

ESCOLA DE GUERRA NAVAL

CC RODRIGO FRAGA NOGUEIRA

PROTEÇÃO DE CABOS SUBMARINOS:

Avaliação das práticas britânicas e recomendações para o Brasil

Rio de Janeiro

2024

CC RODRIGO FRAGA NOGUEIRA

**PROTEÇÃO DE CABOS SUBMARINOS:
Avaliação das práticas britânicas e recomendações para o Brasil**

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CMG (RM1) PEÇANHA

Rio de Janeiro
Escola de Guerra Naval
2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Os direitos morais e patrimoniais deste trabalho acadêmico, nos termos da Lei 9.610/1998, pertencem ao seu Autor, sendo vedado o uso comercial sem prévia autorização. É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que seja feita a referência bibliográfica completa.

Os conceitos e ideias expressas neste trabalho acadêmico são de responsabilidade do Autor e não retratam qualquer orientação institucional da EGN ou da Marinha do Brasil.

DEDICATÓRIA

Dedico este projeto a todos os professores que me influenciaram na minha trajetória. Em especial ao professor e meu orientador, com quem compartilhei minhas dúvidas e angústias a respeito do tema.

AGRADECIMENTOS

Sou profundamente grato a todos que colaboraram para a finalização deste trabalho acadêmico.

Em primeiro lugar, agradeço a Deus por me conceder a sabedoria necessária para enfrentar os desafios nesta nobre missão de gerar conhecimento.

Agradeço também à minha família por compreender minha ausência, mesmo quando estava presente.

Ao meu orientador, que sempre acreditou no meu sucesso e na minha conquista, sempre me motivando e de fato orientando.

Finalmente, expresso minha gratidão à Escola de Guerra Naval, seus oficiais e praças, pelo suporte indispensável ao meu desenvolvimento profissional e intelectual.

Obrigado.

RESUMO

Esta dissertação investiga a proteção dos cabos submarinos, com foco nas práticas adotadas pelo Reino Unido, e analisa como essas práticas podem ser aplicadas no contexto brasileiro para fortalecer a segurança dessa infraestrutura crítica. Cabos submarinos são essenciais para a comunicação global, transportando a maior parte dos dados digitais que sustentam a economia moderna, a segurança nacional e as interações internacionais. Embora sua importância estratégica seja indiscutível, esses cabos estão vulneráveis a uma variedade de ameaças, incluindo desastres naturais, acidentes, ciberataques e sabotagens. O estudo detalha as políticas implementadas pelo Reino Unido desde 2014, como a criação de centros de segurança marítima, o fortalecimento de parcerias internacionais e a introdução de tecnologias avançadas de vigilância e defesa. Também se destaca a relevância do *Joint Maritime Security Centre* (JMSC) e do navio de vigilância subaquática *Royal Fleet Auxiliary* (RFA) Proteus na resposta às ameaças crescentes. Com base na análise das práticas britânicas, a dissertação propõe cinco medidas para o Brasil: a criação de um centro nacional de coordenação para integrar as ações de diferentes setores; o fortalecimento da vigilância e monitoramento marítimo; o estabelecimento de parcerias internacionais com países experientes na proteção de cabos submarinos; o desenvolvimento de uma legislação específica para regular a proteção dessa infraestrutura; e a realização de exercícios militares conjuntos para melhorar a prontidão das forças de defesa. A conclusão destaca que, ao adotar essas medidas e aprender com as estratégias do Reino Unido, o Brasil estará mais bem preparado para enfrentar os desafios do século 21, garantindo a segurança de sua infraestrutura crítica, a continuidade das comunicações e a estabilidade econômica e política.

Palavras-chave: Proteção de Cabos Submarinos. Infraestrutura Crítica. Reino Unido. Brasil. Segurança Cibernética. Ameaças Geopolíticas. Estações Terrenas. Vigilância Subaquática. Estratégia de Defesa. Sistema de Gerenciamento da Amazônia Azul. Comunicações Globais.

ABSTRACT

Protection of Submarine Cables: Assessment of British practices and recommendations for Brazil

This dissertation investigates the protection of submarine cables, focusing on the practices adopted by the United Kingdom and analyzing how these practices can be applied in the Brazilian context to strengthen the security of this critical infrastructure. Submarine cables are essential for global communication, carrying the majority of digital data that sustains the modern economy, national security, and international interactions. Despite their undeniable strategic importance, these cables are vulnerable to a variety of threats, including natural disasters, accidents, cyberattacks, and sabotage. The study details the policies implemented by the United Kingdom since 2014, such as the creation of maritime security centers, strengthening international partnerships, and the introduction of advanced surveillance and defense technologies. The significance of the Joint Maritime Security Centre (JMSC) and the underwater surveillance vessel Royal Fleet Auxiliary (RFA) Proteus in responding to rising threats is also emphasized. Based on the analysis of British practices, the dissertation proposes five measures for Brazil: the creation of a national coordination center to integrate actions across various sectors; strengthening maritime surveillance and monitoring; establishing international partnerships with countries experienced in protecting submarine cables; developing specific legislation to regulate the protection of this infrastructure; and conducting joint military exercises to improve defense forces' readiness. The conclusion highlights that by adopting these measures and learning from the United Kingdom's strategies, Brazil will be better prepared to face the challenges of the 21st century, ensuring the security of its critical infrastructure, the continuity of communications, and economic and political stability.

Keywords: Submarine Cable Protection. Critical Infrastructure. United Kingdom. Brazil. Cybersecurity. Geopolitical Threats. Ground Stations. Underwater Surveillance. Defense Strategy. Blue Amazon Management System. Global Communications.

LISTA DE ABREVIATURAS E SIGLAS

| | |
|---------|--|
| AJB | Águas Jurisdicionais Brasileiras |
| ACMA | <i>Atlantic Cable Maintenance & Repair Agreement</i> |
| ANATEL | Agência Nacional de Telecomunicações |
| AUKUS | <i>Australia, United Kingdom, United States</i> |
| BMD | Banco multilateral de desenvolvimento |
| CLS | <i>Continuous Linked Settlement</i> |
| CNUDM | Convenção das Nações Unidas sobre o Direito do Mar |
| COMPAAz | Comando de Operações Marítimas e Proteção da Amazônia Azul |
| EDM | Estratégia de Defesa Marítima |
| EU | União Europeia |
| EUA | Estados Unidos da América |
| GIUK | <i>Greenland–Iceland–United Kingdom</i> |
| IBAMA | Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis |
| IC | Infraestrutura Crítica |
| ICPM | Infraestruturas Críticas do Poder Marítimo |
| JMSC | <i>Joint Maritime Security Centre</i> |
| LESTA | Lei de Segurança do Tráfego Aquaviário |
| MB | Marinha do Brasil |
| MECMA | <i>Mediterranean Cable Maintenance Agreement</i> |
| MROSS | <i>Multi-Role Ocean Surveillance Ship</i> |
| NSS | Navio de Socorro Submarino |
| OBE | Objetivo Estratégico |
| ONU | Organização das Nações Unidas |
| OTAN | Organização do Tratado do Atlântico Norte |
| PEM | Plano Estratégico da Marinha |
| PIB | Produto Interno Bruto |
| PNSIC | Política Nacional de Segurança de Infraestruturas Críticas |
| RFA | <i>Royal Fleet Auxiliary</i> |

| | |
|---------|--|
| SACS | <i>South Atlantic Cable Systems</i> |
| SAIL | <i>South Atlantic Inter Link</i> |
| SisGAAz | Sistema de Gerenciamento da Amazônia Azul |
| SSN | <i>Submarino de ataque de uso geral com propulsão nuclear</i> <i>(Nuclear-powered general-purpose attack submarine)</i> |
| SWIFT | <i>Society for Worldwide Interbank Financial</i> <i>Telecommunications</i> |

SUMÁRIO

| | | |
|----------|--|----|
| 1 | INTRODUÇÃO | 11 |
| 2 | CABOS SUBMARINOS: UMA PERSPECTIVA INTERNACIONAL ABRANGENTE | 14 |
| 2.1 | A IMPORTÂNCIA DA INFRAESTRUTURA CRÍTICA DOS CABOS SUBMARINOS..... | 14 |
| 2.2 | GRANDES INTERESSADOS, MAIORES INVESTIDORES E EMPRESAS FABRICANTES DE CABOS SUBMARINOS..... | 16 |
| 2.3 | EMPRESAS DE MANUTENÇÃO DE CABOS SUBMARINOS E OS REPAROS REALIZADOS..... | 19 |
| 2.4 | SEGURANÇA DOS CABOS SUBMARINOS E SUAS ESTAÇÕES TERRENAS: AMEAÇAS E RISCOS..... | 21 |
| 2.5 | IMPACTOS FINANCEIROS E ECONÔMICOS POR DANOS NOS CABOS SUBMARINOS..... | 24 |
| 2.6 | A CAPACIDADE DE SABOTAGEM E ESPIONAGEM EM CABOS SUBMARINOS..... | 25 |
| 2.7 | LEGISLAÇÃO INTERNACIONAL PERTINENTE..... | 26 |
| 2.8 | CONCLUSÃO PARCIAL..... | 27 |
| 3 | O REINO UNIDO E OS CABOS SUBMARINOS | 29 |
| 3.1 | POSTURA ESTRATÉGICA ADOTADA, DE 2014 A 2024, NO QUE SE REFERE À PROTEÇÃO DOS CABOS SUBMARINOS DE COMUNICAÇÕES..... | 29 |
| 3.2 | A IMPORTÂNCIA DADA AOS CABOS SUBMARINOS..... | 30 |
| 3.3 | A PERCEPÇÃO DE AMEAÇAS E RISCOS..... | 32 |
| 3.4 | A INFRAESTRUTURA ESTRATÉGICA DOS CABOS SUBMARINOS INGLESES E SEUS PONTOS MAIS VULNERÁVEIS..... | 33 |
| 3.5 | AS PRÁTICAS ADOTADAS PARA A PROTEÇÃO DESSAS INFRAESTRUTURAS CRÍTICAS..... | 35 |
| 3.6 | CONCLUSÃO PARCIAL..... | 36 |
| 4 | BRASIL E OS CABOS SUBMARINOS | 38 |

| | | |
|----------|---|-----------|
| 4.1 | POSTURA ESTRATÉGICA ADOTADA, DE 2014 A 2024, NO QUE SE REFERE À PROTEÇÃO DOS CABOS SUBMARINOS DE COMUNICAÇÕES | 38 |
| 4.2 | A IMPORTÂNCIA DA DEFESA DOS CABOS SUBMARINOS | 40 |
| 4.3 | A PERCEPÇÃO DE AMEAÇAS E RISCOS | 41 |
| 4.4 | A INFRAESTRUTURA ESTRATÉGICA DOS CABOS SUBMARINOS BRASILEIROS E SEUS PONTOS MAIS VULNERÁVEIS | 43 |
| 4.5 | AS PRÁTICAS ADOTADAS PARA PROTEÇÃO DAS IC DE CABOS SUBMARINOS | 44 |
| 4.6 | CONCLUSÃO PARCIAL | 45 |
| 5 | ANÁLISE DAS PRÁTICAS DO REINO UNIDO E BRASIL PARA DEFENDER SUAS IC DE CABOS SUBMARINOS | 46 |
| 5.1 | ABORDAGEM DO REINO UNIDO NA PROTEÇÃO DE CABOS SUBMARINOS | 46 |
| 5.2 | ABORDAGEM DO BRASIL NA PROTEÇÃO DE CABOS SUBMARINOS | 46 |
| 5.3 | COMPARAÇÃO E SUGESTÕES DE MELHORIAS PARA O BRASIL | 47 |
| 5.4 | CONCLUSÃO PARCIAL | 48 |
| 6 | CONCLUSÃO | 49 |
| | REFERÊNCIAS | 51 |

1 INTRODUÇÃO

Este trabalho possui como propósito geral analisar as práticas de um país avançado como o Reino Unido, com o intuito de apresentar sugestões de melhorias para o Brasil, no que tange à segurança da sua Infraestrutura Crítica (IC) de cabos submarinos de comunicações. Abordará, assim, a importância estratégica dessas IC, destacando a sua relevância mesmo na era dos satélites de comunicações.

Serão apresentadas reflexões sobre a necessidade de uma proteção efetiva desse meio de propagação, com foco na realidade dos referidos países, de 2014 a 2024, considerando as ameaças crescentes observadas nesse período. Será apresentada, ainda, uma pesquisa abrangente, analisando como algumas das principais potências marítimas mundiais tratam a questão dos cabos submarinos em nível estratégico, seus desenvolvimentos no setor, os danos ocorridos e as ameaças mais recentes a essas IC.

Ao evidenciar e compreender os danos ocorridos e seus respectivos impactos às IC subaquáticas da Europa e em outras regiões do globo, especialmente nos cabos submarinos de comunicações e suas estações terrenas, as ameaças atuais e os impactos para a soberania e economia dos Estados afetados, o trabalho espera contribuir para elevar a consciência situacional da Defesa Nacional do Brasil.

O primeiro cabo submarino, instalado em 1850, conectou Dover (Reino Unido) a Calais (França) por meio do canal da Mancha, ligando ambos os países à rede de telégrafos terrestres (Burnett; Beckman; Davenport, 2023). Em 1858, a primeira mensagem telegráfica transatlântica foi transmitida entre Valentia (Irlanda) e Trinity Bay (Newfoundland), e mesmo tendo funcionado por poucas semanas, representou um ponto de inflexão na história (Dibner, 1959; Mwema; Birhane, 2024, p. 10).

Apenas em 1866 foi estabelecida uma conexão telegráfica confiável e permanente entre britânicos e americanos, o que revolucionou as comunicações globais ao permitir comunicação instantânea intercontinental (Dibner, 1959; UNESCO, 2023). Já no início do século 20, a Grã-Bretanha usava seu quase monopólio dos cabos submarinos para filtrar informações em crises, aproveitando o acesso exclusivo à informação para exercer poder sobre aqueles que não tinham essa vantagem (Coutau-Bégarie, 2010). Cabos submarinos e rádio permitiram ao Alto Comando Militar controlar operações em diversos teatros, o que possibilitou a coordenação entre

autoridades políticas aliadas, mesmo separadas por oceanos (Coutau-Bégarie, 2010, p. 562-563).

Na Segunda Guerra Mundial, os Aliados decifraram códigos japoneses e interceptaram comunicações de rádio, mas não mensagens transmitidas pelos cabos submarinos (Australia, 2019). Durante essa guerra, o submarino britânico anão XE-4 cortou o cabo telegráfico japonês para forçar comunicações via rádio, mais suscetíveis à interceptação (Boyd, 2022). Já em 1988, o primeiro cabo de fibra óptica transatlântico foi instalado, conectando os Estados Unidos da América (EUA), o Reino Unido e a França. Isso possibilitou a expansão global dos cabos de fibra óptica, o que conectou economias e sociedades, viabilizando a criação da internet (Frasca; Galantini, 2023, p. 52).

Recentemente, os cabos submarinos tornaram-se mais importantes devido aos avanços tecnológicos e à crescente dependência desse meio de comunicação. Por isso, eles têm sido alvo de ataques, sabotagens e danos acidentais (Davenport, 2023) por transportarem quase a totalidade das comunicações globais, incluindo informações civis, militares, voz e dados, principalmente de cunho financeiro e econômico (Clare, 2024).

Nos últimos dois séculos, cabos submarinos de comunicações destacaram-se como interfaces estáveis entre continentes, conectando pontos separados pelo oceano. Por outro lado, esses cabos têm sido objeto de disputas entre nações em conflito, usados como ferramenta de guerra (Medeiros; Pinto, 2022). A degradação intencional de cabos submarinos intercontinentais pode ter graves consequências, especialmente em termos de conectividade (Davenport, 2023); por exemplo, em 2008, o corte de três cabos submarinos entre o Egito e a Itália causou a perda de 90% das comunicações entre a Ásia e a Europa, afetando a internet em 14 países (Submarine Cable Networks, 2011).

Diante disso, a capacidade de proteger ou ameaçar cabos submarinos será essencial em futuros conflitos devido aos seus impactos econômicos e militares. Ataques coordenados podem forçar um adversário a recuar ou cortar suas forças de comando e inteligência. Tais ataques podem também impedir o controle de armas nucleares, o que levaria o país alvo a aumentar o alerta de segurança dessas armas ou iniciar um ataque preventivo (Clark, 2016).

O desenvolvimento de projetos como o Starlink da SpaceX e seu uso na Ucrânia aumentou a atenção em relação a satélites e segurança espacial, mas os

cabos submarinos permanecem essenciais no sistema de comunicações global. Nakamura (2023) afirma que a proteção desses cabos se tornou uma questão de segurança nacional e internacional, pois danos temporários a essas linhas de comunicação podem ter consequências graves.

Para o *International Cable Protection Committee* (2021), a segurança futura desse sistema depende da compreensão e exploração da tecnologia submarina. Segundo Lars Wedin (2015, p. 87), “estabelecer a vigilância da superfície não é mais o bastante; é todo o volume de água compreendido entre a superfície e o fundo que devem ser levados em consideração [...]”. Além disso, é necessário possuir os meios necessários para se contrapor às ameaças.

Diante do exposto, com base em uma pesquisa bibliográfica e metodologia comparativa, serão extraídos elementos de suporte investigativo para a comparação entre as práticas adotadas por Reino Unido e Brasil, no que tange à proteção dos cabos submarinos de comunicações e suas estações terrenas, com o intuito de apresentar sugestões de melhorias para o Brasil.

O capítulo 2 oferece uma visão geral do contexto histórico e atual dos cabos submarinos de comunicações globais, abordando a legislação internacional, além de examinar os riscos e ameaças a esses cabos e suas estações terrenas, ressaltando sua importância e os seus principais interessados.

Nos capítulos 3 e 4, a análise foca no Reino Unido e Brasil, com o objetivo de identificar: suas posturas estratégicas adotadas, de 2014 a 2024, no que se refere à proteção dos cabos submarinos de comunicações; a importância dada aos cabos submarinos; a percepção de ameaças e riscos; a IC de cabos submarinos de comunicações e seus pontos mais vulneráveis; e as práticas adotadas para a proteção desses cabos.

No capítulo 5, é realizada uma comparação do apurado nos capítulos 3 e 4, buscando-se analisar as práticas de um país avançado e apresentar sugestões de melhorias para o Brasil, voltadas à segurança da sua IC de cabos submarinos de comunicações. No capítulo 6, apresenta-se uma conclusão do trabalho.

2 CABOS SUBMARINOS: UMA PERSPECTIVA INTERNACIONAL ABRANGENTE

Este capítulo apresenta um panorama global do cenário histórico e atual dos cabos submarinos de comunicações no mundo, abordando brevemente a legislação internacional, os principais interessados, destacando os riscos e ameaças enfrentados por essa infraestrutura, ressaltando sua importância, assim como danos ocorridos e seus impactos.

2.1 A IMPORTÂNCIA DA INFRAESTRUTURA CRÍTICA DOS CABOS SUBMARINOS

A expressão “infraestrutura crítica” (IC) foi usada pela primeira vez pela Organização das Nações Unidas (ONU) na Resolução A/65/37, publicada em 7 de dezembro de 2010 (United Nations, 2010), na qual se destacou a relevância dos cabos submarinos para a economia global e a segurança nacional. Essa resolução representa um marco no reconhecimento da importância estratégica do sistema de cabos submarinos:

121. Também solicita aos Estados que tomem medidas para proteger os cabos submarinos de fibra óptica e que abordem integralmente as questões relacionadas a esses cabos, de acordo com o direito internacional, conforme refletido na Convenção; incentiva maior diálogo e cooperação entre os Estados e as organizações regionais e globais relevantes para promover a segurança dessa **infraestrutura crítica de comunicações** [...] ¹ (UNITED NATIONS, 2010, tradução nossa, grifo nosso).

Hendriks e Halem (2024a, p. 8) afirmam que: “Os cabos de fibra óptica submarinos são as artérias invisíveis da comunicação global”. Para Burgess (2022), a vasta rede global de cabos submarinos constitui a espinha dorsal da internet, a qual transporta a maioria dos dados globais e se conecta às redes que suportam torres de celular e conexões Wi-Fi.

Atualmente, a fibra óptica submarina é a única tecnologia capaz de suportar todo o tráfego de dados (Vichi; Pinto; Sá, 2020, p. 327), crucial para a transmissão rápida e a um custo menor que os satélites (Starosielski, 2015, p. 9). Os cabos

¹ 121. *Also calls upon States to take measures to protect fibre optic submarine cables and to fully address issues relating to these cables, in accordance with international law, as reflected in the Convention; encourages greater dialogue and cooperation among States and the relevant regional and global organizations to promote the security of such critical communications infrastructure [...]* (United Nations, 2010, cap. VIII, art. 121).

submarinos interconectam os países globalmente (Bueger; Liebetrau; Franken, 2022, p. 12) – com mais de 1,6 milhão de quilômetros de cabos subaquáticos, transportam mais de 99%² do tráfego de dados digitais mundial (Clare, 2024, p. 5) e têm cerca de 25 anos de vida útil (Clare, 2023). São vitais para a economia global, pois transmitem aproximadamente US\$ 10 trilhões em transações financeiras diárias.

Além do uso civil, os cabos submarinos são essenciais para a segurança nacional, coordenação de operações militares, missões diplomáticas e coleta de inteligência (Bueger; Liebetrau; Franken, 2022, p. 12), refletindo-se nas dinâmicas geopolíticas (Garcia, 2023, p. 70). Em vista disso, é primordial a proteção e a vigilância desses cabos para a funcionalidade dos sistemas sociais, econômicos, políticos e militares (Hendriks; Halem, 2024a, p. 10).

Com o aumento de atividades remotas, armazenamento em nuvem, 5G e Internet das Coisas, a dependência dos cabos submarinos crescerá (Bueger; Liebetrau; Franken, 2022). Toda a infraestrutura da internet depende não apenas de tecnologias na nuvem, mas também de cabos submarinos (Mwema; Birhane, 2024), que continuam sendo a forma mais rápida, eficiente e econômica de transmitir informações globais (Bueger; Liebetrau; Franken, 2022, p. 23).

A capacidade de implantar cabos submarinos é fundamental para a liberdade dos mares, permitindo o desenvolvimento das telecomunicações internacionais (Raha; Raju, 2021, p. 1). Nesse sentido, danos a esses cabos podem causar grandes prejuízos e afetar muitos interessados globalmente (Raha; Raju, 2021, p. 7), pois as economias modernas dependem dessas infraestruturas de comunicação, essenciais para a logística da produção de bens (Vichi; Pinto; Sá, 2020, p. 327).

A infraestrutura de cabos submarinos no Atlântico é primordial para a interconexão global, refletindo disputas de poder geopolítico entre grandes potências (Garcia, 2023, p. 69). A guerra na Ucrânia mudou a percepção das ameaças na Europa, tornando o Mar Mediterrâneo mais instável e vulnerável (Cassetta, 2024, p. 1), e destacando a dependência crescente desses cabos, bem como sua importância estratégica para a estabilidade econômica e política (Garcia, 2023, p. 71).

Segundo Wedin (2015, p. 172), “A guerra moderna no mar está fundamentada em uma grande medida nas informações”. Mudanças econômicas e tecnológicas

² Não há um consenso quanto a esse percentual. Para Mwema e Birhane (2024, p. 15), é considerado um percentual de 95%. Para Mendes (2023), também é apontado 95%, o que não deixa de evidenciar a dependência global desse meio.

estão transformando a segurança marítima, com o aumento dos cabos submarinos de dados e tecnologias de energia renovável *offshore* (Cassetta, 2024, p. 2).

Em 2010, a ONU destacou a importância dos cabos submarinos, essenciais para a economia global e segurança nacional, suportando comunicações militares, missões diplomáticas e transações financeiras. Com a crescente dependência digital, proteger esses cabos é crucial para a estabilidade econômica e política.

2.2 GRANDES INTERESSADOS, MAIORES INVESTIDORES E EMPRESAS FABRICANTES DE CABOS SUBMARINOS

A ONU e a Organização do Tratado do Atlântico Norte (OTAN) têm grande interesse nessa infraestrutura (Garcia, 2023, p. 76). Durante a Guerra do Vietnã, os EUA usaram cabos transoceânicos para comunicações seguras, evidenciando o interesse governamental (Starosielski, 2015, p. 42), com destaque para operações militares, missões diplomáticas e coleta de inteligência (Bueger; Liebetrau; Franken, 2022, p. 12).

Historicamente, os cabos eram propriedade de empresas privadas de telecomunicações, mas, recentemente, provedores de conteúdo como Google, Microsoft e Amazon têm investido em seus próprios cabos (Vichi; Pinto; Sá, 2020, p. 332). Assim, a gestão dos cabos é majoritariamente privada (Bueger; Liebetrau; Franken, 2022, p. 14), tendo as *Big Tech*³, como Google, Facebook⁴ e Microsoft, grande interesse nos cabos submarinos (Garcia, 2023, p. 73).

Empresas de telecomunicações buscam garantir redundância e confiabilidade em suas redes (Starosielski, 2015, p. 133). A crescente demanda por dados motiva investimentos em novos cabos submarinos (Clare, 2024, p. 5). Provedores de internet e telecomunicações dependem dessa infraestrutura para fornecer serviços de alta velocidade (Garcia, 2023, p. 75). Google e Meta justificam projetos de cabos como meios de reduzir a exclusão digital (Mwema; Birhane, 2024, p. 8).

Quanto aos governos nacionais, estes consideram a proteção dos cabos submarinos uma prioridade estratégica (Garcia, 2023, p. 74), pois passam por

³ Termo adotado para referenciar as grandes empresas de tecnologia, que dominam o mercado e alcançam sucesso no segmento em que atuam.

⁴ Desde 28 de outubro de 2021, o Facebook foi renomeado para Meta (Exame, 2022).

diversas jurisdições sem uma identidade soberana, deixando a segurança e proteção sob responsabilidade das empresas privadas (Vichi; Pinto; Sá, 2020, p. 332).

Mas será que essa IC é responsabilidade apenas da iniciativa privada?

Os cabos submarinos geralmente pertencem a consórcios, bancos multilaterais de desenvolvimento (BMD) ou proprietários únicos. O modelo de consórcio, responsável por 90% do financiamento nos últimos 30 anos, é o mais comum. Os BMD, como o Banco Mundial, oferecem financiamento favorável e flexível. O modelo de propriedade única, embora mais arriscado financeiramente, simplifica a gestão e é altamente rentável, impulsionado por economias de escala. *Big Techs* têm investido nesse modelo, adquirindo cabos exclusivos ou com poucos parceiros (Frasca; Galantini, 2023, p. 55-56).

Dessa forma, a expansão das infraestruturas de cabos submarinos foi facilitada por grandes empresas e governos (Starosielski, 2015, p. 35). Empresas de telecomunicações e consórcios multinacionais destinam investimentos bilionários à construção e manutenção de cabos submarinos para garantir a conectividade global (Clare, 2024, p. 8). Empresas como AT&T e Verizon continuam a investir em novas rotas para ampliar a capacidade de suas redes (Garcia, 2023, p. 80). E os governos também investem significativamente em cabos submarinos para garantir a segurança nacional (Raha; Raju, 2021, p. 24).

Os principais investidores em cabos submarinos são consórcios formados por operadoras de telecomunicações e empresas de tecnologia, que buscam assegurar a conectividade global (Raha; Raju, 2021, p. 62). A maior parte do financiamento para a infraestrutura de cabos submarinos provém de empresas privadas, que também são responsáveis por sua manutenção e operação (Vichi; Pinto; Sá, 2020, p. 332).

Nos últimos anos, a participação de empresas chinesas no mercado de cabos submarinos aumentou (Bueger; Liebetrau; Franken, 2022, p. 14), acirrando as disputas com o Ocidente. Novas empresas, como a *Global Crossing* e a *Level 3*, entraram no mercado e passaram a competir com as tradicionais de telecomunicações (Starosielski, 2015, p. 49).

Desde 2016, as *Big Tech* aumentaram seus investimentos, e em 2023 já detinham ou controlavam mais de 50% da capacidade dos cabos submarinos (Frasca; Galantini, 2023, p. 56). Além dos operadores de rede, Google, Amazon, Microsoft e Facebook têm aumentado seus investimentos para garantir a interconexão de seus

*data centers*⁵ (Bueger; Liebetrau; Franken, 2022, p. 14), a fim de atender às grandes demandas de dados e prover redundância (Raha; Raju, 2021, p. 8).

Os fabricantes de cabos submarinos fornecem tecnologia e materiais para transmissão eficiente de dados em longas distâncias (Mwema; Birhane, 2024, p. 9), sendo primordiais para a infraestrutura digital global e responsáveis pela produção e manutenção dos cabos que conectam diferentes localidades do mundo (Bueger; Liebetrau; Franken, 2022, p. 14). Empresas japonesas como *Nippon Electric Company* e *Ocean Cable Company* desenvolveram tecnologias avançadas na era dos cabos coaxiais (Starosielski, 2015, p. 42).

Os avanços tecnológicos possibilitaram o desenvolvimento de cabos mais robustos e com maior capacidade, respondendo à demanda por transmissão de dados (Raha; Raju, 2021, p. 12), no entanto o aumento no tráfego de dados requer mais cabos para suportar o crescimento (Vichi; Pinto; Sá, 2020, p. 332). Cabos modernos, como o Equiano do Google, possuem amplificadores internos para assegurar transmissões a longas distâncias (Mwema; Birhane, 2024, p. 10). Contudo, mesmo com esses avanços, a falta de padronização nos processos da indústria ainda é um desafio (Hendriks; Halem, 2024a, p. 25).

Os principais fabricantes de cabos submarinos são: *Alcatel Submarine Networks* (EUA), *SubCom* (EUA), *Prysmian Group* (Itália), *Huawei Marine Networks* (China), *Nexans* (França), *NKT A/S* (Dinamarca) e *NEC* (Japão) (Bueger; Liebetrau; Franken, 2022, p. 14; Raha; Raju, 2021, p. 24). Essas empresas oferecem tecnologia e *expertise* para assegurar a durabilidade e a eficiência dos cabos (Raha; Raju, 2021, p. 5).

Na última década, houve um aumento significativo dos investimentos ocidentais e da presença de empresas estatais chinesas, como *Huawei Marine Networks* e *Hentong*, no mercado de cabos submarinos. O interesse chinês nesse domínio estratégico (Bueger; Liebetrau; Franken, 2022, p. 14) torna a China um ator importante, com diversos projetos em andamento (Garcia, 2023, p. 84). O

⁵ Segundo o *DataCenter Dynamics* (2023), “Em cada extremidade de um cabo, há uma estação de aterragem de cabos, assim como um *data center*, que abriga equipamentos de rede importantes que alimentam o cabo e controlam suas operações”.

investimento em infraestrutura de cabos é parte da Rota da Seda Digital China, da Iniciativa Cinturão e Rota⁶ (Bueger; Liebetrau; Franken, 2022, p. 32).

Com isso, entende-se que as empresas fabricantes de cabos submarinos são essenciais para a infraestrutura digital global, visto que fornecem tecnologia avançada e materiais robustos. Enfrentam desafios como atrasos na produção e falta de padronização, mas continuam vitais para a conectividade global eficiente. Nesse cenário, o aumento da participação de empresas chinesas nesse setor estratégico atrai atenções.

Em suma, os principais interessados na proteção de cabos submarinos incluem indústrias de internet, telecomunicações, governos, empresas de tecnologia e organizações internacionais. A segurança desses cabos depende da cooperação entre o setor público e privado, essencial para garantir resiliência. Grandes empresas e governos impulsionam a expansão das infraestruturas, enquanto a crescente presença de empresas chinesas no setor destaca sua importância geopolítica. Fabricantes de cabos enfrentam desafios de produção e padronização, mas permanecem fundamentais para a conectividade e segurança da infraestrutura digital global.

2.3 EMPRESAS DE MANUTENÇÃO DE CABOS SUBMARINOS E OS REPAROS REALIZADOS

As empresas de manutenção de cabos submarinos são vitais para garantir a funcionalidade contínua da infraestrutura, efetuando reparos necessários e mitigando danos (Bueger; Liebetrau; Franken, 2022, p. 14). Essas operações de manutenção em ambiente submarino são complexas e desafiadoras, pois exigem tecnologias avançadas, conhecimento especializado (Bueger; Liebetrau; Franken, 2022, p. 22) e um grupo dedicado, capacitado em sistemas de intercomunicações globais (Starosielski, 2015, p. 133).

Para elevar a eficiência operacional, parcerias entre empresas de manutenção e proprietários de cabos buscam aprimorar tecnologias e técnicas de reparo (Mwema;

⁶ Proposta por Xi Jinping, em 2013, é uma estratégia central da China para fortalecer suas relações econômicas globais, buscando criar laços terrestres e marítimos com nações da Eurásia e África por meio de infraestrutura e investimentos, com um potencial de investimento de US\$ 1 trilhão em mais de 60 países (Shen, 2018).

Birhane, 2024, p. 11). Assim, operadores e proprietários firmam contratos com empresas de manutenção que mantêm depósitos de cabos e navios estrategicamente posicionados para pronto reparo (Bueger; Liebetrau; Franken, 2022, p. 28).

A manutenção é organizada por zonas globais e acordos cooperativos, como o *Atlantic Cable Maintenance & Repair Agreement* (ACMA), que cobre o Atlântico Norte e Sul da Europa até a África Ocidental (Bueger; Liebetrau; Franken, 2022, p. 28), visto que a manutenção antecipada é essencial para impedir interrupções severas (Raha; Raju, 2021, p. 63) ou minimizar seus impactos (Vichi; Pinto; Sá, 2020, p. 335).

Destacam-se algumas empresas de manutenção, como a *SubCom*, que fornece a segurança e a estabilidade das comunicações (Mwema; Birhane, 2024, p. 9); bem como a *Global Marine Systems* (Reino Unido) e a *Orange Marine* (França), que utilizam navios e equipamentos dedicados para reparos e conservação (Raha; Raju, 2021, p. 8). Elas realizam inspeções periódicas e ações rápidas em caso de danos (Raha; Raju, 2021, p. 44).

Para consertar cabos em diferentes profundidades e condições, as empresas empregam navios especializados e equipamentos submersíveis (Clare, 2024, p. 12). Utilizam tecnologia de ponta e profissionais altamente especializados para realizar reparos e substituição de cabos avariados (Garcia, 2023, p. 88).

Em relação aos reparos em cabos submarinos, a indústria de reparo de cabos submarinos envolve a mobilização de navios especializados e equipamentos avançados (Mwema; Birhane, 2024, p. 10; Raha; Raju, 2021, p. 45). É uma atividade complexa, devido à dispersão geográfica e à escassez desses navios especializados (Starosielski, 2015, p. 125), realizada em condições adversas no fundo do mar (Garcia, 2023, p. 90). Além disso, a necessidade de coordenação com autoridades regulatórias é um desafio constante (Raha; Raju, 2021, p. 12), que exige recursos substanciais (Vichi; Pinto; Sá, 2020, p. 335).

Em média, um reparo leva mais de duas semanas e fatores diversos contribuem para a vulnerabilidade da ação (Bueger; Liebetrau; Franken, 2022, p. 22), incluindo terremotos e acidentes com redes de pesca. Como exemplo, em 2016, um terremoto perto de Taiwan danificou nove cabos, exigindo a mobilização de 11 navios e 49 dias de trabalho (Vichi; Pinto; Sá, 2020, p. 335).

Um ponto positivo é que a tecnologia para detectar e reparar danos avançou, permitindo intervenções rápidas (Garcia, 2023, p. 91). Tecnologias como o Sensoriamento Acústico Distribuído possibilitam a identificação de danos de forma

precisa (Bueger; Liebetrau; Franken, 2022, p. 28), o que auxilia os esforços de reparo (Clare, 2024, p. 15), e amplificadores internos aumentam a durabilidade e a eficiência dos cabos (Mwema; Birhane, 2024, p. 10).

Para coordenar esforços de reparo em cabos que cruzam diferentes jurisdições, é necessária colaboração internacional (Garcia, 2023, p. 92). Reparos podem incluir substituição de trechos danificados ou medidas de reforço (Clare, 2024, p. 15). A reparação eficiente é vital para restaurar rapidamente as comunicações, minimizando impactos econômicos e sociais (Mwema; Birhane, 2024, p. 12; Raha; Raju, 2021, p. 126).

Resumidamente, empresas de manutenção de cabos submarinos são essenciais para assegurar a continuidade das comunicações globais. Elas realizam inspeções e reparos ágeis, empregando tecnologia avançada para prevenir interrupções. A complexidade do reparo se deve à dispersão geográfica e à escassez de navios especializados, além de desafios como terremotos e redes de pesca. A cooperação internacional e o uso de tecnologias avançadas são essenciais para restaurar rapidamente a comunicação, minimizando os impactos econômicos das interrupções.

2.4 SEGURANÇA DOS CABOS SUBMARINOS E SUAS ESTAÇÕES TERRENAS: AMEAÇAS E RISCOS

Após os ataques de 11 de setembro de 2001, nos EUA, a segurança dos cabos submarinos tornou-se uma preocupação crescente, resultando em medidas reforçadas para proteger as estações contra possíveis ataques terroristas (Starosielski, 2015, p. 125), pois a IC desses cabos, vital para o tráfego marítimo global, é suscetível a acidentes e ações maliciosas (Wedin, 2015, p. 190-191). Tal vulnerabilidade é influenciada pela profundidade do oceano, atividade marítima e condições geológicas. Sua proteção exige que se forneça segurança contra danos físicos e cibernéticos, além de assegurar a resiliência das estações terrenas (Bueger; Liebetrau; Franken, 2022, p. 22, 27).

A geografia é essencial para a configuração da rede de cabos submarinos e a localização dos *hubs*, que são pontos de interconexão e terminação de cabos. E a posição das estações terrenas é vital para a resiliência da infraestrutura (Frasca; Galantini, 2023, p. 53). Os pontos de estrangulamento marítimos, como estreitos e

canais chave, são estratégicos para as rotas dos cabos submarinos, porém representam pontos de vulnerabilidade (Starosielski, 2015).

Muitas estações terrenas não são identificadas por placas, sendo indicadas apenas por coordenadas em documentos de política (Starosielski, 2015, p. 125). Geralmente são protegidas por cercas, arame farpado e vigilância remota (Bueger; Liebetrau; Franken, 2022, p. 28). Além disso, medidas de isolamento dos centros urbanos ajudam a prevenir ameaças (Starosielski, 2015, p. 62). Essas estratégias de isolamento, como zonas de proteção, são cruciais para manter cabos em áreas com grande tráfego marítimo (Starosielski, 2015, p. 256), baseando-se a prevenção de ataques na vigilância de atividades marítimas e detecção de navegação anômala (Bueger; Liebetrau; Franken, 2022, p. 29).

A habilidade de mapear e operar em grandes profundidades é outro fator que aumenta a vulnerabilidade da IC marítima (Hendriks; Halem, 2024a, p. 9). Nesse aspecto, a proliferação de veículos submarinos operados remotamente representa uma preocupação significativa (Vichi; Pinto; Sá, 2020, p. 334). A segurança dos cabos submarinos inclui monitoramento contínuo e pronta resposta a indícios de interferência ou dano (Garcia, 2023, p. 96).

Para o estabelecimento de estratégias eficazes de segurança, faz-se necessária a parceria entre operadoras de cabos, governos e organizações internacionais (Raha; Raju, 2021, p. 57). É essencial iniciar uma operação coordenada e contínua de vigilância marítima para elevar a consciência sobre as IC marítimas (Cassetta, 2024, p. 5). Exercícios navais multinacionais podem ser efetuados para reforçar a segurança (Garcia, 2023, p. 93).

Quanto às ameaças e riscos aos cabos submarinos e suas estações terrenas, um cabo submarino pode ser danificado intencionalmente por métodos simples, como o uso de âncoras; ou complexos, envolvendo mergulhadores e submersíveis. Prevenir esses danos exige inteligência específica, vigilância e monitoramento das atividades marítimas, com a utilização de drones e embarcações de superfície (Davenport, 2023, p. 2).

Além dos problemas técnicos ou falhas no sistema, a IC de cabos submarinos enfrenta quatro tipos principais de ameaça: eventos e desastres naturais; dano acidental resultante da atividade humana; ataques cinéticos e cibernéticos, incluindo sabotagem, por atores estatais e não estatais; e a espionagem submarina (Frasca;

Galantini, 2023, p. 59). Anualmente, entre 150 e 200 falhas ocorrem nessa rede, a maioria de simples solução, pois acontecem em águas rasas (Clare, 2023).

Esses quatro tipos de ameaça são exemplificados a seguir.

- **Eventos e desastres naturais:** um abalo sísmico perto de Taiwan, em 2016, afetou nove cabos submarinos e demandou 49 dias para o reparo (Vichi; Pinto; Sá, 2020, p. 335). Em 2018, uma avaria no cabo *Africa Coast to Europe* causou problemas de comunicação em dez países da África Ocidental, deixando a Mauritânia sem internet por 48 horas (Vichi; Pinto; Sá, 2020, p. 335). A erupção do vulcão Hunga em 2022 causou danos extensivos aos cabos submarinos, o que interrompeu comunicações e expôs a vulnerabilidade dessa infraestrutura (Clare, 2024, p. 30).
- **Dano acidental resultante da atividade humana:** responsáveis pela maior parte das falhas, 57% do total (Clare, 2021). Em 2008, a interrupção de um cabo entre Itália e Egito fez a Força Aérea dos EUA perder comunicação com Veículos Autônomos Não Tripulados no Iraque e Paquistão (Hendriks; Halem, 2024a, p. 20). Um navio de pesca nas Filipinas danificou acidentalmente um cabo, interrompendo o acesso à internet para milhões de pessoas (Raha; Raju, 2021, p. 10). Presume-se que os danos ao cabo que conecta as Ilhas Faroé ao continente da Escócia, em 2022, foram provocados por uma embarcação de pesca (Martin, 2022).
- **Ataques cinéticos e cibernéticos:** danos cinéticos às infraestruturas subaquáticas são frequentes, cuja localização é facilitada por mapas públicos das rotas dos cabos (Cassetta, 2024, p. 4). A China foi acusada de danificar cabos de comunicação submarinos de Taiwan usando dragagem de areia (Bueger; Liebetrau; Franken, 2022, p. 33). Em 2022, o rompimento de cabos nas Ilhas Shetland coincidiu com a presença de um navio russo naquela região (Hendriks; Halem, 2024a, p. 27). As ameaças cibernéticas também são significativas, sendo os ataques geralmente realizados contra equipamentos de rede suscetíveis (Vichi; Pinto; Sá, 2020, p. 334).
- **Espionagem submarina:** ataques intencionais, como sabotagem e espionagem, são as maiores ameaças (Raha; Raju, 2021, p. 10), especialmente nas estações terrenas dos cabos (Vichi; Pinto; Sá, 2020, p. 334). A falta de supervisão expõe os cabos a ataques e à espionagem

(Mwema; Birhane, 2024, p. 7). Em 2017, submarinos russos ao redor dos cabos no Atlântico Norte causaram preocupação na OTAN sobre possíveis interceptações de dados (Vichi; Pinto; Sá, 2020, p. 333). As revelações de Edward Snowden mostraram que EUA e Reino Unido interceptaram diretamente os cabos submarinos (Mwema; Birhane, 2024, p. 8).

Em síntese, desde 11 de setembro de 2001, a segurança dos cabos submarinos tornou-se prioritária devido às ameaças naturais, humanas e cibernéticas, que exigem vigilância constante para evitar interrupções na comunicação e proteger a segurança nacional. Áreas críticas para a navegação coincidem com regiões de alta densidade de cabos, sujeitas a danos acidentais e ataques, como sabotagem e espionagem submarina, supostamente envolvendo países como Rússia e China. Cooperação internacional, monitoramento contínuo e tecnologia avançada são essenciais para proteger essa IC.

2.5 IMPACTOS FINANCEIROS E ECONÔMICOS POR DANOS NOS CABOS SUBMARINOS

Falhas em cabos submarinos causaram apagões significativos na internet (Bueger; Liebetrau; Franken, 2022, p. 16). Nos anos 1990, interrupções em cabos como o *PacRim West* destacaram a falta de capacidade de *backup* por satélite, resultando em graves impactos financeiros (Starosielski, 2015, p. 49). A paralisação de serviços de internet, que pode devastar a economia, afetando setores como finanças, saúde e comércio (Raha; Raju, 2021, p. 3), também pode ser causada pela sabotagem de cabos submarinos (Mendes, 2023).

A paralisação das redes de comunicação pode causar graves impactos no setor financeiro (Hendriks; Halem, 2024a), interrompendo serviços digitais e transações críticas (Bueger; Liebetrau; Franken, 2022). Prolongadas, essas interrupções podem resultar em perdas de bilhões de dólares no PIB (Starosielski, 2015), pois a economia global, com US\$ 10 trilhões em transações diárias, depende desses cabos (Bueger; Liebetrau; Franken, 2022; Starosielski, 2015).

As interrupções podem ainda afetar a posição de um país nas cadeias logísticas globais (Vichi; Pinto; Sá, 2020, p. 341) e, com isso, causar perdas financeiras substanciais, incluindo custos de reparo diretos e interrupções nas

comunicações (Raha; Raju, 2021, p. 12). Em síntese, a infraestrutura de cabos submarinos é vital para a economia global, pois viabiliza milhões de transações diárias (Vichi; Pinto; Sá, 2020, p. 332).

Falhas em cabos submarinos podem causar apagões na internet, paralisando setores críticos como finanças e saúde, acarretando impactos financeiros graves. A economia global, altamente dependente desses cabos, sofre com essas interrupções; diante disso, destaca-se a necessidade urgente de proteção e rápida reparação para minimizar perdas econômicas.

2.6 A CAPACIDADE DE SABOTAGEM E ESPIONAGEM EM CABOS SUBMARINOS

Os norte-americanos possuem o submarino de ataque de uso geral com propulsão nuclear USS Jimmy Carter (SSN-23), capaz de interceptar comunicações em cabos submarinos e lançar dispositivos de vigilância sobre o fundo do mar (Wedin, 2015, p. 190-191). Esse submarino da classe Seawolf foi comissionado em 2005, sendo o único adaptado para operações no fundo do mar, incluindo missões não divulgadas visando às IC como cabos de energia e telecomunicações (Suciu, 2024).

A China tem capacidade militar para danificar cabos submarinos, mas é improvável que o faça fora do Indo-Pacífico, apesar da crescente preocupação com o envolvimento da União Europeia (EU) na região (Bueger; Liebetrau; Franken, 2022). Em maio de 2023, o chefe de inteligência da OTAN alertou que a Rússia pode sabotar cabos submarinos em retaliação às nações que apoiam a Ucrânia, levando a OTAN a intensificar a proteção da IC submarina (Siebold, 2023).

A Rússia emprega submarinos e embarcações operados pelo GUGI, como o minissubmarino Losharik, capaz de operar a até um quilômetro de profundidade, e o navio Yantar, ambos aptos a interceptar ou cortar cabos submarinos. O submarino Belgorod, modificado para transportar o Losharik, apoia essas operações, potencialmente danificando redes de cabos e obtendo dados estratégicos valiosos (Frasca; Galantini, 2023, p. 60).

Grupos apoiados por Estados-nação, especialmente por Rússia e China, são considerados as principais fontes de ameaças de sabotagem a cabos submarinos. A alta interconectividade da rede global geralmente garante a disponibilidade de rotas alternativas, mas um ataque em larga escala poderia causar danos significativos (Mendes, 2023).

Há preocupações crescentes de que o Irã e seus aliados regionais possam atacar cabos submarinos na Península Arábica. O Mar Vermelho e o Golfo Pérsico são pontos críticos para a transmissão de dados globais, o que torna esses cabos alvos estratégicos. Grupos apoiados pelo Irã (Houthis e Hezbollah) podem responder à guerra Hamas-Israel e atacar esses cabos (Hendriks; Halem, 2024a, p. 14).

Em março de 2024, três cabos submarinos foram danificados no Mar Vermelho pela âncora de um navio atacado pelos Houthis, interrompendo 80% do tráfego de dados entre o Ocidente e a Ásia. A preocupação aumentou após a divulgação do mapa de cabos submarinos da região por representantes daquele grupo, mas negaram que os cabos eram alvos (Azevedo, 2024, n. 199, p. 16).

A capacidade de sabotagem e espionagem em cabos submarinos representa um risco crescente à segurança global. Ações de Estados como EUA, Rússia, China e Irã, usando tecnologias avançadas, ampliam as ameaças às comunicações submarinas, exigindo vigilância e cooperação internacional para proteger e fortalecer a resiliência dessa IC. Apesar de medidas de proteção e rotas alternativas, os riscos continuam.

2.7 LEGISLAÇÃO INTERNACIONAL PERTINENTE

O domínio submarino é abordado por três convenções internacionais: a Convenção de 1884, a Convenção de Genebra de 1958 e a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM) de 1982 (Hendriks; Halem, 2024a, p. 19). Essa legislação intrincada inclui normas de segurança para proteger infraestruturas vitais (Starosielski, 2015, p. 256), entretanto é mais condizente com a infraestrutura subaquática das décadas de 70 e 80 (Hendriks; Halem, 2024a, p. 19).

Essas convenções estabelecem as responsabilidades e os direitos dos países quanto à proteção dos cabos submarinos (Clare, 2024, p. 28), mas a ausência de proteção legislativa específica pode dificultar os esforços da indústria em assegurar direitos de desenvolvimento e segurança (Starosielski, 2015, p. 11). A distinção nas responsabilidades legais entre águas territoriais e internacionais é outro fator que complica a gestão e a proteção dos cabos submarinos (Bueger; Liebetrau; Franken, 2022, p. 14).

A CNUDM regula o emprego dos cabos submarinos, estabelecendo jurisdição nas zonas costeiras e exigindo regulamentos para punir danos fora das águas

territoriais (Mwema; Birhane, 2024). No entanto, ela não autoriza navios de guerra a abordarem ou arrestarem navios suspeitos (Bueger; Liebetrau; Franken, 2022). Datada de 1982, a CNUDM define as obrigações e prerrogativas dos Estados quanto à implantação e proteção de cabos (Raha; Raju, 2021, p. 26).

Outros instrumentos legais, como a Convenção de 1884, já mencionada, e as Regulamentações de 1972 (Raha; Raju, 2021, p. 27), buscam proteger cabos contra avarias e paralisações. Organizações como a ONU e a OTAN participam da regulação e proteção dos cabos devido à sua importância global (Garcia, 2023, pp. 76, 107). A UE avançou em projetos de cooperação, sancionou economicamente a Rússia e implementou políticas para autonomia energética (Cassetta, 2024, p. 4).

A Austrália implementou leis para proteger cabos submarinos, proibindo pesca de arrasto e ancoragem em zonas de até 2.000 metros de profundidade. A Nova Zelândia também adotou políticas para proteger os cabos de danos por pesca e transporte (Vichi; Pinto; Sá, 2020). Em 2022, o Comandante das Forças Armadas do Reino Unido alertou sobre a ameaça da atividade submarina russa aos sistemas de comunicações globais (The Guardian, 2022), afirmando que danificá-los poderia ser considerado um “ato de guerra” (Bueger; Liebetrau; Franken, 2022, p. 49).

As regulações internacionais são cruciais para a proteção dos cabos submarinos, facilitando a colaboração global e o cumprimento da CNUDM e outras leis marítimas, essenciais para resolver disputas (Clare, 2024). No entanto, o regime legal atual é considerado desatualizado (Bueger; Liebetrau; Franken, 2022) e insuficiente contra táticas hostis modernas (Hendriks; Halem, 2024a). A variabilidade nas respostas dos Estados evidencia a necessidade de uma estrutura legal mais robusta (Raha; Raju, 2021, p. 47).

Convenções internacionais, como a CNUDM, estabelecem normas para proteger cabos submarinos, mas encontram-se desatualizadas. A legislação deve evoluir para enfrentar ameaças modernas, por meio de colaboração internacional. A sabotagem de cabos submarinos é considerada seriamente, devido aos seus impactos, podendo ser vista como um ato de guerra.

2.8 CONCLUSÃO PARCIAL

A segurança dos cabos submarinos é fundamental para a economia global e segurança nacional, conforme destacado pela ONU em 2010, visto que esses cabos

sustentam comunicações militares, diplomáticas e financeiras. A crescente dependência digital reforça a necessidade de proteger essa IC para a estabilidade econômica e política. A responsabilidade pela proteção dos cabos submarinos não pode recair apenas sobre empresas privadas, sendo essencial a cooperação entre governos e setor privado e, devido à vasta extensão global, a proteção dos cabos submarinos tampouco pode se basear apenas na ação militar. As diversas ameaças exigem vigilância contínua, tecnologias avançadas, colaboração internacional, e a rápida reparação é uma prioridade global urgente. Estratégias nacionais podem adotar métodos alternativos, como aumentar a redundância com cabos adicionais, de modo a fortalecer a resiliência.

3 O REINO UNIDO E OS CABOS SUBMARINOS

Os britânicos, pioneiros na instalação do cabo de fibra óptica transatlântico em 1988, viabilizaram a internet moderna. Embora negligenciada, a princípio, a importância dos cabos submarinos foi reconhecida recentemente, resultando em mudanças estratégicas, como a emissão de documentos de alto nível e o desenvolvimento de meios navais próprios, com o intuito de fortalecer a segurança marítima e a proteção dessas IC.

3.1 POSTURA ESTRATÉGICA ADOPTADA, DE 2014 A 2024, NO QUE SE REFERE À PROTEÇÃO DOS CABOS SUBMARINOS DE COMUNICAÇÕES

Em 2014, o governo lançou sua estratégia inaugural de segurança marítima, destacando a importância de uma abordagem integrada e colaborativa em níveis doméstico e internacional. Isso pavimentou o caminho para uma série de avanços na política de segurança marítima do Reino Unido (Reino Unido, 2022, p. 16).

Como consta no *Maritime 2050*, de 2019, o Reino Unido se destaca no sistema internacional, utilizando meios diplomáticos, militares e legais para fomentar cooperação e fortalecer capacidades. Para manter sua influência e capacidade de intervenção, é essencial avaliar e priorizar os riscos e oportunidades marítimas, alocando recursos de maneira estratégica (Reino Unido, 2019, p. 263).

O relatório de 2017 da *Policy Exchange*, "**Indispensable, insecure**", escrito por Rishi Sunak, ex-Primeiro-Ministro britânico, destacou a vulnerabilidade da infraestrutura digital do Reino Unido. Embora danos acidentais, como pesca, sejam comuns, o foco recaiu sobre as ameaças humanas, como sabotadores e Estados hostis, mostrando que pequenos atos físicos ou cibernéticos podem causar grandes interrupções internacionais (Hendriks; Halem, 2024a, p. 17).

A partir de 2020, o Reino Unido adotou uma nova estratégia para proteger sua IC marítima, participando de várias iniciativas multilaterais, como a recém-estabelecida Célula de Coordenação de Infraestrutura Submarina Crítica da OTAN (Hendriks; Halem, 2024a, p. 10). Com foco em responder às ameaças, o governo britânico aprimorará a Consciência Situacional Marítima e fortalecerá parcerias internacionais, como a OTAN e o pacto entre Austrália, os EUA e o Reino Unido (AUKUS), para enfrentar ameaças emergentes (Reino Unido, 2022, p. 19).

O Reino Unido e a OTAN dão alta prioridade estratégica à proteção dos cabos submarinos (Bueger; Liebetrau; Franken, 2022). Segundo o Ministério da Defesa britânico: “Nosso propósito fundamental é proteger nosso povo, território, infraestrutura nacional crítica e modo de vida” (Reino Unido, 2021, p. 11, tradução nossa). No documento “**Defence in a competitive age**” (Reino Unido, 2021, p. 50), o Ministério da Defesa britânico destaca a importância de fortalecer a proteção da IC subaquática e a detecção de ameaças no Atlântico Norte. Para isso, o Reino Unido fará investimentos estratégicos e de longo prazo para aprimorar a Vigilância Oceânica da Marinha Real.

A **Estratégia Nacional de Segurança Marítima** (Reino Unido, 2022) enfatiza a importância dos cabos submarinos como IC. Entre seus objetivos estratégicos estão: fortalecer a resiliência do setor marítimo em face a ataques cibernéticos e outras ameaças, garantindo proteção de dados, e assegurar prosperidade, desenvolvendo um sistema robusto, seguro e diversificado para proteger essa IC (Reino Unido, 2022, p. 19).

Em janeiro de 2022, o Chefe do Estado-Maior da Defesa alertou sobre a ameaça representada pela atividade submarina russa, afirmando que qualquer dano aos cabos seria visto como um ato de guerra, destacando a importância do tema para a liderança britânica e indicando que sua proteção deve ser uma prioridade de segurança (Bueger; Liebetrau; Franken, 2022, p. 49).

Em resumo, o governo britânico considera os cabos de comunicação subaquáticos interligados ao país como parte de sua conectividade e IC internacional, apesar de seus proprietários e operadores pertencerem ao setor privado (Reino Unido, 2022, p. 67).

O Reino Unido adota uma abordagem integrada para proteger sua IC marítima. Desde 2014, políticas robustas e parcerias internacionais fortalecem a segurança contra ameaças, enquanto investimentos e estratégias de longo prazo aprimoram a vigilância e proteção dos cabos submarinos.

3.2 A IMPORTÂNCIA DADA AOS CABOS SUBMARINOS

A **Estratégia Nacional de Segurança Marítima** (Reino Unido, 2022) ressalta que, embora privados, os cabos submarinos são críticos para a infraestrutura nacional do Reino Unido. A pesca de arrasto é a principal ameaça, e a importância dos cabos

requer conscientização sobre possíveis interrupções por atores maliciosos, que impactariam comunicações, serviços on-line e tráfego financeiro (Reino Unido, 2022, p. 67).

O Reino Unido considera a IC Nacional como composta por ativos, sistemas e trabalhadores essenciais, cuja perda ou comprometimento pode prejudicar serviços vitais, causar perdas de vidas, e impactos econômicos e sociais significativos, o que afetaria a segurança nacional, a defesa ou o funcionamento do Estado (Reino Unido, 2023b).

O Reino Unido, como nação insular e pilar da aliança Euro-Atlântica, depende do domínio marítimo para comércio, energia e comunicação, com cabos submarinos sendo fundamentais para essa infraestrutura (Hendriks; Halem, 2024a, p. 14-15). As exportações do Reino Unido que dependem de cabos submarinos contribuem com £545 bilhões para o Valor Agregado Bruto anualmente (Reino Unido, 2022, p. 66).

A *Society for Worldwide Interbank Financial Telecommunications* (SWIFT) transmite 15 milhões de mensagens diárias por cabos para mais de 8.300 instituições em 208 países. O *Continuous Linked Settlement* (CLS) Bank no Reino Unido, uma IC de mercado, usa a SWIFT para liquidar 17 moedas globalmente, movimentando cerca de US\$ 3,9 trilhões por dia (Burnett, 2018, p. 236).

Os sistemas de cabos estabelecem conexões transnacionais além da cooperação bilateral, com Reino Unido, França e Egito como pontos-chave (Bueger; Liebetrau; Franken, 2022). O Reino Unido prioriza a segurança dos cabos no Indo-Pacífico devido à competição com a China e à interdependência financeira global, onde interrupções afetariam todo o sistema (Hendriks; Halem, 2024a).

Para que o Reino Unido se torne um *hub* seguro e atraente para cabos de dados submarinos e mantenha sua *expertise* digital, o governo atualizará a regulamentação para garantir a segurança e resiliência das comunicações críticas, incluindo reparos e manutenções oportunas na infraestrutura submarina (Reino Unido, 2022, p. 67).

No *Maritime 2050*, o governo britânico planeja liderar a atração de novos cabos submarinos e fortalecer a resiliência da infraestrutura submarina nos próximos 5-15 anos (Reino Unido, 2019). Recentemente, o Reino Unido já alcançou sucesso, emergindo como líder em tecnologias subaquáticas (Hendriks; Halem, 2024a, p. 12).

O Reino Unido considera os cabos submarinos vitais para sua infraestrutura, enfrentando ameaças como pesca de arrasto e atores maliciosos. Cooperação

internacional e regulamentação atualizada são essenciais para garantir sua segurança e resiliência futura.

3.3 A PERCEPÇÃO DE AMEAÇAS E RISCOS

Em fevereiro de 2022, a intensificação das operações militares russas contra a Ucrânia, após a anexação da Crimeia, mostrou que atores estatais superaram os não estatais como a principal ameaça à estabilidade internacional (Patalano, 2023). Diversificar redes é vital para reduzir vulnerabilidades, mas obstáculos nos projetos Euro-Atlânticos favorecem as ameaças russas (Hendriks; Halem, 2024a, p. 25).

Danos acidentais provenientes da pesca, especialmente o arrasto e outras atividades que perturbam o fundo do mar, permanecem como a maior ameaça aos cabos submarinos (Reino Unido, 2022, p. 67). O corte não atribuído de dois cabos submarinos perto das Ilhas Shetland em 2022, junto à presença de um navio russo próximo, levantou suspeitas de intencionalidade (Hendriks; Halem, 2024a, p. 27).

A infraestrutura de reparo e manutenção de cabos no Reino Unido é vulnerável, com apenas um navio de reparo, o que pode causar graves impactos de conectividade em um ataque coordenado (Bueger; Liebetrau; Franken, 2022). A Rússia ameaça as águas britânicas, focando no Mar do Norte, interferindo na retaguarda ocidental (Hendriks; Halem, 2024a, p. 23).

A Rússia investe em capacidades submarinas avançadas, incluindo tecnologias de grande profundidade que ameaçam cabos submarinos (Reino Unido, 2021). Com os percursos dos cabos desconhecidos, a Rússia mapeia essas infraestruturas para obter inteligência crítica sobre o Reino Unido, evitando conflitos diretos e se preparando para interrupções em caso de guerra (Hendriks; Halem, 2024a, p. 24).

Em 2022, a Rússia conduziu exercício naval próximo à Zona Econômica Exclusiva da Irlanda, perto de cabos submarinos que conectam Reino Unido, França e EUA (Bueger; Liebetrau; Franken, 2022). Nesse ano, a Marinha Real monitorou submarinos russos vindos do Ártico e, em 2023, rastreou navios russos no Canal da Mancha (Hendriks; Halem, 2024a, p. 27).

Em resumo, embora distante da destruição física na Europa, o Reino Unido enfrenta ameaças à sua infraestrutura submarina devido à guerra da Rússia na Ucrânia (Hendriks; Halem, 2024a). A perda de cabos submarinos afeta comunicações, serviços e tráfego financeiro (Reino Unido, 2022). No Indo-Pacífico, a República

Islâmica do Irã emerge como outra ameaça significativa, enquanto a China não está nas considerações estratégicas britânicas (Hendriks; Halem, 2024a, p. 39).

A intensificação das operações russas contra a Ucrânia em 2022 revelou a ameaça estatal à infraestrutura submarina do Reino Unido. A vulnerabilidade exige maior proteção, cooperação internacional e fortalecimento da resiliência e liderança tecnológica subaquática pelo governo.

3.4 A INFRAESTRUTURA ESTRATÉGICA DOS CABOS SUBMARINOS INGLESES E SEUS PONTOS MAIS VULNERÁVEIS

Após o referendo do Brexit em 2016, planos para quatro cabos submarinos evitaram o Reino Unido, direcionando-se para outros países da UE (Frasca; Galantini, 2023, p. 54). As conexões transatlânticas diretas do bloco caíram de 18 para 11, mas não afetou o tráfego de dados da UE, pois o roteamento da internet ignora fronteiras políticas (Bueger; Liebetrau; Franken, 2022, p. 17-18).

As relações fortalecidas entre Londres e Paris pós-Brexit melhoram a segurança dos cabos submarinos. Reino Unido e França, enfrentando desafios submarinos semelhantes, promovem maior cooperação bilateral. Ambos são vulneráveis a ameaças russas no Atlântico e Mar do Norte, e compartilham interesses no Pacífico (Hendriks; Halem, 2024a, p. 32-33). Hoje, os dados do Atlântico entram na UE pelo Canal da Mancha, pelos 28 *links* entre o Reino Unido e a Europa, destacando-se as estações em Calais (França), Ostend (Bélgica) e Zandvoort (Países Baixos) (Frasca; Galantini, 2023, p. 54). Cerca de 60 cabos formam a rede do Reino Unido, responsável por transportar 99% dos dados digitais necessários para todas as comunicações internacionais (Hendriks; Halem, 2024a, p. 15).

O Mar do Norte é crucial para o sistema de cabos de fibra óptica Euro-Atlântico, conectando o Reino Unido à Europa e América do Norte, mas sua vulnerabilidade a ações hostis torna essas infraestruturas alvos potenciais (Hendriks; Halem, 2024a). Em um cenário global mais instável, rotas comerciais e pontos estratégicos podem perder acessibilidade para navegação livre (Reino Unido, 2019, p. 274).

Os principais *hubs* são as estações terrenas transatlânticas na costa sudoeste do Reino Unido, que atuam como nodos vitais para as comunicações digitais globais (Hendriks; Halem, 2024a, p. 15). A proteção e o monitoramento eficaz das estações terrenas de cabos são dificultados por sua localização remota em áreas

escassamente povoadas, de difícil acesso por terra e facilmente acessíveis pelo mar (Hendriks; Halem, 2024a, p. 51).

A conectividade da UE depende do Atlântico Norte e das águas britânicas. Monitorar cabos nessas regiões exige capacidades dos EUA e do Reino Unido (Bueger; Liebetrau; Franken, 2022). Sem integrar totalmente o Mar da Irlanda e as Abordagens Ocidentais ao Mar do Norte ao sistema de defesa marítima ocidental, essas áreas permanecem vulneráveis à hostilidade russa, ameaçando a segurança coletiva (Hendriks; Halem, 2024a, p. 31).

A segurança dos cabos submarinos, devido à sua natureza transnacional, mostra que nenhum país pode proteger sua rede sozinho (Hendriks; Halem, 2024a). Atividades cibernéticas maliciosas estão se tornando mais intensas e complexas. Mitigar riscos cibernéticos no setor marítimo é essencial para o Reino Unido, especialmente diante da automação crescente da indústria, para garantir segurança contínua (Reino Unido, 2022, p. 26). A manutenção de cabos é gerida por zonas globais e acordos cooperativos sem fins lucrativos. Para a Europa, o ACMA cobre o Atlântico, concentrando-se no Mar do Norte e na área do Sul da Europa-África Ocidental, com três navios, enquanto o *Mediterranean Cable Maintenance Agreement* (MECMA) cobre o Mediterrâneo, o Mar Negro e o Mar Vermelho com dois navios. Apenas a ACMA tem um navio baseado no Reino Unido (Bueger; Liebetrau; Franken, 2022, p. 28).

A alta densidade de cabos e vulnerabilidade da OTAN tornam o Mar do Norte e o *Greenland-Iceland-United Kingdom (GIUK) Gap* alvos estratégicos para a Rússia, o que incentiva mapeamentos e sabotagens. Isso fornece inteligência sobre infraestrutura ocidental, desvia recursos da Ucrânia, testa capacidades e confunde a estratégia ocidental (Hendriks; Halem, 2024a, p. 28).

Em suma, a dinâmica dos cabos submarinos favorece agressores devido ao fácil acesso e aos desafios de monitoramento, dificultando a dissuasão e atribuição de danos, resultando em impunidade. Após o Brexit, o Reino Unido reforçou a segurança desses cabos com alianças, intensificando a vigilância no Atlântico e Mar do Norte. Proteção conjunta e monitoramento eficaz são essenciais para enfrentar ameaças transnacionais e garantir resiliência.

3.5 AS PRÁTICAS ADOTADAS PARA A PROTEÇÃO DESSAS INFRAESTRUTURAS CRÍTICAS

O relatório de 2017 da *Policy Exchange*, “**Indispensable, Insecure**”, escrito por Rishi Sunak, ex-Primeiro-Ministro britânico, recomendou medidas para o Reino Unido e aliados protegerem suas redes de cabos submarinos. Algumas sugestões foram adotadas, incluindo mais exercícios navais da OTAN e a criação da Célula de Coordenação de Infraestrutura Submarina Crítica em Bruxelas, promovendo maior coordenação estratégica (Hendriks; Halem, 2024a, p. 19).

Em 2019, o governo fortaleceu a segurança marítima do Reino Unido criando o *Joint Maritime Security Centre* (JMSC), central para a resposta às ameaças. O JMSC coordena com várias agências governamentais para desenvolver uma “Resposta Sistêmica Completa” e enfrentar novos desafios e ameaças emergentes (Reino Unido, 2022, p. 16).

Recentemente, o Reino Unido reforçou sua estratégia submarina em resposta a ameaças crescentes, ampliando parcerias com aliados para fortalecer a resiliência da infraestrutura submarina (Hendriks; Halem, 2024a). Junto aos EUA e à OTAN, a Marinha Real investirá em capacidades submarinas avançadas, incluindo uma automatizada Capacidade de Caça-Minas, desenvolvida em parceria com a França (Reino Unido, 2021, p. 48).

Nesse sentido, o Ministério da Defesa britânico está aumentando os investimentos em equipamentos para prevenir ameaças subaquáticas (Hendriks; Halem, 2024a, p. 13). Dessa forma, foi lançado um programa naval para proteger cabos de telecomunicações submarinos e gasodutos, destacando a importância da vigilância e defesa subaquáticas (Cassetta, 2024, p. 4).

Lançado em 2021, o programa *Multi-Role Ocean Surveillance Ship* (MROSS) visa a proteger cabos submarinos contra ameaças e fornecer vigilância (Hendriks; Halem, 2024a). Houve a compra de um navio MROS para monitorar a IC submarina e detectar atividades próximas aos cabos, equipado com drones submarinos não tripulados (Bueger; Liebetrau; Franken, 2022, p. 49).

Em 10 de outubro de 2023, o Reino Unido apresentou o Proteus, novo navio de vigilância subaquática da *Royal Fleet Auxiliary* (RFA), sendo o primeiro do programa MROSS (Felstead, 2023). O RFA Proteus apoiará a proteção da IC do Reino

Unido, operando como “navio-mãe” com sistemas remotos e autônomos para vigilância submarina e operações de guerra no fundo do mar (Reino Unido, 2023a).

Em 2023, Reino Unido e Noruega formaram uma aliança estratégica para enfrentar ameaças submarinas no Mar do Norte, Atlântico Norte e Ártico, compartilhando capacidades como P-8A e F-35 para proteger a IC. O Reino Unido também colabora com a França no programa de caça às minas Artemis Trident (Reino Unido, 2023b).

O governo britânico colaborará com diversas indústrias para atrair novos cabos submarinos, explorando novos modelos de entrega. Compromete-se a aumentar a resiliência da IC submarina, garantindo contingência suficiente. A longo prazo, buscará parcerias internacionais para liderar a IC submarina futura e manter a conectividade global (Reino Unido, 2019, p. 246).

Os interesses britânicos no Indo-Pacífico incluem pactos de segurança e inteligência com Austrália, Japão e Nova Zelândia, essenciais para a conectividade digital via cabos submarinos (Hendriks; Halem, 2024a). Com a comunidade de inteligência, o Reino Unido protegerá suas redes cibernéticas e IC em face à espionagem e às ameaças (Reino Unido, 2021, p. 20).

Em resumo, o Reino Unido adota um mecanismo voluntário de relato de falhas de cabos, essencial para identificar padrões, realizar análises de risco e avaliar reparos (Bueger; Liebetrau; Franken, 2022). O governo colaborará com aliados para atribuir responsabilidades e apresentar provas contra ameaças estatais inaceitáveis (Reino Unido, 2022, p. 51).

A recomendação de Sunak em 2017 impulsionou a proteção dos cabos submarinos do Reino Unido, levando à criação do JMSC e a parcerias com a OTAN. Investimentos contínuos, o lançamento do RFA Proteus e novas alianças estratégicas, incluindo no Indo-Pacífico, fortaleceram a resiliência da IC submarina.

3.6 CONCLUSÃO PARCIAL

O Reino Unido adota uma abordagem estratégica integrada para proteger sua IC marítima. Desde 2014, políticas robustas e parcerias internacionais fortaleceram a segurança contra ameaças cibernéticas e físicas. A intensificação das operações militares russas em 2022 destacou a necessidade de proteção dos cabos submarinos, essenciais para a infraestrutura nacional, assim como a ameaça iraniana

representada no Indo-Pacífico. Investimentos contínuos, como o lançamento do RFA Proteus e alianças com França, Noruega e OTAN, são fundamentais para enfrentar ameaças transnacionais e garantir a resiliência da infraestrutura digital. A atualização regulatória e cooperação internacional são cruciais para fortalecer a liderança tecnológica subaquática do Reino Unido, assegurando a segurança nacional e a conectividade global.

4 BRASIL E OS CABOS SUBMARINOS

Neste capítulo será apresentada a abordagem brasileira no que diz respeito à proteção dos cabos submarinos de comunicações. A forte vocação da sociedade brasileira com o mar e suas normatizações não são traduzidas em prática efetiva de defesa marítima, mas, como será exposto, o cenário pode mudar, ou já está mudando. Uma nação com extenso litoral como o Brasil não pode negligenciar a importância e a proteção da estratégica IC dos cabos submarinos.

4.1 POSTURA ESTRATÉGICA ADOTADA, DE 2014 A 2024, NO QUE SE REFERE À PROTEÇÃO DOS CABOS SUBMARINOS DE COMUNICAÇÕES

O primeiro cabo parcialmente submarino no Brasil, pertencente à primeira linha telegráfica brasileira, foi inaugurado em 1857, ligando o Rio de Janeiro a Petrópolis. Em 1874, foi concluído o primeiro cabo totalmente submarino, conectando as cidades do Rio de Janeiro, Salvador, Recife e Belém. Em 1875, foi instalado o primeiro cabo submarino internacional, ligando o Brasil a Portugal (Santos *et al.*, 2022, p. 205). Na década de 1990, foi instalado o primeiro cabo de fibra ótica no Brasil. Nesse sentido, observa-se a dependência histórica desses cabos para o Brasil.

De acordo com a **Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)** (2018, art. 1, inc. I), no Brasil, as IC são definidas como sendo “instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade”, competindo ao Gabinete de Segurança Institucional da Presidência da República a participação na supervisão das questões relacionadas às IC no âmbito da administração pública federal (Brasil, 2018), o que evidencia a elevada preocupação com as IC.

Na **Estratégia de Defesa Marítima (EDM)** (2023), apesar da excelente iniciativa, nota-se que o Objetivo Estratégico (OBE) 3, “Proteger as Infraestruturas Críticas do Poder Marítimo (ICPM)”, não menciona os cabos submarinos como pertencente às ICPM, negligenciando sua importância estratégica e, nesse aspecto, carece de uma revisão para que seja dado um maior destaque ao tema:

O OBE 3 diz respeito, especificamente, à **proteção dos ativos do poder marítimo** representados, principalmente, pelas **instalações portuárias, plataformas e terminais de petróleo e gás e suas estruturas de apoio**. O OBE em lide busca garantir o funcionamento normal dessas infraestruturas em momentos de crise e conflito, **dada sua essencialidade para o País** (Brasil, 2023, p. 1-2, grifo nosso).

Outro aspecto observado na EDM (2023) está relacionado à consciência situacional, por meio da qual a Marinha do Brasil (MB) priorizará a ampliação da Consciência Situacional Marítima⁷ nas áreas referentes ao Projeto Piloto do Sistema de Gerenciamento da Amazônia Azul (SisGAAz), buscando gradualmente expandi-la, de forma sequencial, para “a Elevação do Rio Grande, as Ilhas Oceânicas, a Foz do Rio Amazonas, a Bacia de Santos, a Margem Equatorial brasileira e o Arquipélago de São Pedro e São Paulo” (Brasil, 2023, cap. 2, pp. 2-4, 2-5), o que ampliará as duas regiões costeiras de particular importância para a Defesa previstas na **Estratégia Nacional de Defesa**: o trecho entre Santos e Vitória e a área ao redor da foz do rio Amazonas (Brasil, 2024, p. 47). Nota-se, contudo, que as IC dos cabos submarinos e suas estações terrenas (*landing points*) ainda não possuem o destaque necessário.

A Defesa Marítima é essencial para o Brasil em um mundo de incertezas. O Poder Naval, crucial ao Poder Marítimo, deve proteger a soberania, o patrimônio e os interesses nacionais diante de desafios complexos (Brasil, 2020a, p. 19). Nesse sentido, a **Estratégia Nacional de Defesa** menciona que as capacidades da MB de controle marítimo, negação do uso do mar e projeção do Poder Naval visam a aumentar a segurança e proteger, dentre outras, as IC marítimas (Brasil, 2024, p. 47).

Na **Política Nacional de Defesa** (Brasil, 2024, p. 25), o Objetivo Nacional de Defesa II, “Assegurar a capacidade de Defesa para o cumprimento das missões constitucionais das Forças Armadas”, garante que as Forças Armadas tenham capacidades adequadas para proteger o território, águas jurisdicionais e espaço aéreo do Brasil, além de proporcionar a segurança das linhas marítimas de interesse, com recursos orçamentários regulares e IC de comunicações adequadas.

Dessa forma, a MB estrutura suas necessidades em Programas Estratégicos, alinhados às melhores práticas de governança, otimizando investimentos estatais e desenvolvendo a área de Defesa. Dois deles se destacam: o do SisGAAz e o da

⁷ Segundo o Plano Estratégico da Marinha (PEM) 2040, “Consciência Situacional Marítima representa a efetiva compreensão de tudo que está relacionado ao meio marinho e que possa causar impacto na defesa, na segurança, na economia e no meio ambiente do entorno estratégico” (Brasil, 2020a, p. 19).

Mentalidade Marítima (Brasil, 2020a, p. 84), os quais demonstram a mais alta importância a esses conceitos com profunda aderência à proteção das IC dos cabos submarinos.

Em resumo, a vocação marítima do Brasil é evidenciada por seu vasto litoral, hidrovias, comércio marítimo e a importância estratégica do Atlântico Sul, que abriga a Amazônia Azul, rica em recursos, incluindo as maiores reservas de petróleo e gás natural do país (Brasil, 2019, p. 13).

Assim, a proteção dos cabos submarinos, essenciais para a soberania e economia do Brasil, ainda carece de destaque nas estratégias de defesa. A Estratégia Nacional de Defesa e o SisGAAz são cruciais, mas é necessária maior ênfase na segurança dessas IC para garantir a resiliência nacional.

4.2 A IMPORTÂNCIA DA DEFESA DOS CABOS SUBMARINOS

De acordo com o **Plano Estratégico da Marinha (PEM) 2040** (Brasil, 2020a), existe na sociedade brasileira um “pacifismo unilateral”, que dificulta a identificação de ameaças ao Brasil. No entanto, o Poder Naval atual exige prontidão crescente para identificar e enfrentar essas ameaças, de modo que desenvolver uma mentalidade de defesa é essencial para proteger os interesses nacionais (Brasil, 2020a, p. 12), incluindo as IC subaquáticas.

Como destacado no PEM 2040 (Brasil, 2020a, p. 13), a quase totalidade das comunicações globais pela internet ocorre por meio de cabos de fibra ótica instalados no fundo dos oceanos. E o Brasil, com uma das maiores Zonas Econômicas Exclusivas, equivalente à Amazônia Verde, destaca-se como um dos principais *hubs* mundiais de cabos submarinos (Santos *et al.*, 2022).

A Amazônia Azul, com 5,7 milhões de km², é vital para o Brasil, abrigando 95% do comércio marítimo nacional, 99% das comunicações por cabos submarinos, além de vastas reservas naturais, exigindo proteção e exploração sustentável (Santos *et al.*, 2022, p. 546). Para a intercomunicação e a defesa desse vasto território, o mar e as hidrovias cumprem papel essencial. A intercomunicação envolve transporte e comunicação digital por cabos submarinos; e a defesa se baseia na proteção dessas linhas, necessitando do Poder Naval, administrado pela MB e apoiado pela indústria de defesa (Brasil, 2020a, p. 15).

Sob esse prisma, a comunicação via cabos submarinos que atravessam oceanos e rios, assim como o Comércio e Transporte marítimo, são estrategicamente importantes para o crescimento econômico do Brasil, sendo essenciais para a Economia Azul e contribuindo significativamente para o PIB (Santos *et al.*, 2022, p. 206).

Em um panorama mais amplo, a análise da rede de cabos submarinos no Atlântico ajuda a entender as relações de poder geopolítico-territoriais, ilustrando as dinâmicas de inclusão e exclusão na competição entre grandes potências (Garcia, 2023, p. 97). Iniciativas como *Arctic Fibre*, o sistema *spin* e o cabo BRICS, buscando uma nova abordagem, estabeleceram rotas alternativas inovadoras para conectar a América do Sul, África do Sul, Índia e China, evitando Europa e Estados Unidos, desafiando, assim, as trajetórias tradicionais das redes de cabos submarinos (Santos *et al.*, 2022, p. 206).

Os mais recentes pontos de conexão para cabos submarinos, que vinculam não apenas o Brasil, mas toda a América Latina à Europa e África, foram estabelecidos a partir da costa do Ceará, no campo de tráfego de dados e comunicações (Beirão; Marques; Ruschel, 2020, p. 93). O Brasil visa transformar Fortaleza em um *hub* estratégico de cabos submarinos na América Latina. Ao receber nove cabos internacionais, a cidade se tornará um polo tecnológico crucial, o que beneficiará significativamente tanto o Brasil quanto o estado do Ceará (Pinto, 2021).

Em suma, os cabos submarinos são vitais para a comunicação global e a economia do Brasil, que se destaca como um *hub* estratégico mundial. Fortaleza emerge como um polo tecnológico crucial. A defesa das IC e o fortalecimento do Poder Naval são essenciais para proteger os interesses nacionais em um cenário global competitivo.

4.3 A PERCEPÇÃO DE AMEAÇAS E RISCOS

O ciberespaço, o qual não possui fronteiras físicas e abrange todos os setores (marítimo, terrestre, aéreo e espacial), é um campo de operações militares. Sua vulnerabilidade representa uma ameaça moderna que deve ser enfrentada (Brasil, 2020a, p. 31). Os cabos submarinos representam o meio físico desse espaço; por essa razão, precisam de elevada e permanente segurança.

Após as revelações de Edward Snowden sobre a espionagem de dados por cabos submarinos, foi sugerido um cabo BRICS conectando Rússia, Brasil, China, Índia e África do Sul. O objetivo era evitar os centros de dados dos EUA e Europa, por onde atualmente passa a maior parte do tráfego de dados digitais (Shen, 2018, p. 9).

O caso da embarcação russa Yantar que sumiu dos sistemas de monitoramento por alguns dias na costa brasileira, em 2020, levantando suspeitas de espionagem, também merece destaque e serve para recordar que o Brasil não está isento das mesmas ameaças globais enfrentadas pelos EUA e Europa, apesar de mais afastado geograficamente (Brasil, 2020b; Época Negócios, 2020).

As IC, como plataformas de petróleo, gasodutos, refinarias e usinas hidrelétricas, são extremamente vulneráveis a falhas ou ataques terroristas que afetam a comunicação transmitida por cabos, além do setor de telecomunicações (Agência Marinha de Notícias, 2024). Portanto, qualquer ação violenta dirigida a uma IC deve ser tratada como uma ameaça significativa (Brasil, 2020a, p. 26).

Criminosos podem comprometer a exploração, bem como rotas marítimas e fluviais. Dado que tais organizações operam no Brasil e têm o potencial de atacar as IC, é essencial considerar essas ameaças nas áreas costeiras e hidrovias (Brasil, 2020a, p. 31). Assim, as estações terrenas dos cabos submarinos representam pontos de vulnerabilidade na costa passíveis de ataques por esses grupos. Mesmo com acordos bilaterais de segurança, a proteção dos cabos submarinos pode ser insuficiente devido à operação majoritariamente privada desses cabos em solo estrangeiro, como no Brasil e nos EUA (Vichi; Pinto; Sá, 2020, p. 338).

Os mapas de cabos submarinos revelam uma concentração de rotas transatlânticas no Norte, evidenciando a fragilidade do Sul e indicando uma dependência das infraestruturas do Norte. Essa disparidade limita o progresso tecnológico e a autonomia cibernética do Sul (Medeiros; Pinto, 2022, p. 7). Ainda que o cabo BRICS tenha falhado, devido a conflitos internos e desafios econômicos entre seus países-membro, a China, buscando fugir dessa dependência, dentro da Rota da Seda Digital, desenvolveu sua própria infraestrutura de rede global usando cabos submarinos, terrestres e satélites, principalmente com países da Iniciativa Cinturão e Rota (Shen, 2018, p. 9).

Em síntese, a vulnerabilidade dos cabos submarinos, essenciais para o ciberespaço e a comunicação global, representa uma ameaça significativa, especialmente para o Sul, que depende das infraestruturas do Norte. A proteção

dessas infraestruturas é vital, diante de riscos terroristas e criminosos, e a busca por autonomia cibernética é fundamental para fortalecer a segurança nacional.

4.4 A INFRAESTRUTURA ESTRATÉGICA DOS CABOS SUBMARINOS BRASILEIROS E SEUS PONTOS MAIS VULNERÁVEIS

Na gestão do sistema de cabos submarinos brasileiros, a Agência Nacional de Telecomunicações (ANATEL), o Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA) e a MB são os principais órgãos reguladores, cada um com funções específicas. A MB autoriza a instalação de cabos submarinos conforme as normas da Autoridade Marítima e a Lei de Segurança do Tráfego Aquaviário (LESTA), quando em Águas Jurisdicionais Brasileiras (AJB) (Santos *et al.*, 2022, p. 205).

O Brasil possui uma complexa rede de cabos submarinos, com seis dos 278 cabos globais passando pelo país. Fortaleza (CE) é o principal *hub* intercontinental, conectando diversos sistemas de telecomunicações. Outros *hubs* importantes estão em Santos (SP), Salvador (BA) e Rio de Janeiro (RJ) (Santos *et al.*, 2022, p. 205).

Operadoras de telecomunicações como Telxius e Embratel continuam desempenhando um papel crucial na manutenção e expansão da rede de cabos submarinos (Vichi; Pinto; Sá, 2020, p. 339). Atualmente, há apenas três conexões diretas entre a UE e a América Latina, incluindo o recente projeto EllaLink e os sistemas mais antigos Atlantis 2 e Columbus III (Bueger; Liebetrau; Franken, 2022, p. 18).

Os EUA controlam a maioria dos cabos submarinos no Atlântico, o que lhes permite monitoramento e interceptação de dados antes de chegarem ao destino final. Para contornar essa vulnerabilidade, Brasil e UE investiram no EllaLink, conectando diretamente os continentes. Isso ressalta a necessidade de uma governança global eficaz e cooperativa para proteger informações sensíveis (Medeiros; Pinto, 2022, p. 11-12).

A parceria entre Brasil e Europa para o cabo submarino de 6 mil km, ao custo de mais de 170 milhões de euros, liderada e com a maior parte custeada pela EllaLink, visa a diversificar as rotas de comunicação, de maneira a reduzir a dependência dos cabos dos EUA. Inicialmente planejado para descentralizar os serviços virtuais, o cabo

ganhará novas funções com a expansão da tecnologia 5G e a digitalização acelerada pela pandemia (Pinto, 2021).

As redes *South Atlantic Cable Systems* (SACS), ligando Fortaleza a Angola, e *South Atlantic Inter Link* (SAIL), que conectam Fortaleza aos Camarões, são as principais entre América do Sul e África. Instaladas recentemente, essas redes beneficiam os BRICS, utilizando financiamento do Banco de Desenvolvimento dos BRICS para criar alternativas seguras contraespionagem e sabotagem (Medeiros; Pinto, 2022, p. 7-8).

Em resumo, a infraestrutura de cabos submarinos brasileiros, regulada por ANATEL, IBAMA e MB, com Fortaleza como principal *hub*, é fortalecida pela parceria Brasil-Europa com EllaLink e redes SACS e SAIL. Essas iniciativas visam a diversificar rotas, reduzir dependência dos EUA e proteger informações contraespionagem, ações essenciais em um cenário de digitalização crescente.

4.5 AS PRÁTICAS ADOTADAS PARA PROTEÇÃO DAS IC DE CABOS SUBMARINOS

A Amazônia Azul é um conceito político-estratégico promovido pela MB para destacar a importância do espaço marítimo e fluvial em AJB, conforme direitos e deveres da CNUDM III. Com tamanho semelhante à Amazônia, é onde o Brasil possui direitos soberanos para explorar recursos naturais no mar e subsolo, os quais representam um patrimônio vital para a nação (Brasil, 2020a, p. 18-19). A disseminação desse conceito tem sido bastante promissora em despertar na sociedade brasileira o reconhecimento da importância do mar e suas riquezas que podem ser alvo de cobiça estrangeira.

A fiscalização de atividades que possam comprometer os sistemas é conduzida em coordenação entre o Comando de Operações Marítimas e Proteção da Amazônia Azul (COMPAAz) e os Distritos Navais. Se o COMPAAz identificar um navio suspeito, a estrutura é imediatamente acionada para iniciar investigações (Agência Marinha de Notícias, 2024). A criação desse Comando tem proporcionado uma elevadíssima Consciência Situacional Marítima, possibilitando tomadas de decisão e ações mais tempestivas no domínio marítimo. A MB está desenvolvendo o SisGAAz, um complexo sistema de monitoramento e controle das AJB, com funções militares e civis. Sua implementação melhoraria a vigilância, ajudando a mitigar crimes ambientais, como o

ocorrido no litoral nordestino em 2019 (Brasil, 2020a, p. 40). Nota-se que se trata de uma condição *sine qua non* exercer o controle da vasta extensão da Amazônia Azul.

Em maio de 2024, a MB conduziu, de forma inédita, um treinamento de defesa envolvendo navios, mergulhadores escafandristas, tropas de Operações Especiais e drones de superfície. O foco foi a proteção de infraestruturas submarinas e estações terrestres de cabos no litoral do Rio de Janeiro. Coordenado pelo Comando Naval de Operações Especiais, a bordo do Navio de Socorro Submarino (NSS) Guillobel, o exercício envolveu órgãos governamentais, inclusive de Portugal, e empresas de telecomunicações, para simular situações de ocorrências reais recentes, a fim de manter a MB preparada para proteger suas ICPM (Agência Marinha de Notícias, 2024). Dessa forma, foi demonstrada a complexidade dessas ações, o elevado grau de aprestamento da MB e a necessidade de parcerias público-privadas nacionais e internacionais.

Em suma, a Amazônia Azul ressalta a importância estratégica das AJB. A fiscalização, o desenvolvimento do SisGAAz e treinamentos inéditos reforçam a proteção desse território, envolvendo parcerias público-privadas nacionais e internacionais. Essas ações demonstram a prontidão da MB em garantir a segurança e soberania nas AJB, protegendo as IC submarinas.

4.6 CONCLUSÃO PARCIAL

A proteção dos cabos submarinos, essenciais para a soberania e economia do Brasil, ainda necessita de maior atenção nas estratégias nacionais. A Estratégia Nacional de Defesa e o SisGAAz são fundamentais, mas faz-se necessário reforçar a segurança dessas IC para garantir a resiliência nacional. O caso do Yantar acendeu um alerta para a MB. Com Fortaleza emergindo como um *hub* tecnológico, o Brasil se destaca globalmente, mas a vulnerabilidade dos cabos, especialmente no Sul, exige medidas para fortalecer a segurança cibernética. Iniciativas como EllaLink e redes SACS e SAIL ajudam a diversificar rotas e reduzir a dependência dos EUA. A dimensão da Amazônia Azul e os esforços da MB demonstram a importância de parcerias nacionais e internacionais para proteger essas IC e assegurar a soberania nas AJB. O ineditismo do exercício realizado em maio de 2024, visando à proteção de ICPM, evidenciou que a MB não é a única responsável pela proteção das IC de cabos submarinos, de forma que a colaboração público-privada é essencial.

5 ANÁLISE DAS PRÁTICAS DO REINO UNIDO E BRASIL PARA DEFENDER SUAS IC DE CABOS SUBMARINOS

A infraestrutura de cabos submarinos é essencial para a comunicação global e a segurança econômica das nações. Tanto o Reino Unido quanto o Brasil dependem desses cabos para suas comunicações internacionais, mas adotam abordagens distintas em sua proteção. Este capítulo compara as práticas de proteção de cabos submarinos entre os dois países, sugerindo melhorias para o Brasil com base nas práticas avançadas do Reino Unido.

5.1 ABORDAGEM DO REINO UNIDO NA PROTEÇÃO DE CABOS SUBMARINOS

O Reino Unido, com longa experiência no uso de cabos submarinos desde a instalação do primeiro cabo de fibra óptica transatlântico em 1988, reconhece a importância estratégica desses cabos. A Estratégia Nacional de Segurança Marítima identifica os cabos submarinos como parte da IC, abordando ameaças físicas e cibernéticas (Reino Unido, 2022). Desde 2014, o país intensificou seus esforços, criando a Célula de Coordenação de Infraestrutura Submarina Crítica da OTAN, que o permitiu uma coordenação internacional mais eficaz. Também participa ativamente de parcerias, como a AUKUS, que oferecem suporte tecnológico e de inteligência (Hendriks; Halem, 2024b).

O governo britânico investiu em tecnologias de vigilância oceânica para proteger seus cabos submarinos, como o RFA Proteus, garantindo resposta rápida a ameaças (Hendriks; Halem, 2024b). Além disso, realiza regularmente exercícios militares com aliados, focados na proteção de cabos submarinos, essenciais para testar e aprimorar a resposta das forças armadas, fortalecendo a resiliência contra ameaças (Reino Unido, 2021).

5.2 ABORDAGEM DO BRASIL NA PROTEÇÃO DE CABOS SUBMARINOS

O Brasil possui uma vasta rede de cabos submarinos, sendo Fortaleza o principal *hub* intercontinental, mas a proteção dessas infraestruturas ainda carece de atenção nas estratégias nacionais de defesa. A EDM (Brasil, 2023) e a Política Nacional de Defesa (Brasil, 2024) destacam a importância de proteger as IC sob Poder

Marítimo, mas os cabos submarinos são frequentemente negligenciados em favor de outras instalações, como portos e plataformas de petróleo.

Um avanço importante foi a criação do SisGAAz pela MB, destinado a aumentar a vigilância e o controle das AJB. Embora o SisGAAz represente progresso significativo, falta-lhe uma ênfase específica na proteção de cabos submarinos e uma abordagem mais integrada que envolva o setor público e privado (Santos *et al.*, 2022). Nesse sentido, a reestruturação administrativa da MB, com a criação do COMPAAz, aprimorou a Consciência Situacional Marítima na Amazônia Azul.

A MB intensificou esforços com exercícios militares, como o de maio de 2024, focados na proteção de cabos submarinos, envolvendo tropas especiais, drones e colaboração internacional. No entanto, é necessário ampliar e institucionalizar essas ações para garantir proteção eficaz (Agência Marinha de Notícias, 2024). A cooperação robusta entre Forças Armadas e setor privado, seguindo o exemplo britânico, é essencial (Vichi; Pinto; Sá, 2020).

5.3 COMPARAÇÃO E SUGESTÕES DE MELHORIAS PARA O BRASIL

A comparação entre as práticas adotadas pelo Reino Unido e o Brasil revela áreas onde o Brasil pode melhorar significativamente na proteção de seus cabos submarinos, como apontado a seguir.

- **Desenvolvimento de parcerias internacionais:** o Brasil poderia se beneficiar do estabelecimento de parcerias internacionais semelhantes às do Reino Unido, como a participação em iniciativas da OTAN ou outras coalizões regionais. Essas parcerias permitiriam ao Brasil melhorar suas capacidades de monitoramento e resposta a ameaças submarinas, além de desenvolver tecnologias avançadas para a proteção de suas infraestruturas (Reino Unido, 2022).
- **Fortalecimento da cooperação público-privada:** o Reino Unido demonstrou a importância de uma colaboração estreita entre governo e setor privado na proteção dos cabos submarinos. O Brasil deveria seguir esse exemplo, intensificando a integração entre operadoras de telecomunicações, reguladores e Forças Armadas, para garantir uma resposta mais rápida e coordenada a ameaças (Reino Unido, 2021).

- **Aumento dos investimentos em vigilância oceânica:** assim como o Reino Unido, o Brasil deve investir em tecnologias avançadas para a vigilância e monitoramento de suas AJB. A expansão do SisGAAz é um passo importante, mas deve ser complementada com a aquisição de equipamentos e sistemas que permitam a detecção e neutralização de ameaças a cabos submarinos em tempo real. A implementação de capacidades específicas, como a introdução de um navio similar ao RFA Proteus, seria um grande avanço para a MB (Hendriks; Halem, 2024b). Estudos são necessários para determinar se o NSS Guillobel poderia ser adaptado para desempenhar as mesmas funções do Proteus.
- **Realização de exercícios militares conjuntos e combinados:** o Brasil deveria instituir regularmente exercícios militares conjuntos e combinados, tanto a nível nacional quanto internacional, focados na proteção de cabos submarinos. Esses exercícios não só aprimorariam a prontidão das forças brasileiras, mas também fortaleceriam parcerias estratégicas, permitindo o compartilhamento de melhores práticas e a cooperação em tempo real durante situações de crise (Agência Marinha de Notícias, 2024).
- **Revisão das estratégias nacionais pertinentes:** as estratégias nacionais do Brasil precisam incluir explicitamente a proteção de cabos submarinos como uma prioridade estratégica. Isso incluiria a atualização de documentos como a EDM para refletir a importância desses ativos e a necessidade de protegê-los de forma abrangente (Brasil, 2023, 2024).

5.4 CONCLUSÃO PARCIAL

O Reino Unido adotou medidas eficazes de proteção de cabos submarinos, mas o Brasil precisa avançar para prover a proteção das IC no Brasil: investindo em parcerias; cooperação público-privada; vigilância oceânica; realizando exercícios militares combinados; e estudando se o NSS Guillobel pode realizar as mesmas funções do RFA Proteus. O exercício da MB, em 2024, destacou a importância da colaboração público-privada. A reestruturação administrativa, com a criação do COMPAAz, foi outro acerto da MB digno de nota. Integrar essas práticas e desenvolver capacidades específicas é essencial para garantir a soberania e a segurança nas AJB, assegurando a resiliência nacional diante de ameaças globais emergentes.

6 CONCLUSÃO

Esta dissertação analisou a proteção dos cabos submarinos, com ênfase nas práticas do Reino Unido e sua relevância para o Brasil. Esses cabos são cruciais para a comunicação global, transportando a maioria dos dados digitais que sustentam economias modernas, segurança nacional e interações internacionais. Embora invisíveis para a maioria, sua importância estratégica é inegável, especialmente em um mundo cada vez mais dependente da conectividade digital.

Os capítulos iniciais destacaram a importância dos cabos submarinos como IC. Eles não apenas facilitam a comunicação civil e econômica, mas também desempenham um papel essencial na segurança nacional e internacional, transmitindo informações sensíveis necessárias à defesa e soberania dos Estados. Com o aumento da dependência dessa infraestrutura, especialmente devido às novas tecnologias e à digitalização global, a necessidade de proteção contra ameaças como desastres naturais, acidentes, ataques cibernéticos e sabotagens se torna urgente. A proteção eficaz desses cabos exige colaboração estreita entre governos, setor privado e organizações internacionais, uma vez que a responsabilidade por sua segurança não pode ser atribuída a um único ator.

O estudo das práticas do Reino Unido revelou um país que compreendeu cedo a importância estratégica dos cabos submarinos e adotou uma abordagem integrada para sua proteção. Desde 2014, o Reino Unido implementou políticas sólidas, fortaleceu parcerias internacionais e investiu em tecnologias avançadas de vigilância e defesa. A criação do JMSC e a introdução do navio de vigilância subaquática RFA Proteus exemplificam a preparação do país para enfrentar ameaças crescentes, especialmente no contexto geopolítico atual, marcado pela guerra na Ucrânia e pelo aumento das atividades submarinas de potências como Rússia e China. O Reino Unido também se destacou ao adotar uma estratégia de longo prazo, modernizando suas capacidades submarinas e formando alianças estratégicas, como o pacto AUKUS, voltadas à proteção da IC submarina.

No Brasil, embora o país possua uma extensa costa atlântica e uma vocação natural para o mar, a proteção dos cabos submarinos ainda carece de uma abordagem estratégica mais desenvolvida e coordenada. A vocação marítima do Brasil, aliada à crescente importância dos cabos submarinos para a economia e segurança nacional,

torna imperativo o aprimoramento das capacidades de defesa e vigilância. O Brasil pode aprender com as práticas britânicas, implementando medidas como a criação de centros de segurança marítima e o fortalecimento de alianças internacionais, adaptando essas estratégias à sua realidade regional e às suas necessidades específicas.

No capítulo 5, foram propostas cinco medidas para fortalecer a proteção dos cabos submarinos no Brasil. A primeira é criar um centro nacional de coordenação, integrando agências governamentais e setor privado. A segunda envolve o fortalecimento da vigilância e monitoramento marítimo, com investimentos em tecnologia e maior presença naval em áreas estratégicas. A terceira sugere promover parcerias internacionais com países experientes, como Reino Unido e EUA. A quarta medida é desenvolver uma legislação específica para regular a proteção dos cabos, com penalidades claras para sabotagem e danos acidentais. Por fim, a quinta propõe a realização de exercícios militares conjuntos, simulando ataques a cabos submarinos, para melhorar a prontidão das forças de defesa e a resposta a incidentes.

A dissertação também destacou as boas práticas da MB, que tem realizado significativos investimentos na modernização de suas capacidades de monitoramento e vigilância. Isso inclui o desenvolvimento de avançados sistemas de sensoriamento remoto e o fortalecimento da frota de navios de patrulha. A reorganização administrativa, com a criação do COMPAAz, foi fundamental para melhorar a capacidade de monitoramento e controle na Amazônia Azul, área de grande importância estratégica para o país. Além disso, a MB tem conduzido exercícios militares regulares que simulam cenários de ataques às IC, elevando a prontidão operacional das Forças Armadas. Esses exercícios promovem a integração entre diferentes setores do governo e do setor privado, fortalecendo a resiliência geral da infraestrutura submarina brasileira.

Em conclusão, a proteção dos cabos submarinos é uma prioridade estratégica que transcende fronteiras e requer uma abordagem global coordenada. O Reino Unido, com suas políticas proativas e investimentos substanciais, oferece um modelo de resiliência e adaptação que pode ser valioso para o Brasil. Ao adotar as sugestões apresentadas e integrar as boas práticas já realizadas pela MB, o país estará mais bem preparado para enfrentar os desafios do século 21, garantindo a segurança de sua IC, a continuidade das comunicações e a estabilidade econômica e política.

REFERÊNCIAS

- AGÊNCIA MARINHA DE NOTÍCIAS. Exercício inédito da Marinha garante manutenção de cabos submarinos. **Agência Marinha de Notícias**, Brasília, 17 jun. 2024. Disponível em: <https://www.agencia.marinha.mil.br/defesa-naval/exercicio-inedito-da-marinha-garante-manutencao-de-cabos-submarinos>. Acesso em: 8 ago. 2024.
- AUSTRALIA. Department of Veterans' Affairs. **Cutting cables**. Austrália: DVA Anzac Portal, 2019. Disponível em: <https://anzacportal.dva.gov.au/wars-and-missions/world-war-ii-1939-1945/events/little-known-operations-1939-1945/cutting-cables>. Acesso em: 13 jul. 2024.
- AZEVEDO, Luísa Barbosa. A Indústria Naval como meio de competição entre Estados Unidos da América e China. **Boletim Geocorrente**, Rio de Janeiro, n. 199, p. 7, mar. 2024. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/Boletim_Geocorrente_199%20v3.pdf. Acesso em: 5 ago. 2024.
- BEIRÃO, André Panno; MARQUES, Miguel; RUSCHEL, Rogerio Raupp. **O valor do mar: uma visão integrada dos recursos do oceano do Brasil**. 2. ed. São Paulo: Essential Idea Editora, 2020.
- BOYD, Andrew. **The security of subsea cables: an enduring naval challenge**. Bristol: Maritime Foundation, 2022. Disponível em: <https://www.maritimefoundation.uk/publications/maritime-2023/the-security-of-subsea-cables-an-enduring-naval-challenge/>. Acesso em: 13 jul. 2024.
- BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 8 ago. 2024.
- BRASIL. Marinha do Brasil. Centro de Comunicação Social da Marinha. **Nota à Imprensa [informando sobre o Navio de Pesquisa Oceanográfico russo “Yantar”]**. Brasília: Centro de Comunicação Social da Marinha, 2020b. Disponível em: https://www.marinha.mil.br/sites/default/files/nota_navio_russo.pdf. Acesso em: 8 ago. 2024.
- BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Estratégia de Defesa Marítima**. Brasília: Estado-Maior da Armada, 2023. Disponível em: <https://www.marinha.mil.br/sites/default/files/ema-310-edm-1ed.pdf>. Acesso em: 8 ago. 2024.
- BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Plano Estratégico da Marinha (PEM 2040)**. Brasília: Estado-Maior da Armada, 2020a. Disponível em: https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/book.html. Acesso em: 8 ago. 2024.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa; Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2024. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/politica-nacional-de-defesa. Acesso em: 8 ago. 2024.

BRASIL. Marinha do Brasil. **Política Naval**. Brasília: Ministério da Defesa, 2019. Disponível em: <https://www.marinha.mil.br/politicanaval>. Acesso em: 8 ago. 2024.

BROOKE-HOLLAND, Louisa. **Seabed warfare**: protecting the UK's undersea infrastructure. London: House of Commons Library, 2023. Disponível em: <https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure/>. Acesso em: 26 jul. 2024.

BUEGER, Christian; LIEBETRAU, Tobias; FRANKEN, Jonas. **Security threats to undersea communications cables and infrastructure – consequences for the EU**. Brussels: Policy Department/Directorate-General for External Policies, 2022. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA\(2022\)702557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf). Acesso em: 9 jul. 2024.

BURGESS, Matt. The most vulnerable place on the internet. **Wired**, San Francisco, Nov. 2 2022. Disponível em: <https://www.wired.com/story/submarine-internet-cables-egypt/>. Acesso em: 22 jul. 2024.

BURNETT, Douglas R. OSPAR and coastal state encroachment on high seas submarine cable freedoms. *In*: KOTZUR, Markus *et al.* (ed.). **Sustainable ocean resource governance**: deep sea mining, marine energy and submarine cables. Leiden; Boston: Brill/Nijhoff, 2018. p. 234-277.

BURNETT, Douglas R.; BECKMAN, Robert; DAVENPORT, Tara M. **Submarine cables**: the handbook of law and policy. Leiden: Brill, 2013.

CASSETTA, Marco. How to respond to the emerging threats to critical underwater infrastructure at the time of Russia's war against Ukraine. **IAI Commentaries**, Roma, v. 24, n. 31, June 2024. Disponível em: <https://www.iai.it/en/publicazioni/how-respond-emerging-threats-critical-underwater-infrastructure>. Acesso em: 10 jul. 2024.

CLARE, Mike. **Submarine cable protection and the environment**. Lymington: International Cable Protection Committee, 2021. Boletim n. 2. Disponível em: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf. Acesso em: 12 jul. 2024.

CLARE, Mike. **Submarine cable protection and the environment**. Lymington: International Cable Protection Committee, Lymington, 2023. Boletim n. 7. Disponível em: <https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/?id=7>. Acesso em: 13 jul. 2024.

CLARE, Mike. **Submarine cable protection and the environment**. Lymington: International Cable Protection Committee, 2024. Disponível em: <https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/?id=8>. Acesso em: 13 jul. 2024.

CLARK, Bryan. Undersea cables and the future of submarine competition. **Bulletin of the Atomic Scientists**, [s. l.], v. 72, n. 4, p. 234-237, 2016. Disponível em: <https://www.tandfonline.com/doi/pdf/10.1080/00963402.2016.1195636>. Acesso em: 15 jul. 2024.

COUTAU-BÉGARIE, Hervé. **Tratado de Estratégia**. Rio de Janeiro: EGN/DPHDM, 2010.

DATACENTER DYNAMICS. O que é um cabo submarino? Entenda como funciona a fibra óptica submarina. **DataCenter Dynamics**, Madrid, 10 jul. 2023. Disponível em: <https://www.datacenterdynamics.com/br/an%C3%A1lises/o-que-e-um-cabo-submarino-entenda-como-funciona-a-fibra-optica-submarina/>. Acesso em: 15 jul. 2024.

DAVENPORT, Tara. Intentional damage to submarine cable systems by states. **Aegis Series Paper**, Califórnia, n. 2305, Oct. 2023. Disponível em: <https://www.lawfaremedia.org/article/intentional-damage-to-submarine-cable-systems-by-states>. Acesso em: 13 jul. 2024.

DIBNER, Bern. **The Atlantic cable**. Norwalk: Burndy Library, 1959.

ÉPOCA NEGÓCIOS. Navio russo suspeito de espionagem coloca Marinha Brasileira em alerta. **Época Negócios**, São Paulo, 21 fev. 2020. Disponível em: <https://epocanegocios.globo.com/Brasil/noticia/2020/02/epoca-negocios-navio-russo-suspeito-de-espionagem-coloca-marinha-brasileira-em-alerta.html>. Acesso em: 23 jul. 2024.

EXAME. Há um ano o Facebook se tornou Meta: veja os resultados até agora. **Exame**, São Paulo, 28 out. 2022. Disponível em: <https://exame.com/future-of-money/ha-um-ano-o-facebook-se-tornou-meta-veja-os-resultados-ate-agora/>. Acesso em: 15 jul. 2024.

FELSTEAD, Peter. UK's first multi-role ocean surveillance ship enters service. **European Security & Defense**, [s. l.], Oct. 11, 2023. Disponível em: <https://eurosd.com/2023/10/news/34540/first-mross-enters-service/>. Acesso em: 7 ago. 2024.

FRASCÀ, Domenico; GALANTINI, Luca. The issue of submarine cable security. *In*: Cappelletti, Francesco (ed.). **Towards a new European security architecture**. Brussels: European Liberal Forum, 2023. p. 51-61. Disponível em: https://liberalforum.eu/wp-content/uploads/2023/06/BOURCHIER_ELF_New_European_Security.pdf. Acesso em: 3 ago. 2024.

GARCIA, Francisco Proença (coord.). **Great power competition in the Atlantic**. Lisboa: Atlantic Centre, 2023.

THE GUARDIAN. UK military chief warns of Russian threat to vital undersea cables. **The Guardian**, London, 2022. Disponível em: <https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables>. Acesso em: 3 ago. 2024.

HENDRIKS, Marcus Solarz; HALEM, Harry. **From space to seabed**: protecting the UK's undersea cables from hostile actors. London: Policy Exchange, 2024a. *E-book*. Disponível em: <https://policyexchange.org.uk/wp-content/uploads/From-space-to-seabed.pdf>. Acesso em: 2 ago. 2024.

HENDRIKS, Paul; HALEM, Sarah van. Securing the subsea: the UK's maritime strategy and the challenge of undersea infrastructure protection. **Journal of Maritime Security**, v. 5, n. 2, 2024b.

MARTIN, Alexander. Fishing vessel likely cause of SHEFA-2 fault. **Submarine Telecom Forum**. [S. l.], Oct. 27, 2022. Disponível em: <https://subtelforum.com/fishing-vessel-likely-cause-of-shefa-2-fault/>. Acesso em: 2 ago. 2024.

MEDEIROS, Sabrina Evangelista; PINTO, Danielle Jacon Ayres. Cabos submarinos e segurança cibernética no Atlântico. **Atlantic Centre Policy Brief**, Lisboa, n. 11, mar. 2022.

MENDES, Fábio. Cabos submarinos podem ser os novos alvos da Rússia. **CNN Brasil**, São Paulo, 3 jun. 2023. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/cabos-submarinos-podem-ser-os-novos-alvos-da-russia/>. Acesso em: 17 jul. 2024.

MWEMA, Esther; BIRHANE, Abeba. Undersea cables in Africa: the new frontiers of digital colonialism. **First Monday**, [s. l.], v. 29, n. 4, 2024. Disponível em: <https://firstmonday.org/ojs/index.php/fm/article/view/13637>. Acesso em: 10 jul. 2024.

NAKAMURA, Hotaka. Defending submarine cables in the Black Sea: a challenge for NATO and the region. **Middle East Institute**. Washington D.C., Mar. 2, 2023. Disponível em: <https://www.mei.edu/publications/defending-submarine-cables-black-sea-challenge-nato-and-region>. Acesso em: 10 jul. 2024.

PATALANO, Alessio. Unseen but vital: Britain and undersea security. **Britain's World**, [s. l.], 8 Mar. 8 2023. Disponível em: <https://www.geostrategy.org.uk/britains-world/unseen-but-vital-britain-and-undersea-security/>. Acesso em: 7 ago. 2024.

PINTO, Danielle Jacon Ayres. **The Europe and Brazil submarine cable initiative**: challenges and opportunities. Valetta: InterAgency Institute, 2021. (Policy Briefs Series, v. 7). Disponível em: <https://zenodo.org/records/5069820>. Acesso em: 10 jul. 2024.

RAHA, Utpal Kumar; RAJU, R. K. **Submarine cables protection and regulations**: a comparative analysis and model framework. New York: Springer, 2021.

REINO UNIDO. Department for Transport. **Maritime 2050: navigating the future**. London: Department for Transport, 2019. Disponível em: <https://www.gov.uk/government/publications/maritime-2050-navigating-the-future>. Acesso em: 29 July 2024.

REINO UNIDO. **Joint Maritime Security Centre**. London: Joint Maritime Security Centre, c2024. Disponível em: <https://www.gov.uk/government/groups/joint-maritime-security-centre>. Acesso em: 29 jul. 2024.

REINO UNIDO. Ministry of Defence. **Defence in a competitive age**. London: Her Majesty's Stationery Office, 2021. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf. Acesso em: 7 ago. 2024.

REINO UNIDO. Ministry of Defence. **UK and Norway to increase cooperation on undersea capabilities**. London: Ministry of Defence, 2023b. Disponível em: <https://www.gov.uk/government/news/uk-and-norway-to-increase-cooperation-on-undersea-capabilities>. Acesso em: 29 jul. 2024.

REINO UNIDO. National Protective Security Authority. **Critical national infrastructure**. London: National Protective Security Authority, 2023a. Disponível em: <https://www.npsa.gov.uk/critical-national-infrastructure-0>. Acesso em: 26 jul. 2024.

REINO UNIDO. **National Strategy for Maritime Security**. [Apresentado ao Parlamento pelo Secretário de Estado dos Transportes por ordem de Sua Majestade]. Londres: Her Majesty's Stationery Office, 2022. Disponível em: <https://assets.publishing.service.gov.uk/media/62fcbf748fa8f504bd84581f/national-strategy-for-maritime-security-print-version.pdf>. Acesso em: 29 jul. 2024.

SANTOS, Thauan *et al.* **Economia azul: vetor para o desenvolvimento do Brasil**. São Paulo: Essencial Idea, 2022.

SHEN, Hong. Building a digital silk road?: situating the internet in China's Belt and Road Initiative. **International Journal of Communication**, Los Angeles, v. 12, p. 2683-2701, 2018. Disponível em: <https://ijoc.org/index.php/ijoc/article/view/8405>. Acesso em: 22 jul. 2024.

SIEBOLD, Sabine. NATO says Moscow may sabotage undersea cables as part of war on Ukraine. **Reuters**, [s. l.], May 3, 2023. Disponível em: <https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/>. Acesso em: 17 jul. 2024.

STAROSIELSKI, Nicole. **The Undersea Network**. Durham: Duke University Press, 2015.

SUBMARINE CABLE NETWORKS. Undersea cable cuts in the Mediterranean affected 14 countries. **Submarine Cable Networks**. [S. l.], Mar. 18, 2011. Disponível em: <https://www.submarinenetworks.com/en/nv/news/cable-cuts-affected-14-countries>. Acesso em: 13 jul. 2024.

SUCIU, Peter. USS Jimmy Carter: The Navy's Seawolf-class submarine China can't match. **The National Interest**, Washington D.C, May 9, 2024. Disponível em: <https://nationalinterest.org/blog/buzz/uss-jimmy-carter-navys-seawolf-class-submarine-china-cant-match-207454>. Acesso em: 11 jul. 2024.

UNITED NATIONS. **Resolution A/ 65/37, of December 7, 2010**. Oceans and the law of the sea. New York: UN General Assembly, 2010. Disponível em: <https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F65%2F37&Language=E&DeviceType=Desktop&LangRequested=False>. Acesso em: 21 jul. 2024.

VICHI, Leonardo Perin; PINTO, Danielle Jacon Ayres; SÁ, André Luiz Nery de. A defesa da infraestrutura de cabos submarinos: por uma interface entre a defesa cibernética e a segurança marítima no Brasil. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 26, n. 2, p. 326-346, maio/ago. 2020. Disponível em: <https://www.portaldeperiodicos.marinha.mil.br/index.php/revistadaegn/article/view/4209/4096>. Acesso em: 3 jul. 2024.

UNESCO – Organização das Nações Unidas para a Educação, a Ciência e a Cultura. **Transatlantic Cable Ensemble (Ireland)**. [S. l.]: UNESCO, 2023. Disponível em: <https://whc.unesco.org/en/tentativelists/6634/>. Acesso em: 12 jul. 2024.

WEDIN, Lars. **Estratégias marítimas no século XXI: a contribuição do Almirante Castex**. São Paulo: Editora NUVIS, 2015.