SEGURANÇA DOS TRANSPORTES MARÍTIMOS E PORTOS - VISÃO PROSPETIVA

Manuel Dinis C. Dias
Eng.º Civil – Consultor
mdinisdias@gmail.com

Introdução

O século XXI vai ser o século do MAR, sendo reconhecida a importância dos transportes e portos, neste contexto.

Analisando alguns impactos atuais que se sumarizam no quadro seguinte, conclui-se que os oceanos vão estar cada vez mais no centro da atividade humana, face aos seus imensos recursos vivos e não vivos e, à importância das vias de transporte marítimo, no contexto logístico global.

Impactos atuais (valores aproximados)

70 por cento do planeta é coberto por água
80 por cento da população mundial vive a menos de 200Km da linha de costa
90 por cento do comércio mundial faz-se por via marítima
100 mil navios operam nos transportes marítimos
1,5 milhões de pessoas trabalham neste setor
6,5 mil milhões de toneladas de carga é transportada anualmente

No âmbito da exploração de recursos marítimos, particularmente os existentes nos fundos do oceano, Portugal reúne potencialidades excecionais face à extensão da sua Zona Económica Exclusiva (ZEE) com 1.727.408 km², sendo a 5.ª maior da Europa e 20.ª maior do mundo, estando em curso o processo, junto da ONU, para a sua expansão em mais 2,15 milhões de km², podendo, assim, atingir uma área da ordem de 3,88 milhões de km². Contudo, este potencial só será viável com elevados investimentos no estudo e identificação geológica desses fundos e, no desenvolvimento de ferramentas tecnológicas adequadas a uma exploração rentável e respeitadora do ambiente marinho.

O futuro reserva-nos grandes impactos: económicos, financeiros, sociais, políticos, científicos e culturais, cuja prospetiva se apresenta mais adiante com base numa visão pessoal do autor.

A segurança e proteção dos transportes marítimos e portos é transversal a esses grandes impactos futuros.

Conceitos e Pontos de Vista

A segurança nos transportes marítimos e portos, tem três vertentes distintas: a segurança (*safety*) contra acidentes; a proteção (*security*) contra ameaças (atos ilegais e deliberados) e, o salvamento (*rescue*) no mar.

O termo segurança e, particularmente, a «segurança marítima» pode assumir diferentes significados para pessoas ou organizações distintas, dependendo dos interesses ou inserções

(sociais, económicas, políticas ou ideológicas) das mesmas, ou do seu enquadramento profissional: na área militar e policial, centra-se no âmbito da defesa, da geoestratégia, do combate ao crime e ações de salvamento; na área jurídica, trata-se da elaboração, interpretação e aplicação da legislação; na área técnica, envolve a conceção e operacionalização dos meios materiais e de equipamento; e, no âmbito académico, a investigação de conceitos e políticas.

Um conceito associado é o da prevenção, normalmente ligado à área da Segurança, Higiene e Saúde no Trabalho, correspondendo a um conjunto de atividades que têm em vista a análise e controle dos riscos, para tomar medidas no sentido de evitar acidentes e doenças profissionais. Nos navios e portos, além destas, acrescem necessidades de prevenção na área da proteção contra a concretização de ameaças.

Acrescem, neste contexto, outros conceitos nomeadamente: redundância, como capacidade de resposta, em caso de falha, por escolha de uma ou várias alternativas; resiliência, como capacidade que permite prevenir, minimizar ou superar os efeitos nocivos das adversidades, saindo dessas situações mais fortalecidos e, mais atual, a cibersegurança, como procedimentos de proteção de computadores e servidores, dispositivos móveis, sistemas eletrónicos, redes e dados, contra ataques informáticos maliciosos.

Ameaças

As ameaças subjacentes à intenção de infligir dano ou perda a outro(s), sejam pessoas ou bens, grupos sociais, atividades económicas, políticas, religiosas, etc. que, por sua vez, podem ter impactos mais ou menos alargados a nível geral (mundial, regional ou local) ou individual, evoluem e manifestam especificidades ao longo da história.

Analisadas as últimas décadas, até ao momento atual, podemos sintetizar, com impacto mundial, uma evolução das ameaças gerais a partir de dado momento ou acontecimento histórico. Assim, temos: após a 2ª guerra mundial, no período da "Guerra Fria", destacam-se ações de espionagem, sabotagem e terrorismo; após a implosão da URSS, sobressai o crime organizado e, mais recentemente, o crime cibernético; após os atentados de 11 de setembro de 2001, ocorre uma alteração qualitativa do terrorismo com ações de novo tipo; atualmente, assiste-se à conjugação das ameaças convencionais com a globalização, terrorismo com meios sofisticados, com maior periculosidade e letalidade e, expansão do crime cibernético. "A média semanal de ciberataques a organizações portuguesas aumentou, no ano passado, 81%, face a 2020, com uma organização a ser atacada 881 vezes numa semana" (Dados do *Check Point Research* (*CPR*) citados pela Agência Lusa - janeiro2022).

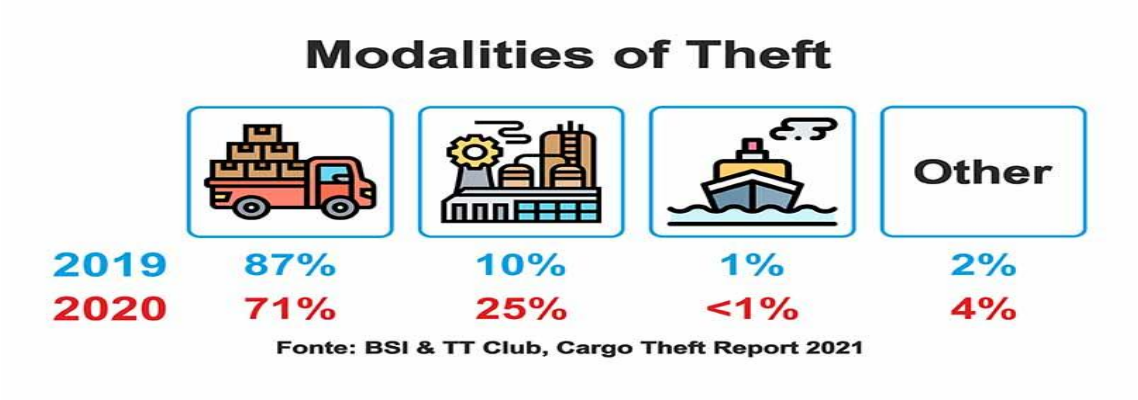
Na área dos transportes marítimos e portos, podemos também sintetizar as principais ameaças, nos últimos anos, que tiveram ou têm fortes impactos na atividade, consequentes de: conflitos inter-estados com particular incidência no Médio Oriente; atos de pirataria no Estreito de Malaca, Corno de África e Golfo da Guiné; atos de terrorismo de incidência mais local, de carácter étnico, político e religioso. A estes somam-se os decorrentes: de crises económicas como a gerada na sequência da falência do *Lehman Brothers* em 2008, conhecida por "Crise da Divida Soberana"; da crise gerada pela pandemia Covid 19, iniciada no final de 2019 e ainda em curso; e, de acidentes como a do navio *Ever Given* no Canal de Suez, em 2021.

Destas ameaças têm resultado consequências das quais se sintetizam as seguintes: os casos de pirataria no estreito de Malaca, na costa da Somália, no oceano Índico e no golfo da Guiné, têm contribuído para o debate sobre as dimensões geopolíticas da segurança marítima; os perigos ou ameaças que enfrentamos hoje são muito diferentes das ameaças clássicas à segurança, com origem num Estado e, de natureza militar; a segurança, a conflitualidade e a definição genérica das ameaças tornaram-se mais opacas e difusas; o reconhecimento de que, parte do domínio marítimo, particularmente no alto mar, devido à sua dimensão e natureza, permanece fora da jurisdição direta de qualquer Estado. Cada vez mais se compreende que tudo

o que se relaciona com o Mar, se enquadra num sistema complexo e vulnerável, onde qualquer ação que o afete tem consequências nas vertentes política, económica e social.

Em conclusão, a segurança dos espaços marítimos ocupa um lugar central entre as preocupações atuais, assumindo-se como um pré-requisito para o desenvolvimento de quaisquer atividades no mar.

Contudo, não podemos deixar de sublinhar, como exemplo que, no contexto de toda a cadeia logística global, os transportes marítimos e os portos são os que oferecem maior segurança às cargas contra roubos, como se pode concluir dos dados que se seguem, referentes a roubo de cargas ao longo da cadeia de transportes:



Enquadramento Institucional

Existe uma pluralidade de organizações de caracter nacional, europeu e internacional que têm funções de regulação, operacionais e de formação na área da segurança e proteção dos transportes marítimos e portos, entre outros, que a seguir sumariamos.

Nacional

Gabinete Nacional de Segurança (GNS) é um serviço central da administração direta do Estado, na dependência do Primeiro-Ministro, cujo diretor-geral, que é por inerência a Autoridade Nacional de Segurança. O GNS tem por missão garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e, exerce a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado (SCEE).

O Sistema de Informações da República Portuguesa (SIRP) é o organismo público que tem a responsabilidade de prestar apoio ao decisor político, antecipando e avaliando as diferentes ameaças que visem Portugal e os seus interesses: a segurança interna e externa, a independência, os seus interesses nacionais, a integridade da unidade do Estado. O SIRP, com as informações que produz, contribui para a salvaguarda, segurança e defesa desses mesmos interesses. Fá-lo numa vertente interna, pela ação do Serviço de Informações de Segurança (SIS) e, numa vertente externa, onde conta com o Serviço de Informações Estratégicas de Defesa (SIED).

Gabinete Coordenador de Segurança (GCS) e Unidade de Coordenação Anti-Terrorista (UCAT), tratam, no quadro da Lei de Segurança Interna e no domínio das ameaças terroristas, funções relevantes pela horizontalidade interdepartamental que envolvem e, pelos circuitos de

informação institucionalizados que utilizam.

Centro Nacional de Cibersegurança (CNCS), criado no âmbito da Estratégia Nacional de Segurança do Ciberespaço, o CNCS atua como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço seja utilizado como espaço de liberdade, segurança e justiça, para proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático.

O CNCS integra o CERT.PT (*Computer Emergency Response Team*) que é o serviço português (PT) que coordena a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais, operadores de infraestruturas críticas nacionais e prestadores de serviços digitais, ou seja, do ciberespaço nacional, incluindo qualquer dispositivo pertencente a uma rede ou bloco de endereçamento atribuído a um operador de comunicações eletrónicas, instituição, pessoa coletiva ou singular com sede em território Português, ou que esteja fisicamente localizado em território Português.

Por sua vez o CERT.PT é membro e representante nacional na Rede Europeia CSIRT (*Computer Security Incident Response Team*), que visa estabelecer laços de confiança entre elementos responsáveis pela segurança informática, de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança, criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contra-medidas pró-activas e reactivas, criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão e, promover uma cultura de segurança em Portugal.O CERT.PT é membro acreditado do TI (*Trusted Introducer Service*), que assegura um banco de dados europeu dos CSIRTs e, credencia e certifica equipas de segurança.

O CERT.PT é também membro efetivo do *Forum of Incident Response and Security Teams* (FIRST), cuja missão é reunir equipas de resposta a incidentes e segurança de todos os países do mundo, para garantir uma Internet segura para todos.

A Escola NATO de Comunicações e Sistemas de Informação (*Cyber Academia and Innovation Hub - CAIH*), recentemente sediada em Portugal (Oeiras), como centro de investigação e formação nos domínios das comunicações e da cibersegurança, pode vir a ser uma referência europeia e no âmbito dos países da Nato, nesta área.

Marinha de Guerra Portuguesa (Armada ou simplesmente Marinha), ramo das Forças Armadas que se integra na administração do Estado, através do Ministério da Defesa Nacional. desenvolve ações de dissuasão, defesa militar e apoio à política externa e que dispõe, fundamentalmente, de 3 conjuntos de forças e meios: Forças Permanentes em ação de soberania orientadas para missões de patrulhamento, vigilância e fiscalização marítima, busca e salvamento e de resposta a catástrofes nas áreas de jurisdição ou responsabilidade nacional; uma Força de Reação Imediata orientada para missões de resposta a crise e catástrofe, como seja a evacuação de cidadãos nacionais; um Conjunto Modular de Forças orientado para resposta a compromissos internacionais, por exemplo no âmbito da NATO, da União Europeia ou das Nações Unidas, onde se enquadra a contribuição para o combate à pirataria. A Marinha coopera com múltiplas entidades nacionais e estrangeiras, designadamente em matérias de: Fiscalização e proteção de recursos; Combate à criminalidade marítima; Controlo de fronteiras e da migração ilegal; Apoio em situações de crise e de catástrofe; e Apoio à sustentação dos meios da Autoridade Marítima Nacional.

Autoridade Marítima Nacional (AMN), dependente do Ministro de Defesa Nacional, por ligação à Marinha, é responsável pela segurança da faixa costeira e, no domínio público marítimo, das fronteiras marítimas e fluviais, quando aplicável, exercendo as competências que lhe são

atribuídas no âmbito da lei da segurança interna, sendo a cúpula hierárquica da Direcção-Geral da Autoridade Marítima (DGAM), e das capitanias dos portos como órgãos locais desta, designadamente nas matérias relativas à segurança interna e, igualmente, nas matérias de proteção.

Direção Geral de Recursos Naturais, Segurança e Serviços Marítimos (DGRM), é a Autoridade nacional Competente para a Proteção do Transporte Marítimo (navios), dos Portos e Instalações Portuárias (ACPTMP), que coordena, implementa e supervisiona a aplicação das medidas de proteção, sendo, em articulação com a DGMA, o ponto de contacto para assistência aos navios e, também com a DGMA e as respetivas Administrações Portuárias (AP), o ponto de contacto para a proteção dos portos, reunindo especiais competências em todo o processo de Proteção. As atribuições da DGRM são particularmente importantes no âmbito dos designados: Estado de Bandeira (Navios, Marítimos, Náutica de Recreio, Organizações Reconhecidas (OR), Prevenção da Poluição, Responsabilidade Civil Marítima, Segurança Marítima, Resoluções IMO que não carecem de aprovação para adesão,Convenções ratificadas por Portugal; Estado do Porto (Controlo pelo Estado do Porto (*Port State Control - PSC*), Proteção dos Navios e das Instalações Portuárias (ISPS) e Meios Portuários de Receção de Resíduos; Estado Costeiro (Zonas Marítimas sob Jurisdição e ou Soberania Nacional, Exploração, Conservação e Gestão dos Recursos Vivos, Autoridade Nacional de Controlo de Tráfego Marítimo (VTS).

AP - Administrações Portuárias**,** tuteladas diretamente pelo Governo, são as Autoridades de Proteção Portuária (APP), nos respetivos portos.

Outros organismos nacionais, que também intervêm no âmbito da Segurança dos Transportes Marítimos e Portos: A Polícia Judiciária (PJ), em matéria de prevenção e investigação criminal; A Direcção-Geral das Alfândegas (DGA), no âmbito do controlo de mercadorias e bens pessoais, bem como em matéria de investigação criminal; O Serviço de Estrangeiros e Fronteiras (SEF), na vigilância e fiscalização da circulação de pessoas nos postos de fronteira, podendo impedir o desembarque de passageiros e tripulantes de embarcações, quando os mesmos não satisfaçam os requisitos legais exigíveis para o efeito; A Autoridade Nacional de Saúde (ANS), em matéria de riscos para a saúde pública; A Polícia de Segurança Pública (PSP), no exercício das suas competências territoriais, especialmente no âmbito da prevenção, investigação e repressão da criminalidade e das competências que lhe estão exclusivamente atribuídas; A Guarda Nacional Republicana (GNR), no âmbito das suas competências em razão da matéria e do território.

Europeu e Internacional

Convenção das Nações Unidas sobre o Direito do Mar de 1982, conhecida por “Lei do Mar”, estabelece o direito de atuação dos Estados nos espaços marítimos.

Agência Europeia da Segurança Marítima (EMSA) é uma organização da União Europeia (EU), sediada em Lisboa, cuja missão é servir os interesses marítimos da UE para um setor marítimo seguro, ecológico e competitivo e atuar como um ponto de referência confiável e respeitado no setor marítimo na Europa e em todo o mundo. Trabalha em questões e tarefas de segurança marítima, proteção, clima, meio ambiente e mercado único, primeiro como um prestador de serviços para os Estados-Membros e a Comissão, mas também como um parceiro inovador e confiável e centro de conhecimento para o cluster marítimo europeu e, como uma referência internacional.

Maritime Liaison Office (MARLO) é um organismo da Marinha dos Estados Unidos (US Navy) que tem por missão facilitar a troca de informações entre a US Navy, as Forças Marítimas Combinadas (CMF) e a comunidade comercial na área da responsabilidade do Comando Central dos Estados Unidos (CENTCOM). O MARLO atua como um canal de informações com foco na segurança e proteção do transporte marítimo e, tem o compromisso de ajudar todos os membros da comunidade marítima comercial, agilizada por departamentos regionalizados para apoio em áreas fora da águas territoriais dos Estados Unidos, a saber: Miami, Flórida US para a América

Central e do Sul; Nápoles, Itália para a Europa e África; Manama, Bahrain para o Corno de África; e Yokohama, Japão para a Asia e Pacífico.

Organização Marítima Internacional (IMO), como agência especializada das Nações Unidas, tem como missão promover o transporte marítimo seguro, protegido, ambientalmente correto, eficiente e sustentável, por meio da cooperação realizada através da adoção dos mais altos padrões de proteção e segurança marítima, eficiência da navegação e prevenção e controle da poluição por navios, bem como pela consideração das questões jurídicas pertinentes e, pela efetiva implementação de instrumentos (Convenções), com vista à sua aplicação universal e uniforme. As três Convenções da IMO que constituem a base mais importante dos instrumentos internacionais que regulam as questões relacionadas com a segurança marítima, a prevenção da poluição e a atividade de transporte marítimo são:

- A Convenção Internacional para a Salvaguarda da Vida Humana no Mar **-** SOLAS (*Safety of Life at Sea*);
- A Convenção Internacional para a Prevenção da Poluição por Navios - MARPOL (*Marine Pollution*);
- A Convenção Internacional sobre Normas de Formação, de Certificação e de Serviço de Quartos para os Marítimos - STCW (*Standards of Training, Certification and Watchkeeping for Seafarers*).

Sistema SAR de busca e salvamento (*Search And Rescue)* define e descreve todas as organizações e operações destinadas a localizar e salvar pessoas em situação de risco, tendo por base de orientação o *"International Handbook of Research and Aeronautical and Maritime – SAR)* estabelecido pela IMO e *a* Organização da Aviação Civil Internacional I*CAO (International Civil Aviation Organization),* sendo de aplicação internacional e, em princípio, sem levar em conta as fronteiras, sendo aplicável aos Estados participantes da Convenção SOLAS. Todos os sistemas SAR devem ser estruturados para executar, de maneira efetiva, as seguintes funções: receber notificações de desastres, registrar e retransmitir; coordenar as respostas de busca e salvamento; conduzir as operações de busca e salvamento. O sistema *SAR,* em Portugal é da responsabilidade da Armada, que gere o Centro de Coordenação de Busca e Salvamento-MRCC (*Maritime Rescue Coordination Center*).

Em síntese, os instrumentos que, de forma mais imediata e efetiva, contribuem para a segurança (*safety*) da navegação marítima são o RIEAM 72, a organização das zonas de separação de tráfego marítimo, o VTS, o assinalamento marítimo e o SAR, na outra vertente, o código ISPS é o que regula, de forma mais direta, a proteção (*security*) dos transportes marítimos (navios) e portos.

Proteção de Portos, Instalações Portuárias e Navios

Código ISPS

O Código ISPS, adotado pela OMI, é um capítulo da Convenção SOLAS, que visa a proteção do transporte marítimo através da adoção, a nível mundial, de regras a observar pelos navios utilizados no comércio internacional e pelas instalações portuárias que os servem, sendo constituído por duas partes – a "A", que é obrigatória e, a "B", que é facultativa.

A União Europeia adotou medidas consagradas no Regulamento CE/ 725/2004 do Parlamento Europeu e do Conselho, de 31 de março, relativo ao reforço da proteção dos navios e das instalações portuárias complementadas pelas previstas na Diretiva CE/65/2005 do Parlamento Europeu e do Conselho, de 26 de outubro, relativas ao reforço da proteção nos portos, sendo ambas as partes do código, obrigatórias para Portugal.

A Diretiva foi transposta para a ordem jurídica portuguesa pelo Decreto-lei n.º 226/2006, que

define a estrutura básica de organização nacional necessária à operacionalização e implementação do código.

A DGRM, como já referido, é a Autoridade Competente para a Proteção dos Navios, das Instalações Portuárias e dos Portos, sendo a Autoridade de Proteção do Porto a respetiva Administração Portuária e, para os navios, as respetivas Companhias.

Política de Proteção

A política de proteção baseia-se numa gestão pragmática (ativa e prática), que engloba um vasto leque de medidas, incluindo avaliações, planos, procedimentos e organização, visando a salvaguarda de pessoas e bens materiais.de ações criminosas desencadeadas por indivíduos ou grupos de terroristas ou outras organizações criminosas.

Assim, a política de proteção está definida de modo a assegurar que a unidade em causa (Porto, Instalação Portuária ou Navio) está protegida contra ações de terrorismo, sabotagem ou outros atos ilícitos que possam colocar em risco a integridade física, a atividade e os interesses de todos os que, para ou com ela trabalham ou dela dependem, quer a nível local, regional, nacional ou internacional.

Objetivos da Proteção

Genericamente a implementação de medidas de proteção contra perdas, danos ou roubos, cobrem também toda a documentação sensível de proteção, incluindo os sistemas informáticos, que deverão estar protegidos de acessos não autorizados.

As medidas a implementar que têm como principal objetivo a proteção, visam: respeitar as Leis Internacionais e outros instrumentos que regulam a proteção marítima, nomeadamente o código *ISPS,* na sua versão atualizada e, a regulamentação e legislação comunitária e nacional aplicável; proteger os trabalhadores (portuários e tripulações) e visitantes, as instalações, a carga e os navios; nomear o Oficial de Proteção (OPP-OPIP-OPN) com uma responsabilidade global em matéria de proteção, dando apoio à realização destas tarefas e responsabilidades; Proceder à Avaliação de Proteção da unidade respetiva, tendo em linha de conta a sua natureza e o tipo interface Porto, Instalação Portuária e Navios e, na sua sequência, elaborar o respetivo Plano de Proteção, sua implementação, monitorização, revisão e auditorias; promover a consciencialização entre todo o seu pessoal, para a importância das questões da proteção; formar, instruir e aconselhar os elementos envolvidos na proteção sobre as respostas a dar em caso de ameaça à proteção, mantendo os respetivos procedimentos e orientações, devidamente atualizadas; testar as medidas implementadas e organizar, periodicamente, exercícios com simulacros (cenários) de ocorrências expectáveis; promover um sistema de comunicação e veicular a informação selecionada para os elementos e as autoridades envolvidas na proteção aos seus diferentes níveis; garantir um método comunicacional seguro, de forma a que todo o pessoal, utilizadores e visitantes, estejam informados sobre os procedimentos de proteção aplicáveis; Reconhecer a sobrecarga que constitui para o pessoal os procedimentos de proteção adicionais; constatar que os objetivos que visam a proteção podem comprometer as metas do pessoal em matéria de segurança (safety) e, assim, assumir que deve haver entre ambos um equilíbrio adequado; apoiar os Oficiais de Proteção no exercício da sua autoridade para que estes possam tomar decisões independentes na área da proteção e, ainda quando tenham necessidade no exercício das suas funções, de recorrer a auxílio.

Avaliação de Proteção

A Avaliação de Proteção (Porto, Instalação Portuária ou Navio) tem por finalidade conhecer e identificar riscos e vulnerabilidades, de forma a estabelecer medidas preventivas e/ou de reação para as condições de proteção no âmbito do Código ISPS e, seu alargamento aos Portos.

Risco = Ameaça x Vulnerabilidade x Consequência

Parte-se de uma análise exaustiva da situação local, identificando as vulnerabilidades da unidade em estudo, definindo as contramedidas adequadas, de modo a poder interagir entre o Porto e as Instalações Portuárias e, entre estas e os Navios que as demandam, permitindo-lhes utilizar, em pleno, todo o seu potencial de proteção em condições de possíveis ameaças.

Metodologicamente, a Avaliação da Proteção deve iniciar-se pelo preenchimento da Lista de Verificação de Avaliação de Risco (*Checklist "On-Scene Security Survey"*), que deverá, no final, constar dos anexos do dossier com a Avaliação

Partindo da Lista de Verificação devem ser analisados, com o maior detalhe possível, os seguintes elementos: caracterização da unidade em estudo; medidas de proteção existentes; identificação dos bens e infraestruturas que são importantes para proteger (Alvos).

Segue-se uma Avaliação da Criticidade dos Alvos, com os seguintes graus: Crítico (alvos que constituem o suporte das atividades e que impedem o exercício de quaisquer outras, sendo difíceis de recuperar em tempo útil); Moderado (alvos que servem de apoio, afetando uma ou duas áreas de atividade, com razoável capacidade de recuperação em tempo útil); Marginal (alvos que não sejam suportes de qualquer atividade importante, com efeitos de consequências mínimas e, facilmente recuperáveis ou substituíveis).

Para cada alvo deve-se fazer uma descrição dos Efeitos com a sua Destruição e a Capacidade de Recuperação**,** esta com base no critério seguinte: Nenhuma - a recuperação pode ser inviável ou superior a 1 ano; Deficiente - a recuperação pode significar vários meses; Fraca - a recuperação pode ser feita em poucos meses; Boa - a recuperação na escala das semanas; Excelente - recuperação quase imediata ou na escala dos dias.

Com base nestas duas análises, faz-se a Avaliação da Criticidade dos Alvos através da identificação das principais atividades e operações mais importantes.

Segue-se a Avaliação de Ameaças e a Seleção do Cenário. Entende-se, como cenário de ataque, uma ameaça potencial a um alvo em determinadas circunstâncias. A seleção do cenário deve ser confinada a possibilidades reais e, as capacidades e intenções devem estar de acordo com acontecimentos anteriores e com a informação disponível.

Para a avaliação da vulnerabilidade de um alvo consideram-se, à partida, quatro elementos que concorrem para a sua aferição, embora, nem sempre de aplicação direta e que são: Disponibilidade, a existência e presença do alvo, a sua exposição e grau de probabilidade de sofrer um ataque; Acessibilidade, condições de acesso para um ataque ao alvo, considerando a existência (ou não) de barreiras físicas/geográficas para conter uma ameaça sem recurso a medidas de proteção; Organização da Proteção, capacidade do sistema e do pessoal de proteção em deter um ataque, incluindo planos de contingência, capacidade de comunicação, sistemas de deteção, etc.; Resistência, capacidade do alvo em conter, por si só, um ataque, considerando a complexidade do alvo, a sua conceção e as características dos materiais usados.

A vulnerabilidade, a partir dos elementos aferidores atrás descritos, é posteriormente classificada em três graus: Baixo, Médio e Elevado, de acordo com critérios pré-definidos.

Combinando os Graus de Consequência com os Graus de Vulnerabilidade constrói-se uma matriz definidora das ações a tomar, em que: Conter, significa que devem ser adotadas e desenvolvidas estratégias de contenção, no sentido de reduzir os riscos, devendo o Plano de Proteção conter o cenário avaliado, os resultados da avaliação e as medidas de contenção; Considerar, significa que a combinação cenário / alvo deve ser considerada e que as estratégias de contenção devem ser desenvolvidas caso a caso, devendo o Plano de Proteção conter o cenário avaliado, os resultados da avaliação e razão pela qual foram decididas ou não, medidas de contenção; Documentar, significa que a combinação cenário / alvo não necessita de medidas de contenção no momento e, por isso, apenas deve ser documentado, devendo o Plano de Proteção conter o cenário avaliado e os resultados da avaliação.

A identificação, seleção e hierarquização, por ordem de prioridades, das contramedidas de contenção e mudanças de procedimento, destinam-se a garantir que são propostas e utilizadas as medidas consideradas mais eficazes para reduzir a vulnerabilidade do alvo.

As medidas de proteção (contramedidas) deverão ser selecionadas com base em fatores, como por exemplo, a sua eficácia para reduzir a probabilidade de um ataque e devem ser avaliadas com base em informações que incluam, nomeadamente: vistorias, inspeções e auditorias anteriores, quer de proteção quer de segurança (safety); consultas a outros, armadores, operadores, concessionários das estruturas adjacentes e às autoridades portuárias; historial de incidentes de proteção anteriores; tipo de operações a realizar nas Instalações, Porto ou Navio.

Nesta perspetiva há que identificar as operações e áreas chave, assim como os pontos vulneráveis, de modo a que as contramedidas possam incidir, com mais objetividade, nas ameaças definidas.

Na avaliação, considera-se alta criticidade sempre que a operação seja determinante no âmbito de, pelo menos, um dos seguintes aspetos: potenciar/incrementar qualquer fator de risco identificado; proteção/dissuasão/limitação de qualquer fator de risco identificado; constitua um alvo a proteger.

Nas medidas de proteção no local, regista-se a existência de medidas de proteção (materiais, humanas e/ou organizacionais), sendo indicadas eventuais medidas complementares ou substitutas que se considerem adequadas. Sempre que necessário, os aspetos referidos são complementados nas observações.

Após a avaliação da vulnerabilidade e consequências e, subsequente nível de ação, passamos à fase de definição de contramedidas de contenção adequadas. Para tanto, definimos níveis hierárquicos para a definição das prioridades das ações, consoante a sua capacidade e eficácia, considerando:1º Nível, medidas capazes de reduzir o grau de consequência e vulnerabilidade; 2º Nível, medidas capazes de reduzir o grau de vulnerabilidade, visando evitar a eventual concretização da ameaça sobre o alvo; 3º Nível, medidas atenuadoras das consequências ou efeitos de uma dada ameaça sobre o alvo.

A definição das contramedidas de contenção deve ser desenvolvida para todos os cenários cuja avaliação possui o nível "conter". Para o nível "considerar", será, em sede de desenvolvimento do Plano de Proteção, onde será tratado cada cenário caso a caso, visando a pertinência da definição de medidas concretas de contenção. Uma análise de benefícios com a introdução das contramedidas de contenção deverá ser feita no final da avaliação.

Como resumo final das análises, devem-se sintetizar as áreas mais vulneráveis e as medidas mitigadoras (contramedidas) dessas vulnerabilidades que deverão ser contempladas no Plano de Proteção, que será elaborado após a aprovação da Avaliação de Proteção pelas entidades competentes. A Avaliação de Proteção, depois de aprovada, deve constar de um dossier, datado e com reserva de Confidencialidade, permitindo que os Oficiais de Proteção possam efetuar registos de atualização.

Plano de Proteção

O Plano de Proteção deve ser elaborado no seguimento da Avaliação de Proteção, para garantir a aplicação de medidas destinadas a reforçar a proteção e incorporar outros Planos de Proteção de interface e, deve conter os procedimentos a desencadear em caso de ameaça de proteção, seguindo as conclusões da avaliação efetuada, nomeadamente as respetivas Estratégias de Contenção.

No âmbito da diretiva, as zonas a proteger englobam as Áreas Restritas e as Áreas Controladas que constituem, no seu conjunto, a unidade objeto do Plano, pelo que, com base na avaliação

da proteção aprovada, são consideradas como zonas com impacte, devendo ser-lhes aplicadas medidas de proteção para os diversos Níveis de Proteção.

As Áreas Restritas são zonas de acesso condicionado, com o propósito de proteger: passageiros, pessoal/tripulantes e visitantes; navios que utilizam o porto e o porto que recebe os navios; infraestruturas e equipamentos; locais sensíveis de segurança e/ou proteção e outras zonas no interior das unidades; equipamentos e sistemas de vigilância e proteção.

Todos os espaços que delimitam os ativos críticos são considerados por si só, Áreas Restritas, encontrando-se condicionados os acessos a pessoas que não estejam devidamente autorizadas.

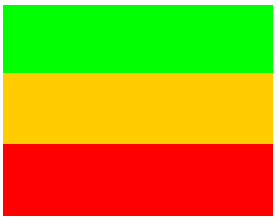
Às Áreas Restritas, espaços que deverão encontrar-se sempre fechados e a sua abertura controlada, só deverão ter acesso, aqueles que, por inerência de funções ou responsabilidades, estão autorizados a frequentá-las, devendo a permanência nas mesmas ser pelo período de tempo mínimo necessário e justificado.

O conceito de área fechada e por consequência de área restrita é extensível aos locais de interface, por exemplo dos navios com os cais, cuja entrada nos seus limites pressupõe a satisfação de necessidades de carácter operacional.

É entendido que áreas restritas fechadas não deverão conflituar com a necessidade funcional de permanecerem abertas, por questões de segurança (safety).

Todas as demais áreas que compõem a unidade em toda a sua abrangência serão consideradas como Áreas Controladas.

Existem três Níveis de Proteção que seguir se identificam com a respetiva sinalética:



Nível de Proteção 1 – Normal

Nível de Proteção 2 – Reforçado

Nível de Proteção 3 – Excecional

O Nível de Proteção 1 significa nível de proteção normal em que devem vigorar permanentemente medidas de proteção mínimas que correspondem a condições normais de operacionalidade em matéria de proteção.

Este nível de proteção representa a possibilidade (geral) de surgir uma ameaça contra o porto, a instalação ou o navio, razão pela qual os requisitos de proteção para uma ameaça do Nível 1 devem estar sempre em vigor.

Neste nível de proteção consideram-se como mais importantes as seguintes medidas: assegurar procedimentos de vigilância durante as 24 horas; identificar todas as pessoas e os veículos que acedam, por qualquer razão, ao interior das áreas restritas, procedendo à revista aleatória das viaturas, aleatoriedade que será determinada pelo respetivo Oficial de Proteção; superintender às operações, o que incluirá operações de abastecimento de sobressalentes, provisões, bancas, aguada ou saída de resíduos dos navios; requerer informação atempada sobre a chegada de navios, veículos transportando provisões, fornecimentos, peças, sobressalentes e vendedores/visitas que saiam da rotina; inspecionar o transporte de entrega de provisões, em conjunto com o Oficial de Proteção do Navio (OPN); assegurar que as comunicações funcionam relativamente aos navios; manter uma elevada vigilância situacional para atividades suspeitas; comunicar qualquer atividade anormal ao respetivo Oficial de Proteção; identificar todas as pessoas que pretendam ir a bordo após autorização dada pelo Oficial de Proteção e OPN ou

Comandante do Navio; ligar a iluminação devida durante as horas de escuridão; assegurar que todos os acessos não habituais estão fechados à chave.

O Nível de Proteção 2 significa um nível de proteção reforçado em que devem vigorar durante determinado período medidas de proteção adicionais adequadas, devido a risco acrescido de incidente de proteção.

Todo o pessoal afeto às áreas restritas estará atento ao desenrolar da situação, de forma a parar rumores e a prevenir desnecessários alarmes. Este pessoal deverá estar informado sobre o que representa a entrada em vigor do Nível de Proteção 2 e, cada um destes trabalhadores redobrará a sua atenção no local de trabalho.

Este nível de proteção entra em vigor quando for determinado pela ACPTMP (DGRM), devido a ameaça feita ao porto, à instalação, ou a determinado tipo de navio, ainda que nenhum alvo, em particular, tenha sido denunciado.

Medidas a desenvolver pelo respetivo Oficial de Proteção: designar pessoal adicional, para estabelecer vigilância aos pontos de acesso e passar rondas a todo o perímetro das áreas restritas; convocação e reunião da CCOPP; notificar as empresas de vigilância, a fim de procederem ao reforço de pessoal; averiguar e aprovar, antecipadamente, a entrada de qualquer pessoa que queira aceder ás áreas restritas e que não esteja autorizada; aumentar o acompanhamento de provisões para navios coordenando esta ação com o OPN; limitar o acesso físico às áreas restritas de pessoas e veículos, particularmente às áreas mais sensíveis; emitir uma Declaração de Proteção (DoS) entre o navio e o porto ou a instalação; aumentar as revistas a embrulhos/pacotes/fornecimentos/provisões; incrementar a frequência das revistas a veículos; manter uma elevada vigilância situacional para atividades suspeitas; estabelecer comunicações internas de proteção entre os Oficiais de Proteção do Porto (OPP) e das Instalações Portuárias (OPIP's) e destes com os Oficiais de Proteção dos Navios (OPN's), aumentando o fluxo comunicacional.

O Plano de Proteção, instruções, tarefas que envolvem o pessoal da proteção e as exigências de logística que se relacionam com a entrada em vigor do nível de proteção 2, são, pelo respetivo Oficial de Proteção, periodicamente revistos, de forma a confirmar a sua atualidade.

O Nível de Proteção 3 corresponde ao nível de proteção excecional em que devem vigorar, durante um período limitado, medidas de proteção suplementares especiais, devido à probabilidade ou iminência de um incidente de proteção, mesmo que não seja possível identificar o alvo.

Este nível de ameaça à proteção representa o mais elevado nível de ameaça e é baseado em informações de confiança obtidas pelos serviços de "inteligência". Indica que o porto, uma instalação ou um navio, foram identificados como "alvo" e que a ameaça, não só é altamente provável de originar um incidente de proteção, como está eminente.

Algumas das medidas que o Oficial de Proteção tem que implementar, para além de estabelecer de imediato comunicação com as autoridades adequadas e o navio, são: aumentar os índices de vigilância e incrementar as infraestruturas de iluminação; proibir o acesso ao alvo de quem considere não essencial, instruindo, no sentido de ser facilitada a entrada a autoridades que acorram a emergências; encerrar a portaria respetiva; suspender a movimentação de pessoas e veículos; cooperar com as autoridades locais na proteção e vigilância dos possíveis acessos de terra e do mar; suspender todas as operações e trabalhos em curso; considerar a evacuação do pessoal, parcial ou total, da área do alvo; considerar a saída do(s) navio(s) para o largo, informando o departamento de pilotagem; estar atento a informações vindas das autoridades governamentais ou da companhia, que visem a operacionalidade e a proteção; Implementar medidas/ações específicas/adicionais adequadas de proteção, ordenada pelas autoridades governamentais; incrementar as comunicações internas de proteção.

As disposições genéricas, atrás descritas, para cada um dos Níveis de Proteção, são implementadas em conjunto com requisitos mais detalhados inscritos na Tabela de Requisitos dos Níveis de Proteção, especificas para cada instalação (porto, instalação portuária ou navio).

Organização da Segurança e Proteção

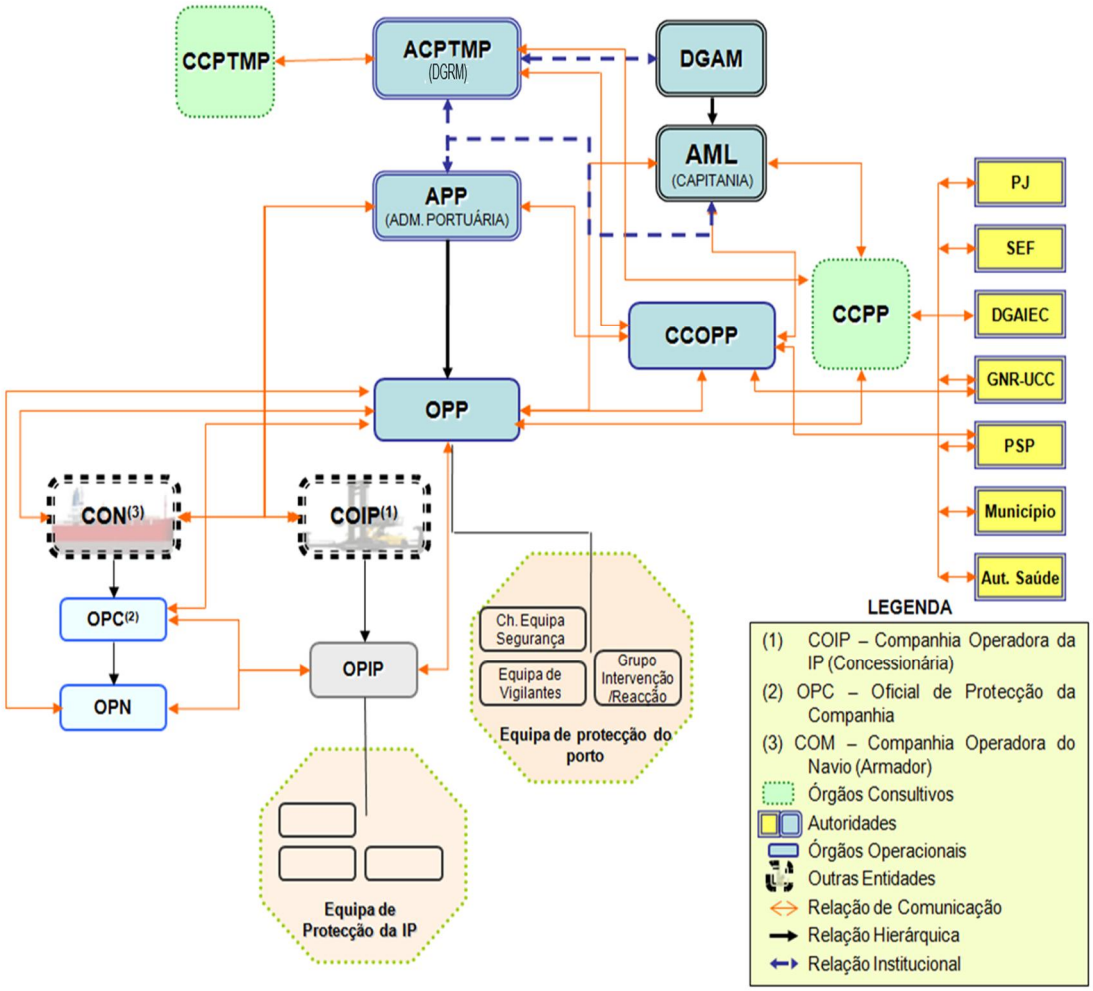
Em termos organizacionais e, ao nível dos sistemas de segurança e proteção, particularmente, os Portos e as Instalações Portuárias, dispõem de quatro instrumentos principais, que podem ter, entre outras, as seguintes designações: Regulamento de Segurança; Normas de Segurança Marítima e Portuária e Regulamento VTS; Plano de Emergência Interno; Plano de Proteção.

O Regulamento de Segurança contempla quer a zona marítima (inspeção, lavagem, desgaseificação dos navios, operação e reparação de navios, e lastro, poluição, cargas perigosas, movimentação de mercadorias, etc.), quer a zona terrestre (acessos e circulação na zona portuária, realização de trabalhos, etc.).

As Normas de Segurança incluem procedimentos para demandar o Porto durante a permanência do navio, serviço de pilotagem, fundeadouros, etc.

O Plano de Emergência Interno, contempla um sistema integrado de prevenção e intervenção destinado a fazer face, principalmente, a riscos de incêndio e poluição.

O Plano de Proteção**,** já descrito, é gerido, quer na fase de implementação/aprovação quer na sua operacionalização, pela estrutura constante do Organograma que se segue, refletindo as atribuições e os contactos hierarquizados estabelecidos no Decreto-Lei nº 226/2006 de 15 de novembro.



Desafios para um Futuro Próximo

Em geral

- Promover economias prósperas ao serviço dos cidadãos, num contexto de justiça e paz social.
- Dinamizar economias circulares, limpas, resilientes e preparadas para adoção de metas ambiciosas de redução de emissões, com o objetivo de conseguir emissões nulas e, preservar e restaurar o ambiente natural.
- Preparar as organizações e a sociedade, em geral, para a era digital, aproveitando as oportunidades das novas tecnologias digitais dentro de limites éticos.
- Aumentar a capacidade e segurança digitais (cibersegurança) no acompanhamento da integração nos serviços digitais das partes interessadas e, dos normativos a implementar (leis

dos serviços digitais).

Nos transportes marítimos e portos

- Contribuir para a competitividade e o crescimento das indústrias marítimas, como importante fonte de emprego e rendimento para as economias;
- Desenvolver ações destinadas a prevenir a poluição por navios e a responder, quer à poluição causada pelos mesmos, quer à poluição marinha causada pelas grandes instalações portuárias de movimentação de granéis (petrolíferas, químicos e minerais).
- Desenvolver a vertente marítima da descarbonização dos transportes, contribuindo para prevenir e mitigar a poluição marinha e atmosférica, bem como as alterações climáticas.
- Pugnar pela criação de infraestruturas e estruturas atrativas, redundantes, resilientes e competitivas para um transporte marítimo de qualidade, operadores de qualidade e empregos de qualidade, com o objetivo de contribuir para a construção de economias prósperas e equitativas
- Simplificar os procedimentos dos Transportes Marítimos e dos Portos, reduzindo encargos e aumentando a eficiência no que se refere à multiplicidade de requisitos administrativos e comunicação de informação, através da implementação de ferramentas digitais (janelas únicas) para facilitar o seu cumprimento pelos responsáveis do setor e, contribuindo para um ambiente logístico cada vez mais integrado e global e, sem barreiras.
- Reforçar a integração de dados e o processamento inteligente de informações, tirando partido da nova geração de tecnologias digitais, incluindo a inteligência artificial e o seu potencial na procura de soluções para uma série de desafios.
- Desenvolver fortes procedimentos de proteção contra ameaças de segurança, focada na navegação, nos navios e nos portos em ligação com toda a cadeia logística e, com particular incidência, nos ataques cibernéticos.

Previsões para um Futuro Próximo

Negócios: Se pensarmos numa oportunidade de negócio, antes de investir tempo e dinheiro, devemos equacionar se o mesmo irá funcionar no *smartphone*; se não funcionar, a probabilidade de êxito é reduzida ou nula. Ao acompanhamento e gestão de toda a cadeia de transportes por smartphone, seguir-se-á gestão autónoma da cadeia de transportes com recurso a Inteligência Artificial (IA);

Eletricidade: O consumo será, tendencialmente, cada vez maior e generalizado a todos os setores (indústria, habitação, transportes, …), mais barata e "limpa", por outro lado, viabilizará, através da dessalinização da água do mar, a disponibilidade de água em qualquer parte do mundo, incrementando a produção local de alimentos. Prevê-se significativo impacto nos meios e na cadeia logística, dos transportes;

Trabalho: A maior parte dos empregos tradicionais desaparecerão nos próximos tempos. Haverá novos empregos, mas ocupando um número cada vez menor de pessoas. As tripulações e trabalhadores portuários tenderão a desaparecer;

Agricultura: Será cada vez mais intensiva e robotizada, com transformação e produção local de produtos acabados e prontos para consumo. Os agricultores serão mais gestores, que trabalhadores diretos. As hidroponia e aeroponia serão técnicas cada vez mais generalizadas, altamente produtivas e, necessitarão progressivamente de menos adubos químicos e pesticidas. Grande impacto na cadeia logística dos transportes;

Pecuária: O consumo de carne tenderá a desaparecer, acabando com a criação tradicional de

animais (vacas, ovelhas, etc.). As fontes alternativas de proteína serão os vegetais e os insetos. Produção de alimentos impressos em 3D. Grande impacto na cadeia logística dos transportes;

Indústria: A robotização, que já hoje se encontra instalada nas grandes unidades industriais, embora em processos muito ancorados ao mesmo espaço físico, evoluirá com as máquinas de impressão 3D cada vez maiores e sofisticadas (numa futuro mais longínquo a impressão 4D com materiais inteligentes), capazes de fabricar desde pequenas peças a casas de habitação, permitindo a produção em qualquer lugar, reduzindo a cadeia logística ao transporte das máquinas e das matérias-primas de abastecimento dessas máquinas.

Administração: Será totalmente desmaterializada e gerida por aplicações de Inteligência Artificial. Os registos, 100% fiáveis, serão feitos em Blockchain;

Moeda: As moedas tradicionais serão todas substituídas por uma moeda digital baseada na tecnologia Blockchain, tornando-se numa única moeda-reserva-padrão;

Saúde: A utilização dos smartphones, como ferramenta de apoio ao diagnóstico, a utilização da robótica, a impressão 3D e a inteligência artificial, nos processos cirúrgicos e nos cuidados de saúde, em geral, conduzirão a uma medicina acessível mundialmente e, praticamente gratuita;

Educação/Informação: Os smartphones mais baratos (já têm custos da ordem de US$ 10,00 na Ásia e em África) permitirão que, praticamente todos os humanos tenham acesso a um, com internet e tradução automática. A educação/informação tornar-se-á comum a nível mundial, esbatendo-se os atuais desníveis culturais entre nações;

Longevidade: Atualmente, a expectativa de vida aumenta uns 3 meses por ano. Estima-se que, daqui a 20 anos, esse aumento seja de um ano por ano. Assim, as vidas serão bem mais longas, possivelmente muito para além dos 100 anos (impacto nas ofertas de lazer ex. navios cruzeiros).

Transportes Marítimos e Portos: Resultante do aprofundamento da aplicação dos sistemas de informação, automação e inteligência artificial, as novas tecnologias digitais irão conduzir-nos aos navios autónomos e aos *smart ports*. Atualmente, já se assiste a aplicações pontuais, tirando partido da integração das novas tecnologias, como: 5G, Cloud, Big Data, NotN, IoT, ML, Blockchain, Digital Twin, entre outras. Estas inovações levarão o setor dos transportes marítimos e portos a um futuro mais eficiente e conectado.

Prospetivas de Médio e Longo Prazo

Á luz de fatos técnicos, científicos, económicos e sociais, de que já hoje existem indícios, de que demos atrás alguns exemplos, os desenvolvimentos futuros vão ser exponenciais. A evolução do mundo a médio e muito menos a longo prazo, não terá qualquer paralelo com o ritmo do passado. Assim, e com base numa visão pessoal, a prospetiva relativamente a pontos chave do sistema de transportes marítimos e portos, é o que a seguir arriscamos:

Próximos 20 anos: Digitalização integral dos sistemas de gestão da operação portuária e transportes marítimos. Início da quebra de utilização de bens reais por bens digitais (Metaverso);

Próximos 30 anos: Integração global das cadeias logísticas e a aplicação da Inteligência artificial aos portos e transportes marítimos. Navegação autónoma (dispensa de pessoal a bordo). Operações portuárias automáticas (dispensa de trabalhadores de estiva e na operação de equipamentos). Impressão 3D (1.ª revolução logística);

Próximos 50 anos: Impressão 4D (2.ª revolução logística);

Próximos 70 anos: Deixam de existir navios de carga e, consequentemente, os portos comerciais;

Próximos 100 anos: Os bens necessários à sobrevivência humana (alimentação, habitação,

equipamentos, …) serão gerados no local de consumo/uso, com matérias primas "inteligentes". Apenas circularão matérias primas que não possam ser produzidas localmente. As costas marítimas serão objeto de renaturalização, integrada esta num movimento à escala de todo o planeta.

Conclusão

Voltando ao nosso tema "Segurança dos Transportes Marítimos e Portos", à medida que os instrumentos da IMO entraram em vigor e são implementados, a evolução da tecnologia e as lições aprendidas com os acidentes e ameaças, levam à adoção de convenções, códigos, normas e emendas, sendo um processo contínuo sustentado na cooperação internacional.

Na mesma linha do código ISPS e, mais recentemente, das disposições relativas à pandemia COVID 19, a IMO tem vindo, desde 2017, a pôr à disposição da indústria marítima, guias e resoluções, nomeadamente o "*Maritime Cyber Risk Management in Safety Management Systems*"), referentes a Cibersegurança.

O ciberespaço acaba de ser reconhecido pela NATO como um novo domínio operacional, tão crítico para a defesa e segurança, quanto os domínios da terra, do mar, do ar e do espaço.

Como conclusão, recomenda-se que todo o exercício das atividades humanas, cada vez mais digitalizadas, devem estar particularmente livres de ameaças, através de respostas adequadas de CIBERSEGURANÇA

Bibliografia

"Conceito estratégico de defesa nacional - Contributos e debate público (2013). Imprensa Nacional-Casa da Moeda/Instituto de Defesa Nacional.

Correia, A. J. D. C. (2010). "O Mar do Século XXI". Fedrave.

Cunha, Tiago Pitta e (2011). "Portugal e o mar. À redescoberta da geografia". Fundação Francisco Manuel dos Santos.

DGRM (2022) www.dgrm.mm.gov.pt

Dias, M.D.C. (2016). "Manual de Formação para os Cursos de Oficiais de Proteção dos Portos e Instalações Portuárias". Logistel.

Dias, M.D.C. (2021) "Segurança dos Transportes Marítimos e Portos – Curso de Altos Estudos de Transportes". ISG/Logistel.

Graça, Pedro Borges; Martins, Tiago (coords.) (2014). O mar no futuro de Portugal, ciência e visão estratégica". Centro de Estudos Estratégicos do Atlântico.