OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 11, Nº. 2 (Novembro 2020-Abril 2021)

JANUS.NET
e-journal of International Relations

O IMPACTO DA CIBERSEGURANÇA NO QUADRO JURÍDICO REGULATÓRIO DA SEGURANÇA MARÍTIMA

DUARTE LYNCE DE FARIA
duarte.faria@apsinesalgarve.pt
Doutor em Direito (Universidade da Extremadurae e Faculdade de Direito de Lisboa) na área de Direito Marítimo, mestre e licenciado em Direito e licenciado em Ciências Militares-Navais. Enquanto oficial de Marinha frequentou diversos cursos na área das operações navais e desempenho de funções a bordo de navios e em terra no Estado-Maior da Armada (Portugal). É professor convidado da Faculdade de Direito da Universidade Nova de Lisboa, Escola Naval e Escola Superior Náutica Infante D. Henrique, conferencista no Instituto Universitário Militar e investigador do CEDIS, CINAV e CIDIUM. Desempenhou diversos cargos de gestão e direção no Instituto Marítimo-Portuário, na Administração dos Portos de Setúbal e Sesimbra e na Administração dos Portos de Sines e do Algarve. Publicou livros e artigos nas áreas do direito do mar, direito marítimo e segurança marítima.

Resumo

Os conceitos de segurança marítima e de proteção marítima tiveram na sua base diferentes finalidades, objetos e perspetivas. Contudo, atualmente, as mesmas convenções internacionais aplicáveis aos transportes marítimos regulam ambas as vertentes. Na análise da maioria dos incidentes e acidentes no mar é bastante difícil delimitar as matérias de segurança e de proteção e, normalmente, após uma avaria, é inútil fazê-lo já que o planeamento e a resposta aos riscos são normalmente dados de forma integrada. Por outro lado, assiste-se a uma progressiva extensão do conceito de segurança marítima para englobar as matérias da proteção em simultâneo com o aparecimento de um novo tipo de ameaças que estão sempre presentes desde o momento que se ligam os computadores às redes em qualquer lugar do mundo: as ciberameaças! Estando os navios equipados com novas avançadas tecnologias, a proteção contra os ciberataques é mais importante do que nunca. Estes avanços tecnológicos tornaram-se um alvo fácil e de alta prioridade para os criminosos cibernéticos. Com este comportamento, podem prosseguir o seu propósito de atacar os sistemas do navio e, a partir deles, os diferentes sistemas em terra. A digitalização da indústria marítima ocorreu de forma muito rápida. Contudo, tornou-se essencial para os marítimos não só compreenderem e adotarem estas novas tecnologias como, igualmente, assumirem uma postura cautelosa e de alerta de em relação a certos acontecimentos e ocorrências que podem correr perigosamente mal num curto espaço de tempo. Vislumbra-se um novo estádio da prontidão marítima que necessita de um robusto e bem definido "código" que alargue e concretize um "novo" conceito de segurança marítima em sentido lato que reforce as convenções internacionais marítimas e a sua aplicação. As responsabilidades dos "Estados de Bandeira" e dos "Estados do Porto", nos termos do disposto na Convenção das Nações Unidas sobre o Direito do Mar e das convenções internacionais marítimas como se estabelece nos diferentes Memorandos de Entendimento ao nível mundial e nos documentos da OMI e de outras organizações internacionais (como a União Europeia), deverão ser atualizadas e passarem a considerar, também, as matérias da proteção marítima. Para além disso, é essencial apoiar uma cooperação estreita nos campos da segurança marítima e da proteção tendo e vista a elaboração de um novo e robusto "Código Marítimo". Esta será a linha de orientação prosseguida, pretendendo-se, neste momento, "agitar e rolar" esta matéria rumo a um novo estádio regulatório.

Palavras-chave

Segurança marítima, proteção marítima, cibersegurança, Estado de bandeira, Estado do porto

Como citar este artigo

Faria, Duarte Lynce de (2020). "O impacto da cibersegurança no quadro jurídico regulatório da segurança marítima". In Janus.net, *e-journal of international relations*. Vol. 11, Nº 2 Consultado [online] em data da última consulta, DOI: https://doi.org/10.26619/1647-7251.11.2.10

Artigo recebido em Março 21, 2020 e aceite para publicação em Setembro 23, 2020

O IMPACTO DA CIBERSEGURANÇA NO QUADRO JURÍDICO REGULATÓRIO DA SEGURANÇA MARÍTIMA

DUARTE LYNCE DE FARIA

I. Introdução[1]

Quando em julho de 2017, a maior empresa armadora mundial no transporte de contentores (a dinamarquesa "MAERSK") sofreu um ciberataque que paralisou totalmente os seus sistemas de tecnologias de informação (TI) durante várias semanas, o setor marítimo-portuário "acordou" para o enorme impacto desta nova ameaça.

Os danos cifraram-se entre 250 a 300 milhões de dólares[2] e implicaram a reinstalação de 45.000 estações de trabalho e de 4.000 servidores em todo o mundo e o responsável foi identificado como o *ransomware* "NotPetya". De resto, este *malware* já tinha atacado a empresa holandesa *TNT Express,* em junho de 2017, conforme reconhecido pela FedEx (NYSE: FDX)[3].

Na verdade, estando os navios equipados com novos equipamentos dotados das mais modernas tecnologias para a ponte, para a casa das máquinas e para todo o navio em geral, a ameaça dos ciberataques é mais importante do que nunca dado que a maioria dos novos sistemas funcionam de forma automática e estão extremamente dependentes das TI e dos fluxos de dados.

---

1 Este artigo estava próximo da sua conclusão quando eclodiu a pandemia do COVID-19. Para além de obrigar a (re) pensar o mundo global - com os seus pontos fortes e fraquezas, as suas oportunidades e ameaças (numa verdadeira análise SWOT) - é importante mencionar que a "infeciologia" pode, também, ultrapassar, em muito, o domínio da saúde. O exemplo da virulência dos diversos *malwares* ao nível de todos os sistemas ligados à rede pode igualmente, em períodos de crise como o que se atravessa, limitar drasticamente a resposta dos equipamentos de saúde e da proteção civil que exigem a adoção de respostas pré-planeadas associadas a diversos sistemas. Por isso, há que planear, igualmente, a adoção de medidas alternativas, ainda que com uma eficácia menor, mas com maior resiliência á fragilidade que alguns sistemas ainda apresentam, particularmente, nestes períodos de maior perigo para a Humanidade.

2 De custos diretos. Segundo estimativas mais recentes, os custos totais poderão ter chegado a 600 M€. Vale a pena perspetivar as ameaças à cibersegurança em 2020. Num recente artigo de título *"2020 Vision: Check Point's cyber-security predictions for the coming year"*, de 24 de outubro de 2019, in https://www.checkpoint.com, blog.checkpoint.com, https://usercenter.checkpoint.com/usercenter/index.jsp, o cenário das ameaças relativo à cibersegurança foi assim descrito:
1. A new cyber 'cold war'; 2. Fake news 2.0 at the U.S. 2020 elections; 3. Cyber-attacks on utilities and critical infrastructures will continue to grow; 4. High profile US brands, beware of cyber-attacks targeting high-profile American companies; 5. Increased lobbying to weaken privacy regulations.
No que respeita às perspetivas relativas à tecnologia da cibersegurança, são as seguintes as principais ameaças e formas de atuação expectáveis para 2020:
1. Targeted ransomware; 2. Phishing attacks go beyond email; 3. Mobile malware attacks step up; 4. The rise of cyber insurance; 5. More IoT devices, more risks; 6. Data volumes skyrocket with 5G; 7. AI will accelerate security responses.

3 Vide notícia *in* John Gallagher*, Freight Wave,* 29-03-2019.

Estes são apenas dois exemplos de alvos à mercê de ciberataques. Tal como noutros setores económicos, o setor marítimo-portuário tende a confiar e a depender cada vez mais nas tecnologias para ser mais competitivo, mais eficiente na gestão dos seus recursos ou para estar conformes com *standards* ou políticas.

À escala global, assiste-se a uma cada vez maior integração processual dos atores das cadeias logísticas e, por consequência, dos portos, pela utilização de serviços baseados em sistemas de informação.

A *"Janela Única Logística"* (vulgarmente designada por *"JUL"*) - desenvolvida pelos portos portugueses e que estabelece a ligação numa plataforma eletrónica por cada porto entre autoridades, agentes de navegação, transitários e operadores portuários, ferroviários, rodoviários e logísticos, garantindo a fluidez do tráfego de mercadorias e da movimentação de passageiros sem a produção de documentos em papel - é um bom exemplo deste tipo de sistemas e do nível de integração de otimização que proporciona dos portos e das demais plataformas servidas nas cadeias logísticas.

Estes novos avanços tecnológicos tornaram-se um alvo fácil para os criminosos[4]. São vários os desafios de cibersegurança que os portos e as plataformas associadas têm que enfrentar, qualquer que seja o tipo de tecnologia ou sistema de informação usados nas várias atividades portuárias.

As ameaças são várias, vão desde a interceção de comunicações, bloqueio de serviço, *malware,* roubo de identidade, roubo ou manipulação de dados e fuga de informação, entre outras mais relevantes. Os impactos podem também ser de vária ordem e nefastos, como por exemplo, paralisia total das operações, morte ou lesões nas pessoas, rapto, roubo de cargas e perdas financeiras ou de reputação, que urge evitar a todo o custo.

Torna-se crítico impedir a entrada criminosa nos sistemas do navio de pessoas não credenciadas o que implica um controlo efetivo do acesso de um tripulante que utiliza, por exemplo, uma rede livre de *"Wi-Fi"* para chamadas telefónicas e mensagens de correio eletrónico *("e-mails")* junto a terra. A vulnerabilidade é o resultado imediato da interconexão quase permanente que hoje em dia um navio moderno possui, o que leva a que, devido à utilização do mesmo equipamento dos sistemas do navio com acessos não autorizados das redes comuns, os sistemas de bordo possam ser facilmente "infetados" e assim comprometidos (por exemplo, a abertura de um *"phishing email attachments or hyperlinks"* ou de uma notícia dos media previamente "infetada"[5]).

Os impactos deste acesso não credenciado e criminoso podem ser gravíssimos: disrupção da rede, ausência de fluxos de informação entre os sistemas de controlo do navio, acesso não autorizado ao controlo e aos sistemas TI, alterações não autorizadas dos parâmetros dos sistemas, consequências nefastas no ambiente, na segurança marítima a bordo e nos procedimentos críticos e de emergência do navio, levando a que, se nada for feito atempadamente, um problema de *"security"* se possa rapidamente transformar num problema de *"safety"*[6].

[4] Uma vez que a introdução de uma tecnologia nova num determinado processo incrementa a possibilidade de falha humana, altera comportamentos e altera o panorama do risco.

[5] *Infected removable media.*

[6] Alguns autores já citados começam, igualmente, a perspetivar as hipóteses de uma ocorrência de *"safety"* se transformar num incidente de *"security"* no setor marítimo. Trata-se, por exemplo, de acontecimentos

Outro modo de atuação muito em voga consiste na mistificação *("spoofing")* do sinal do GPS[7] através de estações em terra que podem, igualmente, aproveitar os sistemas GPS diferencial em terra (que se servem das plataformas de muitos faróis de navegação) destinados a melhorar a precisão daquele sistema de posicionamento, como foi relatado, em 2018, no Mediterrâneo Oriental, no Mar Negro e no Golfo Pérsico.

Em 2019, foi reportado[8] por diversas entidades e, em particular, pela *U.S. Coast Guard,* uma mistificação "agressiva" do sinal de GPS em 20 zonas costeiras da R.P da China, incluindo os portos de Shangai, Fuzhou (Huilutou), Qingdao, Quanzhou (Shiyucun), Dalian, e Tianjin. A revista *MIT Technology Review* de novembro de 2019, contempla um artigo sobre este fenómeno em que o analista Bjorn Bergman avaliou uma quantidade substancial de informação constante de AIS *("Automatic Identification System")* de navios. Nessa análise, identificou, pelo menos, 20 locais próximos da costa chinesa em que a mistificação ocorreu em moldes idênticos durante o ano de 2019, em que 14 deles eram terminais petrolíferos. Também a organização C4ADS *("Center for Advanced Defense Studies"),* com sede em Washington DC, veio a constatar que a mistificação do sinal se mantinha durante algum tempo naquelas mesmas zonas[9].

Estas ocorrências foram mais persistentes no porto de Dalian, no norte da China junto à Coreia do Norte, podendo suspeitar-se que, dado o momento escolhido - em que vigoravam as sanções norte-americanas que proibiam a compra de petróleo iraniano – e a constatação, por terceiros, da receção daquele produto na China, se terá tratado de uma operação para evitar a localização exata dos navios envolvidos na transferência do produto. Noutros casos, a mistificação do sinal de GPS poderá, igualmente, estar relacionado com importantes visitas oficiais, um recurso, também, utilizado pela Rússia na proteção (i.e., no encobrimento) de visitas de VIP oficiais.

Este tipo de mistificação "em massa" é mais fácil de detetar nas áreas costeiras onde existe uma ampla disponibilidade de dados AIS por via terrestre ou satélite, podendo ter

de mar (encalhe, abalroamento, água aberta, etc.) que impliquem que se concretizem um conjunto de ameaças sobre os sistemas TI – agora, em funcionamento degradado - impedindo-os de contribuírem para a limitação de avarias a bordo.

7 O Sistema GPS *("Global Positioning System")* é um sistema de navegação por satélite que se destina a indicar a posição de um recetor móvel a partir da receção simultânea de três satélites, no mínimo. Estão em funcionamento dois desses sistemas: o GPS norte-americano e o GLONASS russo. No entanto, estão já em lançamento dois outros sistemas: o GALILEO da União Europeia e o COMPASS (ou Beidou-2) chinês. O sistema norte-americano é gerido pelo Governo dos Estados Unidos e começou por ter uso exclusivamente militar (no entanto, manteve-se a precisão do sistema encriptado para uso militar, designadamente, para o auxílio ao guiamento de mísseis de cruzeiro). A sua utilização civil pode rapidamente ser alterada ou mesmo levar ao seu bloqueio em períodos de tensão ou de crise, inclusivamente, dando informações erradas de posicionamento (*"spoofing"* de fonte interna), tal como pode suceder com o aproveitamento das estações GPS diferencial (que estão aptas, em funcionamento normal, a aumentar a precisão da posição geográfica do recetor) para a introdução de erros no posicionamento do veículo.
O *"spoofing"* (ou mistificação) do GPS consiste, assim, na introdução deliberada de sinais nos recetores móveis por estações alheias e que visa indicar uma posição geográfica errada. Esta utilização na mistificação do sinal GPS coincide, normalmente, com o acesso não autorizado aos sistemas TI que procura esconder a verdadeira identidade do utilizador.

8 Vide o artigo de Goward, Dana A., *"Patterns of GPS Spoofing at Chinese Ports",* MAREX, *in Daily Collection of Maritime Press Clippings 2019-356,* pps. 31 e 32.

9 A C4ADS é uma organização privada sem fins lucrativos que tem como objetivo a análise e relato de dados num panorama de conflito ou de questões de *"security"* transnacional.

como causa a mistificação de um sinal satélite e de um outro tipo associado a uma estação ou a um dispositivo em terra[10].

Recuando algumas décadas, a mistificação dos sinais eletrónicos é algo que remonta ao tempo da "Guerra Fria", juntamento com as medidas de empastelamento e contra-empastelamento *("jamming"* e *"anti-jamming"*, respetivamente e medidas ECM e ECCM, *"Electronic Countermeasures"* e *"Electronic Counter Countermeasures",* respetivamente). Assim, a transmissão de eco radar falso para induzir em erro o opositor na sua consola radar era classificada como *"deception jamming"* (i.e., mistificação por empastelamento).[11]

Quando o sistema GPS entrou em produção, foi de fácil perceção que o seu código era vulnerável à mistificação pois tratava-se de um código aberto,[12] reproduzível por qualquer pessoa, através de um simulador (i.e., o mistificador do sinal GPS). Naturalmente que foi esta a razão para o sistema GPS transmitir, igualmente, um sinal militar encriptado (o chamado "P(Y)-code"), para além de permitir uma precisão muito superior na condução de operações militares, particularmente, no guiamento de armas.

Contudo, como o sistema GPS passou a ter uma utilização universal civil, a grande maioria dos recetores não têm capacidade para receber sinais codificados e o desenvolvimento de codificação para efeitos civis não é de fácil harmonização e de decisão pelos responsáveis pela gestão do sistema. Relembre-se, no entanto, que existem atualmente infraestruturas críticas vulneráveis e que deverão merecer uma atenção especial quanto à receção de sinais de GPS, particularmente, no que respeita aos veículos que as frequentam diariamente[13].

Sucede que o crescimento exponencial no mercado de determinados transmissores específicos (apelidados de SDR – *Low Cost Software - Defined Radio*) tornou o *"spoofing"* disponível para qualquer pessoa que pode simular a transmissão de satélite nas mesmíssimas frequências e características de sinal. A época em que as frequências de comunicação com os satélites só estavam disponíveis nos meios militares acabou há muito…. e até já existem instruções na "internet" como proceder para mistificar os sinais radio de controlo dos *"drones"*….

Estas novas ameaças vieram, claramente, exigir uma reflexão sobre como se deverá abordar a *"segurança no mar"* pois, por um lado, as tradicionais divisões entre *"safety"* e *"security"* não se apresentam estanques e são mutuamente influenciáveis e, por outro

[10] Vide o relato da *U.S. Coast Guard* das situações relativas à mistificação do sinal de GPS in https://navcen.uscg.gov/?Do=GPSReportStatus. Vide igualmente o artigo da autoria de "The American Club",*" Mass Global Positioning System (GPS) spoofing at ports in The People's Republic of China" in* "Daily Collection of Maritime Press Clipping 2010-002", pps. 25.

[11] Vide https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/. Sucede, porém, que o que era restrito ao campo militar – elenco das ameaças, planos de contingência, deteção atempada e anulação/limitação dos danos – é hoje partilhada por toda a sociedade e, por isso, há que encarar uma nova realidade, sobretudo, no âmbito das chamadas *"soft kills",*i,e., o uso de equipamentos e sistemas que neutralizem as ameaças sem as destruírem fisicamente através, designadamente, da sua disrupção e que deverão ser utilizados também fora do campo estritamente militar.

[12] Vide Kaplan, Elliott D., e Hegarty, Christopher J., *"Understanding GPS Principles and Applications",* 2nd Edition, ARTECH HOUSE, Boston-London, Norwood, MA, USA, 2006.

[13] Para mitigar esta situação, a União Europeia, no âmbito do sistema GALILEO, irá disponibilizar um conjunto de serviços adicionais, designado *Public Regulated Services* (PRS), que visa fornecer, a entidades estatais e fornecedoras de serviços essenciais e de infraestruturas críticas, um sinal de geoposicionamento mais resistente ao *spoofing* e ao *jamming.*

lado, elas próprias exigem a consagração de uma nova figura a montante que as enquadre e que beneficie, igualmente, do pensamento estratégico (e soberano) de cada Estado no *"uso do mar"*.

Embora o conceito de *"segurança no mar"* não seja novo, o papel do meio marítimo na segurança dos Estados assume, hoje, uma relevância estratégica que se reforçou a partir do início da presente década, numa visão cada vez mais holística, particularmente, ao nível da União Europeia[14]. Na verdade, é *"sobre o mar e nos portos"* que se materializam a maioria das trocas comerciais essenciais ao bem-estar das populações, com especial referência para as importações de hidrocarbonetos (ou fontes energéticas, em geral) e como alternativa aos meios terrestres.

É, assim, desejável que o paradigma concetual seja, progressivamente, alterado e expandido, i.e., por um lado, a tradicional segurança marítima terá de ser robustecida com medidas de proteção contra ataques ilícitos e disruptivos e, por outro, em sede legal, as condutas ditas "desculpáveis" ou "meramente culposas" das tripulações deverão ter, cada vez, menor aplicação tendo em conta a regulamentação existente – em que se incluem os códigos de boas práticas - e as graves consequências que podem daí decorrer. As citadas medidas assumem uma natureza cautelar ou preventiva, mas, igualmente, características reativas, quer na limitação do dano quer na adoção de procedimentos alternativos previstos em planos de contingência.

Esta abordagem terá, necessariamente, consequências em relação à caracterização da reação e ao combate dos sinistros marítimos graves (como, por exemplo, os derrames de hidrocarbonetos nos espaços de jurisdição de um Estado) que se considera com uma forte componente de *"security"* desde a sua origem, i.e., considerando "dolosa" (e não "meramente culposa") a conduta da tripulação que viole as regras da segurança marítima tendo como consequência a criação de um "perigo" ou de um "dano", qualificados juridicamente como "graves".

Parece assim que, ao alargarem-se as condutas "dolosas" do agente (e ao reduzirem-se as "meramente culposas" que, em tempos, exoneravam ou limitavam a responsabilidade dos agentes e das companhias), poderá estar traçado o caminho para que a grande maioria dos grandes sinistros marítimos, como, por exemplo, os derrames de hidrocarbonetos dos navios seja considerada, essencialmente e desde a sua origem, no

[14] Vide Pedra, José Rodrigues, *"A União Europeia e a Segurança no Mar", in* Cajarabille, Victor Lopo e outros, "A Segurança no Mar – uma visão holística", Mare Liberum, Aveiro, 2012, pps. 143 a 162. O autor faz uma breve referência ao conceito de "Segurança no Mar" baseado na obra de Grove, Eric, *"Maritime Strategy and European Security"*, Londres, Brassey's, 1990, que, com reminiscências da estratégia de dissuasão nuclear do período da Guerra-Fria, alude à importância do mar para a segurança europeia. No entanto, é com a apresentação da Estratégia Marítima para o Atlântico em 2011, juntamente com o *Livro Verde para a Política Marítima Integrada Europeia* e com a *Política Marítima Integrada Europeia* propriamente dita que renasce esta perspetiva estratégica para o uso do mar. Mais do que o valor de comunicação e transporte, o mar é fonte de recursos essenciais e um meio indispensável para o controlo das atividades em terra com a própria projeção de poder e defesa antecipada e "em profundidade" que são essenciais para fazerem valer os interesses europeus. Vide Pedra, José Rodrigues, *ob. cit,* a pps. 149 a 155.
Por outro lado, esta relevância estratégica também emergiu como resultado do impacto que a prospeção e exploração dos recursos marinhos estão a assumir progressivamente nas economias dos Estados, confrontados com a crescente escassez e, igualmente, com a limitação do acesso aos recursos terrestres. Esta situação veio a colocar na agenda internacional as disputas dos países nas delimitações dos fundos marinhos contíguos e as candidaturas às extensões das plataformas continentais. Entre todos, vide Duarte, António Rebelo, *"Políticas e Estratégias Marítimas da Europa e de Portugal",* Cadernos Navais, n.º 48, abril-junho de 2018, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt.

âmbito da *"security"* e, consequentemente, como um papel acrescido de regulação no âmbito da soberania dos próprios Estados[15].

II. A influência da segurança nacional e de uma estratégia setorial no conceito de "Segurança no Mar"

A palavra *"segurança"* apresenta inúmeros significados, embora com um sentido comum, quer no âmbito da atividade em si mesma quer no que respeita ao resultado: *o de proteção (ou garantia) de um certo direito ou bem face aos riscos ou obstáculos que sobre eles impendem.* Tal significa que, não havendo obstáculos ao seu exercício, é desnecessária a adoção de meios suplementares garantísticos[16].

Diversas classificações de segurança podem, igualmente, emergir em função de diferentes critérios, designadamente, o sujeito protegido (ou entidades destinatárias), os bens ou matérias a proteger, o âmbito territorial de intervenção, as estruturas que a asseguram e a intensidade da perturbação realizada (i.e., o efeito das ameaças, riscos e perigos sobre os citados bens ou direitos)[17].

Para além destes critérios, a figura da *"segurança"* assume, igualmente, diversas outras formas em função do seu objeto específico[18] entre as quais se contam a segurança energética, a segurança no mar, a segurança marítima, a segurança aérea e a própria segurança nos transportes. Neste pequeno elenco, trata-se de delimitar a segurança em função, igualmente, da atividade realizada que, em alguns casos, envolve segmentos de

---

15 Cabe, neste ponto, invocar uma matéria que iniciou, igualmente, a sua doutrina no Direito Penal e que, posteriormente, saltou para o domínio do Direito Internacional. Tratava-se, então, no âmbito criminal, de legitimar, por exemplo, a ação de um deficiente grave motor (i.e., paraplégico) quando conhecia, com quase absoluta certeza, que alguém o viria assassinar no local onde se encontrava sozinho e sem acesso a quaisquer contactos. E, perguntava-se, se seria legítimo a putativa vítima neutralizar o agente, alvejando-o antecipadamente antes de entrar no local em que se encontrava (por exemplo, por uma janela).
Este exemplo veio a consubstanciar a diferença, em Direito Internacional, entre o ataque *"preventivo"* e o ataque *"preemptivo"*, legitimando-se, neste último caso, a intervenção antecipada face à intenção (e prova) de um ataque iminente. Assim, o ataque *"preventivo"* foi perdendo legitimidade jurídica, dada a sua arbitrariedade e colocado ao serviço de um *"direito da força"* de escrutínio impossível, visando, apenas, prosseguir uma estratégia para evitar alterações no equilíbrio de poder que pudessem favorecer o adversário. Relembre-se que, de acordo com o artigo 51.º da Carta das Nações Unidas, o *"direito de legítima defesa"* só é reconhecido no caso de ataque armado e, com aquela extensão, procurou-se abranger a intenção de "ataque armado".
Ora, no caso vertente, o "ataque iminente" (ou dito de outra forma, a "ameaça real") existe a partir do momento em que os sistemas TI do navio se ligam ao exterior e, dessa forma, caberá ao Estado de bandeira atualizar aos seus regulamentos e procedimentos para que tenha em conta a *"preemptividade"* do exercício do navio e da companhia. Vide, *inter alia,* Santos, Sofia, *"Defesa preemptiva"* e *"Defesa preventiva"* in Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), "Enciclopédia de Direito e Segurança", Almedina, Coimbra, 2015, pps. 102 a 105.

16 Vide Gouveia, Jorge Bacelar, *"Direito da Segurança Cidadania, Soberania e Cosmopolitismo",* Almedina, Coimbra, 2018, a pps. 89ss. Com esta obra, iniciou-se a conceptualização de um novo ramo do Direito: o Direito da Segurança, emergindo a fundamentação dogmática deste novo ramo e a análise das entidades estatais e internacionais de segurança. Define-se o Direito da Segurança como o *"sistema de normas e princípios jurídicos que definem a organização e o funcionamento das estruturas de segurança, estabelecendo os seus poderes e limites, com vista à proteção dos direitos e bens jurídicos fundamentais dos cidadãos e das comunidades políticas"* (a pps. 119). Esta obra é essencial para o enquadramento do atual tema, tanto mais que procuraremos, no futuro, *"largar as amarras",* sejam elas *"lançantes, regeiras, contra-regeiras ou traveses"* do "novo" *Direito da Segurança Marítima* já que nos parece, igualmente, o momento de lhe "conceder" autonomia, em confronto com o *Direito do Mar* e com o *Direito Marítimo.*

17 *Ibidem,* pps. 90 a 91.

18 O *Direito Marítimo* trata de um objeto específico (a atividade do transporte marítimo) no âmbito do *Direito Comercial*, de âmbito mais geral e que, nem por isso, desmereceu a sua classificação como ramo do Direito. Vide, igualmente, *ibidem* pps.93 a 96.

transporte diversos (terrestre, fluvial, marítimo e aéreo) e, noutros, em determinados equipamentos essenciais e nas redes que os interligam (segurança energética e a cibersegurança, por exemplo).

A atividade de segurança que se projeta no âmbito territorial de atuação dos meios num determinado Estado deve obedecer a uma dimensão espacial e material a montante que se designa por *"segurança nacional"* (a par da segurança, local, regional, internacional e global).

Constata-se assim que, na atualidade, a *"segurança nacional" "deixou de ser apenas uma segurança contra atos criminosos para igualmente acolher a prevenção e solução dos riscos naturais, no âmbito da proteção civil, avultando a segurança na sua aceção de "safety""*, sem, contudo, se descurar a sua *"dimensão supraestadual, em consonância com a magnitude dos riscos de ataques terroristas que deixaram de ser nacionais, localizados, públicos e com armas convencionais, assim se revigorando a segurança na sua aceção de "security"".*[19] No âmbito expresso, a *"segurança nacional"* respeita a uma visão associada à defesa nacional e que, naturalmente, interage com opções políticas e estratégicas a montante da própria *"segurança no mar".*

O conceito de *"segurança nacional"*[20] dá corpo a uma estratégia do próprio Estado, tradicionalmente centrada nas ameaças militares à sua fronteira ou a outras ameaças

[19] *Ibidem,* pps. 96.

[20] No quadro legislativo nacional, não foi definido, formalmente, o conceito de *"Segurança Nacional".* Contudo e em sede doutrinal, vide Gouveia, Jorge Bacelar, *"Direito da Segurança Cidadania, Soberania e Cosmopolitismo",* Almedina, Coimbra, 2018, a pps. 92ss e Couto, Abel Cabral, *Elementos de Estratégia, Volume I,* IAEM, Lisboa, 1988, pps. 172ss. Vide, igualmente, Garcia, Francisco Proença, *"Defesa Nacional"* in Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), "Enciclopédia de Direito e Segurança", Almedina, Coimbra, 2015, pps. 99 a 101. Este autor discorre sobre a diferenciação entre os conceitos de Defesa Nacional e de Segurança Nacional, propondo que se adote este último *"resultante de um conjunto de políticas do Estado devidamente articuladas, na vertente militar mas também em outras políticas sectoriais como a económica, cultural, educativa, que englobe ações coordenadas de segurança interna e externa, cuja fronteira esta atualmente desvanecida"*. Quanto ao desvanecimento entre a segurança interna e externa, vide Santos, Ana Miguel dos, *"Uma segurança interna cada vez mais europeia? Uma segurança externa cada vez mais nacional?"* in RDeS - Revista de Direito e Segurança, Ano VI, jul-dez 2018, pps. 27 a 51, Guedes, Armando Marques, *"Segurança externa"* e *"Segurança interna", in* Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), "Enciclopédia de Direito e Segurança", Almedina, Coimbra, 2015, pps. 411 a 418 e 425 a 431 e Lourenço, Nelson, *"Segurança interna", ibidem,* pps. 431 a 433. Relativamente à conceção integrada na Constituição, vide Gouveia, Jorge Bacelar, *"Direito Constitucional da Segurança", ibidem,* pps. 131 a 136. Enveredámos nessa coletânea, por iniciar a concetualização da *"segurança no mar"* que deverá abranger as *"matérias da segurança marítima e da proteção marítima e, em termos espaciais, nos navios e nos portos"* (pps. 435) no artigo *"Segurança no mar", ibidem,* pps. 433 a 439.
No entanto, o *"Conceito Estratégico de Defesa Nacional"* (CEDN), aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 21 de março, ainda que se baseie no conceito de "segurança nacional", integra elementos muito importantes sobre a relevância do mar neste contexto, considerando-se, designadamente, que *"como ativo estratégico, o mar deve estar integrado numa perspetiva ampla de segurança e defesa nacional".*
Uma outra componente que poderá influenciar a "segurança no mar" respeita à definição de estratégias setoriais. A nível nacional, vigora a *"Estratégia Nacional para o Mar para o período 2013-2020"* (ENM), aprovado pela Resolução de Conselho de Ministros n.º 12/2014, de 23 de janeiro e que coloca a tónica na utilização e preservação do mar como ativo nacional o que reforça a relevância estratégica da *"segurança no mar".* Vide supra nota n.º 13
Está hoje em discussão pública a nova Estratégia Nacional para o Mar – ENM 2021-2030 (in https://www.dgpm.mm.gov.pt/enm) – da qual se cita o seguinte enquadramento, a pps. 3 e 4:
"Portugal passou a acompanhar a relevância económica do Mar na sua economia nacional através de uma Conta Satélite do Mar, que resultou de um protocolo entre o Instituto Nacional de Estatística (INE) e a Direção-Geral de Política do Mar (DGPM) celebrado em 2013. Segundo estimativas da Comissão Europeia, em 2018, o valor acrescentado bruto (VAB) em economia azul representou 3,2% do VAB da economia nacional. O emprego gerado representou 5,5% do emprego nacional. Estes valores estão entre os mais altos nos Estados-Membros da UE.

não convencionais, como as alterações climáticas e as crises económicas e financeiras mundiais, incluindo as de natureza híbrida as quais, no domínio marítimo, podem ter implicações de natureza bastante diversa[21]. Para que haja uma delimitação mínima da *"segurança nacional",* exige-se uma relação com a estratégia e, mais concretamente, que contribua (ou seja essencial) para a realização de objetivos político-estratégicos[22].

Ora, a *"segurança no mar"* - como definida anteriormente - só mediata e parcialmente comunga da *"segurança nacional"* pois continua a ter uma vertente transnacional, qualquer que seja o Estado em causa. No entanto, serão, essencialmente, as exigências de *"security"* que poderão modelar a *"segurança no mar"* pela via da *"segurança nacional"* ao invés das matrizes de *"safety"* que tendem a ser perenes e técnicas, visando a melhoria das condições de navegabilidade do meio utilizado, sem prejuízo de se considerarem abrangidos os fenómenos naturais[23].

Na verdade e na grande maioria dos casos, só a *"security"* interessa ao quadro político-estratégico, envolvendo outros Estados ou atores do sistema internacional, o que significa que se quadra no âmbito da soberania dos Estados e dos correspondentes mecanismos unilaterais de *"enforcement"*.

Ao invés, na *"safety",* as regras de segurança marítima advêm das convenções internacionais e a coercibilidade resulta do que a lei internacional (ou os acordos internacionais como é o caso dos *MoU* no âmbito do "Controlo pelos Estados do Porto" ou *"Port State Control"*) vier a determinar[24].

A sustentabilidade da economia azul depende da conservação do ambiente marinho, e dos serviços dos seus ecossistemas, bem como da salvaguarda do património cultural marítimo. O Plano de Situação de Ordenamento do Espaço Marítimo Nacional, as Linhas de Orientação Estratégica e Recomendações para a Implementação de uma Rede Nacional de Áreas Marinhas Protegidas aprovados em 2019, assim como a avaliação do Bom Estado Ambiental das Águas Marinhas reportada recentemente em cumprimento da Diretiva-Quadro "Estratégia Marinha", representaram importantes marcos para assegurar o nosso compromisso na defesa dos ecossistemas marinhos e do património cultural náutico e subaquático.
Portugal deve assumir definitivamente as vantagens competitivas da sua posição geoestratégica, das suas competências tecnológicas e da sua tradição marítima, minimizando barreiras administrativas ou fiscais que se revelem prejudiciais à mesma, e exercendo a autoridade do Estado no mar. O padrão que estabelecermos na gestão sustentável do nosso mar será uma contribuição decisiva para a sustentabilidade do planeta, num futuro que desejamos mais azul para as gerações vindouras".

21 Vide The European Centre of Excellence for Countering Hybrid Threats, *"Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans"*, November 2019.

22 Vide Fernandes, António Horta., *"Conceito Estratégico de Defesa Nacional (CEDN) ou Conceito Estratégico de Segurança Nacional (CESN)? Um falso dilema",* Observatório Político, wp #43, abril 2014, in http://www.observatoriopolitico.pt/wp-content/uploads/2014/04/WP_43_AHF.pdfla, pps 4ss, e Branco, Carlos, *"Porquê uma Estratégia de Segurança Nacional?",* Opinião, Jornal Expresso, 2018-05-11. Por todos, Cajarabille, Victor Lopo, *"Enquadramento Estratégico",* in Cajarabille, Victor Lopo e outros, *"A Segurança no Mar – uma visão holística",* Mare Liberum, Aveiro, 2012, pps. 21 a 35. Vide Escorrega, Luis Falcão, *"A Segurança e os "Novos" Riscos e Ameaças: Perspetivas Várias"*, Revista Militar, n.º 2491, agosto/setembro 2009 (https://www.revistamilitar.pt/). Este autor ser-nos-á de grande utilidade pois vem admitir que o moderno *conceito* de "ameaças" engloba os "riscos" e as "ameaças" tradicionais (a pps. 14). Vide igualmente Duarte, António Rebelo, "*Políticas e Estratégias Marítimas da Europa e de Portugal"*, Cadernos Navais, n.º 48, abril-junho de 2018, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt. Este autor reforça o desenvolvimento da "segurança marítima" nos termos da *Estratégia de Segurança Marítima*, aprovada pelo Conselho Europeu em 24 de junho de 2014, e o seu enquadramento no âmbito da *Política Comum de Segurança e Defesa* (PESD), com uma descrição dos riscos e das ameaças à segurança marítima europeia, reforçando a importância da *"security"* naquela Estratégia.

23 Vide nota n. º 18 *supra* e o texto de remissão.

24 Em Espanha o Comité de Segurança Marítima responde perante o Conselho de Segurança Nacional. Por sua vez, no Reino Unido, o *"Ministerial Working Group on Maritime Security"* está a jusante do *"National Security Council"*. Vide *"Estrategia de Seguridad Marítima Nacional",* Gobierno de España, 2013 e *"The UK National Strategy for Maritime Security",* MOD UK, May 2014.

Uma outra componente que poderá influenciar a *"segurança no mar"* respeita à definição de estratégias setoriais. É hoje essencial a articulação das questões do "mar" com os "portos", com os "transportes" e com a "logística", seja numa visão mais vertical e/ou transversal dos assuntos do mar[25].

Por outro lado, as ameaças e os riscos, existem em documentos militares ou civis – porque decorrem das análises de componentes civis (designadamente, de índole económica, cultural, científica, tecnológica ou ambiental) ou estritamente militares – mas têm repercussões ao nível da política estratégica de qualquer país marítimo e, assim, em última instância, na segurança nacional.

Delimitados que estão os conceitos de *"segurança" ("safety")* e de *"proteção" ("security")*, importa entender que a *"segurança no mar"* terá sempre uma dependência da estratégia (global) do Estado[26], embora, ainda assim, a sua perspetiva holística se baseie no aprofundamento das condições tecnológicas das atividades no "mar" - em particular, no âmbito dos transportes marítimos e dos portos - e do grau de exigência no cumprimento das boas práticas e da consequente responsabilização das tripulações, das companhias e dos operadores portuários[27].

---

[25] As opções políticas e estratégicas em sede de "Defesa e Segurança" devem ser seguidas em permanência quando se abordam os assuntos do mar tanto mais que a proteção, fiscalização, prospeção e exploração sustentável dos seus recursos exigem meios aptos para o efeito, inventariando-os, em permanência e evitando a sua predação.

[26] A introdução do vocábulo "segurança" nos documentos conceptuais emerge quando se desenvolve a "estratégia" que se estriba num determinado "conceito". A nível nacional, dão-se como referências o *"Conceito Estratégico de Defesa Nacional"* e a *"Estratégia de Segurança e Defesa Nacional".*

[27] Em termos tradicionais, a *"segurança"* relaciona-se com a minimização dos "riscos" (da navegação) ao passo que a *"proteção"* visa combater a concretização, de forma intencional, das "ameaças" – embora não de forma completamente estanque – a começar por um simples derrame de hidrocarbonetos. Dito de outra forma, a *"proteção"* tem como núcleo essencial a ameaça e a intenção de provocar dano e, por isso mesmo, há que fazer constar a sua origem humana *("threat actors")*. Ao invés, a "segurança" centra-se no "risco" das atividades marítimas, ou seja, em eventos naturais ou não intencionais que têm consequências graves e com uma certa probabilidade de se materializarem (i.e., tradicionalmente, as avarias inopinadas, os elementos da natureza, etc.).
O nosso desafio está, igualmente, em provar que, nos tempos atuais, o "risco" tende a ser reduzido a situações ditas "naturais" já que uma conduta da tripulação de um navio que foi exposto a um "perigo" ou a um "dano" grave pode, na maior parte das vezes, configurar uma atuação "dolosa" (e não "meramente culposa") por violação – ainda que não de forma intencional – das regras de segurança marítima. A ser assim, trata-se de um *"upgrade"* destas condutas – consideradas, até hoje, meramente culposas - para o campo das "ameaças" e, portanto, da *"security"*.
Também neste campo, a prevenção e o combate (ou minimização) dos danos resultantes de ocorrências de "proteção" e de "segurança", embora com origens conceptuais distintas, tendem a sobrepor-se e a articularem-se, cada vez mais, nas ações, o que é evidente quando se caminha para conexões globais como é o caso das que decorrem do facto de vivermos num mundo digitalmente interconectado, quer física quer virtualmente, e assim retendo em permanência a respetiva cibersegurança. Na página da internet da norte-americana CISA *("The Cybersecurity and Infrastructure Security Agency"),* criada em 2018, constata-se que se parte do conceito de *"safety"* com a premência da *"security"* de uma forma muito simples, afirmando o seguinte:
"*Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment. Every time we connect to the Internet-at home, at school, at work, or on our mobile devices-we make decisions that affect our cybersecurity. Emerging cyber threats require engagement from the entire American community to create a safer cyber environment-from government and law enforcement to the private sector and, most importantly, members of the public".*
Importa, contudo, reiterar que foi, de facto, a *ameaça ciber* e, em consequência, a cibersegurança que veio alavancar a tese do relacionamento concêntrico entre a *"safety"* e a *"security"* e que uma recente apresentação sobre o reposicionamento das ciberameaças nos sistemas OT – *Operational Technologies* - (em Lisboa, na PwC, a 5 de fevereiro de 2020). O seu autor (Rafael Maman), um perito israelita na área da cibersegurança e abordando a matéria a título pessoal, referiu, a determinado momento, o seguinte:
"Corresponding to a shift in the cyber risk equation: traditional IT risks – data privacy, IP theft, etc. – are augmented by higher-order risks – to unman life, disruption of critical operations, environmental disasters,

Ora, a *"segurança no mar",* ao enquadrar aqueles dois conceitos, desdobra-se em dois tipos de perigos: as "ameaças" e os "riscos" que envolvem a utilização do mar, seja nos navios ou nos portos.

As *"ameaças"* são, essencialmente, de duas naturezas: os ilícitos genéricos no mar e os ilícitos específicos que tenham influência na liberdade de navegação. Na primeira, constam, designadamente, o tráfico de estupefacientes e de substâncias psicotrópicas, o contrabando em geral e o de armamento, a proliferação de armas de destruição maciça, a exploração ilegal de recursos marinhos, da plataforma ou do património cultural subaquático, os atentados ambientais (em que se inclui a poluição) e a imigração ilegal. Na segunda, contam-se, entre outros, o terrorismo, a pirataria, os ataques cibernéticos aos sistemas de informação e outras atividades de cariz criminoso classificadas como tal pelo Direito Internacional.

Por sua vez, os "riscos"[28] apresentam uma natureza tendencialmente acidental ou natural e têm a sua identificação principal (que não exclusiva) com a *"segurança do transporte*

etc.(it should have as a consequence that) governments and industrial enterprise recognise the importance of OT Security for Critical Infrastructure protection and the risks involved, and initiate proactive action".
Com esta alteração qualitativa da equação dos riscos cibernéticos, importa, cada vez mais, identificar as diferenças fundamentais entre a cibersegurança no IT e no OT, em todas as suas dimensões - incluindo a jurídica - precisamente por ser no domínio do OT que as interdependências entre a *"safety"* e a *"security"* são mais relevantes, atendendo a que o OT liga o mundo cibernético ao físico.
Como consequência direta, a presença permanente do risco dos ciberataques para as infraestruturas críticas e para os serviços essenciais (em que se incluem os transportes marítimos e os portos) implica que a *"security"* deva ser sempre considerada. No nosso caso, a criação de condições para uma navegação safa, nos tempos atuais, deve sempre levar em linha de conta o ciberespaço e, portanto, a figura representativa que se propõe, consistindo em dois círculos concêntricos em que o central corresponde à *"safety".*
Nesta ótica, Rafael Maman vai ainda mais longe ao considerar nas micro tendências das ameaças cibernéticas a seguinte evolução: *"From "military-grade cyberweapons" to "industrial-grade ransomware".*
O que antigamente eram consideradas armas de guerra cibernéticas utilizadas pelas forças armadas podem hoje ser usadas na disrupção de indústrias críticas e de serviços essenciais por qualquer ator suficientemente apto tecnologicamente para o executar. *In* Maman, Rafael, "*The Reshaping Cyber Threat Landscape of Operational Technology"*, apresentação, in "Conferencia organizada pela PwC*, "Cibersegurança – Os desafios da Tecnologia Operacional (OT)",* Lisboa, 5 de fevereiro de 2020.
Por outro lado, desde o início do século, a grande maioria dos incidentes de dimensões apreciáveis em indústrias sensíveis têm como causas associadas ataques deliberados (cibernéticos e outros), danos colaterais de ataques ou o funcionamento deficiente dos sistemas, não sendo possível, na sua maioria, isolar as fontes na tradicional bipartição *"safety/security"* ou, sendo possível, perderá todo o interesse dada a necessidade de resposta integrada. Vide *https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.*
Por isso, não só se pretende provar que as condutas da tripulação violadoras das regras da segurança marítima e que causem um "perigo" ou um "dano" qualificados juridicamente "graves" caem no âmbito do "dolo" como, igualmente, a representação pelos dois círculos concêntricos.
A divisão tradicional entre a neutralização dos agentes das ameaças *("security")* e a ajuda a conter as consequências negativas *("safety"),* concorrem, em nossa opinião, para um plano comum que farão parte das regras de segurança marítima a cumprir a bordo, não se destrinçando, no limite, a sua diferente origem nem as medidas de limitação de avarias.
Também a *Estratégia Europeia de Segurança* e o *Relatório sobre a Execução da Estratégia Europeia de Segurança* destacam um conjunto de *"ameaças"* com implicações no uso do mar em que se incluem as atividades ilegais, o crime organizado, a pirataria, o terrorismo, a proliferação de armas de destruição em massa, os conflitos regionais, os Estados Fragilizados, a poluição marítima, a segurança energética e as alterações climáticas. O que significa que este enfoque é essencialmente sobre a *"security"*. Vide *http://www.consilium.europa.eu/uedocs* (pesquisa pelos respetivos títulos). Ao invés, a EMSA *("European Maritime Safety Agency")* desempenha atividades no âmbito da *"safety"* e não será por essa razão que não deixa de ser invocada numa perspetiva conjunta e alargada de "segurança" *("safety"* + *"security").*

[28] O "risco" é o produto da probabilidade de ocorrência de uma ameaça (ou dano) pela gravidade (ou intensidade) dos seus efeitos. Tradicionalmente, associado à *"safety",* tende-se hoje a expurgar dele as condutas da tripulação violadoras das regras da segurança marítima com consequências graves. A origem destes conceitos radica no Direito Internacional e, mais especificamente, na teoria da resolução de conflitos.

marítimo" e com a *"segurança portuária"*. Os danos potenciais associados (ou a condição da criação de um "perigo") podem incidir sobre os navios e embarcações, sobre as pessoas embarcadas, sobre as plataformas ou infraestruturas no mar (e, igualmente, sobre aeronaves e submarinos) e sobre o ambiente marinho, designadamente, através dos acidentes de poluição.

Esta tendencial identificação da *"segurança"* (em sentido estrito) com os "riscos" e a "proteção" com as "ameaças" tem a grande vantagem de poder colher os ensinamentos de áreas que, até há bem pouco tempo, evoluíram autonomamente e que os atentados de 11 de setembro de 2001 vieram a exigir a sua estreita articulação, tendo em conta a necessidade de adotar medidas aplicáveis aos navios e às instalações portuárias no âmbito da *"proteção"* e considerando que a identificação de ameaças à segurança e à tomada de medidas para a prevenção de acidentes passaram a desenrolar-se, cumulativa e coordenadamente, de acordo com o Código ISPS[29].

Uma outra circunstância, que sucede com o aprofundamento e desenvolvimento das regras da segurança marítima - traduzidas, na sua essência, pelas convenções atinentes da IMO - respeita ao progressivo exaurimento de cláusulas de exoneração e de limitação da responsabilidade em contratos de transporte marítimo (e de convenções) que se traduzam em condutas consideradas, apenas e a esse título, como *"meramente culposas"*. Como exemplo paradigmático, refere-se a célebre *"falta náutica"* constante das convenções internacionais sobre o transporte marítimo que exonera o transportador por avarias na carga (pelo menos, desde os anos 20 do século passado).

Deste exemplo poder-se-á retirar que as progressivas exigências tecnológicas e de boa conduta para uma navegação safa (i.e., as normas sobre a *"segurança marítima"*) tornam as circunstâncias consideradas *ab initio* como *"meramente culposas",* bastante mais restritas no âmbito da responsabilidade civil (contratual e aquiliana), incluindo, as que estão presentes nos derrames de hidrocarbonetos[30].

Desta forma, também o cumprimento dos padrões de segurança marítima, ao mesmo tempo que minimizam os "riscos" (e os erros), dão maior robustez ao combate às "ameaças" e, em simultâneo, limitam a aplicação das cláusulas de exoneração e de limitação da responsabilidade que estão presentes, por exemplo e entre outros instrumentos, nas convenções sobre a poluição resultante de derrames de hidrocarbonetos e nas respeitantes ao transporte marítimo de mercadorias[31].

De forma sucinta e nesse quadro, "ameaça" corresponde a uma circunstância ou evento que faz perigar a prossecução dos objetivos políticos e estratégicos e o "risco" como o grau de exposição à ameaça em causa.

29 A sigla ISPS designa o *"International Ships and Port Facilities Security Code"* que constitui o capítulo XI-2 da Convenção SOLAS desde 2002.

30 Matéria esta que se definiu como no âmbito da "proteção", mesmo na sua origem, já que, na apreciação feita, na maioria dos casos com consequências graves, resulta de uma conduta "dolosa" da tripulação.

31 A *"falta náutica"* como cláusula de exoneração vem prevista na alínea a) do parágrafo 2.º, do artigo 4.º da Convenção Internacional para a Unificação de Certas Regras em Matéria de Conhecimentos, assinada em Bruxelas a 25 de agosto de 1924 – conhecida como "Regras de Haia". Refere-se, especificamente que a cláusula só se aplica aos *"Atos, negligência ou falta do capitão, mestre, piloto ou empregados do transportador na navegação ou na administração do navio".* Assim, se a *"falta náutica"* consistir na violação das regras essenciais da segurança marítima (em sentido lato) dificilmente poderão justificar a exoneração do transportador/armador pela avaria na carga.
Lembre-se que, em sede aquiliana e de acordo com as convenções vigentes – particularmente, nos termos da Convenção sobre a Responsabilidade Civil por Prejuízos devidos à Poluição por Hidrocarbonetos, de 1969 (*Civil Liability Convention* 1969 ou CLC/69) e da sua alteração de 1992 (CLC/92) - o proprietário do navio é responsável por um erro de navegação que conduziu a um encalhe do navio e ao posterior derrame de

Entende-se, assim, que a noção ampla de *"segurança no mar"* (ou de *"segurança marítima"* em sentido amplo que é, de resto, a expressão mais utilizada) deve abranger as valências materiais da segurança (marítima) (em sentido estrito) e da proteção (marítima) e, em termos do seu arco espacial, com incidência nos navios e nos portos[32]. Particularmente, quanto ao objeto, a *"segurança no mar"* – com ambas as valências - abrange o transporte marítimo - em que o enfoque se traduz no «navio» e na sua movimentação - e os portos - que respeita, essencialmente, à segurança nas áreas sob jurisdição portuária, abrangendo os diversos terminais, a área terrestre adjacente e a área molhada contígua.

A *"segurança do transporte marítimo"* (ou "segurança marítima em sentido estrito"), envolve o conjunto de medidas destinadas a garantir uma navegação segura por parte dos navios, i.e., quer na envolvência das condições de bordo (qualificação dos tripulantes, estiva e movimentação da carga e, em geral, as condições de navegabilidade estruturais e de equipamentos do navio), quer no sistema de ajudas à navegação e de ordenamento das aproximações a um porto que permitem, aos navios, uma navegação segura.

No outro polo, a *"proteção do transporte marítimo"* e a *"proteção portuária"* consoante o objeto - envolvem todas as medidas de segurança física[33] e outras aplicáveis no espaço sob jurisdição portuária, aos tripulantes e passageiros dos navios e aos demais funcionários que operam nos portos, bem como aos próprios navios destinadas a garantir a atividade normal segundo as regras técnicas aplicáveis[34].

---

hidrocarbonetos (caso do M/V *"Exxon Valdez"* com o derrame de cerca de 38.000 toneladas de crude nas costas do Alasca). Na verdade, o artigo V/2 da CLC/92 vem estabelecer que o proprietário pode perder a faculdade de limitar a sua responsabilidade desde que o prejuízo devido à poluição resulte de ação ou de omissão que lhe seja imputada *"cometida com a intenção de causar tal prejuízo ou com imprudência e o conhecimento de que tal prejuízo se poderia vir a verificar"*. Esta fórmula é muito próxima da utilizada na alínea e) do parágrafo 5.º do artigo IV Protocolo de Visby de 1968 ("Regras de Visby") à Convenção de Bruxelas de 1924 referida que afasta a limitação da responsabilidade se a ação ou omissão se desenrolou com a intenção de provocar um dano ou temerariamente e com conhecimento de que provavelmente dela resultaria um dano. Em sede civilista, trata-se de uma forma de culpa grave e que corresponde ao dolo. Vide Coelho, Carlos, *"Poluição Marítima por Hidrocarbonetos e Responsabilidade Civil"*, Almedina, Coimbra, 2007, a pps. 86ss.
Em conclusão: entende-se que a culpa grave *("negligência grosseira"* para alguns autores ou *"wilful misconduct"* em língua inglesa) na violação das regras da segurança marítima deverá afastar o benefício da cláusula de exoneração *"falta náutica"* por parte do transportador/armador.
No nosso trabalho *"O Contrato de Volume e o Transporte Marítimo de Mercadorias – Dos granéis aos contentores, do "tramping" às linhas regulares",* Coleção Teses, Almedina, Coimbra, 2018, a pps. 73ss, nota n.º 80, já vínhamos defendendo esta posição embora, nessa altura, sem a generalização que agora se defende.

[32] Em sede de "cadeia de valor", não se descarta a hipótese de se abrangerem também os agentes e operadores com responsabilidade na área logística pois o seu desempenho está diretamente relacionado com os sistemas de informação e de comunicação como é o caso dos portos portugueses que utilizam a moderna *"Janela Única Portuária"* ou a sua sucedânea, a nova *"Janela Única Logística"* que passou a abranger os portos secos e os operadores terrestres bem como os transitários.

[33] Nesta ótica, perspetiva-se, igualmente, a necessidade de se credenciar o pessoal que interaja com os sistemas TI em função do tipo de navio, dos portos de origem, do tipo de mercadoria ou, dito de outra forma, de acordo com o padrão de risco assumido para o navio de forma idêntica ao que hoje é feito para o cumprimentos das condições de segurança marítima em que se avaliam, por exemplo, as condições do reabastecimento de bancas (combustível para navios) por barcaça nos portos.

[34] A Conferência Diplomática da Organização Marítima Internacional (OMI), reunida em 12 de dezembro de 2002, alterou a Convenção SOLAS *("Safety of Life at Sea"),* veio a adotar o Código Internacional para a Proteção dos Navios e Instalações Portuárias (designado por *"Código ISPS"*), que entrou em vigor em 1 de julho de 2004. Este novo Código é bem uma expressão da valência da "proteção" dos transportes marítimos, dos terminais e dos portos. Esclarece-se que a Convenção SOLAS integra diversos códigos específicos visando a padronização da gestão da segurança a bordo (o caso do *ISM Code – Código Internacional de*

III. A perspetiva moderna da defesa contra os ciberataques no setor marítimo

Perspetiva-se, assim, que o objeto tendente à autonomização do *"Direito da Segurança Marítima"*[35] deverá assumir uma natureza lata e abranger os dois vetores da *"safety"* e da *"security"*, por diversas ordens de razões: em primeiro lugar, a *"safety"* é a mais antiga[36], a mais estável e a que é tratada na maioria das convenções da IMO; depois, porque a interpenetração entre os dois conceitos é cada vez maior; em terceiro lugar, porque há traduções que já não voltam atrás (o caso da "cibersegurança"), nem um famigerado e "artificial" "Direito da Proteção Marítima" teria condições para se autonomizar; e, finalmente, porque, nos tempos atuais, os dois vetores tendem a apresentar-se como dois círculos concêntricos – a *"safety"* (mais interior) e a *"security"*, que a envolve. Na verdade, esta última pode robustecer (ou enfraquecer) aquela no centro[37], numa dialética e interação constantes.

Esta estrutura proposta vem ao encontro de uma constatação cada vez mais presente: os incidentes de *"security"* poderem ter consequências graves em sede de *"safety"* o que significa que se exige que se passem a considerar os procedimento de *"security"* como essenciais para que aqueles incidentes não tenham impacto e se evitem ocorrências

Gestão para a Segurança da Exploração dos Navios e para a Prevenção da Poluição, a partir de 1992) ou visando as normas para a investigação de acidentes ou incidentes marítimos (o CIA ou *Código de Investigação de Acidentes)* que agrega um conjunto de resoluções da IMO, merecendo especial referência a Resolução A.849 820) de novembro de 1990 – que estabelece as regras para a investigação dos fatores humanos nos acidentes e a Resolução MSC.255 (84), de 16 de maio de 2008, que contempla as normas e recomendações a adotar em investigações de acidentes ou incidentes marítimos.

35 A autonomia do Direito da Segurança enquanto ramo do Direito foi defendida por Gouveia, Jorge Bacelar, na obra "*Direito da Segurança Cidadania, Soberania e Cosmopolitismo",* Almedina, Coimbra, 2018. Nesta obra, em particular na sua *segunda parte* que respeita à *"explicitação do Direito da Segurança como novo setor jurídico e no contexto das respetivas fontes*" (a pps. 17*),* o autor *"trilha"* um caminho no trabalho que, em alguma medida, poderá dificultar "*a busca em profundidade em alguns mais complexos pontos"* (a pps. 15). No entanto, foi a sua abrangência e a forma inovadora da abordagem que faz, em nossa opinião, emergir, entre outros âmbitos especiais, o *Direito da Segurança Marítima* como discípulo do *Direito da Segurança* e, em simultâneo, *"largando as amarras"* dos ramos tradicionais do *Direito do Mar* e do *Direito Marítimo*.

36 Importará esclarecer que se parte de uma perspetiva iminentemente comercial, i.e., para se estabelecer a atividade do transporte marítimo é necessário, em primeiro lugar, recorrer a meios tecnologicamente seguros. Só depois emerge a importância do controlo das ameaças. Claro que este postulado pode ser (e é), em certas circunstâncias, reversível, garantindo-se a prioridade de estabelecer um ambiente minimamente adequado à utilização ou emprego dos meios.

37 O que significa que, como já foi mencionado, que incidentes de (*"cyber") "security"* podem dar origem a incidentes de *"safety"*, numa contínua interação que não devem ser tratados verticalmente. Aproximamo-nos, neste ponto, da evolução da tradicional missão de "defesa naval" da NATO para uma noção alargada de *"segurança marítima"* em que se visa *"impedir o uso do mar para atividades ilícitas e assegurar a liberdade de navegação"* cf. Pereira, Luis Sousa, *"A NATO e a Segurança no Mar"* in Cajarabille, Victor Lopo e outros, *"A Segurança no Mar -uma Visão Holística",* Mare Liberum, Aveiro, 2012, a pps. 132. Simplesmente, o conceito por nós defendido não se esgota na perspetiva de "defesa naval" e exige uma componente muito significativa de *"safety"* em sentido estrito. No entanto, a tradução que é feita, por exemplo, de documentos NATO, como seja, o *"Maritime Security Operations Concept",* ("Conceito de Operações de Segurança Marítima") faz com que - e uma vez mais – ao termo *"security"* corresponda o vocábulo "segurança" (e não "proteção"). Num recente trabalho (de 30 de agosto de 2019), sob o título *"Polemologia da Segurança Marítima – Golfo da Guiné como estudo de caso"* (inédito), elaborado pelo Comandante Luis Cuco de Jesus, no âmbito do Curso de Doutoramento em Direito e Segurança da Faculdade de Direito da Universidade Nova de Lisboa, este autor utiliza a figura da "segurança marítima" com o objetivo de eleger mecanismos legais de repressão das novas ameaças em ambiente marítimo o que significa que o quadro proposto se desenvolve, essencialmente e de forma estrita, no âmbito da *"security".*

graves em sede de *"safety",* fazendo-os, inclusivamente, constar da obrigatoriedade dos códigos internacionais de gestão da segurança (marítima).

Contudo, o robustecimento da importância da *"security"* não se traduziu, no âmbito convencional, numa atualização e revisão dos conceitos, nem seria de esperar tal posição. Na verdade, a própria convenção SOLAS iniciou o seu longo percurso, em 1914, com uma vertente essencial de segurança marítima e de salvaguarda da vida humana no mar (que, aliás, advém da sua sigla SOLAS – *Safety of Life at Sea*), tendo sofrido, no seu seio, quer o alargamento a novas matérias (o Código ISPS, por exemplo), quer a autonomização de outras (como foi o caso da convenção COLREG que, em 1972, aprovou o Regulamento para Evitar Abalroamentos no Mar).

Assim, o *Direito da Segurança Marítima*, no âmbito do Direito Internacional, tem como fontes essenciais as convenções específicas da IMO que se baseiam na classificação tradicional da *"safety"*, estendendo paulatinamente a sua regulamentação à *"security"* - como sucede com o Código ISPS anexo à Convenção SOLAS ou, de forma autónoma, com a Convenção SUA[38].

Esta expansão instrumental da tradicional matéria da segurança à proteção marítima não é mais do que uma tentativa de resposta aos novos riscos e ameaças no mar e nos portos que, contudo, ainda esbarram na dificuldade da regulamentação em zonas claras do exercício da soberania dos Estados avessas, tradicionalmente, ao Direito Internacional.

Entende-se, contudo, que será inexorável, pelo menos, uma progressiva harmonização e articulação das capacidades e meios de atuação por parte dos Estados na vertente *"security"* pois a dimensão global dos riscos e ameaças exige essa abordagem.

Tome-se, como exemplo, nos tempos de hoje, uma matéria que, cada vez mais, interessa ao transporte marítimo e aos portos: a chamada *"cibersegurança marítima"*[39].

Não é demais referir que a interconexão entre um incidente de *"security"* e a sua transposição para um incidente de *"safety"* assume, neste quadro, uma probabilidade real pois não é difícil de prever que a mistificação na posição geográfica de um navio leve ao seu desvio de rota e ao consequente encalhe ou abalroamento.

A partir de 2002, o Código ISPS veio a reconhecer o papel das estruturas portuárias (terminais e portos) no âmbito da proteção marítima e estabeleceu requisitos obrigatórios e recomendações aplicáveis aos navios e àquelas instalações. Ora, aqueles

[38] *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,* 1988.

[39] Que, na verdade, se deveria chamar *"ciberproteção marítima"* face ao que foi anteriormente exposto pois trata-se de matéria de *"security"*. Vide igualmente o artigo de Marques, António Gameiro, *"Cibersegurança no Setor Marítimo"*, in Revista de Marinha, n.º 1004, jul-ago 2018, a pps. 30 a 32. O autor aborda esta matéria de forma pioneira, talhando a evolução na União Europeia e o regime jurídico recentemente aprovado no que respeita ao ciberespaço. Vide igualmente, do mesmo autor, *"A Segurança do Ciberespaço em Portugal e no Setor Marítimo",* Cadernos Navais, n.º 52, abril-junho de 2019, Centro de Estudos Estratégicos da Marinha, *in* www.marinha.pt. Quanto aos conceitos de Cibersegurança e de Segurança da informação, vide Santos, Lino, *"Cibersegurança"* e *"Segurança da informação" in* Gouveia, Jorge Bacelar Gouveia e Santos, Sofia (coordenação), *op. cit.,* pps. 63 a 67 e 422 a 425. Este autor refere que "*a cibersegurança pode ser vista a partir de duas perspetivas, independentemente de o objeto da cibersegurança ser o Estado, as organizações ou os indivíduos: a segurança do ciberespaço (na aceção física deste como entidade autónoma) e a segurança da componente "ciber" de um qualquer sistema (segurança do ciberespaço desse sistema)"* (a pps 63). Por seu lado e segundo o mesmo autor, a segurança da informação é indispensável para *"garantir a todo o tempo, a confidencialidade, a integridade e a disponibilidade da informação*" (a pps. 422).

requisitos podem igualmente abranger medidas de cibersegurança relativas ao controlo de acessos e à autenticação das autorizações[40].

Na verdade, o Código ISPS exige que cada terminal elabore o designado *"Port Facility Security Assessment"* (PFSA) no qual se identificam as estruturas e os equipamentos, as possíveis ameaças e contramedidas e o *"Port Facility Security Plan"* (PFSP) no qual se identificam, para os diferentes níveis de alerta, os procedimentos, medidas e ações a executar. O PFSA deve abordar os seguintes aspetos: segurança física, integridade estrutural, sistemas de proteção pessoal, políticas procedimentais, sistemas de radio e de telecomunicações – incluindo sistemas computacionais e redes informáticas – e infraestruturas relevantes de transporte. Por seu lado, o PFSP especifica as condições de acesso à infraestrutura, de acesso às áreas restritas, de movimentação da carga, de entrega dos abastecimentos aos navios e da monitorização das condições de proteção da infraestrutura.

Também as Convenções SOLAS e FAL *("Facilitation on International Maritime Traffic")* vieram definir nove formas-padrão para serem utilizadas na troca de informações no ecossistema marítimo, especialmente, entre os portos (ou terminais) e partes terceiras que é obrigatoriamente processada por meios eletrónicos a partir de 9 de abril de 2019, especialmente através do uso dos sistemas de *"single window"* ("janela única"). Trata-se da padronização do intercâmbio de informação que tem um forte impacto nos sistemas TI e que lhe coloca novos desafios.

No que respeita à cibersegurança para o "ecossistema" marítimo, em particular para os navios, só a partir de 2017 começaram a ser endereçadas recomendações em sede internacional.

O Comité da Facilitação *("IMO Facilitation Committee"* ou FAL) o Comité de Segurança Marítima (*"IMO Maritime Security Committee"* ou MSC) da IMO elaboraram as linhas de ação na gestão do risco da cibersegurança marítima através do documento MSC-FAL 1/Circ.3[41]. Ambas aquelas estruturas reconhecem a necessidade urgente de se aumentar o alerta para as ameaças e vulnerabilidades do ciberespaço marítimo e de elaborar recomendações de alto nível na gestão dos riscos daquele ciberespaço relativamente às ameaças e vulnerabilidades atuais e emergentes, incluindo áreas principais que se consideram essenciais para o apoio à gestão do ciberespaço (identificar, proteger, detetar, responder e recuperar).

Estas linhas de ação procederam à distinção entre sistemas TI (ou IT) (tecnologias de informação, i.e., utilização de dados como informação) e TO (ou OT) (tecnologia operacional, i.e., constata-se que os sistemas TI estão cada vez mais interligados à TO de cada empresa que exige uma nova perspetiva de gestão na utilização de dados para controlar ou monitorizar os processos físicos, numa interação ciberfísica constante e bidirecional) e revelam que todas as organizações da indústria do transporte marítimo são diferentes e que o papel dos Governos e dos Estados de bandeira na sua regulação

[40] Vide, mais recentemente, o documento ENISA *("European Union Agency for Cybersecurity")*, *Port Cybersecurity - Good practices for cybersecurity in the maritime sector,* Nov. 2019, ISBN 978-92-9204-314-8, DOI 10.2824/328515.

[41] Ver *"Guidelines on Maritime Cyber Risk Management"* (MSC-FAL.1/Circ.3) in http://www.imo.org/en/OurWork/*Security*/Guide_to_Maritime_*Security*/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

é essencial. Estes dever-se-ão, igualmente, pautar pelo prosseguimento das recomendações dos instrumentos e das boas práticas internacionais mais relevantes, visando a melhoria das medidas de proteção.

Claramente se constata que ficou a cargo de cada Estado tomar as medidas consideradas mais adequadas, num ambiente bem longe da progressiva uniformização exigida pela conexão global dos sistemas.

Ao nível da União Europeia[42], o papel marcante da sua agência especializada (ENISA – *"European Union European Union Agency for Network and Information Security"*) sobre o setor marítimo iniciou-se em 2011 com a publicação do relatório sobre a cibersegurança marítima[43].

Este documento, em síntese, começou por caracterizar os sistemas que a comunidade marítima utiliza, de uma forma geral, altamente complexos, com diversas tecnologias, inúmeros fabricantes e enorme dispersão de nacionalidades. Sucede que as questões associadas à segurança (ou proteção no sentido de evitar a intrusão e disrupção) são, em geral, consideradas despiciendas, aumentando o risco dos ciberataques, ampliado pelas fáceis ligações à "internet" de forma livre e sem a adoção de boas práticas.

Mas mais grave ainda foi a constatação de ausência de capacidade de resposta quer a incidentes quer mesmo a ciberataques, numa completa ausência de coordenação entre os diversos atores do setor marítimo-portuário.

Em termos gerais, também a transposição e aprofundamento dos capítulos atinentes da Convenção SOLAS respeitantes à *"security"* poderão abranger ações de resposta aos ciberataques, particularmente, quando inseridos nas medidas gerais de proteção dos navios e dos portos.

A este título, merecem especial referência os seguintes diplomas comunitários:

- O Regulamento (CE) n.º 725/2004 que respeita à aplicação do Código ISPS aos navios e às estruturas portuárias;
- A Diretiva n.º 2005/65/CE no que respeita à proteção portuária;
- O Regulamento (CE) n.º 336/2006 sobre a aplicação do Código ISM *("International Safety Management Code")* no setor marítimo – salvaguardando-se, contudo, que este Código não é aplicável aos portos; e
- A Diretiva n.º 2010/65/UE que estipula sobre a aceitação dos Estados-membros das formas-padrão *("FAL forms")* para facilitação do tráfego. Esta Diretiva introduz igualmente no ordenamento jurídico os sistemas *"SafeSeaNet"* ao nível nacional e da União Europeia promovendo o tráfego seguro de dados entre as administrações marítimas de cada Estado e outras autoridades.

[42] Respigando a Estratégia da Segurança Marítima da União Europeia, de 24 de julho de 2014, a pps. 3,*"Maritime security is understood as a state of affairs of the global maritime domain, in which international law and national law are enforced, freedom of navigation is guaranteed and citizens, infrastructure, transport, the environment and marine resources are protected".* Deste parágrafo se extrai, igualmente, a ideia já aventada da apresentação dos 2 círculos concêntricos que correspondem à *"safety"* e à *"security"*, ou seja, a garantia da liberdade da navegação em condições seguras para os cidadãos, para as infraestruturas, para os transportes, para o ambiente e para os recursos marinhos. Vide COUNCIL OF THE EUROPEAN UNION, Brussels, *European Union Maritime Security Strategy*, 24-06-2014, doc. 11205/14.

[43] https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security.

De forma breve, o Regulamento (CE) n.º 725/2004 e a Diretiva n.º 2005/65/CE constituem o quadro jurídico de referência que sustentam a avaliação e os planos de proteção dos portos e das infraestruturas portuárias, bem como dos navios e das companhias de navegação.

Entretanto, em 2014, o documento que aprovou a Estratégia Europeia para a Segurança Marítima *("European Maritime Security Strategy"* ou EUMSS), revista em 2018[44], foi definido como um instrumento destinado a identificar, prevenir e dar resposta a qualquer desafio que possa afetar a proteção dos europeus, atividades e meios no ecossistema marítimo incluindo os portos.

A EUMSS identifica as ameaças e riscos à segurança marítima (num sentido lato) que se consubstanciam *em "terrorismo e outros atos intencionais e ilícitos no mar e nos portos contra os navios, mercadorias, tripulações e passageiros, portos e infraestruturas portuárias e infraestruturas críticas marítimas e energéticas, incluindo os ciberataques"*. A revisão de 2018 da Estratégia focou-se essencialmente no procedimento de relato com vista à melhoria do alerta e à monitorização das ações subsequentes.

Entretanto, só a partir da vigência da Diretiva n.º 2016/1148 *("Directive on Security of Network and Information Systems",* com o acrónimo NIS ou SRI em língua portuguesa[45]) a União Europeia passou a dispor de legislação habilitada a harmonizar as capacidades nacionais de cibersegurança, à colaboração nas fronteiras e à supervisão dos setores críticos no espaço da União.

Trata-se da primeira legislação da União Europeia sobre segurança do ciberespaço, visando aumentar a cooperação e criar uma cultura de segurança em sectores essenciais para a sociedade que dependam fortemente das TI.

---

[44] Vide a versão original de 2014 in *"The European Maritime Security Strategy"* in https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en. Claramente que fica patente que os documentos de estratégia sobre questões de "safety" e/ou de "security" são, quase invariavelmente, traduzidos por "segurança", argumento também a favor de se propugnar o "novo" Direito da Segurança Marítima como abrangendo ambas as vertentes que, cada vez mais, se apresentam interrelacionadas e cujos limites são cada vez mais fluidos.
E, a sua revisão de 2018, *in* https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/.
Em 2016, o Regulamento (UE) n.º 2016/679 *("General Data Protection Regulation")* que se destinou à proteção dos dados pessoais das pessoas singulares e da sua comunicação, também abrangeu, naturalmente, o setor marítimo, mas sem qualquer especialidade.

[45] Esta diretiva foi transporta para a legislação portuguesa pela Lei n.º 46/2018, de 13 de agosto que estabelece o regime jurídico da segurança do ciberespaço. Entretanto, em setembro de 2020, a Comissão Europeia lançou uma consulta pública no âmbito do processo de revisão da Diretiva NIS com o objetivo de reforçar a resiliência das redes e dos sistemas contra os riscos da cibersegurança. Neste âmbito, a Diretiva identifica os "operadores de serviços essenciais" entre os quais constam os portos marítimos. Um dos problemas identificados pela Comissão traduziu-se na falta de harmonização por parte dos Estados-membros na identificação daqueles operadores e que se refletiu também nos portos marítimos selecionados (por exemplo, se os portos mais pequenos deverão ou não ser excluídos da aplicação da Diretiva). Por esta razão, pretende-se igualmente revisitar os termos previstos para os "portos marítimos" na definição nela estabelecida que segue:*"Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC, including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports".*
Uma das questões nucleares a merecer ponderação respeita à obrigação que a Diretiva impõe da notificação dos incidentes de cibersegurança às autoridades competentes. Quanto a nós e desde que o operador faça parte de uma *"rede ou sistema de serviços essenciais"*, deverá ser abarcado pela Diretiva, não interessando se, por exemplo, o porto marítimo é grande ou pequeno. Trata-se de estender as obrigações do *"operador de serviços essenciais"* a todos os que façam parte de uma *"rede ou sistema de serviços essenciais",* independentemente da sua classificação como *"operador".*

Os parágrafos n.º 10 e n.º 11 da Diretiva do preâmbulo são específicos do setor marítimo:

> *"10. No setor do transporte marítimo e por vias navegáveis interiores, os requisitos de segurança aplicáveis às empresas, navios, instalações portuárias, portos e serviços de tráfego marítimo ao abrigo de atos jurídicos da União abrangem todas as operações, incluindo os sistemas de rádio e telecomunicações e os sistemas de informação e as redes. Parte dos procedimentos obrigatórios a seguir inclui a notificação de todos os incidentes e, como tal, deverá ser considerada como "lex specialis", na medida em que esses requisitos sejam, no mínimo, equivalentes às disposições correspondentes da presente diretiva".*

E no parágrafo n.º 11:

> *"11. Ao identificarem operadores do setor do transporte marítimo e por vias navegáveis interiores, os Estados-Membros deverão ter em conta os códigos e as orientações internacionais — atuais e futuros — elaborados pela Organização Marítima Internacional, a fim de permitir que os diversos operadores marítimos sigam uma abordagem coerente".*

Nos termos do n.º 4 do artigo 4.º da Diretiva, é considerado "operador dos serviços essenciais" uma entidade pública ou privada pertencente a um dos tipos referidos no anexo II e que cumpre os critérios previstos no artigo 5.º, n.º2 (isto, é, uma entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais, a prestação desse serviço depende de redes e sistemas de informação; e um incidente pode ter efeitos perturbadores importantes na prestação desse serviço).

Ora, no que respeita ao ecossistema do transporte marítimo e por vias navegáveis interiores são os seguintes os operadores constantes do anexo II:

- Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, tal como definidas, para o transporte marítimo, no anexo I do Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho não incluindo os navios explorados por essas companhias;
- Entidades gestoras dos portos na aceção do artigo 3.º ponto 1, da Diretiva 2005/65/CE do Parlamento Europeu e do Conselho, incluindo as respetivas instalações portuárias na aceção do artigo 2.º, ponto 11, do Regulamento (CE) n.º 725/2004, e as entidades que gerem as obras e o equipamento existentes dentro dos portos
- Operadores de serviços de tráfego marítimo na aceção do artigo 3.º, alínea o), da Diretiva 2002/59/CE do Parlamento Europeu e do Conselho.

Finalmente, em 2019, o "Ato Europeu sobre a Cibersegurança" *("EU Cybersecurity Act")*[46] veio robustecer a posição da ENISA em relação os Estados-Membros e definiu o quadro

[46] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

da certificação sobre cibersegurança dos produtos ICT, serviços e processos, passando-se a exigir o cumprimento de determinados requisitos.

Adicionalmente, foram vários os Estados-Membros que reforçaram a aplicação da regulamentação e políticas internacionais e comunitárias sobre a cibersegurança, desenvolvendo as suas próprias iniciativas para melhorar a gestão dos riscos do ciberespaço através de legislação nacional[47].

IV. Conclusões

Se desde os tempos da Antiguidade o mar era sinónimo de globalização para o comércio, a mesma globalização conduz à emergência de diversos riscos e ameaças que exigem condições mais exigentes dos produtos ICT *("Information and Communication Technologies")* e dos serviços associados.

Os ciberataques no setor marítimo-portuário vieram robustecer a necessidade de se abordar a nova segurança marítima de uma forma holística, integrando as duas vertentes (a *"safety"* e a *"security"*) mas com uma modelação que deriva da estratégia nacional prosseguida para o mar por cada Estado.

Só assim será possível que a *"segurança no mar"* seja uma realidade que se equilibra pela interação de dois círculos concêntricos: a *"safety"*, de natureza essencialmente técnica e a *"security"* que reforça aquela (ou a torna, infelizmente, mais vulnerável) e que assume contornos de prevenção e de contenção das ameaças.

O salto qualitativo dado pela União Europeia no que respeita à cibersegurança foi dado pela Diretiva n.º 2016/1148 *("Directive on Security of Network and Information Systems")* passando a dispor de legislação habilitada a harmonizar as capacidades nacionais de cibersegurança, à colaboração nas fronteiras e à supervisão dos setores críticos no espaço da União.

E "navegar no ciberespaço" em "segurança" corresponde, afinal, a enfrentar novos "escolhos" – acidentais ou deliberados – em que a globalização "desregulada" é o novo arquétipo do "Cabo das Tormentas" e do "Mar Tenebroso".

Tal como este foi navegável e safo, também o ciberespaço o deverá ser em segurança, com uma regulação apertada e com novos instrumentos, como Pedro Nunes o fez com a carta das "latitudes crescidas"[48] ou como Bartolomeu Dias, ao dobrar o promontório, veio

---

47 Lei "CIIP" em França - https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/.
Lei específica para os portos no Reino Unido - *https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice;*
Lei "IT-Grundschutz" na Alemanha - https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html;
A nível nacional: a Lei n.º 46/2018 de 13 de agosto transpôs para o ordenamento jurídico nacional a Diretiva (UE) n.º 2016/1148 e a Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho veio estabelecer a Estratégia Nacional de Segurança do Ciberespaço.
Note-se que a cibersegurança foi tema relevante na agenda da última Cimeira da Nato em Londres, no mês de dezembro de 2019.

48 Embora em cartas de pequena escala, deixando a Gerardo Mercator, mais tarde, a glória da sua generalização. Pedro Nunes, enquanto o primeiro cosmógrafo-mor do Reino, nomeado em 1547, desempenhou um papel crucial no desenvolvimento do estudo dos problemas matemáticos da cartografia náutica e que se tornou imprescindível nos métodos e nos equipamentos utilizados na navegação oceânica. Foi o primeiro a conceptualizar a diferença entre a *"loxodromia"* e a *"ortodromia"*, i.e., referindo que a linha

a designá-lo como a nova "Boa Esperança", um repositório de novos conhecimentos e técnicas de navegação com os quais foi possível iniciar-se a "Globalização"!

Referências bibliográficas

Branco, Carlos (2018). *"Porquê uma Estratégia de Segurança Nacional?",* Opinião, Jornal Expresso, 11 de maio.

Cajarabille, Victor Lopo (coordenação) (2014). *"A Segurança nos Portos – uma visão integrada",* Mare Liberum, Aveiro.

Cajarabille, Victor Lopo e outros (2012). *"A Segurança no Mar – uma visão holística",* Mare Liberum, Aveiro.

Cajarabille, Victor Lopo (2012). *"Enquadramento Estratégico",* in Cajarabille, Victor Lopo e outros, "A Segurança no Mar – uma visão holística", Mare Liberum, Aveiro, pps. 21 a 35.

CISA, *"The Cybersecurity and Infrastructure Security Agency",* in www.cisa.gov.

Coelho, Carlos (2007). *"Poluição Marítima por Hidrocarbonetos e Responsabilidade Civil",* Almedina, Coimbra.

COUNCIL OF THE EUROPEAN UNION, *"European Union Maritime Security Strategy",* 24-06-2014, doc. 11205/14.

Couto, Abel Cabral (1988). *"Elementos de Estratégia"*, Volume I, IAEM, Lisboa.

CSIS, *"Center for Strategic & International Studies",* in https://www.csis.org.

Direção-Geral da Política do Mar (DGPM), ENM 2021-2030, *"Estratégia Nacional para o Mar",* documento provisório para consulta pública, in https://www.dgpm.mm.gov.pt/enm.

Duarte, António Rebelo (2018). *"Políticas e Estratégias Marítimas da Europa e de Portugal",* Cadernos Navais, n.º 48, abril-junho, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt.

ENISA ("European Union Agency for Cybersecurity") (2019)*." Port Cybersecurity - Good practices for cybersecurity in the maritime sector",* Nov, ISBN 978-92-9204-314-8, DOI 10.2824/328515.

ENISA, *"The European Maritime Security Strategy"* (2014), in https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en.

ENISA, *"The European Maritime Security Strategy"* (rev. 2018) in https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/.

de rumo constante não era a distância mais curta entre dois pontos. No seu *"Tratado em Defensa da Carta de Marear"*, argumentou que uma carta náutica deveria ter circunferências paralelas e meridianos *"desenhados como linhas retas".* Mas poderíamos referir muitos mais e, mais recentemente, o Almirante Gago Coutinho e a sua assombrosa preparação - matemática e cartográfica - da viagem da Primeira Travessia Aérea do Atlântico Sul, entre Lisboa e o Rio de Janeiro, em 1922.

ENISA, Report, in https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security.

Escorrega, Luis Carlos Falcão (2009). *"A Segurança e os "Novos" Riscos e Ameaças: Perspetivas Várias",* Revista Militar, n.º 2491, agosto/setembro (https://www.revistamilitar.pt/).

Faria, Duarte Lynce de (2018). *"O Contrato de Volume e o Transporte Marítimo de Mercadorias – Dos granéis aos contentores, do "tramping" às linhas regulares",* Coleção Teses, Almedina, Coimbra.

Faria, Duarte Lynce de (2015). *"Segurança no mar"* in Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), *"Enciclopédia de Direito e Segurança"*, Almedina, Coimbra, pps. 433 a 439.

Fernandes, António Horta (2014). *"Conceito Estratégico de Defesa Nacional (CEDN) ou Conceito Estratégico de Segurança Nacional (CESN)? Um falso dilema",* Observatório Político, wp #43, abril, in http://www.observatoriopolitico.pt/wp-content/uploads/2014/04/WP_43_AHF.pdfla, pps. 4ss.

Gallagher, John (2019), in "Freight Wave" (Revue), 29th of March.

Garcia, Francisco Proença (2015). "Defesa Nacional" in Gouveia, Jorge Bacelar e Santos, Sofia (coordenação*), "Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pps. 99 a 101.

GOBIERNO DE ESPAÑA (2013). *"Estrategia de Seguridad Marítima Nacional"*.

Gouveia, Jorge Bacelar e Santos, Sofia (coordenação) (2015). "*Enciclopédia de Direito e Segurança",* Almedina, Coimbra.

Gouveia, Jorge Bacelar (2015). *"Direito Constitucional da Segurança" in* Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pps. 131 a 136.

Gouveia, Jorge Bacelar (2018). *"Direito da Segurança Cidadania, Soberania e Cosmopolitismo",* Almedina, Coimbra.

Goward, Dana A. (2019. *"Patterns of GPS Spoofing at Chinese Ports",* in MAREX, Daily Collection of Maritime Press Clippings 2019-356, pps. 31 e 32.

GPS WORLD, in https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.

Guedes, Armando Marques (2015). *"Segurança externa"* e *"Segurança interna",* in Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pps. 411 a 418 e 425 a 431.

IMO, *"Guidelines on Maritime Cyber Risk Management"* (MSC-FAL.1/Circ.3) in http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20-Management%20(Secretariat).pdf.

Jesus, Luis António Cuco de (2019). "*Polemologia da Segurança Marítima – Golfo da Guiné como estudo de caso",* inédito.

Kaplan, Elliott D. e Hegarty, Christopher J. (2006). "*Understanding GPS Principles and Applications"*, 2nd Edition, ARTECH HOUSE, Boston-London, Norwood, MA, USA.

Lourenço, Nelson (2015). "*Segurança interna"* in Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), "*Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pps. 431 a 433.

Maman, Rafael (2020). "*The Reshaping Cyber Threat Landscape of Operational Technology",* apresentação in "*Conferencia organizada pela PwC, "Cibersegurança – Os desafios da Tecnologia Operacional (OT)",* Lisboa, 5 de fevereiro.

Marques, António Gameiro (2019). "*A Segurança do Ciberespaço em Portugal e no Setor Marítimo",* Cadernos Navais, n.º 52, abril-junho, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt.

Marques, Antonio Gameiro (2018). "*Cibersegurança no Setor Marítimo", in* Revista de Marinha, n.º 1004, jul-ago, a pps. 30 a 32.

MINISTERY OF DEFENSE (MOD UK) (2014). "The UK National Strategy for Maritime Security", MOD UK, May.

Pedra, José Rodrigues (2012). "*A União Europeia e a Segurança no Mar", in* Cajarabille, Victor Lopo e outros, "*A Segurança no Mar – uma visão holística"*, Mare Liberum, Aveiro, pps. 143 a 162.

Pereira, Luis Sousa (2012). "*A NATO e a Segurança no Mar" in* Cajarabille, Victor Lobo e outros, "*A Segurança no Mar - uma Visão Holística"*, Mare Liberum, Aveiro, pps. 129ss.

Santos, Ana Miguel (2018). "*Uma segurança interna cada vez mais europeia? Uma segurança externa cada vez mais nacional?"* in RDeS - Revista de Direito e Segurança, Ano VI, jul-dez, pps. 27 a 51.

Santos, Lino (2015). "*Cibersegurança"* e "*Segurança da informação" in* Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), "*Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pps. 63 a 67 e 422 a 425.

Santos, Sofia (2015). "*Defesa preemptiva"* e "*Defesa preventiva" in* Gouveia, Jorge Bacelar e Santos, Sofia (coordenação), "*Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pps. 102 a 105.

THE AMERICAN CLUB 2010). "*Mass Global Positioning System (GPS) spoofing at ports in The People's Republic of China" in* Daily Collection of Maritime Press Clipping 2010-002, pps. 25.

THE EUROPEAN CENTRE OF EXCELLENCE FOR COUNTERING HYBRID THREATS (2019). "*Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans",* November.

UNKNOWN (2019). "*2020 Vision: Check Point's cyber-security predictions for the coming year",* de 24-10-2019, in https://blog.checkpoint.com/2019/10/24/2020-vision-check-points-cyber-security.

US COAST GUARD (cyber report), in https://navcen.uscg.gov/?Do=GPSReportStatus.