Centro de Estudos Estratégicos da Marinha

CADERNOS NAVAIS

N.º 52 – Abril – Junho de 2019

A segurança do ciberespaço em Portugal e no setor marítimo

Contra-almirante António Gameiro Marques

Edições Culturais da Marinha

LISBOA

Centro de Estudos Estratégicos da Marinha

CADERNOS NAVAIS

N.º 52 – Abril – Junho de 2019

A segurança do ciberespaço em Portugal e no setor marítimo

Contra-almirante António Gameiro Marques

Edições Culturais da Marinha

LISBOA

O Centro de Estudos Estratégicos da Marinha (CEEM) foi criado pelo Despacho número 13/18, de 12 de abril, do Almirante Chefe do Estado-Maior da Armada (CEMA), sucedendo ao Grupo de Estudos e Reflexão Estratégica (GERE), cuja origem remonta ao ano de 1999.

O CEEM, situado na direta dependência do Almirante CEMA, tem como principais incumbências a reflexão e o estudo nas áreas da estratégia marítima, doutrina naval e projeção externa da Marinha.

No âmbito das suas competências, o CEEM promove a publicação de textos sobre temas da sua vocação, através das coleções dos Cadernos Navais, editados pela Comissão Cultural da Marinha.

TÍTULO:
A segurança do ciberespaço em Portugal e no setor marítimo

COLEÇÃO:
Cadernos Navais

NÚMERO ANO:
52/Abril-Junho 2019

EDIÇÃO:
Comissão Cultural de Marinha
Centro de Estudos Estratégicos da Marinha (CEEM)

ISBN: 978-989-8159-89-2
Depósito legal n.º 183119/02

EXECUÇÃO GRÁFICA: Instituto Hidrográfico/Luís Gonçalves

TIRAGEM: 200 exemplares

O AUTOR

Contra-almirante António Gameiro Marques

(Autoridade Nacional de Segurança)

O Contra-almirante António Gameiro Marques nasceu na Figueira da Foz a 4 de maio de 1959. Ingressou na Escola Naval em 1976 e concluiu a Licenciatura em Ciências Militares Navais, Classe de Marinha, em 1981. Após prestar serviço em vários navios da Armada, frequentou a especialização em Comunicações na Marinha e concluiu em 1987 o Mestrado em *Electrical and Computer Engineering* que frequentou na *Naval Postgraduate School* em Monterey na Califórnia, EUA.

Depois de frequentar o *Senior Course* no Colégio de Defesa da NATO em Roma, de 2004 a 2007 foi o conselheiro militar de Marinha do Embaixador de Portugal junto da Aliança Atlântica no Quartel-General da NATO em Bruxelas, onde foi também o representante permanente de Portugal no *NATO Consultation Command and Control Board.*

Foi promovido ao posto de Contra-Almirante a 27 de novembro de 2008, e de Janeiro de 2009 a junho de 2013 foi o *Chief Information Officer* (CIO) da Marinha.

De 1 de Julho de 2013 a 31 de Agosto de 2016 exerceu as funções de Secretário-Geral Adjunto do Ministério da Defesa Nacional e o representante do Ministério da Defesa Nacional na Comissão Instaladora do Centro Nacional de Cibersegurança.

Entre Novembro de 2013 e Abril de 2014, frequentou o 39º Programa de Alta Direção de Empresas (PADE) da AESE/IESE - Escola de Direção e Negócios.

Desde 1 de Setembro de 2016 exerce o cargo de Diretor Geral do Gabinete Nacional de Segurança, sendo, por inerência, a Autoridade Nacional de Segurança. O Centro Nacional de Cibersegurança encontra-se na estrutura do GNS.

ÍNDICE

1. Introdução

Através do estudo da história fica claramente demonstrado que não há desenvolvimento económico sustentado sem segurança. De facto, os períodos mais ou menos longos de paz que se têm observado, nomeadamente na Europa, são disso um exemplo marcante e significativo.

No Mundo de hoje, o ambiente é manifestamente de natureza híbrida, em que o ambiente físico e o virtual interagem permanentemente, interação essa que é propiciada pela digitalização da sociedade, e através da qual a economia se desenvolve em novos contextos, nos quais a dicotomia desenvolvimento e segurança também se aplicam. De facto, a realidade do dia a dia demonstra-nos que, também este contexto de simbiose física/digital, não há lugar a desenvolvimento e prosperidade económica duradouras sem segurança.

Se tal realidade não for levada em linha de conta pelos diversos agentes da sociedade, sejam eles públicos ou privados, ao mais alto nível das organizações, o insucesso pode surgir a qualquer momento, seja por via da perda reputacional, seja por via do decremento da confiança nas organizações e consequente diminuição da sua influência no seio dos seus públicos de interesse e inerente perda de proveitos tangíveis e intangíveis.

É neste enquadramento que as sociedades do século XXI necessitam de ter nas suas agendas o assunto da segurança da vertente digital da sociedade, a qual comummente se apelida de cibersegurança, que, na moldura legislativa nacional[1]"... consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem."

Com efeito, a cibersegurança, ou de uma forma mais ampla a segurança do ciberespaço, embora nunca possa ser completa, pode ser melhorada através da concretização de uma combinação de medidas, quer no âmbito das políticas públicas quer de natureza interna às organizações, que deverão ter como característica principal a sua natureza abrangente, contemplando várias áreas do conhecimento, desde os tecnológicos aos comportamentais, passando pelos aspetos de natureza sociológica, jurídica, comportamental, comunicacional e mesmo estratégica, numa lógica transversal à sociedade.

Assim, nas páginas seguintes, iremos procurar caracterizar a organização e estruturas existentes em Portugal que contribuem para a segurança no ciberespaço de interesse nacional, as políticas públicas existentes mais relevantes, a importância de colocar as pessoas no centro das decisões que impactam o digital na nossa sociedade, o papel dos dirigentes nas organizações, terminando com uma breve caracterização do que se está a passar no setor marítimo e uma sucinta alusão às tendências futuras neste campo e áreas afins.

[1] RCM 92/2019 de 13 de junho – Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

2. Organização e Estrutura

Em Portugal as estruturas existentes para a segurança do ciberespaço visam aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas.

Assim, existe o Centro Nacional de Cibersegurança (CNCS), que funciona no âmbito do Gabinete Nacional de Segurança, e que foi criado em outubro de 2014[2]. Na dependência do Primeiro Ministro através da Ministra da Presidência e do Conselho de Ministros, o CNCS tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais. No CNCS funciona a equipa nacional de resposta a incidentes de cibersegurança, conhecida por CERT.PT. Esta equipa coordena a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais, operadores de Infraestruturas Críticas nacionais e prestadores de serviços digitais. O seu âmbito de atuação contempla o 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.

São ainda entidades relevantes para a segurança do ciberespaço de jurisdição nacional o Centro de Ciberdefesa[3] (CCD), que funciona no âmbito do Estado-Maior General das Forças Armadas, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) da Polícia Judiciária[4], e a unidade de cibersegurança que opera no âmbito dos Serviços de Informação de Segurança. Estas quatro entidades formam o núcleo operacional que coopera permanentemente em Portugal para a promoção da segurança no ciberespaço de interesse nacional. Para que a sua ação seja ainda mais abrangente e efetiva existe ainda a rede nacional de equipas de resposta a incidentes de cibersegurança (Rede Nacional de CSIRTS[5]) que conta com mais de quatro dezenas de membros, sendo a maioria do setor privado. A densidade desta rede é um contributo assinalável para a resiliência do sistema nacional como um todo.

---

[2] Decreto-Lei n.º 69/2014 de 9 de maio (2ª alteração à Lei Orgânica do GNS - Decreto-Lei n.º 3/2012, de 16 de janeiro).
[3] Decreto-Lei n.º 184/2014 de 29 de dezembro.
[4] Decreto-Lei n.º 81/2016 de 28 de novembro.
[5] https://www.redecsirt.pt/.

Para conferir coerência a todo este conjunto de atores existe o Conselho Superior de Segurança do Ciberespaço[6] (CSSC) que é o órgão que, sendo o órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço, contribui, entre outros, para a monitorização da execução da Estratégia Nacional de Segurança do Ciberespaço, que abaixo se descreve.

3. Políticas Públicas

No âmbito das políticas públicas, a segurança do ciberespaço em Portugal está enquadrada por vários documentos e iniciativas estruturantes, que passaremos a descrever seguidamente:

a. Estratégia Nacional de Segurança do Ciberespaço

Portugal possui, desde 12 de junho de 2015, uma Estratégia Nacional de Segurança do Ciberespaço (ENSC) que, entretanto, foi revista com a participação de representantes do setor público e do setor privado, designadamente através da rede nacional de CSIRTS acima mencionada. Este documento, estruturante para o incremento da maturidade da sociedade portuguesa na área da respetiva resiliência digital, contém medidas específicas para o setor público, para o setor privado e para os cidadãos, que foram propostas pelos representantes dessa comunidade. Após aprovação no seio do CSSC, foi aprovada em Conselho de Ministros e publicada através da RCM 92/2018 de 05 de junho. No prazo de 120 dias após a sua publicação, será elaborado o respetivo plano de ação, cuja coordenação e monitorização serão realizadas pelo CNCS e CSSC respetivamente.

A ENSC 2019-2023 estabelece a visão de que Portugal seja um país seguro e próspero através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade. Identifica três objetivos estratégicos (1 - Maximizar a resiliência, 2 - Promover a inovação e 3 - Gerar e Garantir recursos), e seis eixos de atuação que incorporam as linhas de ação que permitem que sejam alcançados aqueles objetivos:

Eixo 1 - Estrutura de segurança do ciberespaço;
Eixo 2 - Prevenção, educação e sensibilização;
Eixo 3 - Proteção do ciberespaço e das infraestruturas;

[6] Art.º 5º da Lei 46/2018 de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a UE.

Eixo 4 - Resposta às ameaças e combate ao cibercrime;
Eixo 5 - Investigação, desenvolvimento e inovação;
Eixo 6 - Cooperação nacional e internacional

A ENSC 2019-2023 será objeto de avaliação anual pelo CSSC, sendo que esta incluirá uma verificação dos objetivos estratégicos e do plano de ação e adequação dos mesmos à evolução das circunstâncias. Concomitantemente, a rápida evolução intrínseca ao ciberespaço exige que a o documento seja objeto de acompanhamento regular no contexto dos efeitos que a concretização das medidas que incorpora está a produzir na sociedade, devendo ser integralmente revista num prazo máximo de cinco anos.

b. Observatório de Cibersegurança

O Observatório de Cibersegurança pretende ser uma plataforma de análise, discussão e sistematização de conhecimento, com uma abordagem multidisciplinar à cibersegurança, produzindo indicadores e séries temporais e articulando as várias partes interessadas na recolha de informação, com vista a uma sociedade mais segura e consciente dos riscos inerentes ao ciberespaço. O Observatório propõe-se produzir um relatório anual, bem como dossiers temáticos nas seguintes áreas: Espectro de Conflitos, Economia, Sociedade, Ética e Direito e Políticas Públicas. Destina-se, ainda, a aferir o estado da cibersegurança nacional, constituindo-se não só como como um instrumento de apoio na definição de políticas públicas e de produção científica nesta área, como também um meio de medir os efeitos da concretização da ENSC nos diversos setores da sociedade.

c. Quadro Nacional de Referência em Cibersegurança

O Quadro Nacional de Referência em Cibersegurança (QNRC) tem como objetivo providenciar às organizações um guia de cibersegurança que sistematiza um conjunto de medidas e controlos para as problemáticas mais relevantes da atualidade nesta matéria. Destinando-se a gestores e técnicos de organismos públicos e privados, pretende disponibilizar as bases para uma organização cumprir os requisitos mínimos de segurança da informação aconselhados, bem como um conjunto de recomendações adicionais, fundamentais para que as organizações possam cumprir, por um lado, com a legislação em vigor, e por outro, estar preparadas, de forma efetiva, para gerir o risco e mitigar o impacto decorrente de eventuais incidentes, através da definição de uma estratégia particular que envolva toda a organização.

d. Modelos de Maturidade

Tendo por base o QNRC acima mencionado, os Modelos de Maturidade em Cibersegurança têm como propósito estruturar e priorizar as

competências e as capacidades mínimas em cibersegurança que uma organização deve possuir numa escala com cinco níveis no âmbito da prevenção, deteção, reação a ciberincidentes e gestão da segurança da informação. Associados a estes modelos está a ser desenvolvida uma ferramenta de autoavaliação a ser utilizada pelas organizações e de uma base de recursos técnicos e formativos para apoio às entidades aderentes no desenvolvimento das suas capacidades dentro de cada um dos modelos. O conjunto do QNRC e dos Modelos de Maturidade capacitará as organizações aderentes a aferir onde estão no que respeita o respetivo nível de maturidade em cada um dos temas referidos (prevenção, deteção, reação a ciberincidentes e gestão da segurança da informação), viabilizando a identificação das medidas e das competências que têm que existir nas organizações para incrementar aqueles níveis, incluindo a elaboração do plano necessário a levar a organização ao incremento dos respetivos níveis de maturidade.

4. A importância do fator humano

Tal como em outros domínios, o fator humano é o mais determinante no contexto da cibersegurança nacional, uma vez que, apesar de estarmos num ambiente que é um resultado da curiosidade, do engenho, da ambição e do desenvolvimento científico do ser humano, este é igualmente o elemento mais frágil da cadeia de valor. Por esta razão é, frequentemente, o originador, por via do seu comportamento, de situações que levam a que comprometimentos perpetrados através do ciberespaço, penetrem as organizações, vulnerabilizando-as e comprometendo o seu cabal funcionamento, e fragilizando a respetiva reputação nacional e internacional, com impactos no respetivo património tangível e intangível.

Neste contexto, o CNCS, em parceria com entidades públicas e privadas, e em linha com o preconizado no documento de Estratégia acima aludido, tem vindo a desenvolver um vasto leque de iniciativas na área da sensibilização da sociedade em cibersegurança, consubstanciado num alargado programa de sensibilização, formação e de treino.

Este programa, que está diretamente relacionado com o Eixo 2 da ENSC 2019-2023, congrega um conjunto de instrumentos para o desenvolvimento de competências digitais em cibersegurança, designadamente um MOOC[7] alojado na plataforma NAU[8] designado de "Cidadão Ciberseguro" e ações de sensibilização em "ciberhigiene", ministradas presencialmente. Para alavancar o alcance desta última iniciativa, está a ser criada uma bolsa de formadores acreditados, que conta já com cerca de 60 elementos espalhados

[7] *Massive Open Online Course.*
[8] https://lms.nau.edu.pt/.

pelo país que, de forma voluntária, espalham este conhecimento por todo o território nacional, num modelo de parceria virtuosa.

Ainda na componente de sensibilização está prevista a criação de um novo MOOC designado "Cidadão Ciberinformado", com o objetivo de desenvolver o espírito crítico no consumo de informação digital e uma ação de sensibilização destinada a decisores e altos quadros de empresas e do Estado, com o objetivo de alertar para a necessidade de introduzir a cibersegurança como mais um fator de risco de negócio.

A componente de treino deste programa destinada a técnicos, está a ser articulada com o desenvolvimento dos modelos de maturidade em cibersegurança acima referidos. O objetivo é criar, com o apoio das Universidades e Politécnicos, uma rede nacional de cursos especializados no desenvolvimento das competências necessárias para a instalação e operação dos diversos instrumentos e tecnologias identificados como necessários nos modelos de maturidade.

Num outro registo e para referência, importa mencionar um documento recentemente publicado pela ENISA, que caracteriza o atual "estado da arte" sobre a componente humana da cibersegurança, e identifica caminhos para melhor envolver as pessoas nos processos ligados ao digital em geral, e à cibersegurança em particular[9]. Sem se pretender ser exaustivo, mencionam-se algumas conclusões apresentadas pelo estudo, que importa levar em linha de conta quando se pretende estabelecer programas se sensibilização, de formação e de treino em qualquer organização:

- A sensibilização deve centrar-se nas boas práticas e no seu efeito positivo e não na atemorização das pessoas;
- É mais eficaz as organizações promoverem a adesão à cibersegurança com participação ativa, do que forçarem a conformidade com normas que as pessoas não compreendem;
- A cibersegurança nas organizações só é percecionada como importante se não colidir com o valor da produtividade;
- Sacrifica-se muitas vezes a usabilidade a favor da segurança – tal situação é negativa para o fator humano, devendo procurar-se encontrar um equilíbrio entre as duas características;
- As diferentes áreas disciplinares, desde as técnicas às sociais, devem trabalhar em conjunto, interagindo virtuosamente;
- O fator humano deve ser articulado com as capacidades técnicas: não basta por isso fortalecer o ser humano, sem a existência de soluções técnicas adequadas;

Sabemos que a melhor forma de estarmos protegidos é estarmos preparados. O investimento na sensibilização, na formação e no treino das pessoas que constituem a componente mais importante de qualquer organização é algo estruturante com impacto perene na maturidade digital da organização e assim na sua resiliência digital.

[9] https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

5. O papel dos líderes no incremento da resiliência digital das organizações

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue[10].

Com efeito, e apesar do que vários organismos internacionais preconizam[11], ainda se encontram muitos altos responsáveis nas organizações que não dão o devido valor ao risco que decorre do facto de terem as suas atividades muito dependentes e expostas ao ciberespaço, considerando estes assuntos uma questão exclusiva do departamento de tecnologias de comunicação e informação, um custo e não um investimento estratégico. Por essas razões, nunca colocam na agenda estes assuntos, a despeito da realidade inexorável em que hoje a generalidade da humanidade se encontra: um mundo permanente ligado em que a hiperconectividade é uma realidade e genericamente considerada uma *commodity*, que traz oportunidades mas que aporta também vários riscos[12] que importa compreender, identificar, gerir e mitigar.

Assim, quando, na sociedade eminentemente digital em que hoje vivemos, a atividade das entidades públicas e privadas em muito depende das transações efetuadas através do ciberespaço com os seus públicos de interesse, julgamos importante que o líder altere aquela postura e inclua nos processos decisórios de nível corporativo o tema dos riscos decorrentes desta inexorável mudança que nos últimos anos ocorreu na sociedade. Desta forma, tirará partido das oportunidades que o alargamento da esfera de influência lhe proporciona, incluindo a rapidez com que podem alcançar e prestar serviços aos agentes que, de outra forma, estariam fora da sua visibilidade.

Neste enquadramento, iremos partilhar um conjunto de questões que o Dirigente máximo das organizações poderá suscitar ao seu próprio conselho de administração ou seu equivalente[13], para, por um lado, aferir o estado de maturidade da entidade que lidera quanto à respetiva resiliência digital, e por outro definir objetivos para que aquele estado incremente:

1ª pergunta: A organização possui doutrina que enquadre a cibersegurança na organização, incluindo os procedimentos e controlos para gestão da segurança da informação que circula no ciberespaço sob sua jurisdição em todo o seu ciclo de vida? Caso não possua, o QNRC e modelos de maturidade associados poderão contribuir para esse desiderato, que é estruturante em qualquer organização exposta ao ciberespaço.

---

[10] https://www.nacdonline.org/files/NACD%20Cyber-Risk%20Oversight%20Executive%20Summary.pdf.
[11] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.
[12] https://www.aon.com/2019-top-global-risks-management-economics-geopolitics-brand-damage-insights/index.html.
[13] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx.

2ª pergunta: Quais são os cinco maiores riscos relacionados com cibersegurança que a organização possui? Estão identificados, e os respetivos planos de mitigação desenvolvidos, validados e conhecidos por quem tem responsabilidade de os executar?
Neste âmbito, exemplos de riscos que deverão estar identificados são os relacionados com as ameaças (acidentais ou intencionais) à informação mais crítica e importante da organização, face a incidentes de segurança (exfiltração, negação de acesso, deturpação, divulgação não autorizada), que explorem vulnerabilidades existentes (TIC, físicas, humanas e organizacionais). Ainda neste âmbito, riscos relacionados com a mobilidade dos colaboradores, incluindo a gestão cuidada dos dispositivos de acesso a informação corporativa e a política de "outsourcing" existente são outros exemplos que deverão ser levados em linha de conta quando se tenta responder a esta questão.

3ª pergunta: Existe uma organização criada e liderada com enfoque na segurança da informação, seja ela digital ou em suporte físico? Numa lógica de construção e manutenção de uma capacidade de cibersegurança, a organização deverá ser detentora de uma estrutura que seja liderada pelo *Chief Information Security Officer* (CISO)[14], que será o garante da implementação das políticas definidas para a área da cibersegurança. Desejavelmente, o CISO deverá responder operacionalmente pelo menos ao responsável pela auditoria ou inspeção e regularmente deverá relatar ao Dirigente máximo da organização quanto à ocorrência de incidentes que envolvam comprometimentos de informação, incluindo o respetivo impacto na organização e o que foi feito para delimitar os seus efeitos. Deverá ainda ser o responsável pela execução das medidas necessárias à consecução dos objetivos estratégicos relacionados com a cibersegurança, numa lógica transversal a toda a organização.

4ª pergunta: Existem procedimentos treinados e testados para fazer face a um comprometimento grave de informação crítica? Neste enquadramento, está definida a equipa de resposta a incidentes incluindo as respetivas competências e o plano de contingência desenvolvido, testado e treinado?

5ª pergunta: Existe um plano de investimentos em cibersegurança que se baseie na análise da maturidade da organização (baseada num quadro de referência como é o caso do QNRC) e leve em consideração as vulnerabilidades internas e externas à organização? Com efeito, embora os incidentes de origem externa tendam a receber mais exposição e por isso mais visibilidade, a probabilidade de um incidente causado por uma entidade interna é realmente maior do que os causados por

[14] https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html.

ameaças externas. Como já foi referido, o fator humano é o elo mais importante, mas também o mais frágil da organização, situação que é potenciada pela mobilidade que hoje existe no contexto de trabalho o que, só por si, incrementa significativamente o risco para a organização. Neste contexto, ao definir os planos de investimento em cibersegurança devem-se acautelar quer os riscos externos quer os internos.

6ª pergunta: Existe um plano de formação e de treino em cibersegurança para todos os colaboradores, ainda que com níveis de profundidade diferenciados? O investimento na sensibilização, na formação e no treino dos colaboradores, seja nesta área seja noutra qualquer é algo que não só dá potencial estratégico à organização na sua globalidade, como também a prepara para novos desafios que possam surgir. Assim, na área da cibersegurança, formação básica deve existir e ser regularmente frequentada por todos, seja em contexto de aula seja em contexto de formação online, incluindo a realização de exercícios e o confronto com situações semelhantes às que se podem passar regularmente, a fim de se robustecer a capacidade das pessoas destrinçarem o verdadeiro do falso, contribuindo assim para que cada um seja uma barreira proactiva ao comprometimento da organização através do ciberespaço.

Uma vez recebidas as respostas a este conjunto de perguntas, deverá ser definido um plano que enderece as maiores lacunas, cuja execução deverá ser monitorizada pelo CISO acima referido e os resultados regularmente reportados superiormente.

O Dirigente é um dos elementos fundamentais da edificação desta capacidade: se o ele não levar a sério as questões da segurança da informação, a sua organização também não o fará.

6. A cibersegurança no setor marítimo

De acordo com artigo publicado em junho de 2018[15], o setor do transporte marítimo está vulnerável a uma série de potenciais comprometimentos, incluindo alguns que podem levar a que navios de vários milhões de euros tenham acidentes graves, designadamente em zonas marítimas com linhas de navegação de grande densidade de tráfego. De acordo com Ken Munro[16] , pesquisador da *Pen Test Partners*, as falhas são relativamente fáceis de explorar, com impactos muito significativos na atividade marítima.

Com efeito, o tema da cibersegurança no transporte marítimo em geral e dos navios em particular encontra-se numa fase de desenvolvimento relativamente baixa, uma vez que os sistemas IT que dão suporte à respetiva atividade não foram concebidos com as devidas proteções em relação aos

[15] https://threatpost.com/shipping-industry-cybersecurity-a-shipwreck-waiting-to-happen/132625/.
[16] https://www.pentestpartners.com/consultant/ken-munro/.

perigos que advêm da quase permanente conectividade que hoje se verifica na grande maioria dos grandes navios que navegam nos oceanos e mares do Mundo. O facto de existirem ligações via satélite quase sempre ativas, expõe os navios a ataques perpetrados por grupos de indivíduos mal-intencionados. Os armadores e as autoridades precisam, assim, de reconhecer esta realidade e de proceder proactivamente de modo a resolver rapidamente estes problemas, sob risco de um incidente de cibersegurança se transformar num problema de "safety", com impacto significativo e visível na sociedade. Com efeito, um navio a navegar em pleno oceano, ou está ligado à Internet ou esteve ligado à Internet. Por isso, tendo sistemas a bordo que não foram concebidos para estarem expostos às ameaças decorrentes dessa exposição, estão vulneráveis, isto é, ou irão ser comprometidos ou já o foram.

Neste enquadramento, iremos focar-nos no que poderá vir a ser o impacte das Tecnologias da Informação (IT) nas atividades da maioria dos agentes envolvidos no setor marítimo no contexto da cibersegurança, o respetivo "estado da arte" em termos gerais no setor marítimo, incluindo alguns contributos para a respetiva evolução, levando em linha de conta não só o enquadramento geral legislativo para a cibersegurança na União Europeia, como também o existente a nível nacional acima mencionada.

Nesta análise segmentaria este setor em três grandes grupos: o primeiro, englobando as entidades formais, ao nível da União Europeia e dos governos e agências governamentais dos Estados, o segundo, contemplando as entidades que operam em terra para que a cadeia de valor ligada à economia do mar funcione, e em terceiro lugar o mais importante: os navios que materializam organicamente todo o sistema.

Comecemos pela União Europeia: A *European Union European Union Agency for Network and Information Security* (ENISA) publicou em 20 de Dezembro de 2011, i.e. há mais de 8 anos, o primeiro e até à data único relatório sobre Cibersegurança Marítima[17].

O relatório afirmava, já naquela altura, que os sistemas que a comunidade marítima utiliza diariamente, quer a bordo quer em terra, em apoio às atividades ou operações marítimas (aqui num sentido lato), são, de uma forma geral, altamente complexos, e utilizam uma ampla diversidade de tecnologias, provenientes de uma variedade de fabricantes de outras tantas nacionalidades. Com efeito, o rápido desenvolvimento tecnológico, amiúde motivado pelo ímpeto de incrementar a eficiência de todos os processos através da automatização de um grande número de procedimentos (e muitas vezes com o propósito de diminuir custos operacionais fixos e assim aumentar os proveitos), leva a que as questões associadas à segurança sejam, frequentemente, relegadas para segundo plano, incrementando, assim, o risco, o qual deve ser gerido adequadamente, de modo a repor o imprescindível equilíbrio entre benefícios e as potenciais vulnerabilidades.

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

Se a este facto coligarmos a possibilidade da quase permanente conectividade à Internet de quem anda no mar, sem que tal seja levado na devida consideração no que concerne a cibersegurança na conceção e na operação dos sistemas IT que suportam as mais diversas operações, podemos facilmente concluir que estão potencialmente criadas as condições que, se malevolamente exploradas, poderão provocar degradação ou negação do acesso a serviços que hoje são essenciais para as atividades do setor.

O relatório refere ainda que não existe uma adequada padronização, certificação e identificação de boas práticas que, em conjunto, garantam que os assuntos relativos à cibersegurança são devidamente considerados neste ambiente específico. Quando existem, não são consentâneas com a complexidade dos sistemas existentes, não cobrindo tudo o que releva para o efeito.

Se a estes aspetos adicionarmos a multiplicidade e multinacionalidade dos atores envolvidos, os quais, quando a bordo, raramente são da nacionalidade da bandeira do navio, podemos facilmente deduzir que a envolvente, atenta a respetiva heterogeneidade e multiculturalidade, é particularmente e potencialmente vulnerável a ataques realizados através do ciberespaço, que poderão provocar disrupções do serviço com implicações consideráveis em vários domínios.

A ENISA relata igualmente a inexistência de regulamentos específicos alusivos aos assuntos respeitantes à cibersegurança neste setor, designadamente o que fazer e como agir legalmente se forem sujeitos a um ciberataque num determinado contexto marítimo. A maioria dos regulamentos contemplando o assunto da segurança refere a sua componente física, havendo pouca menção explícita à componente "ciber". Este facto era compreensível na altura da produção do relatório porque se constatava que havia, nesta comunidade, uma fraca sensibilidade para estes assuntos, o que resultava num baixo ou inexistente sentido de urgência para os abraçar, tendo em vista a respetiva resolução. Estes dois aspetos contribuíam para o incremento do risco global. Ainda que nos pareça que houve evolução neste âmbito, muito nos parece haver ainda a fazer.

Relativamente à governação dos assuntos do mar no universo da UE o relatório referia que o processo era difuso, desenvolvendo-se em múltiplas agências, patamares ou níveis, lesando dois princípios fundamentais para uma ação efetiva: a unidade de direção e a unidade de esforço. Esta situação conduz a que, em caso de um ciberataque, dificilmente se consiga uma coordenação eficaz da ação, para além de poder trazer discrepâncias significativas relativamente à forma como um mesmo assunto é tratado de uma zona de jurisdição marítima para outra.

Finalmente, o relatório conclui ainda que não existia uma aproximação conjunta e coerente à questão da cibersegurança na UE em geral no contexto das atividades ligadas ao mar: os atores, que pertencem às diversas agências que constituem as comunidades de interesse, quando lidam com os incidentes de cibersegurança, fazem-no de forma eminentemente ad hoc, com pouca coordenação. Apenas parte dos riscos são levados em linha de

conta, não se possuindo o conhecimento global da situação em que se encontram.

Se hoje fosse feito, o relatório apresentaria evoluções nalgumas áreas, mas não nos traria conclusões muito diversas das que foram então apresentadas. Todavia, mais importante que tudo, importa saber o que é que foi feito desde a publicação do documento para mitigar as fragilidades identificadas naquele relatório. O facto inexorável é que o recurso aos processos digitais na economia incrementou de forma generalizada e significativa, o que aumentou as oportunidades, mas também os riscos, se nada tiver sido feito para os identificar e mitigar.

A título de exemplo referiria que *Maritime Security Review*[18] documenta que o seguimento da carga e sua identificação estão a ser cada vez mais sujeitos a incidentes de cibersegurança, que resultam em perda de carga, falhas graves nos sistemas que efetuam o respetivo seguimento e identificação e no roubo de informação relevante, que depois é utilizada para fins ilícitos. No sítio daquela entidade na Internet existem várias recomendações sobre o tema, bem representativos de que não é pelo facto dos navios estarem a navegar, que estão imunes ao perigo que a hiperconetividade traz para a economia digital. Ainda neste contexto, refira-se que a produção de informação enganosa (e.g. *spoofing* do sinal de posicionamento) é igualmente uma realidade, que pode originar erros nos sistemas de navegação eletrónica e assim provocar acidentes marítimos de grande impacto.

Em 24 de Junho de 2014 a União Europeia publicou a *EU Maritime Security Strategy*[19] tendo em 16 de Dezembro desse ano apresentado o respetivo plano de ação[20].

Posteriormente, foram desenvolvidos dois relatórios relativos ao estado de concretização daquele plano, o primeiro de 22 de Junho de 2016[21], o segundo de 14 de Junho de 2017[22]. Em 26 de junho de 2018 foi publicado uma revisão do plano de ação original bem como as conclusões do Conselho sobre esse documento[23].

Da leitura deste conjunto de documentos pode-se apurar que o tema da cibersegurança se encontra contemplado, estando relacionado quer com a EU Cybersecurity Framework, entretanto anunciada pelo Presidente da Comissão Europeia em setembro de 2017 quer, mais importante ainda, com a Diretiva SRI (Segurança das Redes e dos Sistemas de Informação) adotada pelo Parlamento Europeu em 6 de julho de 2016[24] [25]. Esta é a primeira legis-

---

[18] http://www.marsecreview.com/tag/cyber-security/.
[19] https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en.
[20] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf.
[21] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/swd-2016-217_en.pdf.
[22] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/swd-2017-238_en.pdf.
[23] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-06-26-eumss-revised-action-plan_en.pdf.
[24] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT.
[25] Transposta para a legislação nacional através da já mencionada Lei 46/2018 de 13 de agosto.

lação da União Europeia sobre segurança do ciberespaço, que estabelece um conjunto de medidas para prevenir incidentes desta natureza em todo o espaço europeu. Entre outros objetivos, visa aumentar a cooperação entre Estados-Membros nesta matéria e criar uma cultura de segurança em sectores essenciais para a sociedade que dependam fortemente do IT.

A medida em que este assunto interessa no âmbito do tema em apreço está relacionado com o facto do Anexo II da supracitada Diretiva (e também no anexo à Lei 46/2018 de 13 de agosto) elencar os serviços designados como "essenciais" para a sociedade, e neles estarem os transportes em geral e o transporte marítimo em particular, o que inclui toda a cadeia de valor, desde o regulador aos navios, passando pelas infraestruturas portuárias e demais entidades que constituem o ecossistema desta importante área da economia Europeia e nacional.

Setores	Subsetores	Tipo de entidades
	c) Transporte marítimo e por vias navegáveis interores	- Companhias de transporte por vias navegáveis interiores, marítomo 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[2], não incluindo os navios explora dos poe 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[3], 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

Fig. 1 - As entidades da Diretiva SRI do setor do transporte marítimo

Neste enquadramento, e em grande articulação com os reguladores dos setores dos serviços essenciais, está em curso a identificação dos requisitos de segurança que cada setor deverá cumprir em alinhamento com a já referida Lei.

Dada a quantidade e diversidade de atores em jogo, designadamente no setor marítimo, julgamos que importa identificar a entidade que, em Portugal, acautelará a coordenação da operacionalização e cumprimento dos requisitos de segurança que decorrem da Lei que estabelece o regime jurídico da segurança do ciberespaço no setor marítimo. Existem vários modelos possíveis que se julga merecem reflexão ponderada e decisão atempada.

De uma coisa não nos parece restarem quaisquer dúvidas: uma vez que que mais de 80 por cento das importações e exportações nacionais são efe-

tuadas através de cinco portos nacionais e que na costa continental portuguesa navegam diariamente centenas de navios que ligam os diversos portos do Mundo, importa garantir que os sistemas de informação e comunicação, os processos e as pessoas que os gerem, operam e mantêm, formam um conjunto capacitado para fazer face a um qualquer incidente de cibersegurança que possa advir num futuro. Se tal não for o caso, não só se poderá estar a infringir a legislação nacional (e o normativo europeu), como também a impactar negativamente não só a reputação nacional, mas também um pilar relevante da atividade económica portuguesa. Como referência bastará lembrar-nos do que aconteceu em Julho de 2017 no Porto de Roterdão devido ao ciberataques que a MAERSK sofreu, que paralisou os respetivos sistemas IT durante bastante tempo, causando centenas de milhares de euros de prejuízos e tendo exigido a reinstalação de 45000 estações de trabalho e 4000 servidores nas instalações que aquela empresa detém em todo o Mundo[26].

Face ao que antecede diríamos que, o que não devemos é ignorar o que se está a passar à nossa volta no âmbito da digitalização da nossa sociedade e das oportunidades e dos riscos que tal acarreta, esperando tranquilamente que tudo continue como era dantes. Cabe, por isso, às entidades responsáveis encarar que este facto é inexorável, do qual não haverá retrocesso, agindo em conformidade com este "novo normal".

Quanto mais depressa nos convencermos do que o que acima foi descrito é uma realidade, e do facto de não estarmos imunes às ameaças perpetradas através do ciberespaço quando estamos a navegar, mais depressa desenvolveremos os necessários esforços para tirar partido das oportunidades que o imparável desenvolvimento do digital nos aporta, incluindo a capacitação para fazer face às inerentes ameaças que, por aquela via, podemos vir a enfrentar.

7. Tendências e desafios futuros

O famoso general chinês Sun Tzu, autor da obra "A Arte da Guerra" antecipou, de forma brilhante, 2500 anos antes da criação da Internet, que "*Se você conhece o inimigo e se conhece a si mesmo, não precisa recear o resultado de cem batalhas. Se você se conhece a si mesmo, mas não conhece o inimigo, por cada vitória obtida, também sofrerá uma derrota. Se você não conhece nem o inimigo nem a si mesmo, sucumbirá em todas as batalhas.*"

[26] https://www.theinquirer.net/inquirer/news/3025347/maersk-forced-to-reinstall-45-000-pcs-an-4-000-servers-following-notpetya-attack.

O constante e muitas vezes avassalador desenvolvimento tecnológico, que nos pode trazer vantagens e tornar a vida quotidiana mais facilitada, altera os nossos comportamentos e introduz novos riscos, muitas vezes consubstanciados em ameaças à nossa privacidade, num ambiente onde o inimigo não mostra a sua face e se dissimula por detrás do anonimato que o ciberespaço permite, limitando significativamente que o conheçamos, para melhor fazer face aos desafios que nos coloca. Paralelamente, com toda a informação que voluntária e involuntariamente fornecemos quando utilizamos o ciberespaço, damo-nos a conhecer de tal modo que outros nos conhecem melhor que nós nos conhecemos efetivamente[27], correndo assim o risco de, segundo Sun Tzu, perdermos todas as batalhas que travarmos no ciberespaço.

A incerteza é, assim, por paradoxo, a única certeza com que podemos contar, num ambiente de natureza cada vez mais híbrida, onde o físico e o digital se entrelaçam com fronteiras difusas e complexas de compreender para o ser humano e de onde surgem ameaças igualmente complexas[28] que importa compreender e acompanhar, quer no quadro da UE[29], quer no quadro da OTAN[30].

Neste intrincado enquadramento, com o desenvolvimento da Inteligência Artificial, das Tecnologias de Informação e Comunicação Quânticas, do Block Chain, da Internet das Coisas (IoT), do 5G e da imensidão de possibilidades que estas tecnologias criarão na sociedade, julgamos que a nosso enfoque deverá ser na procura de mecanismos para que o seu uso seja focado na prosperidade e no desenvolvimento do ser humano. O problema fulcral é que a tecnologia não conhece a Ética, mas a sociedade que hoje temos e que teremos no futuro é altamente dependente da tecnologia. Para mitigar o seu uso em prejuízo da humanidade, vários autores apelam a que seja desenvolvido um código internacional de ética digital e um quadro de regulação e de governação da Inteligência Artificial, incluindo um Conselho Ético para o Digital, eventualmente sob os auspícios da ONU, que limite o seu uso às aplicações que beneficiem a humanidade, fazendo prevalecer a vontade dos seres humanos em detrimento do poder do digital. Com efeito, quer a EU[31] quer a OCDE[32] produziram recentemente orientações desta natureza, o que, por si só, denota uma preocupação na centralidade do ser humano na utilização de tecnologias na sociedade e é um sinal positivo.

O progresso científico está a ajudar a curar doenças mortais, a alimentar uma população em crescimento, a impulsionar o crescimento económico e a aproximar empresas, comunidades, famílias e amigos. O rápido desenvolvimento das áreas tecnológicas acima referidas oferece um grande potencial para melhorar o bem-estar e gerar soluções inovadoras para os desafios globais.

---

[27] Times Magazine, 29 de janeiro de 2019.
[28] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.
[29] https://eeas.europa.eu/topics/security-defence-crisis-response/46397/joint-communication-increasing-resilience-and-bolstering-capabilities-address-hybrid-threats_en.
[30] https://www.nato.int/cps/en/natohq/topics_156338.htm.
[31] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
[32] https://www.oecd.org/going-digital/ai/principles/.

Todavia, e conforme declarado recentemente pelo SG da ONU, Eng.º António Guterres[33], "*... também devemos reconhecer as ameaças que resultam das novas tecnologias. Armas que podem identificar e matar de forma autónoma estão mais próximas de se tornarem realidade, uma inovação moralmente repugnante. As redes sociais estão a ser utilizadas para espalhar o ódio e a mentira. A tecnologia está a ser aproveitada por terroristas e redes criminosas organizadas escondem-se na dark web, aproveitando-se da criptografia e de pagamentos anónimos feitos com criptomoedas para o tráfico de pessoas e drogas ilegais*".

Preocupado com esta situação, o SG da ONU estabeleceu um Painel de Alto Nível sobre Cooperação Digital[34], que acaba de publicar o seu primeiro relatório[35].

Liderado por Melinda Gates, da Fundação Gates, e por Jack Ma, da Alibaba, o Painel reuniu diversos especialistas que recolheram opiniões em todo o mundo, analisaram um grande leque de desafios e apresentaram recomendações para aproveitar o melhor que as novas tecnologias têm para oferecer em prol da humanidade.

Com efeito, preconiza-se que as linhas que deverão ser traçadas a nível internacional deverão estabelecer limites claros entre a eficiência e os direitos liberdades e garantias dos cidadãos, entre a segurança e a privacidade, entre a superinteligência e a economia da felicidade. Por isso, devermos ser cautelosos e procurar não nos inebriar e deslumbrar com a magia de todas estas tecnologias porque, se não tivermos os pés bem assentes, corremos todos o risco de, quando acordarmos, estar num futuro que nunca desejámos.

Por outro lado, estas preocupações de natureza ética também poderão constituir uma oportunidade de diferenciação positiva para as empresas e produtos que desenvolvem e assim no modo como as mesmas serão percecionados pela sociedade e pelos potenciais clientes. Da mesma forma que, já hoje em dia, as preocupações ambientais das empresas cada vez mais contam na escolha dos clientes, num futuro, as sociedades, mais maduras e conscientes, rejeitarão as marcas que não incluam, nos seus produtos, de forma explícita preocupações de natureza societária e ética[36].

Enquanto seres inteligentes, devemos procurar que a tecnologia seja criada com um propósito, num quadro de ética que preserve a dignidade do ser humano, que tenha um intento humanista e que nos permita efetivamente conhecermo-nos melhor do que um qualquer algoritmo, possibilitando que, na lógica da reflexão de Sun Tzu, almejemos ganhar algumas das batalhas que temos que continuar a travar no ciberespaço.

A segurança, incluindo a cibersegurança, é uma responsabilidade coletiva onde todos os atores, sejam públicos ou privados, devem cooperar para que, juntos, possamos estar mais preparados para as ameaças que conhe-

[33] Conferência Mundial de Ministros Responsáveis pela Juventude 2019 e o Fórum da Juventude Lisboa + 21: https://news.un.org/pt/story/2019/06/1677521.
[34] https://www.un.org/en/digital-cooperation-panel/.
[35] https://digitalcooperation.org/panel-launches-report-recommendations/.
[36] Philip Kotler, Professor na Universidade de Harvard, no MIT e na Universidade de Chicago, defende os valores sociais como algo fundamental para as empresas, através do conceito de marketing 3.0.

cemos e sobretudo para as que desconhecemos. Cada vez mais dependemos da tecnologia para viver como vivemos. Mas não podemos deixar que seja a tecnologia a determinar como vivemos. São, sem dúvida, as pessoas que devem continuar a contar. E também devem ser as pessoas que devem determinar e marcar a diferença.

Bibliografia

RCM 92/2019 de 13 de junho – Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

Decreto-Lei n.º 69/2014 de 9 de maio (2ª alteração à Lei Orgânica do GNS - Decreto-Lei n.º 3/2012, de 16 de janeiro).

Decreto-Lei n.º 184/2014 de 29 de dezembro – Criação de Centro de Ciberdefesa (EMGFA).

Decreto-Lei n.º 81/2016 de 28 de novembro – Criação da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) da Polícia Judiciária.

Lei 46/2018 de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a UE.

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity – ENISA, 16/04/2019 – (https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity)

World Economic Forum Global Risks Report 2019 - (http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf)

Cybersecurity: What the board of directors needs to ask, The Institute of Internal Auditors Research Foundation (IIARF), 2014 (http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx)

What is a CISO responsibilities and requirements for this vital leadership role, CSO, 2019 (https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html)

First EU report on maritime cybersecurity – ENISA, 2011 (https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security

DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT)

Revista TIMES de 29 de janeiro de 2019

Future Crimes – Inside the Digital Underground and the Battle for Our Connected World, Marc Goodman, 2015

Technology versus Humanity - The Coming Clash Between Man and Machine Gerd Leonhard, 2016

CADERNOS NAVAIS

Volumes Publicados

1. **A Marinha e a Revolução nos Assuntos Militares**
   Vice-Almirante António Emílio Sacchetti

2. **Papel das Marinhas no Âmbito da Política Externa dos Estados**
   Contra-Almirante Victor Manuel Lopo Cajarabille

3. **Conceito Estratégico de Defesa Nacional**
   Vice-Almirante António Emílio Sacchetti,
   Contra-Almirante Victor Manuel Lopo Cajarabille

4. **O Contexto do Direito do Mar e a Prática da Autoridade Marítima**
   Dr. Luís da Costa Diogo

5. **Considerações sobre o Sistema de Forças Nacional**
   Vice-Almirante Alexandre Reis Rodrigues

6. **Portugal e a sua Circunstância**
   Professor Doutor Adriano Moreira,
   Vice-Almirante António Emílio Sacchetti,
   Dr. João Soares Salgueiro,
   Professora Doutora Maria do Céu Pinto,
   Professora Doutora Maria Regina Flor e Almeida

7. **O Poder Naval. Missões e Meios**
   Capitão-de-Mar-e-Guerra Carlos Nélson Lopes da Costa

8. **Sobre o Vínculo do Militar ao Estado-Nação. Breve Abordagem Filosófico-Estatutária**
   Segundo-tenente Carla Cristina Martins Pica

9. **Portugal e os EUA nas Duas Guerras Mundiais: a Procura do Plano Bi-Lateral**
   Prof. Dr. José Medeiros Ferreira

10. **A Estratégia Naval Portuguesa**
    Vice-Almirante António Emílio Sacchetti,
    Professor Doutor António José Telo,
    Vice-Almirante Magalhães Queiroz,
    Almirante Vieira Matias,
    Contra-Almirante Lopo Cajarabille,
    Capitão-de-fragata Marques Antunes,

Dr. Nuno Rogeiro,
Vice-Almirante Ferreira Barbosa,
Dr. Tiago Pitta e Cunha,
Vice-Almirante Reis Rodrigues,
Contra-Almirante Melo Gomes,
Vice-Almirante Alexandre Silva Fonseca,
Vice-Almirante Pires Neves,
Vice-Almirante Rebelo Duarte

11. **O Direito Humanitário, as Regras de Empenhamento e a Condução das Operações Militares**
Capitão-de-Mar-e-Guerra José Manuel Silva Carreira

12. **As Forças Armadas e o Terrorismo**
Contra-Almirante José Augusto de Brito

13. **O Mar, um Oceano de Oportunidades para Portugal**
Almirante Vieira Matias

14. **Opções Estratégicas de Portugal no Novo Contexto Mundial**
Professor Doutor Ernani Lopes,
Professor Doutor Manuel Lopes Porto,
Dr. João Salgueiro,
Professor Doutor José Carlos Venâncio,
Dr. Salgado Matos,
Dr. Félix Ribeiro,
Professor Doutor Fernando Santos Neves,
Dr. Joaquim Aguiar,
Professor Doutor Adriano Moreira

15. **A Security em âmbito marítimo. O Código ISPS**
Dr. Luís Manuel Gomes da Costa Diogo,
Capitão-tenente José António Velho Gouveia

16. **O Mediterrâneo, Geopolítica e Segurança Europeia**
Vice-Almirante António Emílio Ferraz Sacchetti

17. **As Grandes Linhas Geopolíticas e Geoestratégicas da Guerra e da Paz**
Capitão-tenente José António Zeferino Henriques

18. **A NATO e a Política Europeia de Segurança e Defesa. Em Colisão ou em Convergência?**
Vice-Almirante Alexandre Reis Rodrigues

19. **Segurança e Cidadania. Conceitos e Políticas**
Dr. António Jorge de Figueiredo Lopes

20. Continentalidade e Maritimidade
A Política Externa dos Impérios e a Política Externa da China
Professor Doutor António Marques Bessa

21. O Poder na Relação Externa do Estado
Professor Doutor Luís Fontoura,
Embaixador Leonardo Mathias

22. Seminário "Uma Marinha de Duplo Uso"
Intervenções dos Conferencistas

23. A Definição de Agressão da Assembleia-Geral das Nações Unidas: História de uma Negociação
Dr.ª Maria Francisca Saraiva

24. Uma Visão Estratégica do Mar na Geopolítica do Atlântico Coordenadores:
Professor Doutor António Marques Bessa,
Professor Doutor Pedro Borges Graça

25. A Europa da Segurança e Defesa
Vice-Almirante António Rebelo Duarte

26. 1º Simpósio das Marinhas dos Países de Língua Portuguesa

27. Formulação da Estratégia Naval Portuguesa. Modelo e processo
Contra-Almirante António Silva Ribeiro

28. O Sistema de Planeamento de Forças Nacional. Implicações da Adopção do Modelo de Planeamento por Capacidades.
Capitão-de-Mar-e-Guerra Carlos César Martinho Gusmão Reis Madeira

29. Reflexões sobre o Mar
Uma Homenagem ao Vice-Almirante António Emílio Ferraz Sacchetti
Almirante Fernando Melo Gomes,
Professor Doutor Adriano Moreira,
Vice-Almirante António Ferraz Sacchetti,
Almirante Nuno Vieira Matias,
Vice-Almirante Victor Lopo Cajarabille

30. A "Guerra às Drogas"
Capitão-de-Mar-e-Guerra J. Margalho Carrilho

31. Contributos para uma caracterização da Geopolítica Marítima de Portugal
Primeiro-tenente Humberto Santos Rocha

32. 60 anos da Aliança Atlântica. Perspectivas navais
Almirante Fernando José Ribeiro de Melo Gomes,
Vice-Almirante José Carlos Lima Bacelar

33. A Plataforma Continental Portuguesa e o Hypercluster do Mar
Vice-Almirante Victor Lopo Cajarabille,
Vice-Almirante António Rebelo Duarte,
Dr.ª Patrícia Viana Afonso

34. Estratégia Naval Portuguesa - O processo, o contexto e o conteúdo
Contra-Almirante António Silva Ribeiro,
Capitão-de-Mar-e-Guerra Francisco Braz da Silva,
Capitão-de-Mar-e-Guerra Jorge Novo Palma,
Capitão-de-fragata Nuno Sardinha Monteiro

35. O Papel da União Europeia e da União Africana na Prevenção e Gestão de Conflitos em África
Capitão-de-Mar-e-Guerra Edgar Marcos Bastos Ribeiro

36. Oxigénio e medicina subaquática e hiperbárica. Perspectiva histórica e realidade militar em Portugal
Capitão-de-Mar-e-Guerra José de Gouveia de Albuquerque e Sousa

37. Liderança e exercício de comando contributos
Capitão-de-Mar-e-Guerra Francisco José Costa Pereira,
Capitão-de-Mar-e-Guerra Henrique Eduardo de Gouveia e Melo,
Capitão-tenente Pedro Eduardo Fernandes Fonseca

38. O Papel das Forças Armadas nas Operações Inter-Agências de Combate às Ameaças Emergentes em Portugal
Capitão-de-Mar-e-Guerra Jorge Novo Palma

39. Espaços Marítimos sob Soberania ou Jurisdição Nacional. Um Modelo para Potenciar o Exercício da Autoridade do Estado no Mar
Capitão-de-Mar-e-Guerra António Manuel de Carvalho Coelho Cândido

40. Os Media como Vectores na Prossecução dos Objectivos Estratégicos das Forças Armadas
Capitão-de-Mar-e-Guerra Vladimiro José das Neves Coelho

41. O combate à pirataria marítima
Vice-almirante Alexandre Daniel Cunha Reis Rodrigues

42. Conceitos e Tecnologia das Operações Navais: da II Guerra Mundial aos nossos dias
Almirante Fernando José Ribeiro de Melo Gomes,
Capitão-de-fragata Armando José Dias Correia

43. A Plataforma Continental Portuguesa. Análise do Processo de Transformação do Potencial Estratégico em Poder Nacional
Capitão-tenente Jaime Carlos de Vale Ferreira da Silva

44. A Maritimidade Portuguesa: Do Reavaliar da Consciência à Oportunidade de Desenvolvimento
Vice-almirante Ref João Manuel Lopes Pires Neves,
Vice-Almirante Ref António Carlos Rebelo Duarte

45. Mahan. 7 Virtudes e 7 Pecados
Capitão-de-fragata Nuno Sardinha Monteiro

46. O Processo Estratégico na Marinha
Almirante António Silva Ribeiro

47. Vis per Mare
Breve análise das obras de alguns autores contemporâneos sobre poder no mar
Capitão-de-mar-e-guerra Nuno Sardinha Monteiro

48. Políticas e Estratégias Marítimas da Europa e de Portugal
Vice-Almirante Ref. António Carlos Rebelo Duarte

49. Centro de Decisão de Alcance Global em Contexto Marítimo
Dr. Miguel Marques

50. O mar em perspetiva
Professor Doutor Adriano Moreira

51. Portugal, como potência costeira
Vice-almirante Alexandre Reis Rodrigues

Nota: Os Cadernos Navais encontram-se disponíveis na internet, no portal da Marinha, sob o título Estudos e Reflexões: http://www.marinha.pt/pt/a-marinha/estudos-e-reflexoes/cadernos-navais/Paginas/default.aspx


COMISSÃO CULTURAL DA MARINHA