Cabos Submarinos: Natureza Crítica e Vulnerabilidade Estratégica no Contexto da Aliança do Atlântico Norte

Inês Aguiar Branco
Consultora de Política do Mar.

Resumo

Num mundo cada vez mais global e tecnológico, as infraestruturas que suportam a conetividade digital, célere e permanente, adquirem um carácter imprescindível, uma vez que a transmissão da mesma quantidade de dados por outras vias é mais lenta, mais dispendiosa e insuficiente para atender às necessidades atuais a nível mundial.
Eventos recentes tornaram claro que os cabos submarinos estão em risco. Os adversários da OTAN estão não só cientes das vulnerabilidades existentes e conexas a este tipo de infraestrutura como, também, prontos e dispostos a explorá-las. Isto origina, inevitavelmente, implicações diversas para a segurança e interesses dos Estados aliados, às quais Portugal, como único país do mundo com ligações diretas de cabos submarinos estabelecidas com todos os continentes, à exceção da Antártida, não se deve alhear.

Palavras-chave: Cabos Submarinos; OTAN; Segurança Marítima; Infraestrutura Crítica; Vulnerabilidades; Danos; Ameaças.

Abstract
Subsea Cables: Critical Nature and Strategic Vulnerability in the North Atlantic Alliance Context

In an increasingly global and technological world, the infrastructures that support rapid and permanent digital connectivity become essential as the transmission of the same amount of data by other means is slower, more expensive, and insufficient to meet current needs worldwide.
Recent events have made it clear that subsea cables are at risk. NATO's adversaries are not only aware of the existing vulnerabilities related to this type of infrastructure, but also ready and willing to exploit them. This inevitably gives rise to numerous implications for the security and interests of allied States, implications which Portugal, as the only country in the world with direct subsea cable connections established with all continents, apart from Antarctica, should not ignore.

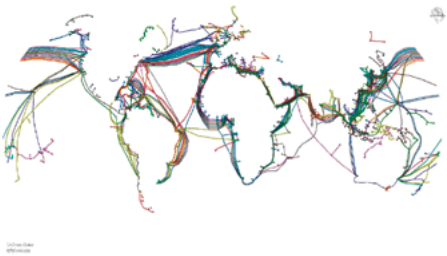
Keywords: *Subsea Cables; NATO; Maritime Security; Critical Infrastructure; Vulnerabilities; Damages; Threats.*

Artigo recebido: 31.01.2024
Aprovado: 16.04.2024
https://doi.org/10.47906/ND2024.168.04

Introdução

A conjuntura das sociedades contemporâneas está tão intrinsecamente dependente de uma ligação rápida e permanente à Internet que vários relatórios e estudos falam do acesso à Internet como sendo um Direito Humano (Kravets, 2011; Tully, 2014; Howell e West, 2016; Euronews, 2016; United Nations Human Rights Council 47th Session, 2021). Os cabos submarinos, artérias principais da Internet e da conectividade global, asseguram esse acesso, sendo responsáveis por 99% das telecomunicações mundiais, transmitindo rapidamente enormes quantidades de dados de origem pública e privada (Pérez, 2023; Miranda, 2023; Davenport, 2023; Medeiros e Pinto, 2023).

Figura 1
Traçado Mundial de Cabos Submarinos



Fonte: Symington (2023).

Figura 2
Rotas de Comércio Mundial

Fonte: Symington (2023).

O desenho traçado por estes cabos (Figura 1) mostra não só como circula a informação, mas também como flui o poder económico entre os diferentes continentes (Miranda, 2023; Medeiros e Pinto, 2023; Bueger *et al.*, 2022). Note-se que África é um dos continentes menos conectados, contrariamente à Europa e à América do Norte, e que, maioritariamente, os cabos submarinos seguem as rotas marítimas mais utilizadas pelos navios comerciais (Miranda, 2023; Medeiros e Pinto, 2023; Bueger *et al.*, 2022) (Figura 2).

O Atlântico Norte torna-se, assim, na rota marítima digital mais movimentada e densa do mundo (Medeiros e Pinto, 2023; Bueger *et al.*, 2022). Este facto, traduz-se em inúmeras oportunidades e desafios. Se, por um lado, este aumento da capacidade e qualidade da transmissão de dados permite comunicar de forma instantânea e permanente entre continentes, diminuindo as possibilidades de perda de ligação – por existir muita redundância –, por outro, o aumento da dependência societária desta infraestrutura gera preocupações securitárias com a manutenção do seu regular funcionamento (Bueger *et al.*, 2022). Assim, o Sul Global está mais vulnerável e suscetível a sofrer interrupções e demoras nos seus serviços de comunicações e Internet, em virtude do menor número de ligações que possui. Isto traduz-se numa

menor redundância e capacidade de resposta em caso de danificação da estrutura de cabos submarinos em toda esta área geográfica (Bueger *et al.*, 2022).

Embora a maior parte dos danos a cabos submarinos tenha, atualmente, carácter não intencional, a elevada dependência desta infraestrutura, para efeitos de comunicações sensíveis de natureza financeira e militar, preocupa, cada vez mais, a Organização do Tratado do Atlântico Norte (OTAN) e a União Europeia (UE) que, no atual contexto geopolítico, perspetivam a ocorrência de danos intencionais, coordenados e maliciosos (Bafoutsou *et al.*, 2023; Bueger *et al.*, 2022). Esta mudança de paradigma, relativamente ao carácter intencional dos danos a infraestruturas críticas, origina diversas preocupações a nível nacional e internacional tendo provocado a criação de vários grupos de trabalho e estudos para a identificação e mitigação de vulnerabilidades associadas a este tipo de infraestrutura (Pérez, 2023).

Em janeiro de 2023, a OTAN e a UE criaram um grupo de trabalho conjunto para proteger estas infraestruturas críticas. Meses mais tarde, a OTAN criou, ainda, uma Célula de Coordenação da Infraestrutura Crítica Submersa (EuroNews, 2023; NATO, 2023). Este novo organismo pretende coordenar esforços para mapear e dirimir vulnerabilidades entre os seus aliados, parceiros e setor privado.

Em outubro de 2023, o Conselho Europeu aprovou a Estratégia de Segurança Marítima da UE revista, bem como o seu Plano de Ação, justificando a revisão com a necessidade de fazer face a novas ameaças e desafios securitários, incluindo os ataques híbridos e cibernéticos contra as infraestruturas marítimas (Conselho Europeu, 2023). Este documento identificou a necessidade estratégica de aumentar a resiliência e a proteção das infraestruturas críticas submersas, reforçando as recomendações que o próprio Conselho já tinha emitido, em 2022 (Conselho Europeu, 2022).

Em Portugal, o Decreto-Lei n.º 20/2022, de 28 de janeiro veio aperfeiçoar o regime legal de identificação e proteção de infraestruturas críticas nacionais veiculado pelo Decreto-Lei n.º 62/2011, de 9 de maio, passando a incluir os setores das comunicações e infraestruturas digitais como setores onde deve ser feita a identificação de infraestruturas críticas nacionais. No entanto, trata-se de um processo de elevada complexidade pelo que, até ao momento, nenhuma infraestrutura crítica foi ainda identificada. Consequentemente, a infraestrutura nacional de sistemas de cabos submarinos permanece sem qualquer proteção jurídica ou securitária relevante[1].

1 A título de exemplo, a danificação intencional de um cabo submarino de comunicações, se excluirmos a criminalização desta conduta pelos crimes de terrorismo ou de sabotagem, que preconizam dolos específicos, só pode ser feita pelo Art.º 5.º n.º 2 do Decreto-Lei n.º 507/72 – cujas sanções são uma pena de multa de "20.000$00 a 100.000$00" e uma pena de prisão de 4 meses a dois anos, sendo a tentativa punível com pena até quatro meses de prisão – ou, em alternativa pelo crime de dano (Art.º 212.º do Código Penal português), cuja sanção é uma condenação até três anos de prisão ou uma pena de multa. Acresce, ainda, a existência de um amplo leque de normas sancionatórias que, de forma direta e indireta, contribuem para a segurança dos cabos

Este artigo aborda, simultaneamente, a natureza crítica e a vulnerabilidade estratégica que os cabos submarinos representam para a OTAN e, por maioria de razão, para o nosso país.

1. A Natureza Crítica dos Cabos Submarinos

No fundo do mar operam, presentemente, mais de 500 cabos submarinos suportados por mais de 1.400 estações de amarração (Telegeography, 2023). Estes cabos são essenciais para o funcionamento regular da sociedade global já que, constituindo a base estrutural da atividade social, governamental, militar e económica, a sua danificação, e consequente interrupção no fornecimento de serviços, pode provocar a paralisação total de um Estado (Guimarães, 2023; Miranda, 2023; Davenport, 2023; Medeiros e Pinto, 2023).

Quando comparados com outras tecnologias de transmissão de dados sem fios[2], os cabos submarinos oferecem vantagens imbatíveis nos campos da capacidade, velocidade e segurança de transmissão de dados (Submarine Telecoms Forum, 2022/2023). Estes adquirem, assim, natureza crítica uma vez que a transmissão da mesma quantidade de dados por outras vias não se coaduna com as necessidades mundiais atuais por ser, incomparavelmente, mais lenta e dispendiosa (Miranda, 2023; Pérez, 2023).

Não obstante a importância crítica, a abrangência geográfica e a dificuldade de monitorização deste tipo de infraestruturas, dispersas por diferentes ambientes operacionais e reguladas por distintos regimes jurídicos, há várias vulnerabilidades que tornam os cabos submarinos alvos atrativos para atores hostis (Guimarães, 2023; Medeiros e Pinto, 2023; Davenport, 2023). Prova disso é o interesse persistente da Federação Russa[3] na recolha de informação sensível sobre estas infraestruturas através da presença, frequentemente reportada, de cruzeiros científicos deste país em território marítimo de diversos Estados da OTAN (Medeiros e Pinto, 2023; Nunes, 2023; Donn, 2023; Colavito, 2023). Prova adicional é a preocupação generalizada dos Estados Aliados com o quase monopólio da República Popular da China como proprietária destas infraestruturas (Pérez, 2023; Brock, 2023; Schochet e Carr, 2023; Colavito, 2023).

submarinos de comunicações, mas que, além de serem de natureza contraordenacional, incidem sobre aspetos que não se reconduzem à sua proteção contra atos hostis.

2 Onde se incluem, por exemplo, as tecnologias de transmissão de ondas rádio (TV/Satélites), Wi-Fi, Bluetooth, NFC (comunicação por campo de proximidade) e RFID (ou identificação por radiofrequência).

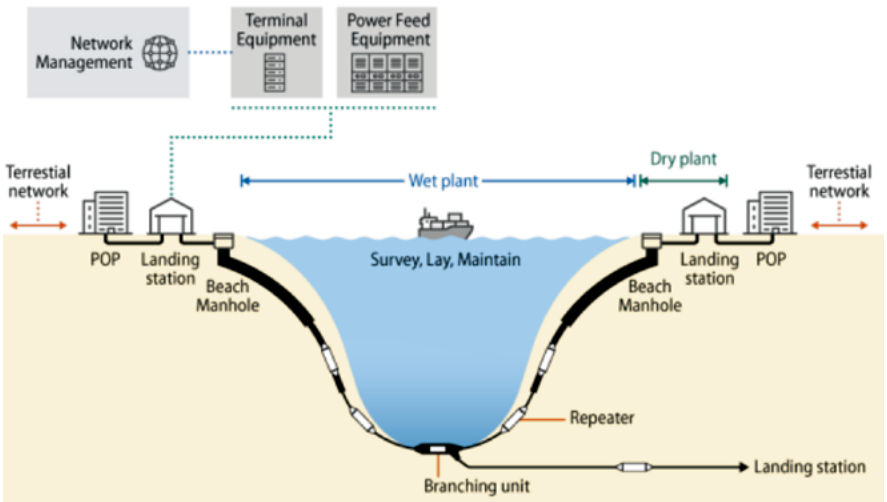
3 Neste domínio, importa referir que a possibilidade de a Rússia vir a realizar ataques contra cabos submarinos de comunicações e do sector energético tem sido veiculada por declarações de altos responsáveis políticos russos.

Este tipo de interesses e monopólio adivinham-se potenciadores de ações de mapeamento e, no contexto geopolítico atual de conflito armado, preocupam profundamente os Aliados da OTAN (Siebold, 2023; Davenport, 2023). Tal preocupação deve-se à potencial utilização desse mapeamento para ações de disrupção simultânea de vários cabos submarinos que, devido às limitadas e morosas capacidades de reparação existentes, bem como à dificuldade de atribuição de responsabilidade pelos danos ocorridos, representam um risco significativo para toda a Aliança (Davenport, 2015; Trakimavičius, 2021; Bueger *et al.*, 2022; Miranda, 2023; Pérez, 2023).
Assim, pela sua relevância estratégica, económica e securitária, importa analisar mais em pormenor as vulnerabilidades associadas a este tipo de infraestrutura crítica, bem como o aproveitamento que os Estados não aliados poderão fazer dessas vulnerabilidades.

2. Vulnerabilidades dos Cabos Submarinos

Para melhor se compreenderem as vulnerabilidades associadas à infraestrutura dos cabos submarinos, é importante considerar que estes são estruturas complexas que atravessam dois ambientes operacionais distintos (Figura 3): o ambiente marítimo que inclui o cabo em si, os repetidores nele instalados (para amplificação de sinal) e as unidades de derivação; e o ambiente terrestre, que inclui o "ponto de ligação"

Figura 3
Estrutura de Sistema de Cabo Submarino



Fonte: Gallagher (2022).

(Beach Manhole) que se liga à "estação de amarração" (Landing Station)[4]. Nas suas proximidades são, normalmente, instalados ainda os "pontos de presença" (PoP), que ficam alojados em centros de dados, que são a verdadeira origem e destino dos cabos submarinos e dos dados que neles circulam (Pérez, 2023; Gallagher, 2022).
Além de atravessarem diversos ambientes operacionais, os cabos estão, também, sujeitos a diferentes regimes jurídicos, por transporem e estarem "fixos" – tanto em mar, como em terra – a territórios sob soberania e/ou jurisdição de diferentes Estados e, ainda, fora da soberania e/ou jurisdição de qualquer Estado[5] (Davenport, 2018; Medeiros e Pinto, 2023).
Adicionalmente, os cabos submarinos são infraestruturas particularmente onerosas, normalmente financiadas através da constituição de consórcios entre empresas de tecnologia ou operadoras de telecomunicações de forma a partilhar os custos e os riscos associados a este modelo de negócio (Brock, 2023; Pérez, 2023; Medeiros e Pinto, 2023). Assim, na gestão e operação de um cabo submarino, participam diferentes entidades muito especializadas e diferenciadas, desde proprietários, fabricantes, instaladores e reparadores, até entidades governamentais.
Esta multiplicidade de parceiros, ambientes operacionais e regimes jurídicos, está na génese de uma série de vulnerabilidades que se manifestam em ambiente marítimo, terrestre e digital.

2.1. Vulnerabilidades Marítimas

As vulnerabilidades marítimas relacionam-se com os componentes do sistema de cabos submarinos que estão submersos (Figura 3). O isolamento geográfico e as condições ambientais adversas do ambiente marinho de grande profundidade, traduzem-se numa capacidade de monitorização e reparação reduzida, morosa e onerosa (Pérez, 2023).
Para além disso, existe uma concentração elevada de cabos em regiões específicas do oceano (Figura 1) o que, aliado ao facto de o traçado dos cabos ser do conhecimento público, favorece o conhecimento exato da localização e do número de cabos que é necessário danificar para provocar interrupções de grande escala ao fornecimento de serviços (Sunak, 2017).
Em 2013, a marinha egípcia deteve três mergulhadores, numa embarcação de pesca, perto da costa da Alexandria, sob suspeita de tentativa de corte do cabo submarino SeaMeWe-4, responsável por um terço do tráfego entre a Europa e o Egito (Arthur,

4 Local físico do país onde o cabo se liga à rede global de cabos submarinos, onde é feita a ligação às redes terrestres e onde residem as capacidades de gestão dos cabos e os equipamentos que fornecem a energia de que o sistema precisa para funcionar.
5 *Vide* Artigos 112.º e 113.º da *Convenção das Nações Unidas sobre o Direito do Mar*.

2013). Muito embora não haja detalhes adicionais, este caso demonstra que, para indivíduos determinados e munidos de equipamento adequado, não é necessário um elevado grau de sofisticação para causar uma disrupção séria às comunicações de Internet (Sunak, 2017).

2.2. Vulnerabilidades Terrestres

As vulnerabilidades terrestres dizem respeito aos componentes do sistema de cabos submarinos que estão em terra (Figura 3). Estes estão, normalmente, localizados na orla costeira e, por razões tanto de adequação geográfica como de redução de custos, alojam vários cabos submarinos criando, desta forma, diversos pontos de estrangulamento da rede (CSRIC, 2016).

A existência de pontos de estrangulamento é exacerbada, em grande medida, pela falta de segurança física característica destas infraestruturas, usualmente localizadas perto de zonas que, embora remotas, são de fácil acesso por não possuírem qualquer proteção por parte de estruturas físicas ou serviços de segurança especializados (Bueger *et al.*, 2022).

Em 2007, o Reino Unido conseguiu impedir uma tentativa de destruição das instalações da sede da Telecom Europe – empresa de centro de dados – por parte da Al-Qaeda (Leppard, 2007). Considerando que, ao contrário da maioria dos componentes terrestres de cabos submarinos, por ser um edifício-sede, este complexo estava dotado de medidas protetivas acima da média, é preocupante a possibilidade de ocorrência de ataques noutros locais (Sunak, 2017).

2.3. Vulnerabilidades Digitais

As vulnerabilidades digitais estão intimamente ligadas aos sistemas de gestão da rede de cabos submarinos, instalados nos centros de dados. Os centros de dados, por serem propriedade privada, oferecem aos seus operadores o controlo centralizado sobre os componentes físicos e digitais dos cabos submarinos, através de uma única localização. Esta localização, pelas suas capacidades integrais de controlo de rede, funciona como um botão de ligar e desligar a transmissão de dados (Sechrist, 2012).

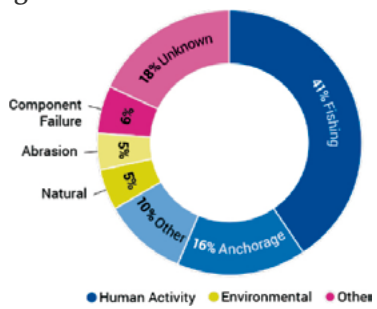
Esta vulnerabilidade é intensificada pela existência de sistemas, de gestão de redes de cabos submarinos, com operação remota. A multiplicação das formas de acesso que cada administrador pode utilizar para aceder ao sistema de gestão da rede de cabos submarinos aumenta o número de dispositivos que podem ser comprometidos para efetuar ações maliciosas contra a infraestrutura (Sunak, 2017).

Em 2022, foi reportado nos Estados Unidos da América o único ataque, desta natureza, contra cabos submarinos (Temple-Raston e Powers, 2022). De acordo com as autoridades americanas, um grupo internacional de *hackers* teve como alvo a infraestrutura em Oahu, violando os servidores de uma empresa privada que gere um cabo submarino que liga o Hawai aos restantes países da região do Pacífico (Boylan, 2022). Independentemente do meio em que se manifestam as vulnerabilidades descritas, destas advêm, forçosamente, ameaças à segurança física dos sistemas de cabos submarinos e à informação digital que neles circula. Essas ameaças originam, anualmente, centenas de danos que afetam a integridade dos sistemas e a capacidade de transmissão dos cabos submarinos (Clare, 2021).

3. Ameaças e Danos aos Cabos Submarinos

Relativamente à origem dos danos a cabos submarinos, podemos identificar três categorias: Humana, Ambiental e Outras (Figura 4). Os danos de origem humana são os mais frequentes por resultarem da atividade de navegação marítima regular – pesca de arrasto, dragagem ou ancoragem. Embora menos comuns, os danos de origem ambiental também podem ocorrer, resultantes da normal atividade geológica e biológica dos oceanos, como terramotos e mordidas de tubarão. Os restantes danos, aqui categorizados como de outra origem, acontecem muito raramente. É o caso das falhas de componentes e, sobretudo, das ações deliberadas de atores estatais e não estatais (Davenport, 2023).

Figura 4
Origem de danos a cabos submarinos



Fonte: Clare (2021).

Dentro das ações deliberadas não estatais encaixam os ataques cibernéticos realizados por *hackers* ou grupos de *ransomware*, com capacidade para perturbar os sistemas operativos dos cabos submarinos (Temple-Raston e Powers, 2022). Não obstante, o

principal desafio para a OTAN, no atual contexto geopolítico, são as ações deliberadas de atores estatais com recurso a sabotagem e espionagem (Davenport, 2018; Clare, 2021; Bueger *et al*., 2022; Pérez, 2023; Davenport, 2023). A este propósito, desde a explosão dos gasodutos[6] Nord Stream 1 e 2, muitos têm sido os relatos europeus de danos a cabos submarinos cuja causa se suspeita ser a sabotagem, deliberada e premeditada, destas infraestruturas submersas, por parte de atores estatais (ZMScable, 2022; Chiappa e Ngendakumana, 2023; Davenport, 2023; Kania, 2023).

Em outubro de 2022, três cabos submarinos foram cortados, interrompendo as ligações de internet entre Marselha, Lyon, Milão e Barcelona, o que tornou o acesso à Internet mais lento para os utilizadores europeus, asiáticos e americanos (PPLWARE SAPO, 2022; BBC NEWS, 2022). Na mesma altura, o cabo submarino que liga as Ilhas Faroé à Escócia, através das Ilhas Shetland e Orkney, foi danificado em dois incidentes separados, deixando a maioria das ilhas sem Internet (BBC NEWS, 2022).

Em fevereiro de 2023, os dois cabos que ligam as ilhas Matsu – controladas por Taiwan –, perto da costa chinesa, foram cortados, impedindo as 14 mil pessoas que lá habitam de aceder à Internet, durante dois meses (Wu e Lee, 2023; Kania, 2023). As autoridades de Taiwan identificaram a passagem de dois navios chineses perto do local onde o dano ocorreu, o que as levou a refletir sobre a falta de segurança e capacidade de reparação própria das 14 ligações por cabo submarino que garantem a sua conectividade (Wu e Lee, 2023; Kania, 2023).

Em outubro de 2023, o gasoduto Balticconector foi danificado, juntamente com dois cabos submarinos de comunicações que ligam Estónia, Finlândia e Suécia (Euronews, 2023). As autoridades finlandesas identificaram a passagem de um navio chinês e de um navio russo perto das zonas onde ocorreu o dano, suspeitando de ação estatal russa e chinesa neste incidente (Kubiak, 2023).

A ocorrência de falhas múltiplas de carácter simultâneo no mesmo cabo submarino ou em cabos submarinos próximos, excluindo causas naturais, é altamente incomum (PPLWARE SAPO, 2022; Bueger *et al*., 2022). O atual contexto geopolítico, aliado aos exemplos descritos *supra,* sustenta as preocupações da OTAN e da UE no domínio dos cabos submarinos, originando uma nova realidade quanto à possibilidade de os danos a esta infraestrutura passarem a ser de ações estatais deliberadas e maliciosas (Bueger *et al*., 2022).

Esta nova realidade acarreta implicações securitárias e políticas significativas, não só para a OTAN mas também para Portugal que, pela sua centralidade atlântica, tem vindo a assumir uma importância cada vez mais nevrálgica nas rotas de cabos

6 A 26 de setembro 2022, uma série de explosões e vazamentos de gás ocorreram nos gasodutos Nord Stream 1 e Nord Stream 2, construídos para transportar gás natural da Rússia para a Alemanha. Sabe-se que os vazamentos foram causados por sabotagem intencional.

submarinos, contando já com ligações de cabos submarinos a todos os continentes, exceto a Antártida (ANACOM, 2020).

4. Implicações Securitárias e Políticas para a Aliança

As implicações securitárias e políticas, decorrentes de ações estatais de sabotagem e espionagem a sistemas de cabos submarinos, não são totalmente desconhecidas, especialmente, em contexto de conflito armado (Davenport, 2023; Pérez, 2023; Guilfoyle, *et al.*, 2022; Medeiros e Pinto, 2023). A dependência militar desta infraestrutura, para efeitos defensivos e de guerrilha, é bem conhecida, tendo a danificação de sistemas de cabos submarinos sido, historicamente, utilizada para destabilizar inimigos durante conflitos armados[7] (Davenport, 2023; Guilfoyle *et al.*, 2022; Sunak, 2017; Kania, 2023). Apesar disso, a evolução da tecnologia dos cabos submarinos, agora considerada como universal e indispensável para o funcionamento "normal" das sociedades, bem como de outras tecnologias de sensorização, recolha, tratamento e armazenamento de dados, aporta novas ramificações. As capacidades e meios disponíveis para efetuar ações hostis desta natureza foram ampliadas, ao mesmo tempo que se maximizaram as consequências resultantes dessas ações (Guilfoyle *et al.*, 2022). Assim, Estados não aliados estão capacitados para efetuar ações coordenadas e simultâneas a vários cabos submarinos, o que poderá isolar e paralisar os Estados-alvo, comprometendo as suas capacidades militares, económicas e políticas de defesa e fragilizando a atuação da OTAN.

4.1. Implicações Securitárias de Ação Estatal: os Modi Operandi *da China e da Rússia*

A República Popular da China, com a crescente relevância mundial de empresas estatais chinesas, como a HMN Technologies, principal fabricante de sistemas de cabos submarinos, e operadoras de telecomunicações estatais, como a China Mobile e a China Telecom, constitui uma ameaça à integridade digital da informação que circula nos cabos submarinos (Brock, 2023; Pérez, 2023; Kania, 2023). Mudanças nos padrões de roteamento da rede teriam um efeito direto no tráfego, e o monopólio de negócios internacionais relacionados com o fabrico, a instalação e a reparação de cabos submarinos, pode gerar dependência tecnológica entre os países que interligam os sistemas de cabos (Schadlow e Helwig, 2020). Adicionalmente, os Estados Aliados, muito embora descartem, de momento, a capacidade para extração de dados

7 A 5 de agosto de 1914, a primeira ação militar do Reino Unido contra a Alemanha, após a declaração de guerra, foi o corte dos seus cinco cabos submarinos transatlânticos.

a grandes profundidades, estão convencidos de que existe a capacidade tecnológica para interferir nas comunicações, através de *backdoors* inseridos nos sistemas de cabos submarinos, durante o processo de fabrico e instalação (Schadlow e Helwig, 2020; Pérez, 2023; Walland e Morcos, 2021).

Já a Federação Russa representa um tipo de ameaça mais convencional à integridade física dos sistemas de cabos submarinos. O seu extenso programa de rearmamento, focado no aumento das suas capacidades navais e submersas, resultou na criação da maior frota de embarcações de profundidade do mundo (GFP Strenght in Numbers, 2024; Sunak, 2017; Nilsen, 2018). Esta frota de submarinos e navios de superfície equipados com submergíveis tripulados e não tripulados permite à Rússia manipular objetos a grandes profundidades, intercetar comunicações e destruir infraestrutura submersa (Metrick *et al*., 2016; Sunak, 2017).

É sabido, por isso, que tanto a Rússia como a China dispõem dos meios navais necessários para realizar ataques contra os sistemas de cabos submarinos em águas profundas: submarinos, embarcações submergíveis tripuladas e não tripuladas, e embarcações de superfície com capacidade cartográfica e grande alcance de profundidade (Sunak, 2017). Além destes meios operacionais, ambos os países possuem meios científicos e tecnológicos que permitem a colocação de sensores nos cabos submarinos, que aliados ao mapeamento das rotas de cabos submarinos e ao estudo do comportamento dos objetos submersos, poderá, a longo prazo, informar, de forma inédita, a atividade militar, comprometendo a capacidade de as embarcações Aliadas, tripuladas e não tripuladas, circularem de forma indetetável (Chen *et al*., 2022; Iqbal, 2023; Hlongwa, 2021; Jankowski, 2021; NATO STO-CMRE, 2023).

4.2. Implicações Políticas: a Gestão e Manutenção dos Cabos Submarinos

Pela sua natureza crítica, seria desejável que a gestão e manutenção dos sistemas de cabos submarinos fosse delineada de forma estratégica e coordenada, entre as entidades estaduais e os proprietários da infraestrutura. No entanto, tal não acontece (Kania, 2023).

Sendo a maior parte da infraestrutura de cabos submarinos propriedade de entidades privadas, essas entidades têm o poder de decidir quais os cabos que instalam, quando instalam e onde os instalam. Daqui resultam jogos de poder financeiro e geopolítico entre estas empresas e os Estados, verificando-se uma concentração de cabos muito maior no Atlântico Norte do que no Atlântico Sul (Figura 1) (Medeiros e Pinto, 2023; Pérez, 2023).

A fragilidade e dependência que os Estados do Atlântico Sul possuem em relação à estrutura de cabos submarinos existentes no Atlântico Norte traduz-se, de forma inequívoca, numa menor capacidade para desenvolvimentos tecnológicos e de defesa

cibernética (Medeiros e Pinto, 2023). Desta forma, é expectável que, na pendência de regime jurídico internacional específico para o efeito, haja a ocorrência de conflitos sobre que cabos devem ser instalados, que traçado devem seguir e que pontos de amarração devem utilizar.

Se a mera decisão sobre a instalação de cabos gera conflitos e desigualdades, as decisões relativamente à manutenção e reparação dos cabos trazem ainda mais dificuldades. Sendo propriedade privada, o ónus da manutenção e reparação dos cabos recai sobre o proprietário da infraestrutura danificada e, como tal, é este que decide que cabos reparar e porque ordem o deve fazer. No entanto, perspetivando-se a ocorrência de danos múltiplos e simultâneos, por parte de ator estatal, parece-nos dúbio que o ónus de reparação continue a recair sobre o proprietário da infraestrutura, estando esta questão pendente de regime jurídico próprio (Burnett, 2022).

O referido regime jurídico deverá acautelar, simultaneamente, a dificuldade de atribuição de culpa/responsabilização pela danificação simultânea de vários cabos por parte de ator estatal, bem como assegurar a existência de equidade relativamente ao ónus da obrigação de cobrir os custos de reparação do cabo em si (Davenport, 2023). Reformulando, muito embora a infraestrutura em causa seja propriedade privada, dada a sua inegável utilidade pública e, podendo a mesma ser alvo de ação hostil estatal causadora de dano, não deve o ónus de reparação recair apenas sobre o proprietário da infraestrutura.

5. Conclusões e Recomendações

À medida que aumenta a dependência societária, económica, militar e governamental dos sistemas de cabos submarinos, aumentam as preocupações relativas à sua segurança. Desta forma, é expectável que a temática da natureza crítica dos cabos submarinos continue a ganhar relevância a nível global. Não só por trazer consigo o desejado aumento da conectividade e de avultados investimentos, mas sobretudo pelas implicações e vulnerabilidades securitárias que acarreta, especialmente, no contexto geopolítico atual.

A este propósito, muitas têm sido as situações reportadas de danos a cabos submarinos em que existe forte suspeita sobre o carácter intencional e estatal do dano. A OTAN e a UE já reconheceram tanto a natureza crítica como a vulnerabilidade estratégica adjacente aos cabos submarinos. Os esforços individuais e conjuntos para identificação e mitigação de vulnerabilidades a estas infraestruturas, bem como o desenvolvimento de estratégias e planos de ação, são prova disso mesmo.

Assim, também Portugal deve mapear as vulnerabilidades existentes e desenvolver os mecanismos jurídicos necessários para regular a proteção física, cibernética e geopolítica dos cabos submarinos que atravessam o seu território, em estreita coo-

peração com as entidades privadas proprietárias da infraestrutura e com todos os parceiros envolvidos na operação e reparação dos sistemas de cabos submarinos. A Segurança Nacional e da Aliança disso depende.
As recomendações que se seguem são um contributo para que Portugal comece a caminhar na direção certa:

- **Assegurar a segurança física dos componentes terrestres dos sistemas de cabos submarinos** – é necessário adotar medidas de segurança física de forma a manter os colaboradores, as instalações e ativos dos sistemas de cabos submarinos protegidos das ameaças existentes. Isto inclui, de forma não exaustiva, a obrigatoriedade de implementação de medidas relativas à instalação de controlos de acesso (cartões de identificação e restrições biométricas) e a adoção de medidas de vigilância ativa permanente (por exemplo, alarmes, guardas e videovigilância).
- **Tornar obrigatória a instalação de equipamentos de monitorização nos componentes marítimos dos sistemas de cabos submarinos** – a instalação de sensores para frequências sonar nos cabos submarinos permitirá identificar, em tempo real, a ocorrência de situações suspeitas nas proximidades dos cabos (como a passagem de veículos submersíveis) e originar uma comunicação célere às autoridades responsáveis pela sua segurança.
- **Aumentar a diversidade geográfica tanto das rotas de cabos como das estações de amarração** – a dispersão geográfica de rotas e estações de amarração (por exemplo, no Algarve e no norte de Portugal continental) aumentará a redundância e a resiliência da rede diminuindo eventuais pontos de estrangulamento.
- **Acelerar a classificação dos sistemas de cabos submarinos como infraestruturas críticas** – embora já esteja em curso o processo espoletado pelo Decreto-Lei n.º 20/2022, de 28 de janeiro, que veio alargar às comunicações, infraestruturas e prestadores de serviços digitais, os procedimentos para a identificação e designação de infraestruturas críticas, até hoje não se veem avanços neste processo. Dada a necessidade de agir rapidamente, para garantir o reforço da proteção deste tipo de infraestruturas, será importante que seja atribuída aos sistemas de cabos submarinos prioridade máxima.
- **Criar uma estrutura de coordenação para a proteção dos sistemas de cabos submarinos** – esta estrutura, que deverá servir de mecanismo para a partilha de informação sobre incidentes com os cabos submarinos e com a sua infraestrutura terrestre, deverá incluir, não só todas as entidades envolvidas na instalação e operação dos cabos submarinos, mas também todas aquelas que têm competências legais e capacidades operacionais para contribuir de forma efetiva para a segurança destas infraestruturas; a sua criação deverá, também, ser independente do processo de identificação de infraestruturas críticas atualmente em curso neste setor.

- **Incentivar a criação/robustização do regime jurídico internacional para proteção dos cabos submarinos** – os sistemas de cabos submarinos, pela sua criticidade e complexidade, requerem uma abordagem holística e punitiva. Um novo tratado internacional sobre a temática deverá proteger estes sistemas e tornar a interferência com os mesmos mais onerosa para o infrator, incluindo normas sobre cooperação mútua, partilha de informação e facilitadoras da atribuição da responsabilidade em casos de dano.
- **Fomentar a realização de exercícios nacionais e no âmbito da OTAN sobre a proteção de cabos submarinos** – a realização de exercícios/simulacros para proteção dos sistemas de cabos submarinos, contra ameaças internacionais, permitirá instruir todos os intervenientes e identificar oportunidades de melhoria nos procedimentos existentes, incluindo cenários de reconhecimento hostil como os perpetrados, de forma persistente, pela Rússia no Atlântico Norte.

Bibliografia

ANACOM, 2020. *ANACOM* [Online]. Disponível em: https://www.anacom.pt/render.jsp?contentId=1538121 [Acedido 09 01 2024].

Arthur, C., 2013. *The Guardian* [Online]. Disponível em: https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests [Acedido 25 01 2024].

Bafoutsou, G., Papaphilippou, M., Dekker, M. e ENISA, 2023. *SUBSEA CABLES – WHAT IS AT STAKE?,* Luxembourg: ENISA.

BBC NEWS, 2022. *BBC NEWS* [Online]. Disponível em: https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102 [Acedido 25 01 2024].

Boylan, P., 2022. *Star Advertiser* [Online]. Disponível em: https://www.staradvertiser.com/2022/04/12/breaking-news/cyberattack-on-hawaii-undersea-communications-cable-thwarted-by-homeland-security/ [Acedido 25 01 2024].

Brock, J., 2023. *REUTERS* [Online]. Disponível em: https://www.reuters.com/investigates/special-report/us-china-tech-cables/ [Acedido 08 01 2024].

Bueger, C., *et al.*, 2022. *Atlantic Centre* [Online]. Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_13.pdf [Acedido 25 01 2024].

Bueger, C., Liebetrau, T. e Franken, J., 2022. *Europarl* [Online]. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf [Acedido 08 01 2024].

Burnett, D. R., 2022. *A Reboot of Wartime Submarine Fiber Optic Cables,* Virginia, USA: Submarine Telecoms Forum Magazine.

Chen, J., *et al.*, 2022. A Critical Examination for Widespread Usage of Shipping Big Data Analytics in China. *Journal of Marine Science and Engineering,* 10(12), pp. 1-19.

Chiappa, C. e Ngendakumana, P. E., 2023. *Politico* [Online]. Disponível em: https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/ [Acedido 09 01 2024].

Clare, M., 2021. *International Cable Protection Committee* [Online]. Disponível em: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf [Acedido 08 01 2024].

Colavito, C., 2023. *GNOSIS* [Online]. Disponível em: https://gnosis.aisi.gov.it/Gnosis/Rivista74.nsf/ServNavig/74-20.pdf/$File/74-20.pdf?openElement [Acedido 25 01 2024].

Conselho Europeu, 2022. *Consilium Europa* [Online]. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/ [Acedido 24 01 2024].

Conselho Europeu, 2023. *Consilium Europa* [Online]. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2023/10/24/maritime-security-council-approves-revised-eu-strategy-and-action-plan/ [Acedido 24 01 2024].

CSRIC, W. 4. S. C. R., 2016. *Clustering of Cables and Cable Landings,* Washington: CSRIC - Communications Security, Reliability and Interoperability Council.

Davenport, T., 2015. Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. *Catholic University Journal of Law and Technology,* 24(1), pp. 57-109.

Davenport, T., 2018. *Cambridge University* [Online]. Disponível em: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/C67248AD17B1F960E885C83EA-8F537AB/S239877231800048Xa.pdf/the-high-seas-freedom-to-lay-submarine-cables-and-the-protection-of-the-marine-environment-challenges-in-high-seas-governance.p [Acedido 08 01 2024].

Davenport, T., 2023. *Hoover Institution* [Online]. Disponível em: https://www.hoover.org/sites/default/files/research/docs/Davenport_finalfile_WebReadyPDF.pdf [Acedido 09 01 2024].

Donn, N., 2023. *Portugal Resident* [Online]. Disponível em: https://www.portugalresident.com/russia-spies-on-underwater-cabling-has-portugal-on-its-radar/ [Acedido 08 01 2024].

Euronews, 2016. *Euronews* [Online]. Disponível em: https://pt.euronews.com/2016/07/05/acesso-a-internet-e-um-direito-humano-diz-onu [Acedido 08 01 2024].

Euronews, 2023. *Euronews* [Online]. Disponível em: https://www.euronews.com/2023/10/10/baltic-gas-pipeline-leak-likely-caused-by-external-activity-says-finlands-president [Acedido 25 01 2024].

EuroNews, 2023. *EuroNews* [Online]. Disponível em: https://pt.euronews.com/2023/01/11/ue-e-nato-aliam-se-para-proteger-as-infraestruturas-criticas-da-europa [Acedido 12 01 2024].

Gallagher, J. C., 2022. *Congressional Research Service Reports* [Online]. Disponível em: https://crsreports.congress.gov/product/pdf/R/R47237 [Acedido 08 01 2024].

GFP Strenght in Numbers, 2024. *GFP Strenght in Numbers* [Online]. Disponível em: https://www.globalfirepower.com/navy-ships.php [Acedido 11 01 2024].

Guilfoyle, D., Paige, T. P. e Rob, M., 2022. The Final Frontier Of Cyberspace: The Seabed Beyond National Jurisdiction And The Protection Of Submarine Cables. *International & Comparative Law Quarterly,* 71(3), pp. 657-696.

Guimarães, A., 2023. *CNN PT* [Online]. Disponível em: https://cnnportugal.iol.pt/cabos-submarinos/espionagem/a-ameaca-que-se-esconde-no-mar-de-portugal-sabotagem-dos-cabos-submarinos-seria-uma-catastrofe/20230619/6478cc60d34ef47b87548052 [Acedido 05 01 2024].

Hlongwa, L. N., 2021. Artificial intelligence and big data in the Maritime Silk Road Initiative: The road towards Sea Power 2.0. *South African Journal of Military Studies*, 49(2), pp. 113-131.

Howell, C. e West, D. M., 2016. *Brookings* [Online]. Disponível em: https://www.brookings.edu/articles/the-internet-as-a-human-right/ [Acedido 08 01 2024].

Iqbal, A., 2023. *Paradigm Shift* [Online]. Disponível em: https://www.paradigmshift.com.pk/chinas-artificial-intelligence/ [Acedido 11 01 2024].

Jankowski, D. P., 2021. *Center for Strategic e International Studies* [Online]. Disponível em: https://www.csis.org/analysis/russia-and-technological-race-era-great-power-competition [Acedido 11 01 2024].

Kania, E. B., 2023. *Rajaratnam School of International Studies* [Online]. Disponível em: https://www.rsis.edu.sg/wp-content/uploads/2023/08/CO23113.pdf [Acedido 26 01 2024].

Kravets, D., 2011. *WIRED* [Online]. Disponível em: https://www.wired.com/2011/06/internet-a-human-right/ [Acedido 08 01 2024].

Kubiak, M., 2023. *The Jamestown Foundation* [Online]. Disponível em: https://jamestown.org/program/balticconnector-leak-highlights-need-for-stronger-coordination-in-protecting-critical-infrastructure/ [Acedido 25 01 2024].

Leppard, D., 2007. *The Times* [Online]. Disponível em: https://www.thetimes.co.uk/article/al-qaeda-plot-to-bring-down-uk-internet-b8vb32twcwt [Acedido 25 01 2024].

Medeiros, S. E. e Pinto, D. J. A., 2023. *Defesa* [Online]. Disponível em: https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_11.pdf [Acedido 05 01 2024].

Metrick, A., Weinberger, K. e Hicks, K. H., 2016. *Center for Strategic e International Studies* [Online]. Disponível em: https://www.csis.org/analysis/undersea-warfare-northern-europe [Acedido 11 01 2024].

Miranda, N., 2023. *Mapfre Global Risks* [Online]. Disponível em: https://www.mapfreglobalrisks.com/pt-br/gerencia-riscos-seguros/estudos/cabos-submarinos-a-maior-rede-mundial-de-telecomunicacoes/ [Acedido 05 Janeiro 2024].

NATO STO-CMRE, 2023. *CMRE* [Online]. Disponível em: https://www.cmre.nato.int/research/publications/technical-reports/special-publications/1701-cmre-ar-2022/file [Acedido 11 01 2024].

NATO, 2023. *NATO* [Online]. Disponível em: https://www.nato.int/cps/en/natohq/news_211919.htm [Acedido 12 01 2024].

Nilsen, T., 2018. *The Barents Observer* [Online]. Disponível em: https://thebarentsobserver.com/en/node/3381 [Acedido 11 01 2024].

Nunes, F., 2023. *Eco* [Online]. Disponível em: https://eco.sapo.pt/2023/05/04/russia-esta-a-espiar-cabos-submarinos-e-tem-portugal-no-radar/ [Acedido 08 01 2024].

Pérez, R. G., 2023. *IEEE* [Online]. Disponível em: https://www.ieee.es/Galerias/fichero/docs_marco/2023/DIEEEM10_2023_RAFGAR_Submarinos.pdf [Acedido 05 01 2024].

PPLWARE SAPO, 2022. *PPLWARE SAPO* [Online]. Disponível em: https://pplware.sapo.pt/informacao/cabos-submarinos-europeus-de-comunicacoes-foram-cortados-nesta-quarta-feira/ [Acedido 25 01 2024].

Schadlow, N. e Helwig, B., 2020. *Defense News* [Online]. Disponível em: https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/ [Acedido 12 01 2024].

Schochet, N. e Carr, E., 2023. *The Diplomat* [Online]. Disponível em: https://thediplomat.com/2023/08/navigating-china-us-subsea-cable-competition/ [Acedido 08 01 2024].

Sechrist, M., 2012. *New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems,* Boston: Harvard Kennedy School.

Siebold, S., 2023. *REUTERS* [Online]. Disponível em: https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/ [Acedido 08 01 2024].

Submarine Telecoms Forum, 2022/2023. *Industry Report* [Online]. Disponível em: https://issuu.com/subtelforum/docs/submarine_telecoms_indsutry_report_issue_11?fr=xKAE9_zU1NQ [Acedido 10 01 2024].

Sunak, R., 2017. *Policy Exchange* [Online]. Disponível em: https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf [Acedido 11 01 2024].

Symington, A., 2023. *The Wold's Shipping Lanes.* [Art] (PhytonMaps).

Symington, A., 2023. *The World's Undersea Cables.* [Art] (PhytonMaps).

Telegeography, 2023. *Submarine Cable Map* [Online]. Disponível em: https://submarine-cable-map-2023.telegeography.com/ [Acedido 10 01 2024].

Temple-Raston, D. e Powers, S., 2022. *The Record* [Online]. Disponível em: https://therecord.media/who-tried-to-hack-hawaiis-undersea-cable [Acedido 10 01 2024].

Trakimavičius, L., 2021. *NATO ENSEC COE* [Online]. Disponível em: https://www.enseccoe.org/data/public/uploads/2021/12/the-hidden-threat-to-baltic-undersea-power-cables-final.pdf [Acedido 08 01 2024].

Tully, S., 2014. A Human Right to Access the Internet? Problems and Prospects. *Human Rights Law Review,* 14(2), pp. 175-195.

United Nations Human Rights Council 47th Session, 2021. *The promotion, protection and enjoyment of human rights on the Internet,* New York: United Nations.

Walland, C. e Morcos, P., 2021. *Center for Strategic e International Studies* [Online]. Disponível em: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security [Acedido 12 01 2024].

Wu, S. e Lee, Y., 2023. *REUTERS* [Online]. Disponível em: https://www.reuters.com/world/asia-pacific/fear-dark-taiwan-sees-wartime-frailty-communication-links-with-world-2023-03-15/ [Acedido 25 01 2024].

ZMScable, 2022. *ZMScable* [Online]. Disponível em: https://zmscable.es/pt/cortan-cables-submarinos-britanicos-franceses/ [Acedido 09 01 2024].