O posicionamento estratégico de Portugal na rede global de informações. Contributos para o Conceito Estratégico de Defesa Nacional

Coronel
Luís Manuel Brás Bernardino

"Considerando que o objetivo de Portugal integrar a rede mundial de cabos submarinos de fibra ótica consta expressamente do Programa Nacional da Política de Ordenamento do Território (medida 4.8), no qual se reconhece que, com a sua inclusão neste sistema internacional de telecomunicações, «*Portugal pode ganhar competitividade com a sua posição geoestratégica na rede mundial de autoestradas marítimas de fibra ótica, acrescentando valor à grande quantidade de dados de informação que vão chegar de outros países e continentes*»…".

Despacho n.º 1653/2024, de 12 de fevereiro, publicado no

Diário da República n.º 30/2024, Série II de 2024-02-12, pp. 26-27.

Introdução*

O contexto geopolítico atual caracteriza-se pela prevalência da inconstância, imprevisibilidade e da volatilidade na relação entre os múltiplos atores do Sistema Político Internacional. Um paradigma securitário complexo que impele os Estados a apostarem na segurança (e na Defesa Nacional) como forma de analisar, compreender e

prevenir o futuro, procurando antecipar hipotéticas soluções para hipotéticas ameaças à nossa sociedade… nem sempre possível. Para Portugal e no quadro da sua Política de Defesa Nacional, temos vindo a assistir a uma discussão em torno do "novo" Conceito Estratégico de Defesa Nacional (CEDN) e também a uma reflexão, sempre necessária e oportuna, sobre o posicionamento geoestratégico de Portugal na Europa e no Mundo, bem como a relação geopolítica com as novas e velhas alianças.

Contudo, nem sempre, esta discussão teve em conta, adequadamente, alguns dos novos paradigmas da modernidade, nomeadamente a problemática do ciberespaço e da inteligência artificial e mais em concreto, o acesso às redes globais de informação e muito em particular, sobre a relevância e dependência das infraestruturas críticas digitais que estão associadas à rede de cabos submarinos e à informação (e conhecimento) que circulam globalmente nestas infraestruturas. Portugal é neste domínio o exemplo de um Estado que está no centro geoestratégico da revolução global das redes de informação e que porventura não terá ainda percebido, convenientemente, quais as principais oportunidades e desafios que se colocam à Defesa Nacional e quais as soluções que temos de encontrar para fazer face aos "novos" riscos e ameaças à nossa sociedade.

Assim, importa salientar que a convergência de tecnologias e de serviços analógico-digital com protocolos IP, contribuiu para alavancar a dependência económica global da internet (*internet of things*) e permitiu a massificação dos serviços de streaming, *video on demand* e *cloud computing*. Como referência, importaria destacar os seguintes indicadores da relevância da comunicação por cabos nos nossos dias: Entre 2010-2023, o número de utilizadores de internet mais que duplicou, tendo passado de 2 para 5 mil milhões; em 2011, o tempo médio gasto por pessoa na internet/dia era de 1,25 horas e em 2017 passou para 3 horas, sendo atualmente o dobro. Entre 2015-2023, o armazenamento em centro de dados aumentou em cerca de 600%, o que é demonstrativo da relevância do sistema de cabos nas redes de comunicação globais e da economia de dados associado à criação e gestão de centro de dados como parte de um ecossistema digital.

Neste contexto, procurando contribuir com esta investigação para um debate nacional, esta reflexão académica tem como objetivos principais, por um lado, refletir e analisar sobre a temática da rede global de informação e por outro, aprofundar o conhecimento sobre os cabos submarinos como infraestruturas críticas digital neste contexto. Procuramos assim identificar os principais desafios e oportunidades para a Política de Defesa Nacional resultantes do posicionamento geoestratégico de Portugal. Neste contexto, a pergunta que enquadra esta análise é saber: Quais os principais desafios e oportunidades para a Defesa Nacional que decorrem do posicionamento geoestratégico de Portugal na rede global de cabos submarinos?

A hipótese geral que tentaremos validar aponta para que Portugal poderá beneficiar, por via da sua posição geoestratégica favorável como um dos principais *hub* de comunicação global, de um conjunto de vantagens de índole económico-financeira e político-diplomática. Mas que também irá enfrentar alguns riscos acrescidos derivado do

potencial afluxo de poderes erráticos que procuram tirar vantagem das fragilidades dos sistemas de gestão da informação e das dificuldades em garantir uma adequada segurança e proteção às infraestruturas críticas digitais como são as redes de cabos submarinos e os centros de dados.

Neste inovador contexto geopolítico e geoestratégico, em que Portugal se enquadra, e quando discutimos o "novo" Conceito Estratégico de Defesa Nacional, parece-nos fazer sentido apresentar esta temática como tema de debate e a inclusão num artigo académico que nos dê pistas para um futuro melhor para Portugal e para os Portugueses.

1. A Rede Global de Informação e os Cabos Submarinos

Este capítulo pretende contribuir para uma clarificação de conceitos entre o que se entende por *global network* e a gestão de redes de informação que consubstanciam a razão da existência dos centros de dados e a utilização dos cabos submarinos como veículo privilegiado de conexão global no mundo informacional. Procuramos ainda proporcionar um enquadramento técnico sobre o funcionamento do sistema de cabos submarinos e procurar associar aos conceitos definidos, a principal legislação respeitante à temática das infraestruturas críticas e nomeadamente sobre os cabos submarinos e os centros de dados.

A rede global de informação permite-nos estar presente, virtualmente, em todo o lugar e em todo o tempo, possibilitando-nos a todos, aceder à informação em tempo real e possibilita-nos estarmos inseridos nos processos de globalização. Mas na realidade o que significa, qual a sua real abrangência e qual a relação com as redes de cabos submarinos como parte de um ecossistema digital?

Importa definir alguns conceitos que contribuem para melhor compreender a temática. Nomeadamente o conceito de "network" que é a designação que se utiliza, recorrentemente, para definir uma rede de contatos profissionais de grupos de pessoas conectadas remotamente por interesses similares a fim de potenciarem os negócios ou proveitos individuais. Apesar de o termo ser normalmente utilizado em inglês, este está designado ao esforço coletivo para aperfeiçoar o conhecimento e expandir os negócios numa dada conjuntura, ou no seu máximo alcance, numa dimensão planetária, sendo assim designado de "*global network*".

Esta rede global de contactos e de atividades combinam-se nas redes de internet e permitem fazer negócios ou manter relações numa dimensão global à velocidade da luz, usando para o efeito as redes de informações. Robert Half, numa perspetiva mais coerente, salienta que networking significa "…formar e manter uma rede de contatos profissionais, sendo uma maneira de se conectar a outros profissionais que possam ser interessantes para a sua carreira, ou seja, gerar indicações para futuros trabalhos ou mesmo para trocar ideias…" (2021).

Igualmente, mas numa dimensão maior, as Organizações/Empresas e principalmente os Estados, também pretendem exercer influência através do *networking*, impondo regras e normativos que regulam técnica e tecnologicamente o acesso às redes de comunicação globais e que lhes permite tirar vantagens… o que, aplicado à fórmula de perceção do poder dos Estados de Ray Cline, significa que este acesso lhes confere um poder acrescido e, atualmente, o acesso ao designado "poder decisivo"1.

Esta é uma problemática que coloca as redes globais de informação no centro da luta pela influência global e na procura de afirmação das capacidades que cada Estado terá de possuir para poder controlar melhor a informação (e conhecimento) e consequentemente o acesso às redes globais de informação. Este novo paradigma de controlo das redes de comunicação globais tem levado os Estados e as Organizações a desenvolverem estratégias de desenvolvimento tecnológico e a apostar na expansão dos domínios de ação que passa agora pelo espaço e pelo ciberespaço; e na dimensão aérea, terrestre e marítima, cada vez mais relevante, através dos cabos submarinos, onde a conectividade pelo mares e oceanos, se tornaram verdadeiras autoestradas da informação e do conhecimento, tendo-se constituído num fator geopolítico e geoestratégico relevante para as Organizações e para os Estados.

O conceito de "*networking*" evoluiu de uma rede de contactos profissionais e pessoais assente numa plataforma informática tipo *LinkedIn* (designada de social *networking*) e generalizou-se, passando a designar, genericamente, um processo de promoção de troca de informações e de ideias entre indivíduos e grupos com interesses em comum, sejam eles sociais ou profissionais, o que em termos académicos é definido como "…o processo de conhecer e conversar com muitas pessoas, a fim de obter informações que possam ser úteis e necessárias…" (2023). Atualmente, tornou-se mais amplo no seu significado e passou a estar associado às redes de informações globais, ligando Estados e Organizações/Empresas, abrangendo o mundo económico, financeiro e especialmente da segurança e defesa, que é o objeto deste ensaio académico.

O processo de globalização deu um contributo significativo para o *networking*, que se transformou num dos principais veículos de difusão da informação e central no processo de globalização. Por outro lado, a informação que circula nas *networks* globais necessita de ser armazenada num determinado local, não só por motivos de segurança, como porque o *backup* de determinada informação é essencial para Estados e Organizações/Empresas, bem como para as pessoas em geral. Os sistemas virtuais de armazenamento de dados a que designamos comummente por "*cloud* " estão associados a um local físico que armazena dados em máquinas de computação e dispõem de equipamentos de *hardware* relacionados a que designamos por "*Data Center* " ou centros de dados e que corresponde, em geral, a mega centrais de processamento de dados e gestão da informação que consubstancia o ecossistema digital.

Os centros de dados fazem parte do sistema de informações globais e contém a infraestrutura de computação que os sistemas de tecnologia de informática exigem, nomeadamente: servidores, unidades de armazenamento de dados e equipamentos de rede, bem ainda como sistemas de fornecimento de energia e de arrefecimento, o que

conferem a estas infraestruturas as características que iremos encontrar para as definir como infraestruturas críticas digitais.

2. Infraestruturas Críticas. Conceito e Legislação

Consideram-se, em regra, infraestruturas críticas como as instalações físicas, os serviços fornecidos, os bens e sistemas cuja incapacitação parcial ou destruição total podem provocar uma disrupção político-social, ambiental, económico-financeiro, ou à segurança do Estado e da sociedade no geral, necessitando, por norma, de medidas adicionais e meios especiais de proteção. Uma infraestrutura crítica, de acordo com o Decreto-Lei n.º 62/2011[2] de 9 de maio, entende-se globalmente como a componente, sistema ou parte deste, situado em território nacional que é fundamental para assegurar as funções essências na sociedade, e cuja inoperacionalidade teria um impacto significativo nas atividades do Estado e da sociedade.

O artº 2.º do supracitado Decreto-Lei, apresenta-nos uma definição concreta de Infraestruturas Críticas Nacional (ICN), entendendo-se como "…componente, sistema ou parte deste situado em território nacional, que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções…" e daí derivando o conceito inovador de "Infraestrutura Crítica Europeia" (ICE), entendida como a "…infraestrutura crítica situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado membro da UE, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas…" (2011).

Christian Bueger e Tobias Liebetrau corroboram, no geral, com esta definição de infraestrutura crítica e concretizam relativamente aos cabos submarinos que os:

> "…submarine data cables are the core critical infrastructure of the digital age.750,000 miles of cable connect the continents to support our unquenchable demand for digital communication…" e ainda que "…there seems little doubt that the data cable network is a vital critical infrastructure for contemporary and future economies and public life…" (2021, p. 391).

Como temos visto, a guerra na Ucrânia motivou um redobrado interesse global pela temática dos cabos submarinos e especialmente pela sua segurança, como infraestrutura crítica, pois que num passado recente, tem havido disrupções complexas com impacto nesses países e com incidência europeia e global. Mais recentemente registaram-se incidentes com cabos submarinos no Mar Báltico, mas existem registos anteriores de Marselha (França), um importante ponto de amarração para a Europa, e no norte da Escócia (Reino Unido) um importante ponto de ligação Europa-América e que os cabos submarinos, onde passa cerca de 98% da informação global intercontinental (o sistema de comunicação satélite é residual), tornaram-se um alvo remunerador para as grandes potências globais no sentido de quererem controlar a informação que aí circula e

condicionar o poder de decisão global. Por estes motivos, estas infraestruturas simbolizam e garantem a soberania do Estado, congregando os requisitos essências para que devam ser consideradas infraestruturas críticas no âmbito da segurança nacional e estudados no âmbito dos documentos estruturantes nacionais da Defesa Nacional.

Em Portugal, mais recentemente, o Decreto-Lei 20/2022, de 28 de janeiro, reajusta a legislação e aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias3. Estas infraestruturas passaram a ter um estatuto especial no âmbito das preocupações de segurança nacionais, à semelhança do que se passou um pouco por todo o mundo e especialmente na Europa, "obrigando" os países da UE a adotarem medidas de catalogação, gestão e proteção especiais para as infraestruturas críticas e de entre elas os cabos submarinos e as infraestruturas conexas, como os Data Center e os equipamentos que fornecem energia no que se designa por ecossistema digital.

3. Os Cabos Submarinos

Os cabos submarinos tiveram a sua origem no telégrafo (1845), nomeadamente quando a partir da rede em terra se tornou necessário atravessar o Oceano Atlântico, estabelecendo uma rede de comunicações permanente entre a Europa e a América. O primeiro cabo submarino ótico amarrado em Portugal data de 1992 e foi designado por "EURAFRICA", consistindo num sistema de configuração multiponto criando uma rede que unia Portugal (Continental), Madeira, Marrocos e França. Atualmente, um sistema de cabos submarino ótico com capacidade de transmissão de um terabit, suporta 10 mil milhões de conversas telefónicas simultâneas ou o download do conteúdo de 5 milhões de livros por segundo, e que irá crescer exponencialmente em virtude do uso do 5G e do 6G e especialmente pelo uso de inteligência artificial nas nossas atividades diárias.

Nos nossos dias, mais de 650 cabos submarinos óticos totalizando meio milhão de quilómetros atravessam os oceanos e os mares, onde Portugal, continua a ser um dos poucos países do mundo ligado por um cabo submarino direto com todos os continentes (exceto a Antártida) e acresce que na nossa Zona Económica Exclusiva (ZEE), passam cerca de 15 a 20% da rede global de cabos submarinos com possibilidade de crescimento (figura 1).

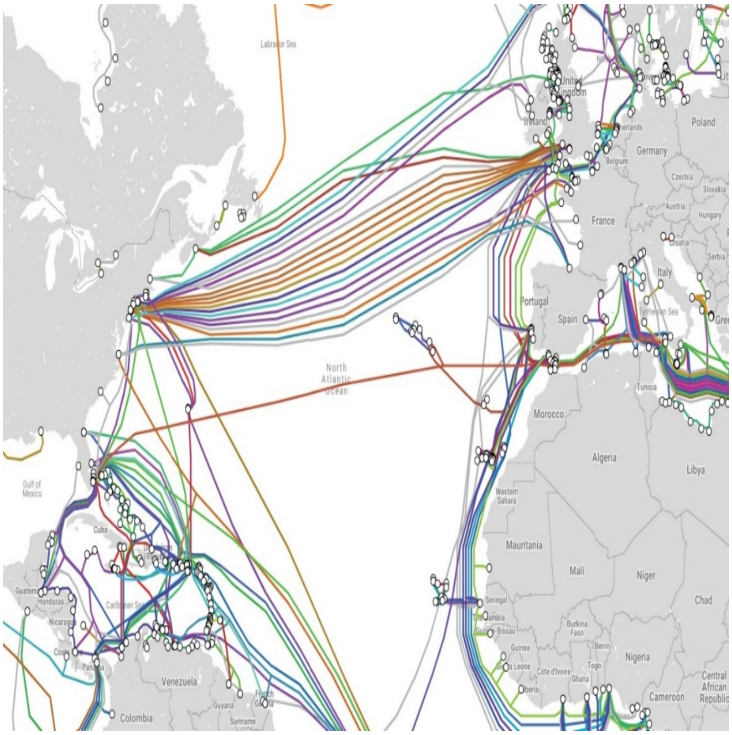

Figura 1 – Rede de Cabos Submarinos que cruza a Zona Economia Exclusiva de Portugal (2023).

Fonte: Submarine Cable Map[4]

Salienta-se que atualmente, podemos constatar que a quase totalidade das telecomunicações internacionais (98%) digitais, incluindo o fluxo de dados, é feito pela via digital utilizando fibra ótica, o que veio a possibilitar a comunicação em tempo real e a transferência de grande volume de dados quase instantaneamente e em segurança. Muitas destas redes são geridas globalmente por empresas de telecomunicações que usam os cabos submarinos com centrais de amarração em terra, como veículos essenciais na comunicação global, com implicações na segurança nacional e global. A expansão dos cabos submarinos neste contexto é significativa e representa uma realidade crescente para Portugal e para um mundo globalizado.

Um sistema de cabos submarinos conecta pela via subterrânea marítima duas ou mais regiões (continentes), designadas por "*landing stations*", integrando infraestruturas significativas nos pontos de amarração e normalmente associados a terminais de centros de dados, tornando estas infraestruturas vitais em termos de conectividade global e de acesso à informação. Motivo pelo qual são, em regra, áreas protegidas e com elevado grau de proteção e secretismo, onde a tecnologia e a energia de ponta se ligam com um desenvolvimento tecnológico constante e uma necessidade de segurança permanente e muito específica no contexto das infraestruturas críticas digitais.

Os cabos submarinos contêm sistemas de fibra ótica protegida e preparada para operar em sistemas de alta pressão, detendo um sistema de alimentação próprio e um conjunto

de repetidores que tornam possível a deteção exata quando existe uma rotura no cabo afetando a fibra ótica… o que também cria enormes desafios para os Estados, mas que pode ainda contribuir para a segurança marítima, nomeadamente através da vigilância e monitorização dos espaços marítimos profundos como podemos constatar com a tecnologia *Science Monitoring And Reliable Telecommunications* (SMART) ou conhecida por *SMART Cable* (Barros e Bernardino, 2023).

Os sistemas de cabos submarinos têm, pela sua especificidade tecnológica e relevância geoestratégica, um impacto económico significativo para os Estados e para as Organizações/Empresas. Impacto que segundo a metodologia económica adotada pela *Swedish Agency for Public Management de Copenhaga*5 se obtém através da soma de determinados fatores multiplicadores, nomeadamente: o investimento, produtividade, comércio e o impacto económico visto numa perspetiva social6. Em Portugal, segundo os autores do estudo para a Google, Bruno Basalisco e Morten Hanseno, salientam que o investimento em Sines no cabo "EQUIANO" poderá, segundo o gestor do *Sines Atlantic Hub Project*, ter um impacto imediato de 2,7 mil milhões de euros, o que corresponde a um incremento direto de 1 a 2% no PIB Português a valores de 2022. Este impacto decorre de vários indicadores económicos fundamentais tais como o impacto no comércio, pois que o cabo submarino "EQUIANO" que liga a Europa a África reduz o custo dos fluxos comerciais entre estes continentes e reduz as barreiras ao comércio, permitindo que mais empresas portuguesas (europeias) comercializem com África e com o mundo. No futuro, outras ligações ou cabos submarinos, tais como o "2AFRICA" ou o "NUVEM", irão revolucionar este paradigma e colocar Portugal no centro do trafico global digital dos *hyperscalers*.

Tem também um impacto significativo no investimento, pois espera-se que este cabo submarino, tenha consequências positivas nos investimentos diretos estrangeiros que se espera venham para Portugal, uma vez que Portugal se tornará, previsivelmente, num local de investimento mais atrativo como uma porta de entrada digital para a Europa e com impacto na produtividade, pois que as principais infraestruturas digitais, permitem e suportam possibilidades de teletrabalho e reuniões online, maximizando assim o tempo de trabalho e tendo consequências positivas para as pessoas, empresas e para o Estado (Basalisco e Hanseno, 2021).

4. A relevância do posicionamento de Portugal na rede global de cabos submarinos

Como vimos, a independência do país está também ligada à internacionalização das suas comunicações, isto é, na capacidade de comunicar internacionalmente, e quanto mais escolha e diversidade houver mais independentes seremos. Quer isto dizer que não estamos dependentes de um único fornecedor, e teremos mais escolhas possíveis em termos comerciais, de qualidade, em quantidade e em termos de segurança… é o mercado livre a funcionar. O que se pretende é gerar oportunidades e encontrar em

Portugal espaços e dinâmicas de investimento que possam contribuir para que este nosso posicionamento na rede global de informações possa ser benéfico para a economia portuguesa… e Sines tem, segundo os especialistas, potencial para gerar este efeito positivo.

Como sabemos, vivemos num mundo global e crescentemente globalizado. A globalização desafiou-nos a estarmos mais perto, mais ligados, interconectados e mais interdependentes, mesmo estando geograficamente mais longe. A distância deixou de ser medida em metros, milhas ou quilómetros para ser estimada em microssegundos, em segundos e percecionada à velocidade da luz…pois a *internet* e a fibra ótica aproximaram as dimensões tempo e espaço, e potenciaram o fluxo global de informações, relativizando o poder dos Estados e das Empresas/Organizações. Esta interdependência e interconetividade é atualmente bem evidente na rede global de internet e no fluxo de dados que conseguimos gerir através dos centros de dados e das empresas que providenciam serviços de *internet* à escala global, conferindo um conjunto de oportunidades e desafios que estão associados à centralidade da Europa no Mundo e de Portugal na Europa e no Mundo.

Portugal, pelo seu posicionamento geográfico privilegiado na confluência entre a Europa, América e África, tendo o mar como veículo de comunicação e estando integrado em organizações internacionais que simbolizam esta trilogia, foi desde sempre um facilitador e um dinamizador das redes globais e da globalização. Para não recuarmos tão longe, à época das epopeias marítimas, dos descobrimentos e dos navegadores que cruzaram os mares a partir de Lisboa, podemos constatar que Portugal foi, na telegrafia e na criação de redes globais de telégrafos e na telefonia um pioneiro, muito também devido ao nosso posicionamento geoestratégico no triângulo virtuoso Europa-América-África. Mais recentemente, a ligação marítima transatlântica e ainda mais recentemente, a amarração de cabos de fibra ótica em terra e a difusão por mar dos cabos submarinos digitais veio evidenciar, novamente, a nossa relevância geoestratégica na rede global de informações (figura 2).

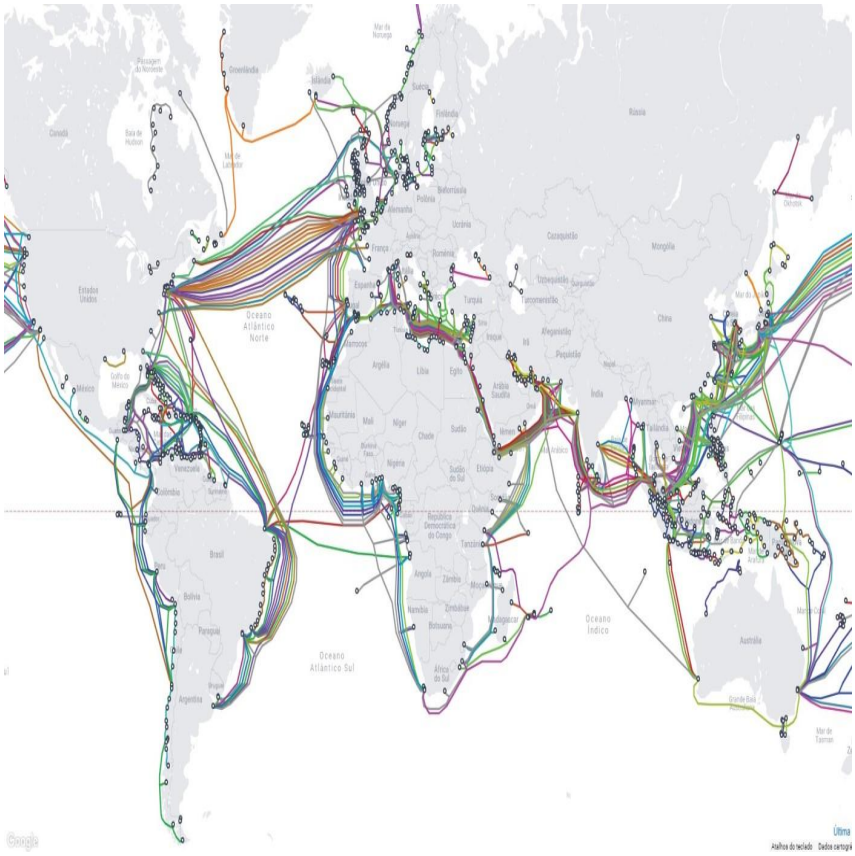

Figura 2 – Portugal e a Rede Global de Cabos Submarinos (2023).

Fonte: Submarine Cable Map

Sabemos que Portugal sempre foi relevante nas redes mundiais de telecomunicações, pois tem uma posição geoestratégica favorável em termos globais que ganhou ainda maior relevância com a saída do Reino Unido da UE, com alguns promotores a querem rotas que evitem jurisdições complementares, no caso as da UE. Até porque o Reino Unido deixou de ser uma opção para as empresas europeias que têm uma legislação própria e obedecem a critérios normativos europeus muito mais exigentes. Portugal tem uma posição geoestratégica favorável para amarração de cabos que venham do Atlântico Norte e Sul para a ligação à Europa, e sabemos que para tirar vantagem económica, o importante não é apenas a amarração, mas tudo o que é possível fazer com centros de dados e o consequente impacto económico para o país.

Esse é um dos nossos maiores desafios, fazer com que Portugal não seja apenas uma "praia" ibérica e europeia para amarração de cabos submarinos que fique a ver passar cabos, mas sim o local onde se faz o *split* do cabo (processamento), o que permite o desenvolvimento de um ecossistema de centros de armazenamento e gestão de dados – logística de dados. Portugal pode tornar-se efetivamente num país atrativo ao nível da designada "Economia de Dados". Esta dinâmica está a acontecer em Portugal e um dos principais exemplos é a amarração do cabo EllaLink em Sines e o EQUIANO da Google

em Sesimbra, que trouxeram um forte aumento da disponibilidade de *internet* em Portugal. Com um contributo potencialmente significativo para o PIB nacional e para o crescimento económico, nomeadamente para a logística e economia de dados.

Esta posição geoestratégica global e prioritária de Portugal no espaço europeu, é para Patrick Christian um elemento potenciador da capacidade nacional de integrar megaprojetos de *data center*, de empresas de *hi-tec* e de centrais de amarração de cabos com ligação a cabos submarinos que ligam, por fibra ótica, os principais sistemas de dados globais, com impacto nos mercados de capitais, na geoeconomia e no mundo das finanças, na esfera das informações e no acesso às bases de dados e especialmente nas políticas de defesa nacional.

Tendo em conta este posicionamento geoestratégico conjunturalmente muito favorável de Portugal na rede global de informações, a criação de um consórcio para a construção de um complexo de amarração de cabos submarinos em Sines, designado por "*Sines Submarine Cable Hub Project*", ligando Europa-África-América, apresenta-se como um investimento estratégico que irá contribuir para colocar Portugal no centro da gestão de dados global, com impacto ao nível da economia interna.

Os cabos submarinos e os centros de dados são, como vimos, consideradas infraestruturas críticas e tal como em Sines, estão ligados à conectividade do país e ao abastecimento de energia, tornando-se relevante para a Segurança Nacional. Parece evidente que Portugal necessite de ter os seus portos protegidos e seguros, nomeadamente o Porto de Sines, pois é o único porto em Portugal onde entra crude e gás natural, e seria necessário criar redundâncias na conectividade e no abastecimento, contribuindo para a Segurança Nacional, assunto a que dedicaremos especial atenção no capítulo seguinte com detalhe sobre os sistemas de cabos submarinos e infraestruturas conexas.

5. Cabos Submarinos: Implicações para a Defesa Nacional

Neste capítulo, dedicado à segurança dos cabos submarinos e implicações para a segurança e defesa nacional, pretendemos, depois de definidos os conceitos base e de algum aprofundamento geoestratégico sobre o posicionamento de Portugal na rede global de cabos submarinos, identificar algumas oportunidades e também alguns riscos, aferindo as principais implicações para a segurança física e para a cibersegurança destas infraestruturas críticas que são os cabos submarinos digitais e estruturas conexas. Em suma, pretende-se analisar o que Portugal está a fazer neste domínio e procurar determinar possíveis contributos para a Política de Defesa Nacional e em concreto para o Conceito Estratégico de Defesa Nacional em revisão.

O tema da segurança internacional dos cabos submarinos há muito tempo que é abordado e discutido, nomeadamente numa organização internacional que é o

International Cable Protection Committee (ICPC). Organização Internacional com 40 anos em que os seus membros são investidores, operadores de cabos, representantes de governos, Marinhas, reguladores, consultores, armadores, etc., e onde se discute e se partilham informações sobre a segurança dos cabos submarinos. Este organismo internacional, que está localizado em Londres, é um órgão agregador, realiza análises, produz sugestões e faz recomendações sobre a segurança dos cabos submarinos, é neste fórum onde se aprende e também se faz *networking* sobre esta temática. Neste contexto, a representação de Portugal está na incumbência da AICEP, o que nos remete para algumas dúvidas dado nos parecer que seria mais adequado estar também no contexto dos organismos responsáveis pela segurança e defesa nacional.

Mais recentemente, a guerra Rússia-Ucrânia motivou um redobrado interesse global pela temática dos cabos submarinos e especialmente pela sua segurança. Na imprensa nacional, salienta-se ainda o artigo do jornalista Vitor Matos, publicado em 26 de maio de 2023 no Jornal Expresso, onde o autor dedica uma página à temática da proteção dos cabos submarinos e a falta de meios em Portugal para garantir uma adequada segurança a estas infraestruturas críticas que proliferam na nossa ZEE. Em complemento, num passado recente, deram-se várias disrupções complexas com impacto nesses países e com incidência global, nomeadamente em Marselha (França), um importante ponto de amarração para a Europa, no Mar Báltico e na ligação entre a Suécia e a Noruega, e no norte da Escócia (Reino Unido) um importante ponto de ligação Europa-América.

Os cabos submarinos, onde circula cerca de 98% da informação global intercontinental tornou-se assim um alvo apetecível para as grandes potências globais no sentido de quererem controlar a informação que aí circula e condicionar o poder de decisão global. Estes são apenas alguns exemplos recentes que nos "obrigam" a ter uma outra atitude de segurança relativamente aos cabos submarinos em Portugal e na relação com os diferentes pontos do globo (Bueger, Liebetrau e Franken, 2022, p. 9).

Portugal é, como vimos, um dos principais países da Europa onde derivam cabos submarinos para todos os continentes, incluindo, o único cabo submarino que liga a Europa-Brasil (América do Sul) – EllaLink. O território nacional, morfologicamente, tem águas mais profundas junto da costa, com condições ideais para construir e operar pontos de amarração, e ligação em terra que podem ser centros de dados ou outras derivações, tornando estas condições muito apetecíveis para empresas multinacionais, mas que exigem condições de segurança adequadas, pois sem essas garantias os investimentos também não irão acontecer.

Neste contexto e sabendo que muitos dos cabos passam na nossa ZEE, temos sido confrontados com a presença de navios de outros países, nomeadamente da Federação Russa, "supostamente" em transito e nem sempre conhecidos, que conduzem "supostamente" operações para monitorizar e confirmar essa localização. Estas atividades suspeitas, têm desde 2018 aumentado substancialmente, especialmente de navios da Rússia que adquiriram capacidades especificas para operar sobre os cabos submarinos, como se constata, pois que:

> "…Russia snipping a handful of cables in the Atlantic, where its submarines have been spotted, would disturb the global internet very little…" e "…the world's internet infrastructure is vulnerable, but snipping a couple of lines is the least of your concerns…" (Matsakis, 2018).

Estamos perante um novo desafio de segurança global, um problema recente no Mar Báltico, que ficou ainda mais evidente com a guerra Rússia-Ucrânia e os problemas com as sabotagens à rede de abastecimento de gás (nomeadamente no mar) e que veio alertar governos para a necessidade de reforçar a segurança nestas infraestruturas críticas e apostar mais na segurança marítima e na cibersegurança.

Em Portugal, o Decreto-Lei 20/2022, de 28 de janeiro, define os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias e no artº 6º estabelece que a identificação e a designação das infraestruturas críticas são efetuadas pelo Conselho Nacional de Planeamento Civil de Emergência (CNPCE). Em termos de metodologia, o seu art.º 10.º define que as "…entidades setoriais elaboram uma lista das infraestruturas do respetivo setor com potencial para serem designadas como infraestruturas críticas nacionais, efetuando uma apreciação qualitativa das consequências provocadas pela inoperacionalidade de cada infraestrutura…", tendo por base três critérios: impacto económico, estimado em termos de importância dos prejuízos económicos e da degradação de bens ou serviços, incluindo também os potenciais efeitos ambientais; impacto na sociedade, avaliado em termos de impacto na soberania nacional, na confiança das populações e na perturbação da vida quotidiana, incluindo a perda de serviços essenciais; e a possibilidade de ocorrência de acidentes, avaliada em termos de número potencial de feridos ou vítimas mortais.

Neste contexto, sob proposta do Ministério da Economia e do Mar (2023), foram identificadas infraestruturas críticas nacionais e europeias, e definido um Plano de Segurança (art.º 13.º) com a identificação dos elementos críticos e a delimitação das áreas de segurança. O art.º 22.º estabelece ainda que o Secretário-Geral do Sistema de Segurança Interna (SGSSI) deve criar e manter atualizada uma Plataforma de Registo de Informação de Infraestruturas Críticas (Plataforma de Registo), acreditada pela Autoridade Nacional de Segurança (ANS), compreendendo a catalogação das infraestruturas críticas nacionais ou europeias localizadas em território nacional, incluindo a sua georreferenciação; e os contactos dos agentes de ligação de segurança e dos elementos de contacto da infraestrutura, relativos a cada infraestrutura crítica, nacional ou europeia (Decreto-Lei 20/2022).

Processo que está em execução, constatando-se que em anexo à supracitada legislação define-se os setores e subsetores de infraestruturas críticas e respetivas entidades setoriais responsáveis, que sem referir explicitamente os cabos submarinos, define o sector genérico das "Comunicações" e as infraestruturas digitais e prestadores de serviços digitais, da responsabilidade da "Comissão de Planeamento de Emergência das Comunicações". Embora nos pareça que existe necessidade de fazer muito mais, nomeadamente de articular com a Defesa Nacional, importa salientar que os cabos submarinos (estruturas conexas) são, atualmente, infraestrutura críticas (nacionais, europeias e até globais) e que por esse facto, carece de um regime próprio de segurança.

A segurança das instalações, quer estejam em terra ou no mar, referem-se, quase sempre e exclusivamente, à segurança física, ou seja, aquela que protege e salvaguarda atos de sabotagem, destruição ou de ações que visam criar danos à infraestrutura, afetando a sua operacionalidade e o serviço à sociedade e ao país. A segurança física, por princípio, exige responsabilidades partilhadas e níveis diferenciados de meios e de capacidades para assegurar essa segurança. Neste caso, os cabos submarinos, sendo uma infraestrutura critica, obriga, em vários níveis, a rigorosos critérios de segurança física e ao cumprimento das normas de segurança nacionais e europeias, incluindo as mais rudimentares, mas essenciais, nomeadamente: o controlo e limitação de acessos, existência de planos de segurança e responsáveis com formação adequada, treino e preparação para a função… o que nem sempre, ou quase nunca, coincide com a realidade nacional.

A segurança física das instalações associadas à rede de cabos submarinos (pontos de amarração) e centro de dados, implica, para as empresas privadas, um assumir de algumas responsabilidades de segurança, até porque garantem a proteção dos seus investimentos (a reparação de um cabo submarino pode levar algumas semanas, pois só existem atualmente quatro países com capacidade de reparação em alto mar de cabos submarinos (EUA, China, França e Japão). Embora, por serem consideradas infraestruturas críticas têm um estatuto especial de segurança que será garantido pelo Estado, até porque a interrupção do serviço pode ser disruptiva para o país e com impacto na segurança nacional.

Em Portugal, o Gabinete Nacional de Segurança (GNS) preocupa-se com esta temática, pois que a soberania do Estado assenta na capacidade de conferir segurança aos cabos submarinos na plataforma continental e na legislação internacional (aplicando nomeadamente a Convenção das Nações Unidas sobre o Direito no Mar – Convenção de Montego Bay) onde existe já alguma legislação sobre a responsabilidade dos Estados e dos privados e devemos adotar preocupações em duas dimensões de segurança…segurança para Portugal e a segurança de Portugal como fornecedor de segurança, pois temos um papel como ator global de segurança (Faria, 2024).

Os cabos submarinos têm dimensões de comunicação física, mas temos de pensar a dimensão dos dados que circulam e a problemática da confidencialidade desses dados, pois sabemos que a maioria das empresas que operam os cabos submarinos são empresas privadas. Assim que a pergunta que se coloca é de saber quem deve responder e ser responsabilizado pela segurança e confidencialidade da informação que circula nesses cabos entre continentes? Pois que as fibras óticas transportam dados que, contextualizados se transformam em informação e posteriormente em conhecimento, e sendo o cabo submarino operado por uma empresa privada, mas como os pontos de amarração (estruturas conexas) situados em território nacional, temos de garantir a segurança, não só de natureza física das infraestruturas, mas também a segurança da informação que por aí circula e tem impacto na salvaguarda da nossa soberania digital.

Uma infraestrutura crítica, se tiver componente digital de segurança, deve estar em estreita ligação com o Centro Nacional de Cibersegurança (CNCS) (estrutura que

funciona no âmbito do Gabinete Nacional de Segurança) conforme preconizado na Lei n.º 46/208, de 13 de agosto e Decreto-Lei n.º 65/2012, de 30 de julho. A legislação que se aplica tem componentes de segurança física (responsabilidade da Autoridade Nacional de Emergência e Proteção Civil) e outra de segurança eletrónica, da responsabilidade quer do GNS quer do CNCS. A questão das infraestruturas críticas é gerida pela ANEPC e existe legislação nacional que enquadra o assunto (Decreto-Lei n.º 20/2022, de 28 de janeiro – Resiliência das Infraestruturas Críticas Nacionais e Europeias) e que estabelece os procedimentos que devem ser adotados para a sua proteção (Jesus, 2023).

Os cabos submarinos são uma infraestruturas crítica que na dimensão de cibersegurança se enquadra na Diretiva Europeia *Network and Information Security* (NIS). Para além da segurança física do cabo e das instalações, temos que numa outra dimensão, garantir que a informação não é comprometida (ou se for comprometida, saber o que temos de fazer para resolver esse problema). Nesse contexto, o que está em curso, no âmbito da legislação existente em Portugal e que decorre da transposição da Diretiva Europeia NIS (Lei n.º 46/2018, de 13 de agosto, e Decreto-Lei n.º 65/2021, de 30 de julho), é garantir que os requisitos definidos no documento contribuem para a segurança nacional. Nomeadamente, que os operadores de serviços essências têm de cumprir, no âmbito da cibersegurança, e que são efetivamente acautelados pelas entidades responsáveis, e com a entrada em legislação decorrente da transposição da NIS2 alargar esse âmbito e ampliar essas medidas de cibersegurança.

Uma qualquer entidade que se relaciona com cabos submarinos (pública ou privada) a operar em Portugal, tem de cumprir esses requisitos, pois caso não cumpra, a Autoridade Nacional de Cibersegurança no âmbito da Lei n.º 46/2018, de 13 de agosto, que diz respeito à segurança do ciberespaço, na qualidade de supervisor, poderá intervir. A cibersegurança deve assim ser entendida, não só como um elemento de segurança associada à informação que circula no ciberespaço, mas mais como um facilitador e promotor do desenvolvimento nacional. Neste âmbito, vamos ter de assegurar que os operadores sediados ou a operar em Portugal cumprem esses requisitos. Na NIS2 vai haver uma forte relação de segurança entre os operadores e os reguladores, que para a dimensão de cibersegurança, será, em primeira análise, da responsabilidade do Gabinete Nacional de Cibersegurança.

A nova diretiva europeia NIS2, publicada em 27 de dezembro de 2022[7], contempla, no seu preâmbulo e articulado, orientações especificas para os Estados-membros quanto aos cabos submarinos e será transposta para a legislação nacional até outubro de 2024. Como sabemos, Portugal não tem uma Estratégia Nacional de Cibersegurança, mas sim uma Estratégia Nacional de Segurança do Ciberespaço (2019-2023)[8], que se encontra atualmente em revisão, precisamente no intuito de incorporar orientações, entretanto emanadas pela UE, como é o caso da NIS2. Esta diretiva vem referir os principais aspetos que os Estados-membros devem contemplar nas suas estratégias de cibersegurança iniciativas concretas relativamente aos cabos submarinos, onde se inclui um levantamento das principais restrições dos mecanismos de reporte em caso de incidente potencialmente disruptivo e definir as medidas corretivas mais adequadas.

Da NIS2 com impacto para a cibersegurança e diretamente sobre a cibersegurança nos cabos submarinos, importa salientar que no domínio da cibersegurança, deve observar-se as obrigações instituídas pelo Regime Jurídico de Segurança do Ciberespaço, estabelecido pela Lei n.º 46/2018, de 13 de agosto9, e regulamentado pelo Decreto-Lei n.º 65/2021, de 30 de julho10, que determina o seu âmbito de aplicação à Administração Pública; aos operadores de infraestruturas críticas; aos operadores de serviços essenciais; aos prestadores de serviços digitais e a outras entidades que utilizem redes e sistemas de informação.

Por outro lado, deve ser também referido que foi adotada a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na UE que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva NIS 2), publicada no Jornal Oficial da União Europeia, em 27 de dezembro de 202211. Este ato legislativo determina que "…os Estados-Membros devem adotar e publicar, até 17 de outubro de 2024, as disposições necessárias para dar cumprimento à presente Diretiva…" (NIS2), devendo, em matéria de cibersegurança de cabos de submarinos, observar-se o seguinte: que o mercado interno depende, mais do que nunca, do funcionamento da internet. Frequentemente constatamos que serviços de quase todas as entidades essenciais e importantes estão dependentes de serviços prestados através da internet. Para evitar problemas na prestação dos serviços assegurados por entidades essenciais e é necessário que todos os fornecedores de redes públicas de comunicações eletrónicas adotem medidas de gestão dos riscos de cibersegurança adequadas e notifiquem incidentes significativos relacionados com as mesmas.

Os Estados-membros deverão assim assegurar a manutenção da segurança das redes públicas de comunicações eletrónicas e a proteção dos seus interesses vitais em matéria de segurança contra sabotagem e espionagem. Uma vez que a conectividade internacional reforça e acelera a digitalização competitiva da UE e da sua economia, os incidentes que afetam os cabos submarinos de comunicações deverão ser notificados à *Computer Security Incident Response Team* (CSIRT) ou, se aplicável, à autoridade competente nacional.

Uma Estratégia Nacional para a Cibersegurança deverá, quando pertinente, ter em conta a cibersegurança dos cabos submarinos de comunicações e incluir um levantamento dos potenciais riscos de cibersegurança e medidas de atenuação para garantir o mais elevado nível de proteção dos mesmos. E por outro lado, refere que de acordo com o artº 7.º (Estratégia Nacional de Cibersegurança), no âmbito da Estratégia Nacional de Cibersegurança a implementar, os Estados-membros devem adotar, em especial, políticas: "…d) Sobre a manutenção da disponibilidade geral, da integridade e da confidencialidade do núcleo público da *internet* aberta, incluindo, quando pertinente, a cibersegurança dos cabos submarinos de comunicações…".

Neste contexto, deve ser assinalado que o âmbito de aplicação da Diretiva NIS2 abrange igualmente as entidades que venham a ser identificadas como críticas no âmbito da

Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho[12] e que, à data, decorre no âmbito do Conselho Superior de Segurança do Ciberespaço o processo de revisão da atual Estratégia Nacional de Segurança do Ciberespaço 2019-2023, tendo sido já destacada a relevância da cibersegurança dos cabos submarinos e o contributo para a Segurança Nacional.

Estamos atualmente (2024) em Portugal num contexto de oportunidade, mas também associado ao potencial surgimento de maiores desafios para a segurança e defesa nacional. Paradigma que tem a ver com o posicionamento de Portugal no mapa da conectividade internacional de cabos submarinos e que por um lado nos abre espaço para acolhermos investimento económico e desenvolvimento tecnológico, mas que nos obriga a pensar estrategicamente em termos de investimentos na segurança e as consequências para a Defesa Nacional.

Este é ainda uma temática pouco desenvolvido em Portugal e que compromete as Empresas, Organizações e os Estados, principalmente num contexto atual em que se discute as Grandes Opções do novo CEDN. O documento referia concretamente a este respeito que "…as ameaças das redes terroristas, da criminalidade organizada e dos conflitos periféricos permanecem uma constante. As infraestruturas críticas, incluindo os gasodutos, as redes de comunicações e os cabos submarinos, são vulneráveis a ações de sabotagem e terrorismo de atores estatais e não estatais hostis…". Do que deriva que sendo identificado como uma ameaças à segurança nacional devem ser desenvolvidas medidas para reforço da segurança, no âmbito do que abordamos no capítulo anterior. Assim, e em continuação, pretendemos analisar em seguida algumas das principais oportunidades que se colocam a Portugal neste contexto e identificar alguns dos principais desafios que deveriam estar, direta ou indiretamente, contemplados no novo CEDN.

6. Contributos para o Conceito Estratégico de Defesa Nacional

A Lei de Defesa Nacional, aprovada pela Lei Orgânica n.º 1-B/2009, de 7 de julho, na sua redação atual, estabelece, no n.º 1 do seu artº 7.º, que cabe ao Conceito Estratégico de Defesa Nacional definir as prioridades do Estado em matéria de Defesa, de acordo com o interesse nacional, sendo, por isso, parte integrante da Política de Defesa Nacional. Em Portugal, a ANACOM tem responsabilidade sobre o controlo dos dados que circulam nos cabos submarinos, mas legalmente não tem qualquer enquadramento, nem existe uma visão estratégica que possa contribuir para esta finalidade…e começa, cada vez mais, a ser um problema em termos nacionais. A questão que se coloca é saber se (e como) os países e as suas entidades reguladoras, devem proteger esses cabos submarinos (incluindo os dados que transportam e gerem) que são das empresas transnacionais?

Esse, parece-nos ser um paradigma securitário que vai ter de mudar, pois a informação crítica dos países circula nos cabos submarinos e estão nas bases de dados protegidas, e estas são da responsabilidade estritamente nacional, pois tem implicação na soberania. Como tal devem estar isolados e protegidos pois, como vimos, são consideradas infraestruturas críticas, e devem inclusive, no caso do CEDN, ser abordadas no sentido de adquirirem maior relevância na nossa política de defesa nacional.

Pensamos assim que o novo CEDN deveria ter algo que mencione não explicitamente os cabos submarinos, mas as infraestruturas críticas digitais em geral, com impacto mundial em que Portugal tenha responsabilidade, e atribui-lhe uma relevância e proteção especial. Incluir ainda algo relacionado com a resiliência digital nacional e não apenas explicitamente sobre os cabos submarinos. Pois que a temática da segurança nacional e do CEDN deveria trazer este assunto mais para o conhecimento e a reflexão pública… deveríamos olhar para um *trade off* que podemos fazer com a NATO, com a UE e outros países parceiros em prol da segurança da nossa ZEE. Em que o Atlântico Norte deve ser navegável e deve ser, tanto quanto possível, uma área de reforço da segurança (por via da vigilância) e as redes de cabos submarinos podem contribuir para esse desiderato, nomeadamente com a tecnologia dos SMART Cables.

Do que constata nas Grandes Opções do CEDN, que estiveram em discussão na Assembleia da República em 2023, referem concretamente a este respeito que "…as infraestruturas críticas, incluindo os gasodutos, as redes de comunicações e os cabos submarinos, são vulneráveis a ações de sabotagem e terrorismo de atores estatais e não estatais hostis…" (2023). O que implica que sendo identificado como um potencial risco à segurança nacional, devem constar (explicita ou implicitamente) no CEDN, levando a que sejam desenvolvidas medidas concretas para reforço da segurança como contributo essencial para a segurança nacional. Neste contexto, parece-nos que existe em Portugal uma legislação adequada, mas excessiva, e algum (pouco) conhecimento sobre esta temática e uma intenção de conferir maior relevância, no contexto do CEDN, à temática dos cabos submarinos, muito em articulação com a legislação europeia e nacional, que já contempla, como vimos, algumas destas preocupações para a segurança nacional de uma infraestrutura crítica, como é o caso dos cabos submarinos e das infraestruturas digitais conexas.

Conclusões

Aproveitando a posição geoestratégica favorável no mundo da informação global, Portugal foi até há bem pouco tempo o único país no mundo a ter ligações por cabo submarino direto com todos os continentes, estando georreferenciado como um dos principais pontos de passagem da rede global de cabos submarinos, o que possibilita um conjunto de oportunidades na vertente económica, tecnológica ou de desenvolvimento; mas que implica também, necessariamente, alguns riscos e ameaças para a segurança nacional. Procuramos nesta reflexão aprofundar esta lógica, e tendo por base alguma (ainda relativamente incipiente) bibliografia, olhar para a realidade em Portugal e

associarmo-nos ao debate teórico sobre o desenvolvimento do novo Conceito Estratégico de Defesa Nacional, como parte da nossa Política de Defesa Nacional para o futuro. Neste contexto, a pergunta que importa responder é identificar: Quais os principais desafios e oportunidades para a Defesa Nacional que decorrem do posicionamento geoestratégico de Portugal na rede global de informação?

A globalização, como fenómeno associado à liberalização e descentralização das redes de informações, veio criar um paradigma de modernidade substancialmente diferente, onde empresas, organizações e Estados, procuram nesta "nova" Era Digital, ganhar vantagem competitiva sobre o tráfego, gestão e armazenamento de dados, pois que a economia de dados será a economia do futuro. Este é também o nosso desafio em Portugal, constatando-se que já existe um conjunto de iniciativas, quer na vertente económica, tecnológica ou de segurança, que colocam Portugal no centro geoestratégico deste movimento global e globalizante, que nos obriga a pensar e a agir de forma diferente.

Exemplos como o "*Sines Submarine Cable Hub Project*" e o "*SMART Atlantic CAM*", na dimensão do desenvolvimento científico-tecnológico e económico; a par da adaptação da nossa legislação à legislação europeia resultante da recente aprovação da NIS2 e das iniciativas da ANACOM e do GNS, na vertente mais da segurança física e da cibersegurança na proteção dos dados, são potencialmente geradoras de mais-valias para a Defesa Nacional.

Contudo, pensámos que Portugal poderia ter outra dinâmica na estratégia de cativar grandes empresas internacionais para amarração de cabos submarinos e na instalação de centros de dados, beneficiando da nossa posição geoestratégica que é de facto relevante. Portugal continental, entre Carcavelos e Sines tem todos os seus pontos de amarração (4) concentrados num curto espaço de um pouco mais do que uma centena de quilómetros e assegurando ligação com todas as ilhas dos arquipélagos dos Açores e da Madeira, derivando das estações de amarração de cabo submarino e possibilitando uma aposta consistente e estratégica neste segmento estratégico. Pois que as águas territoriais portuguesas, são genericamente caracterizadas por declives abruptos, atingindo-se grandes profundidades rapidamente, o que é do agrado dos operadores de cabos submarinos, já que lhes confere maior segurança (havendo menos interação com âncoras e artefactos de pesca de arrasto), o que constitui também fator de atratividade que importa saber capitalizar e integrar numa estratégia nacional virada para o mar e apostando nas redes de cabos submarinos como um ativo nacional que nos pode trazer desenvolvimento e segurança.

Pensamos, conforme é referido por todos os entrevistados, que começa agora a existir uma melhor perspetiva nacional sobre este assunto, e que uma estratégia nacional, deve prestar especial atenção à área de Sines que está vocacionada para amarração de cabos e armazenamento de dados em larga escala. Mas outras áreas deverão merecer especial atenção, tais como as Regiões Autónomas e a região norte do continente, áreas estas onde deverão ser amarrados novos cabos submarinos, de forma que Portugal não seja um mero elo de ligação onde se interligam cabos a outros cabos, mas sim um *Data Hub*, onde os dados chegam por cabos submarinos, são armazenados e processados em Portugal e

são depois disponibilizados internacionalmente por cabos submarinos, gerando desenvolvimento (e segurança) para o país.

Num momento em que iremos novamente discutir as Grandes Opções do Conceito Estratégico de Defesa Nacional, como parte de uma reflexão nacional que, de tempo em tempo, introspetivamente, nos permite refletir sobre a forma de capitalizar as oportunidades que derivam do nosso posicionamento geoestratégico; será importante possibilitar um maior debate sobre o posicionamento de Portugal na rede global de informação e dos desafios e oportunidades que se colocam para a Política de Defesa Nacional.

Em suma, estamos cientes que a principal recomendação que podemos fazer para o atual processo de revisão do CEDN será o de sugerir uma maior aposta nestas tecnologias inovadoras, e desenvolver estratégias sectoriais que possam trazer mais resiliência para a nossa economia no contexto global. Uma aposta na economia digital que não pode ficar desligada de uma aposta, séria e consistente, na Defesa Nacional, apostando na segurança marítima e na cibersegurança, e garantindo que o investimento nas tecnologias inovadoras são uma aposta no desenvolvimento e na segurança, e que ambas representam um reforço da presença de Portugal no mundo global da gestão das redes de informações.

Bibliografia

AUTORIDADE NACIONAL DE COMUNICAÇÕES (2023). Plano Plurianual de Atividades 2024-2026: Objetivos e Ações Estratégicas – Consulta Pública. Julho 2023.

BAFOUTSOU, Georgia e PAPAPHILIPPOU, Maria e DEKKER, Marnix (2023). Subsea Cables – What is at Stake?. European Union Agency for Cybersecurity. July 2023.

BARROS, José e BERNARDINO, Luís (2023). Contributions of SMART Cable Technology to the Sustainable Development in Portugal. Jornal da Economia do Mar. 21 September 2023. [Em linha]. Disponível em: https://www.jornaldaeconomia domar.com/contributions-of-smart-cables-technology-to-sustainable-development-in-portugal/

BASALISCO, Bruno e HANSENO, Morten (2021). The economic impact of the forthcoming equiano subsea cable in Portugal. Forecasting the effect of enhanced connectivity infrastructure on trade and growth. Commissioned by: Google may 2021. [Em linha]. Disponível em: https://copenhageneconomics.com/publication/the-economic-impact-of-the-forthcoming-equiano-subsea-cable-in-portugal/

BERNARDINO; Luís Manuel Brás (2021). O conhecimento em rede e as redes do conhecimento. A “nova” forma de Poder dos Estados. Lisboa. Instituto Universitário

Militar. [Em linha]. Disponível em: https://www.ium.pt/pub/38

BRAKE, Doug (2019). Submarine Cables: Critical Infrastructure for Global Communications. Information Technology & Innovation Foundation. April 2019.

BUEGER, Christian e LIEBETRAU, Tobias (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network, Contemporary Security Policy, 42:3, 391-413, DOI: 10.1080/13523260.2021.1907129

BUEGER, Christian e LIEBETRAU, Tobias e FRANKEN, Jonas (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. European Parliament coordinator: Policy Department for External Relations. Directorate General for External Policies of the Union. PE 702.557 – June 2022.

BUEGER, Christian e COSTA, Rita e LIEBETRAU, Tobias e SIMÂO, Licínia e WALKER, Timothy (2022). Protecting subsea data cables in Europe and the Atlantic – Challenges of a New Era. Policy Brief 13. July 2022. Atlantic Centre.

CABRAL, Costa (2022). A Segurança dos Cabos Submarinos. Segurança de Informação nas Organizações no Mestrado em Segurança de Informação e Direito no Ciberespaço. Escola Naval. Fevereiro 2022.

COPENHAGEN ECONOMICS (2021). The Economic impact of the forthcoming equiano subsea cable in Portugal, Estimates from the Instituto Nacional de Estatistica de Portugal.

DEAN, James et al. (2017). Threats to Undersea Cable Communications. Department of Homeland Security and Office of the Director of National Intelligence Public Private Analytic Exchange Program.

FARIA, Duarte Lynce (2024). Os cabos submarinos. Infraestruturas críticas que desafiam a jurisdição de Portugal e do Direto Internacional. Revista Nação e Defesa. Nº 169, pp.43-84. [Em linha]. Disponível em: https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD169/NeDef169_Duarte%20Lynce%20Faria.pdf

HOWE, Bruce M. et al (2019). SMART Cables for Observing the Global Ocean: Science and Implementation. Journal Frontiers in Marine Science. Volume 6. Article 424.

JESUS, Hélder Fialho (2023). A aplicabilidade do conceito de “Proteção, Segurança e Defesa” para a ciber-resiliência no contexto do Atlântico Português”. Anais do Clube Militar Naval. Volume CLIII, Janeiro-Junho 2023, pp.75-120.

KLAUS, Christoph e CARTER, Lionel (2017). A Bibliography of Submarine Communication and Power Cables. International Committee for Protection of Cables. Publication. June 2017.

MATSAKIS, Laouise (2018). What Would Really Happen if Russia Attacked Undersea Internet Cables?. Wired.

MEDEIROS, Sabrina e PINTO, Danielle (2022). Cabos submarinos e segurança cibernética no Atlântico. Policy Brief 11. Atlantic Centre. March 2022.

NETWORK AND INFORMATION SECURITY (NIS2) 2022. Directiva (EU) 2022/2557 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 sobre a Resiliência de Infraestuturas Críticas.

RECORDED FUTURE (2023). The Escalating Global Risk Environment for Submarine Cables. 2023. Threat Analysis. Insikt Group. 27 de june 2023.

SECHRIST, Michael (2012). New Threats, Old Technology: Vulnerabilities in Undersea Communications in Undersea Communications Cable Network Management System. Belfer Center for Science and International Affairs Harvard Kennedy School.

VILELA, José (2015). Datas e Factos dos Cabos Submarinos em Portugal (1855-2015). Fundação Portuguesa das Comunicações.

_____-

* Trabalho Final Individual (TFI) desenvolvido no âmbito do Curso de Defesa Nacional (2022_2023).

1 Quando falamos de conhecimento e em especial de conhecimento científico, falamos por inerência de redes de conhecimento e de conhecimento em rede. Este é um paradigma dos tempos modernos e também um paradigma de futuro, com impacto na forma como nos organizamos e como vivemos em sociedade. Um paradigma geracional, que transformou a expressão “informação é poder” em “conhecimento é poder”, afetando a forma como as instituições de defesa e segurança se inserem na sociedade do século XXI. Esta temática foi, por conseguinte, o objeto de estudo da lição inaugural proferida no Instituto Universitário Militar (2021) que materializa também o objeto da principal interrogação das novas gerações, atendendo a que o acesso e o controlo das redes de conhecimento será, no futuro, à luz da Teoria Construtivista das Relações Internacionais, uma das mais relevantes “novas” formas de Poder dos Estados. (Bernardino, 2021).

2 O Decreto-Lei n.º 62/2011 de 9 de maio estabeleceu os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, bem-estar económico e social da sociedade, nos sectores da energia e transportes, e da segurança, transpondo a Diretiva n.º 2008/114/CE do Conselho, de 8 de dezembro, e onde se estabeleceu (pela primeira vez) os procedimentos para a identificação das diversas infraestruturas com

funções essenciais para a sociedade, cuja perturbação ou destruição teria um impacto significativo. Com o edifício legislativo criado em 2011, e atualmente em revisão, Portugal adquiriu uma maior capacidade de intervenção ao nível da segurança e da melhoria da resiliência das infraestruturas que venham a ser sectorialmente consideradas críticas e incluídas na listagem nacional de infraestruturas críticas. No âmbito europeu, Portugal passou a integrar o "Programa Europeu de Proteção de Infraestruturas Críticas", suportado numa abordagem transversal dos riscos a que essas infraestruturas estão expostas, com impacto para o espaço europeu.

3O enquadramento legal relativo à identificação e proteção de infraestruturas essenciais (criticas) para a saúde, segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes encontra-se, como vimos, estabelecido no Decreto-Lei n.º 62/2011, de 9 de maio, que transpôs para a ordem jurídica interna a Diretiva n.º 2008/114/CE do Conselho Europeu, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

4 https://www.submarinecablemap.com/

5 A Copenhagen Economics foi designada pela Agência Sueca de Gestão Pública para avaliar a precisão da previsão de algumas das principais variáveis que o Instituto Nacional de Investigação Económica projeta. O relatório inclui uma descrição dos dados utilizados e uma visão geral da análise estatística e dos testes realizados e inclui um apêndice estatístico composto por medidas de desempenho, testes e estatísticas descritivas. (Copenhagen Economics, 2021).

6 Esta pesquisa foi realizada pela Copenhagen Economics para o Google, em 2021, tendo sido analisado o impacto económico do cabo submarino "EQUIANO" implantado entre Portugal e a África do Sul com unidades ramificadas ao longo do caminho. Embora sejam de esperar impactos económicos do cabo para todos os países ligados ao cabo, este estudo centrou-se no impacto para a economia portuguesa. (Copenhagen Economics, 2021).

7 A Comissão Europeia continuará a desenvolver os requisitos técnicos e metodológicos relacionados com a Diretiva Network and Information Security (versão 2). A NIS2 é apenas uma parte de um plano mais amplo de cinco pontos que a UE está a adotar para combater a cibersegurança. A Comissão Europeia continua a dinamizar uma revisão do Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC) de 2008. [Em Linha]. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

8 https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

9 https://dre.pt/dre/detalhe/lei/46-2018-116029384

10https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988

11https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2555

12https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2557