAT – POW PHP com reduzido pré-aviso.

Referências bibliográficas

a. Monografias

BARATA, Pedro. (2010). *A Importância dos Portos Marítimos Portugueses*. Lisboa: IESM

CHALK, Peter. (2008). *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States*. Santa Monica [etc.]: RAND Corporation. Disponível na internet em: http://www.rand.org/pubs/monographs/2008/RAND_MG697.pdf

GREENBERG, Michael D., et. al. (2006), *Maritime Terrorism – Risk and Liability*. Santa Monica [etc.]: RAND Corporation. Disponível na internet em: http://www.rand.org/pubs/monographs/2006/RAND_MG520.pdf

JACKSON, Brian A., et. al. (2007), *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*. Santa Monica [etc.]: RAND Corporation. Disponível na internet em: http://www.rand.org/pubs/monographs/MG481.html

PARFOMAK, Paul W., FRITELLI, John. (2007). *Maritime Security: Potential Terrorist Attacks and Protection Priorities*. [SI]: Congressional Research Service. Disponível na internet em: http://www.fas.org/sgp/crs/homesec/RL33787.pdf

SPENCER, Alexander (2006). *Questioning the Concept of 'New Terrorism'* Peace Conflict & Development, [em linha]. Disponível na internet em: www.peacestudiesjournal.org.uk

b. Artigos de publicações em série

REMUSS, Nina- Luisa (2011). *The Use of Space Resources in the fight against Piracy*. European Journal of Navigation, Volume 9, Number 1, April2011, pp. 19-26.

c. Relatórios e documentos oficiais

Autoridade Marítima Nacional, Directiva 001/2004, de 22 de Março de 2004, Medidas especiais para reforçar a protecção dos navios que pratiquem portos nacionais.

Assembleia da República, Resolução da nº 85/2004, de 9 de Dezembro, Publicada no Diário da República, I Série-A, nº 303, de 29 de Dezembro de 2004. ACORDO ENTRE OS ESTADOS MEMBROS DA UNIÃO EUROPEIA RELATIVO AO ESTATUTO DO PESSOAL MILITAR E CIVIL DESTACADO NO ESTADO-MAIOR DA UNIÃO EUROPEIA, DOS QUARTEIS-GENERAIS E DAS FORÇAS.

Comissão Europeia, Comunicado da Comissão ao Conselho e Parlamento Europeu, COM(2010) 584, de 20 de Outubro de 2010. Disponível na internet em: http://ec.europa.eu/maritimeaffairs/pdf/maritime_policy_action/com_2010_584_en.pdf

Comissão Europeia, Comunicado da Comissão ao Conselho e ao Parlamento Europeu, COM(2002) 233, TOWARDS INTEGRATED MANAGEMENT OF THE EXTERNAL BORDERS OF THE MEMBER STATES OF THE EUROPEAN UNION. Disponível na internet em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0233:FIN:EN:PDF

Comissão Europeia, Comunicado da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões, COM(2003) 229, de 2 de Maio. Disponível na internet em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0229:FIN:EN:PDF

Comissão Europeia, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576, de 17 de Novembro. Disponível na internet em: http://www.espo.be/downloads/archive/0195efca-cab0-437a-9f08-1845f22af6c3.pdf

Conselho da União Europeia, Nota 15708/03, de 10 de Dezembro. Disponível na internet em: http://register.consilium.europa.eu/pdf/en/03/st15/st15708.en03.pdf

Decreto-Lei n.º 226/2006, de 15 de Novembro, publicado no Diário da República, 1.a série — N.º 220 — 15 de Novembro de 2006

Decreto Regulamentar n.º 86/2007, de 12 de Dezembro, publicado no Diário da República, 1.ª série — N.º 239 — 12 de Dezembro de 2007

Despacho Conjunto n.º 168/2004, de 8 de Março, publicado no Diário da República, 2.a série — N.º 72 — de 25 de Março de 2004

DNV CONSULTING (2005), *Study on the impact of possible European legislation to improve transport security, Final report: Impact assessment*. Disponível na internet em: http://ec.europa.eu/transport/security/studies/doc/2005_legislation_to_improve_transport_security.pdf

IMO, Resolução MSC.202(81), de 19 de Maio de 2006. Disponível na internet em: http://www.imo.org/OurWork/Safety/Navigation/Documents/LRIT/MSC.202(81).pdf

IMO, Circular MSC 1111, de 7 de Junho de 2004. . Disponível na internet em: http://www.un.org/en/sc/ctc/docs/bestpractices/1111.pdf

Parlamento Europeu e Conselho Europeu, Directiva 2005/65/EC, de 26 de Outubro de 2005. Disponível na internet em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:EN:PDF

Parlamento Europeu e Conselho Europeu, Directiva 2009/17/EC, de 23 de Abril de 2009. Disponível na internet em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:131:0101:0113:EN:PDF

Parlamento Europeu e Conselho Europeu, Directiva 95/46/CE, de 24 de Outubro de 1995. Disponível na internet em: http://www.umic.pt/images/stories/publicacoes200709/Directiva95_46_CE.pdf

Parlamento Europeu e Conselho Europeu, Regulamento (CE) 725/2004, de 31 de Março de 2004. Disponível na internet em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:PT:PDF

Lei da Protecção de Dados Pessoais, Lei n.º 67/98, de 26 de Outubro. Disponível na internet em: http://www.cnpd.pt/bin/legis/nacional/lei_6798.htm

Lei de Segurança Interna, Lei n.º 53/2008, de 29 de Agosto. Publicada no Diário da República, 1.ª série — N.º 167 — 29 de Agosto de 2008

United Nations Conference on Trade and Development (2007), *Maritime Security: ISPS Code Implementation, Costs And Related Financing*. Disponível na internet em: http://www.unctad.org/en/docs/sdtetlb20071_en.pdf

United States Department of State (2010), *Country Reports on Terrorism 2009*. Disponível na internet em: http://www.state.gov/s/ct/rls/crt/2009/index.htm

NATO, ATP – 74 (change 1) (2008), ALLIED MARITIME FORCE PROTECTION AGAINST ASYMMETRIC THREATS IN HARBOUR AND ANCHORAGE.

Sítios na internet

http://homeport.uscg.mil/WebHelp/Guest/Content/About%20Homeport/Maritime%20Transportation%20Security%20Act.htm

http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/ports_in_csi.xml

http://www.infrastructure.gov.au/transport/security/maritime/pdf/Strengthening_MarSec_Guide_2008.pdf

http://europa.eu/legislation_summaries/foreign_and_security_policy/cfsp_and_esdp_implementation/l33234_en.htm

http://www.state.gov/t/isn/c10390.htm

http://www.state.gov/t/isn/c27726.htm

http://ec.europa.eu/maritimeaffairs/surveillance_en.html

http://www.imo.org/OurWork/Safety/Navigation/Pages/LRIT.aspx

http://www.imo.org/ourwork/safety/navigation/pages/ais.aspx

http://www.imarpor.pt/pdf/agenda/Ferragudo%20GNR%20Agosto%202009.pdf

http://www.portugal.gov.pt/pt/Documentos/Governo/MOPTC/Apres_VTS.pdf

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46051

http://www.iso.org/iso/catalogue_detail?csnumber=44641

http://www.coess.org/pdf/COESS-ISPSmanual.pdf

http://www.mar.ist.utl.pt/mventura/Projecto-Navios-I/PT/PNI-1.2.4-Arquea%C3%A7ao.pdf

Entrevistas

- Engenheiro Carlos Seixas da Fonseca
  (Director de Serviços de Actividades Sectoriais do IPTM), [18 de Março de 2011]

- Comandante Miguel Ângelo Taveira Rodrigues
  (Oficial de Protecção do Porto de Lisboa), [18 de Fevereiro de 2011]

- Vice-almirante Álvaro José Cunha Lopes
  (Director-Geral da Autoridade Marítima e Comandante-Geral da Polícia Marítima), [26 de Abril de 2011]

- Capitão-de-mar-e-guerra Matos Nogueira
  (Oficial de Ligação entre o Comando Naval e a Direcção Geral da Autoridade Marítima), [16 de Fevereiro de 2011]

- Capitão-de-mar-e-guerra Salvado de Figueiredo
  (Comandante do N.R.P. "D. Francisco de Almeida"), [11 de Fevereiro de 2011]