ESCOLA DE GUERRA NAVAL

CMG GUSTAVO SANT´ANA

PROTEÇÃO DOS CABOS SUBMARINOS NO BRASIL:
Análise Comparativa das Governanças do Brasil e Europa

Rio de Janeiro
2024

CMG GUSTAVO SANT´ANA

PROTEÇÃO DOS CABOS SUBMARINOS NO BRASIL:
Análise Comparativa das Governanças do Brasil e Europa

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) Pompeu

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.

gov.br
Documento assinado digitalmente
GUSTAVO SANT ANA COUTINHO
Data: 27/11/2024 09:41:36-0300
Verifique em https://validar.iti.gov.br

DEDICATÓRIA

Dedico este trabalho a Deus, ao meu país, a minha família e a instituição Marinha do Brasil que me fez crescer e acreditar ainda mais na grandeza de todos eles.

AGRADECIMENTO

Agradeço a minha família pela compreensão nos momentos em que tiveram de abdicar da minha presença para que eu pudesse me dedicar ao serviço de minha profissão.

Ao meu orientador, Comandante Pompeu pelo entusiasmo e paciência com que direcionou meus pensamentos que culminaram neste trabalho.

A todos os colegas da turma C-PEM 2024 da Escola de Guerra Naval, pela amizade e pelas demonstrações de apoio durante toda a singradura.

Ao encarregado do C-PEM 2024, Comandante Sousa e toda sua equipe pela forma como conduziram um ano profícuo de trabalho, permitindo o engrandecimento acadêmico de toda a turma.

“Barcos não fazem frotas. O primeiro elemento da marinha é o homem do mar.”

Rui Barbosa

RESUMO

Os cabos submarinos são uma Infraestrutura Crítica essencial para as telecomunicações, sendo responsável por mais de 97% da transmissão de dados entre os países e continentes. São essenciais para várias políticas públicas, não apenas de telecomunicações, como também de transformação digital, educação, saúde, segurança da informação, transações financeiras e segurança cibernética. No entanto, a sua importância estratégica os torna suscetíveis a uma série de ameaças, desde danos acidentais até sabotagem intencional e espionagem cibernética. A presente abordagem teve o propósito de estudar como alguns países europeus estão enfrentando o desafio de proteção desses ativos, tendo em vista o histórico recente de acidentes nessas infraestruturas e em outras infraestruturas submersas. Para isso, foi pesquisada as ações recentes adotadas por alguns países da União europeia, Reino Unido e Noruega para a proteção dos seus cabos submarinos, comparando com o modelo no Brasil e identificar eventuais oportunidades de melhorias. As medidas adotadas na Europa e no Brasil possuem algumas similaridades, embora a percepção de ameaça aos cabos submarinos na Europa seja mais presente. O modelo, da maioria dos países europeus, de conhecer, monitorar e agir em um contexto de cooperação é essencial para a segurança desses ativos. O Brasil caminha para um processo similar, entretanto com uma maturidade ainda mais baixa.

Palavras-chave: Cabos Submarinos. Infraestrutura Crítica de Comunicações. Infraestrutura Crítica do Poder Marítimo. Infraestrutura Crítica Submersa. Proteção.

ABSTRACT

Protection of Undersea Cable in Brazil: Comparative Analysis of Governance of Brazil and Europe

Submarine cables are a critical infrastructure essential for telecommunications, being responsible for more than 97% of data transmission between countries and continents. They are essential for several public policies, not only in telecommunications, but also in digital transformation, education, health, information security, financial transactions and cybersecurity. However, their strategic importance makes them susceptible to a series of threats, from accidental damage to intentional sabotage and cyber espionage. This approach aimed to study how some European countries are facing the challenge of protecting these assets, given the recent history of accidents in these infrastructures and in other submerged infrastructures. To this end, the subsequent actions adopted by some countries of the European Union, the United Kingdom and Norway to protect their submarine cables were researched, comparing them with the model in Brazil and identifying possible opportunities for improvement. The measures adopted in Europe and Brazil have some similarities, although the perception of a threat to submarine cables in Europe is more present. The model, of most European countries of knowing, monitoring and acting in a context of cooperation is essential for the security of these assets. Brazil is moving towards a similar process, although with an even lower maturity.

Keywords: Submarine Cables. Undersea Cable. Critical National Infrastructure. Communications Critical Infrastructure. Submerged Critical Infrastructure. Protection

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AJB	-	Águas jurisdicionais brasileiras
ACGF	-	Fórum de Guardas Costeira do Ártico
CAPN	-	Campos de Atuação do Poder Naval
CENSIPAM	-	Centro Gestor e Operacional do Sistema de Proteção da Amazônia
CNI	-	*Critical National Infrastructure*
CNUDM	-	Convenção das Nações Unidas sobre o Direito do Mar
ComOpNav	-	Comando de Operações Navais
ComPAAZ	-	Comando de Operações Marítimas e Proteção da Amazônia Azul
CUI	-	*Critical Underwater Infrastructure*
ECGFF	-	*European Coast Guard Functions Forum*
EDM	-	Estratégia de Doutrina Marítima
EFCA	-	Agência Europeia de Controle de Pesca
EMSA	-	Agência Europeia de Segurança Marítima
END	-	Estratégia Nacional de Defesa
ENISA	-	Agência da União Europeia para a Cibersegurança
ENSIC	-	Estratégia Nacional de Segurança das Infraestruturas Críticas
EUA	-	Estados Unidos da América
EUROSUR	-	*European Border Surveillance system*
FDM	-	Fundamentos de Doutrina Marítima
FRONTEX	-	Agência Europeia da Guarda Costeira e de Fronteiras
GPS	-	Sistema de Posicionamento Global – *Global Position System*
GSI/PR	-	Gabinete de Segurança Institucional da Presidência da República
GT-CIBER	-	Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica
GTSIC	-	Grupos Técnicos de Segurança de Infraestruturas Críticas

GUGI	-	*Glavnoye Upravlenie Glubokovodnikh Issledovanii* - Diretoria Principal de Pesquisa em Águas Profundas
IA	-	Inteligência Artificial
ICPC	-	Comitê Internacional de Proteção de Cabos
ICPM	-	Infraestrutura Crítica do Poder Marítimo
IMR	-	*Institute of Marine Research*
IoT	-	Internet das Coisas
ISPS	-	Código Internacional de Segurança de Navios e Instalações Portuárias
IVR	-	Inteligência, Vigilância e Reconhecimento
JEF	-	*Joint Expeditionary Force*
JMSC	-	Centro conjunto de segurança marítima - *Joint Maritime Security Centre*
KSAT	-	Kongsberg Satellite Services
LCF	-	Linhas de Comunicação Fluvial
LRIT	-	Sistema de Identificação e Acompanhamento de Navios a Longa Distância
MARCOM	-	*Allied Maritime Command*
MoD	-	*Ministry of Defence*
MROSS	-	*Multi-Role Ocean Surveillance Ship*
NACGF	-	*North Atlantic Coast Guard Forum*
NATO	-	*North Atlantic Treaty Organization*
NJHQ	-	*Norwegian Joint Headquarters*
NMIC	-	Centro nacional de informações marítimas
OBE	-	Objetivos Estratégicos
ONU	-	Organização das Nações Unidas
OTAN	-	Organização do Tratado do Atlântico Norte
OTH	-	*Over The Horizon*
PCF	-	Plano de Configuração de Força
PlanSic	-	Plano Nacional de Segurança das Infraestruturas Críticas
PND	-	Política Nacional de Defesa
PNSIC	-	Política Nacional de Segurança de Infraestruturas Críticas

PREPS	-	Programa Nacional de Rastreamento de Embarcações Pesqueiras por Satélite
RAF	-	*Royal Air Force*
RFA	-	*Royal Fleet Auxiliary*
ROV	-	Veículos Subaquáticos Operados Remotamente - *Remotely Operated Underwater Vehicle*
SIMMAP	-	Sistema de Monitoramento Marítimo de Apoio às Atividades de Petróleo
SisGAAz	-	Sistema de Gerenciamento da Amazônia Azul
SISTRAM	-	Sistema de Informação Sobre o Tráfego Marítimo
SMA	-	Segurança Marítima
SOC	-	*Serious and Organised Crime*
TIC	-	Tecnologias de informação e comunicação
UE	-	União Europeia
UUV	-	*Unmanned Underwater Vehicle*
VAB	-	Valor Acrescentado Bruto
ZEE	-	Zona Econômica Exclusiva

SUMÁRIO

1 - INTRODUÇÃO

O domínio do mar sempre se mostrou um desafio para a humanidade, entretanto, foi sendo superado na evolução da história, trazendo impactos significativos em termos econômicos, geopolíticos e históricos.

Com a Revolução Industrial do século XIX o comércio marítimo foi impulsionado, acompanhado do desenvolvimento de navios a vapor e a expansão das rotas comerciais globais. O transporte marítimo tornou-se ainda mais vital para o movimento de matérias-primas, mercadorias e pessoas em escala mundial, impulsionando o crescimento econômico e a globalização. Com o aumento do comércio e da interconexão global, houve uma demanda crescente por sistemas de comunicação mais eficientes e abrangentes. A Revolução Industrial marcou o início de uma era de rápido progresso e mudança, impulsionando a humanidade em direção a novos horizontes de desenvolvimento econômico, tecnológico e social.

A necessidade de melhorar e expandir as comunicações foi uma das muitas demandas geradas por esse período de transformação, que moldou o mundo em que vivemos até os dias de hoje. A expansão dos cabos submarinos para conectar os continentes foi mais um desafio superado no processo de domínio do mar, atualmente os oceanos sustentam as comunicações digitais da nossa era.

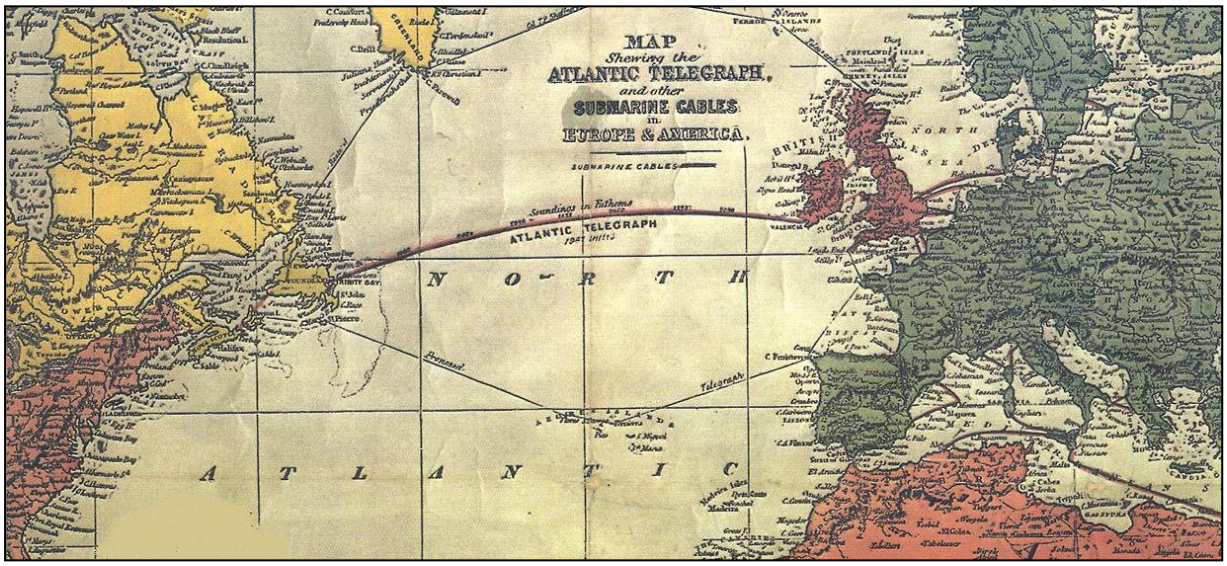
Os primeiros cabos submarinos foram instalados no século XIX, inicialmente entre a Grã-Bretanha e a França, e logo atravessaram o Atlântico, conectando a Irlanda, e *Heart's Content*, na Terra Nova nos Estados Unidos da América (EUA), no ano de 1858, conforme Figura 1. Nessa nova tecnologia, os sinais elétricos eram transmitidos por um fio colocado entre duas estações telegráficas. Surgiram novas tecnologias de comunicação, como o telégrafo elétrico de Samuel Morse e o telefone de Alexander Graham Bell, que permitiram a transmissão rápida e eficaz de informações em longas distâncias. O código Morse foi usado, permitindo assim, a transmissão simples de mensagens complexas aumentado a velocidade de entrega, inaugurando uma era inovadora considerada de grande utilidade para a humanidade (Sunak, 2017).

Em 16 de Agosto desse ano, a Rainha Vitória e o Presidente James Buchanan trocaram telegramas. Levando apenas 17 horas e 40 minutos a ser transmitida, a breve correspondência (menos de 100 palavras no total) representou a

mensagem mais rápida alguma vez enviada entre Washington e Londres (Sunak, 2017).

A conquista, entretanto, foi momentânea e durou pouco, pois o cabo apresentou falha apenas algumas semanas após o início de operação. Embora a sua substituição demorasse mais 6 anos, a expedição dessa instalação marcou o primeiro passo numa revolução nas comunicações que levaria, em última instância, à criação da Internet (Sunak, 2017).

Figura 1 – Mapa do cabo telegráfico Transatlântico de 1858



Fonte: Kavanagh, (2023).

Apesar da sua propagação pelos oceanos do mundo durante essas décadas iniciais, os cabos telegráficos caíram em desuso no início do século XX, sendo substituídos por outras tecnologias emergentes, como o telefone e, mais tarde, o fax. Avanços adicionais na tecnologia de comunicações levaram à instalação do primeiro sistema transatlântico de cabos telefônicos na década de 1950, seguido três décadas depois pelo primeiro sistema transatlântico de cabos de fibra óptica. Trinta e cinco anos se passaram desde então e cerca de 530 sistemas de cabos estão atualmente ativos ou em construção (Kavanagh, 2023).

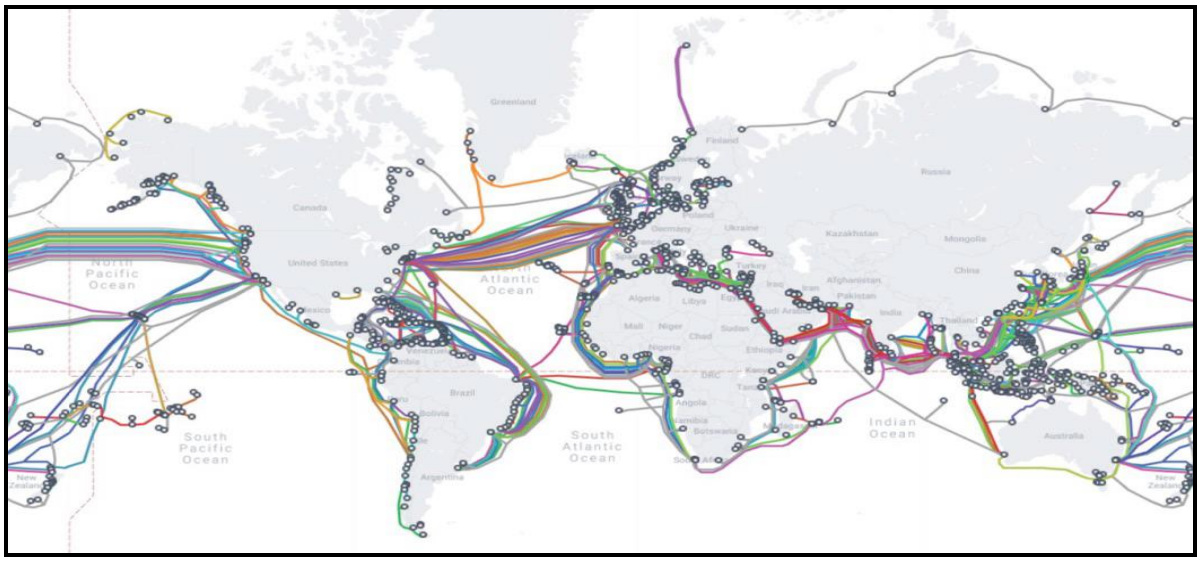
Os cabos submarinos de fibra óptica são agora a espinha dorsal da nossa infraestrutura de comunicações: mais de 95 por cento do tráfego global de Internet, voz e dados transita por essa malha submersa. Literalmente, todas as comunicações privadas, empresariais e militares dependem dessa rede, tal como as transações financeiras globais e muitos sistemas de defesa. O valor estratégico da infraestrutura

continua a crescer em paralelo com a nossa dependência digital, tendo em vista as diversas demandas como o advento do 5G e as necessidades de conectividade de alta qualidade e baixa latência dos centros econômicos, o valor comercial para o acesso a novos mercados e a quantidade de dados hospedados (Kavanagh, 2023).

Como pode-se observar na Figura 2, a conectividade global é altamente dependente de cabos de comunicações submarinos e adicionalmente (Sunak, 2017):

- Cerca de 97% das comunicações globais são transmitidas por meio dos cabos apoiados nas profundezas dos oceanos.
- A rede submarina atual compreende cerca de 213 sistemas de cabos independentes e 545.018 milhas de fibra.
- Não há alternativa à utilização destes cabos submarinos. A tecnologia de satélite não consegue substituir eficazmente às necessidades de comunicação da economia e da sociedade digitais modernas, tendo em vista o volume de dados que são transmitidos, a velocidade de transmissão entre outros requisitos técnicos.
- Num único dia, estes cabos transportam mais de 10 bilhões de dólares em transferências financeiras e processam mais de 15 milhões desses tipos de transações.

Figura 2- Visão geral dos cabos submarinos



Fonte: Telegeography (2023)

O objetivo deste trabalho foi estudar as vulnerabilidades dos cabos submarinos, apresentar eventos de avarias que alguns países enfrentaram, suas consequências e lições aprendidas. Verificou quais ações esses países estão implementando para mitigar as ameaças a essa infraestrutura crítica. A pesquisa abrangeu países como Reino Unido, Noruega e alguns países da União Europeia (UE), tendo em vista a conjuntura regional, onde um conflito envolvendo uma potência tecnológica como a Rússia, que exerce grande influência nos vizinhos, afetou a resiliência e segurança desse sistema de comunicação global.

Embora o objeto de estudo sejam os cabos submarinos de comunicação, esse trabalho observou que várias ações adotadas pelos países ora são consideradas particularmente aos cabos submarinos e ora de uma forma mais ampla, a todas as infraestruturas submersas, como os gasodutos, oleodutos e outras estruturas consideradas críticas incluindo os cabos submarinos.

2 – CARACTERÍSTICAS, LEGISLAÇÃO E AMEAÇAS AOS CABOS SUBMARINOS

Os cabos submarinos atuais usam tecnologia de fibra óptica para transmitir dados. Alguns sistemas de cabos individuais podem ter até 45.000 quilômetros. Juntos, representam aproximadamente 1,3 milhões de quilômetros de cabos em serviço em todo o mundo. Os cabos são compostos de vários pares de fibras ópticas, com aproximadamente o diâmetro de um fio de cabelo humano, que são então cobertos por uma camada de fibra óptica, gel de silicone e revestido com diversas camadas de plástico, malha de aço e cobre. Por vezes, camadas adicionais de fio de aço são aplicadas na parte externa do cabo para protegê-lo contra danos externos. A espessura da blindagem de aço é geralmente determinada pela profundidade do mar (Hendriks; Halem, 2024).

A coordenação de operações militares, a comunicação entre estados via missões diplomáticas, a coleta de informações e todo o fluxo de dados envolvendo operações financeiras, acordos empresariais, em suma, toda conexão global de internet dependem da rede de cabos. A perda de comunicações durante alguns minutos ou horas pode acarretar repercussões desastrosas em operações urgentes e gerar grandes implicações financeiras.

As consequências de qualquer forma de dano a cabos submarinos são, portanto, significativas. Além da utilização para fins civis, os países dependem de cabos submarinos para a segurança nacional.

2.1 - INFRAESTRUTURA DOS CABOS

Para uma boa compreensão das ameaças e das questões legais envolvidas é útil conhecer a arquitetura e os principais componentes da infraestrutura dos cabos submarinos. A vulnerabilidade do componente do cabo difere dependendo da sua posição. Em águas costeiras e rasas, a localização dos cabos geralmente está disponível ao público para evitar acidentes por fundeio de navios e atividades de dragagem.

As posições são marcadas nas cartas náuticas para garantir a conscientização dos usuários marítimos. Por outro lado, as localizações precisas não são publicadas em alto-mar e, portanto, os cabos são muito mais difíceis de

localizar. Dependendo do fundo do mar, os reparos em grandes profundidades são mais difíceis e demorados. Isso implica que uma ruptura nessa região tem um impacto mais severo do que uma ruptura nas águas costeiras (Bueger; Liebetrau; Franken, 2022).

Do ponto de vista legal, é importante reconhecer que o estatuto dos cabos difere substancialmente entre as diferentes zonas jurídicas estabelecidas pela Convenção das Nações Unidas sobre o Direito do Mar, CNUDM. Eles são instalados passando por diversas áreas marítimas, suas extremidades estão nos *landing-points* ou áreas de aterramento, atravessando o mar territorial, Zona Econômica Exclusiva (ZEE) e alto-mar.

Os países têm jurisdição total sobre o cabo nas suas águas territoriais, ou seja, até 12 milhas náuticas da linha de base da sua costa. Os Estados também têm deveres e obrigações específicos de aplicação da lei na zona contígua (24MN). Os estados não têm jurisdição sobre cabos fora dessas zonas. Na verdade, em alto-mar (as áreas fora da jurisdição nacional), bem como nas Zonas Econômicas Exclusivas dos Estados, o estatuto jurídico dos cabos e dos direitos e responsabilidade pela sua proteção é ambíguo (Bueger; Liebetrau; Franken, 2022).

2.1.1 - Estações de Aterragem (*Landpoints*)

As estações de aterragem são os locais onde a rede submarina termina e se conecta à rede terrestre da operadora local. As estações de aterragem (ou aterramento) tendem a estar próximas da costa e são frequentemente protegidas por cercas elétricas ou outras estruturas como equipamentos de vigilância remota, câmeras e sensores. As estações de aterragem comportam servidores, tecnologias de distribuição e comutação que fornecem a ponte para a rede terrestre (Bueger; Liebetrau; Franken, 2022).

A proteção dos pontos de aterragem é de extrema importância para a segurança dos dados que transitam por essas infraestruturas. Esses locais apresentam vulnerabilidades, pois são acessíveis fisicamente e concentram uma grande quantidade de dados sensíveis. A vulnerabilidade física desses pontos torna-os alvos potenciais para ataques, sabotagem ou espionagem. Um ataque bem-sucedido a um *landpoint* poderia interromper comunicações vitais, causar danos econômicos significativos e comprometer a segurança nacional. Além disso, esses

locais são vulneráveis a ataques cibernéticos, pois o acesso físico aos equipamentos pode permitir a exploração de falhas de *hardware* ou *software* para interceptar, manipular ou interromper o fluxo de dados (Bueger; Liebetrau; Franken, 2022).

Além disso, a proteção dos *landpoints* está ligada à implementação de redundâncias e à diversificação das rotas de cabos, contribuindo para a criação de uma rede mais resiliente, capaz de resistir a tentativas de interrupção ou sabotagem. Em suma, a proteção dos *landpoints* é fundamental para a segurança das comunicações globais, sendo essencial garantir a integridade física e cibernética desses locais e, por extensão, para preservar a segurança nacional, a privacidade e a estabilidade econômica (Bueger; Liebetrau; Franken, 2022).

As empresas que operam os cabos submarinos têm a responsabilidade primária de proteger os pontos de aterragem, entretanto, uma legislação governamental deve existir para impor requisitos de segurança e eventualmente trabalhar em parceria com os operadores de cabos para garantir a segurança desses pontos críticos.

2.1.2 - Estrutura de Reparo/Manutenção

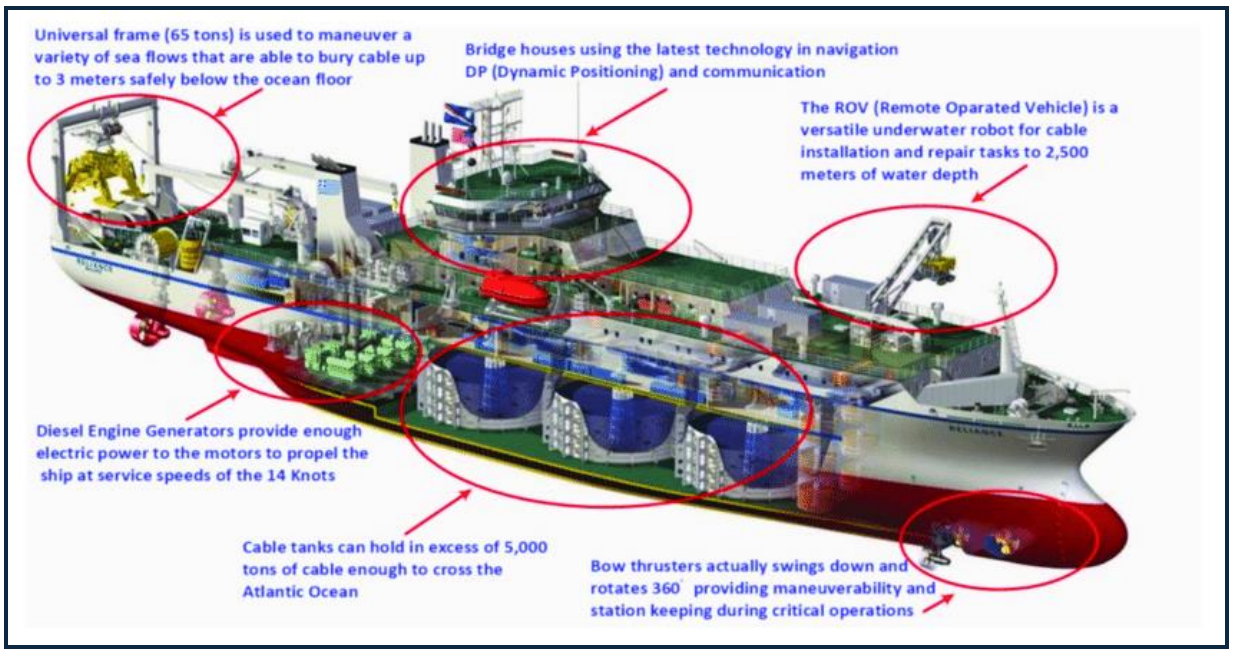
O reparo e a manutenção de cabos são realizados por uma indústria distinta das empresas operadoras e proprietárias de cabos. Os operadores e proprietários firmam contratos com as empresas de manutenção marítima que possuem depósitos de armazenamento de cabos e equipamentos, além de navios específicos chamados de *cableships,* vide Figura 3, estrategicamente posicionados ao redor do mundo, disponíveis 24 horas por dia, 7 dias por semana, para reparar falhas nos cabos (Bueger; Liebetrau; Franken, 2022).

A estrutura de reparo de cabos submarinos é uma operação complexa e altamente especializada, que envolve diversas etapas. Esses navios são equipados com tecnologia avançada para localizar, reparar e, se necessário, substituir seções de cabos danificados.

Os *cableships* utilizam sistemas de posicionamento avançados e veículos subaquáticos operados remotamente (ROVs) para localizar a seção danificada do cabo. Sensores e equipamentos de sonar ajudam na identificação exata do ponto de falha. Após localizar a falha, o cabo é trazido à superfície. A seção danificada é cortada e substituída por uma nova. Em alguns casos, o cabo pode ser emendado

diretamente no fundo do mar utilizando ROVs e equipamentos especializados (Bueger; Liebetrau; Franken, 2022).

Figura 3 - Diagrama típico de um *cableship*



Fonte: Papapavlou *et al.* (2022)

Uma vez que o reparo é concluído, são realizados testes para garantir que o cabo está funcionando corretamente. Isso inclui testes de continuidade e de sinal para verificar a integridade do reparo. São operações sensíveis, bastante especializadas e onerosas.

Os países e empresas proprietárias dos cabos submarinos contratam navios de reparo por meio de acordos com empresas especializadas em manutenção de cabos. Esses contratos geralmente incluem cláusulas para reparos de emergência, garantindo resposta rápida em caso de falhas.

Assim como a indústria de óleo e gás, a estrutura de comunicações de cabos submarinos utiliza meios complexos e especializados, tanto na instalação dos cabos submarinos, como na sua manutenção e reparo. São instalações que também carecem de uma proteção específica a fim de manter sua integridade e efetividade no funcionamento, evitando perda de eficiência dos sistemas de comunicações.

2.2 - LEGISLAÇÃO INTERNACIONAL SOBRE CABOS SUBMARINOS

Como abordado anteriormente, o primeiro cabo de comunicações transatlântico foi instalado em 1858, e embora o projeto tivesse o apoio dos governos britânico e americano, sua instalação não foi uma iniciativa liderada pelo Estado. O empreendimento pertencia e foi financiado pela empresa privada Atlantic Telegraph Company. Esse histórico do primeiro cabeamento transnacional ter sido uma iniciativa e domínio privado e não do governo ficou como herança para a situação presente da estrutura de cabos submarinos de fibras ótica. Hoje as grandes *Big Techs* são as proprietárias da maioria dos cabos submarinos (Sunak, 2017).

Por conseguinte, esta falta de propriedade estatal significa que os cabos não têm uma proteção robusta estabelecida no direito internacional e nas esferas nacionais, dificultando a separação de responsabilidades de sua gestão. Os cabos são geralmente financiados por consórcios de empresas de telecomunicações ou, cada vez mais, por gigantes da tecnologia como a Google e o Facebook.

Embora essa modalidade seja um bom negócio para as economias dos Estados, que deixam de investir nessa infraestrutura, a propriedade privada de cabos submarinos se traduz em governos com um papel menos ativo nas infraestruturas de comunicações transnacionais comparado às atividades de outros setores estratégicos, como a energia e o transporte marítimo, onde os Estados têm tradicionalmente uma ascensão mais forte, com maior envolvimento (Sunak, 2017).

Uma razão para esta relativa negligência é que, ao contrário dos navios, os cabos que passam sob o mar não têm bandeira e, portanto, não são registrados e legalmente associados a qualquer nacionalidade específica. Esse cenário levanta complicações para o estatuto dos cabos ao abrigo do direito internacional, que a comunidade internacional vem tentando resolver com uma série de acordos multilaterais ao longo da história, como podemos observar a seguir (Submarine Telegraph Act,1885 *apud* Sunak, 2017):

- Convenção para a Proteção de cabos Telegráficos Submarinos de 1884 – assinados por cerca de 40 estados diferentes, o documento tornou “uma ofensa punível quebrar ou ferir um cabo submarino, intencionalmente ou por negligência culposa, de maneira que possa interromper ou obstruir a comunicação telegráfica”.

- Convenção de Genebra de 1958 para o Alto-mar – garantiu a legalidade do princípio de que os Estados não poderiam obstruir a construção de cabos submarinos em águas internacionais
- Convenção das Nações Unidas sobre o Direito do Mar de 1982 – um acordo histórico muitas vezes referido como a “constituição para os oceanos”, tal acordo (do qual fazem parte cerca de 167 estados) amplia significativamente as proteções dadas ao cabeamento submarino em águas internacionais.

Por mais vitais que essas proteções legais sejam, é importante entender, especialmente no contexto das vulnerabilidades dos cabos submarinos, que danos podem potencialmente ser causados sem caracterizar uma violação do direito internacional.

A Convenção das Nações Unidas sobre o Direito do Mar de 1982 não proíbe os estados de tratarem os cabos submarinos como alvos militares legítimos durante tempos de guerra. Na verdade, a Convenção de 1884 declara explicitamente que suas estipulações não “restringem de maneira alguma a liberdade de ação dos beligerantes” (Sunak, 2017).

- O Artigo 113 da CNUDM exige que os Estados promulguem leis que criminalizem o rompimento de cabos submarinos por embarcações que ostentem sua bandeira. Na realidade, porém, essa obrigação não foi implementada por muitos dos signatários da convenção, sendo que a penalidade mais comum internacionalmente é somente uma multa. Há um argumento forte de que o dano intencional é um crime que atrai jurisdição universal e que todos os estados devem ter jurisdição sobre o infrator, algo que o Artigo 113 não prevê.
- O Artigo 113 não concede às embarcações de guerra o direito de abordar um navio suspeito de tentar danificar intencionalmente cabos submarinos em águas internacionais, dificultando a atuação das forças navais sobre embarcações hostis.
- O CNUDM se aplica apenas à parte do cabo que está no fundo do mar e não no local de aterramento, onde o cabo chega à terra.

- Um contexto importante ao considerar essas limitações é que a implementação da CNUDM ocorreu cerca de seis anos antes da construção do TAT-8, o primeiro cabo transatlântico de fibra óptica do mundo. Foi esse cabo seminal que começou a inclinar o tráfego de comunicações de volta para os oceanos após duas décadas em que os satélites desempenharam o papel preponderante.

Depreende-se que as salvaguardas legais internacionais estão desatualizadas além de não terem sido objeto de ratificação por muitos países, o que é o caso da CNUDM. Há de se avaliar a adequabilidade das legislações ainda em vigor, e promulgadas antes das novas tecnologias emergentes de comunicação. Estariam os novos cabos de fibra óptica legalmente protegidos pelas normas expeditas para regular os cabos de comunicação dos anos 70? Não diminuindo a importância dos cabos telegráficos e de telefonia, mas esses não eram responsáveis pela quantidade de dados que hoje trafegam pelos atuais cabos de fibra óptica. Atualmente os cabos submarinos de fibra óptica sustentam as grandes redes de internet, suas nuvens de dados e transações financeiras em um mundo totalmente interligado e globalizado.

2.3 - GOVERNANÇA INTERNACIONAL DOS CABOS SUBMARINOS

O Comitê Internacional de Proteção de Cabos (ICPC) foi fundado em 1958 e seus membros são compostos por administrações governamentais e empresas comerciais que possuem ou operam telecomunicações submarinas ou cabos de energia, bem como outras empresas que têm interesse na indústria de cabos submarinos - incluindo a maioria dos principais proprietários de sistemas de cabo e operadores de navios de cabo do mundo. O objetivo principal do ICPC é ajudar os seus membros a melhorar a segurança dos cabos submarinos, proporcionando um fórum no qual informações técnicas, jurídicas e ambientais relevantes possam ser trocadas. O Comitê Internacional de Proteção de Cabos é a organização líder mundial na promoção da proteção e resiliência de cabos submarinos (ICPC, 2024).

O ICPC trabalha com seus membros, governos, organizações internacionais, indústrias marítimas e a comunidade científica para: mitigar os riscos de danos naturais e humanos aos cabos submarinos; desenvolver recomendações e melhores

práticas para a indústria e os governos ao longo do ciclo de vida do projeto dos cabos; promover pesquisas científicas que abordem a gestão dos cabos no ambiente marinho; e promover o Estado de Direito nos oceanos (ICPC, 2024).

O ICPC prevê uma rede global de cabos submarinos confiáveis e resilientes que coexistam com o ambiente marinho. As principais atividades do órgão são (ICPC, 2024):

- Promover a conscientização sobre os cabos submarinos como infraestruturas críticas para os governos e outros utilizadores do fundo do mar;
- Estabelecer recomendações acordadas internacionalmente para instalação, proteção e manutenção de cabos;
- Monitorar a evolução dos tratados internacionais e da legislação nacional e ajudar a garantir que os interesses dos cabos submarinos sejam totalmente protegidos; e ligação com órgãos da Organização das Nações Unidas (ONU).

Há uma divisão de pensamentos sobre a necessidade ou não de uma legislação internacional mais forte relacionada aos cabos submarinos. Uma vertente advoga que há uma base sólida para argumentar que o regime de governança dos cabos submarinos existente é insuficiente para enfrentar os desafios deste século. Sendo assim, seria necessário um novo instrumento global, especialmente dada a dependência de cabos submarinos para conectividade e a realidade de que os instrumentos existentes não refletem a natureza das tecnologias atuais. Por outro lado, muitos especialistas insistem que o direito internacional vigente é suficiente e que os Estados precisam aderir às obrigações e compromissos existentes antes mesmo de considerar um novo instrumento. E mesmo que os Estados concordassem sobre a necessidade de um novo tratado especificamente centrado na proteção dos cabos submarinos, provavelmente levaria décadas para negociar tal documento, seria difícil chegar a algum acordo sobre o seu âmbito, dado que os sistemas de cabos submarinos são apenas um, embora crítico, elemento do ecossistema mais amplo das tecnologias de informação e comunicação (Kavanagh, 2023).

Formas adicionais para o fortalecimento da proteção e o regime de gestão da resiliência dos sistemas de cabos submarinos estão avançando. Por exemplo, a opção de um maior envolvimento das organizações militares na proteção e

segurança dos cabos, por meio de estruturas de coordenação específicas, como detecção, vigilância e patrulhas marítima, bem como vigilância por satélite de áreas estrategicamente relevantes. Normalmente, aproveitando estruturas de segurança marítimas já em operação, incrementando a cooperação interestados e interagências, incentivando assim a mentalidade de proteção para as infraestruturas do poder marítimo (ICPM).

Talvez um ponto de partida para essa conversa global seja reconhecer a natureza sistêmica dos desafios em questão e aprofundar a compreensão dos esforços de mitigação de riscos que a indústria e as comunidades técnicas já estão realizando (por exemplo, maior diversificação das rotas e da capacidade dos cabos; adoção de princípios de cibersegurança como arquitetura de confiança zero, reforço da segurança da infraestrutura terrestre e dos seus componentes, avanços nas técnicas de sensoriamento óptico para monitoramento dos sistemas). Os Estados podem complementar esses esforços implementando e aderindo às recomendações existentes e aos requisitos emergentes relevantes para a infraestrutura crítica de TIC. Como as melhores práticas do ICPC para promover a resiliência dos cabos submarinos de telecomunicações, cuja essência deriva da CNUDM, nas recomendações sobre a segurança em torno das diversas estruturas que envolvem o sistema de cabos submarinos como por exemplo os pontos de aterragem. (KAVANAGH, 2023).

2.4 – AMEAÇAS

Há diferentes tipos de causas de danos à rede de cabos. Cerca de 100 rupturas de cabos acontecem todos os anos em todo o mundo. Os danos aos cabos podem ser causados por atos não intencionais (por exemplo, pesca, ancoragem ou desastres naturais) e danos intencionais (por exemplo, corte de cabos) (Bueger; Liebetrau; Franken, 2022). Essas causas serão apresentadas em mais detalhes a seguir.

2.4.1 - Causas Naturais

Considerando causas envolvendo fatores da natureza, a ruptura de um cabo pode ser o resultado de desastres naturais como maremotos e outras atividades

sísmicas, tsunamis e correntes subaquáticas durante tempestades. Outros fatores naturais são processos de longo prazo que podem levar à abrasão das camadas protetoras dos cabos, como corrosão, marés e correntes relacionadas ao clima. Os usuários finais dificilmente percebem essas falhas porque o tráfego de dados geralmente é redirecionado através de caminhos de cabos alternativos. As interrupções totais da Internet ocorrem apenas quando não há redundância de banda larga disponível.

Geralmente os impactos naturais são responsáveis por cerca de um quinto dos incidentes com cabos. Estes tipos de danos são menos prováveis do que as quebras acidentais causadas pelo homem. No entanto, eles apresentam o potencial de múltiplas falhas simultâneas. Por exemplo, no rescaldo do terramoto de Tÿhoku em 2011, quatro dos 20 cabos submarinos para o Japão se romperam. Estas interrupções simultâneas afetaram seriamente o tráfego interasiático e transpacífico da Internet. Para territórios com menos redundâncias, as interrupções paralelas apresentam maior probabilidade de apagão total da Internet (Bueger; Liebetrau; Franken, 2022).

2.4.2 - Causas Humanas

Os danos causados pelo homem aos cabos submarinos podem ser intencionais ou não intencionais, causados por negligência. Destes, principalmente os danos não intencionais aos cabos causados pela atividade marítima comercial representam, em média, mais de 70% dos incidentes anuais. A maioria dos acidentes ocorre como consequência das atividades marítimas quotidianas, sendo a pesca, o fundeio e a dragagem as causas mais frequentes dos danos (Bueger; Liebetrau; Franken, 2022).

Outros episódios de falhas humanas são imputados a fatores externos, relacionado com as infraestruturas externas e os serviços necessários dos quais dependem. Por exemplo, os cabos de dados de fibra óptica com mais de 150 km requerem energia elétrica para funcionar porque os repetidores precisam compensar as perdas de sinal ao longo da distância. Falhas nesse sistema podem ocorrer, porém é um cenário de interrupção menos provável.

2.4.2.1 - Atividade humana não intencional

Os danos mais comuns causados aos cabos submarinos são erros humanos e negligência. Cerca de 40% das interrupções nos cabos decorrem de equipamentos de pesca comercial e da atividade de dragagem. Outros 15% dos danos são causados por incidentes de ancoragem, tais como âncoras posicionadas inadequadamente, ancoragem fora de áreas aprovadas, condições do mar que afetam o posicionamento da âncora ou seu lançamento de emergência. Outros fatores humanos benignos incluem dragagem e despejo, atividades da explotação de petróleo e gás, desenvolvimento de energia eólica offshore, projetos hidro cinéticos, conversão de energia térmica oceânica e operações de mineração em alto-mar (Bueger; Liebetrau; Franken, 2022).

Possivelmente esses tipos de acidentes ocorrem por uma falta de sinalização adequada e atualizada em cartas náuticas da posição dos cabos submarinos, troca de informações deficiente entre instituições que atuam no setor marítimo, dentre outros fatores.

2.4.2.2 - Atividade humana intencional

Existe o potencial de sabotagem de cabos submarinos durante períodos de conflito, como parte de operações de zona cinzenta, de guerra híbrida ou através do terrorismo transnacional e do crime organizado, embora tais incidentes ainda não foram confirmados. A segurança e a resiliência dos cabos submarinos ainda são elementos pouco estudados da segurança internacional. Tendo em vista que o acesso e os dados à Internet estão definindo os recursos do século XXI, a proteção dos cabos submarinos é um domínio essencial da política internacional para análise de segurança. Diz respeito à forma como o nosso futuro digital será governado e como poderá ser assegurada uma circulação global de dados livres, abertos e seguros. Devido ao papel crucial dos cabos submarinos e às preocupações crescentes em torno da sua segurança, é fundamental que a União Europeia e os seus Estados-Membros garantam a proteção dos cabos submarinos. (Bueger; Liebetrau; Franken, 2022).

A forma mais comum de dano intencional à rede de cabos estava associada ao roubo dos materiais, mais especificamente na busca pelo cobre. Da mesma

forma, as redes terrestres enfrentam esses desafios, uma vez que os cabos são frequentemente roubados na expectativa criminosa de obter tal metal no mercado paralelo. Entretanto, os danos à rede submersa possuem consequências muito maiores pois o reparo é muito mais oneroso e demorado do que na estrutura terrestre (Kavanagh, 2023).

Historicamente aconteceram danos intencionais à estrutura submersa de cabos de comunicação, como será apresentado nesse estudo, entretanto à época, a tecnologia era de cabos telegráficos.

Essas ameaças estão bem representadas na história. Por exemplo, antes da negociação da Convenção para a Proteção dos Cabos Telegráficos Submarinos de 1884, a intervenção estatal em projetos de cabos aumentou significativamente em paralelo com o expansionismo territorial da época. A competição pelo acesso aos recursos críticos para o funcionamento dos cabos intensificou-se. A escuta de cabos e a sabotagem tornaram-se uma característica do conflito – primeiro no contexto de agitação civil e depois em conflitos internacionais, com as grandes potências a integrarem gradualmente a escuta de cabos e a sabotagem no planejamento da guerra (Kavanagh, 2023).

Ao eclodir a primeira Grande Guerra, os efeitos foram significativos, mesmo o mundo não dependendo tanto das tecnologias de informação daquele sistema de cabos telegráficos. Em agosto de 1914, o navio britânico Alert cortou os cabos alemães de Emden, nas proximidades do Canal da Mancha, para a França, Espanha, África e as Américas. Ao longo da guerra, os alemães também dedicaram esforços significativos e considerável engenhosidade ao corte de cabos. Inicialmente, concentraram-se em isolar a Rússia dos seus aliados ocidentais, cortando cabos no Mar Negro e no Báltico (Boyd, 2022).

Na segunda Grande Guerra, outras ações na Europa ocorreram, entretanto destaca-se as ações da Marinha Imperial Japonesa atacando cabos e estações retransmissoras britânicas, por vezes por meio de submarino, e a Marinha Real Britânica desenvolveu submarinos anões para ataque a cabos. Ao final da guerra, o submarino anão *XE-4* cortou o cabo telegráfico japonês que ligava Saigon a Singapura e Hong Kong (Boyd, 2022).

Hoje, há preocupações de que grupos terroristas possam perturbar infraestruturas críticas de cabos submarinos e, da mesma forma, eleva-se o potencial de ameaça representada por Estados à estrutura dos cabos submarinos de

comunicação. Diversos comportamentos mencionados anteriormente são passíveis de ocorrer novamente, refletindo as intensas tensões geopolíticas. Nas instalações terrestres, há relatos de operações cibernéticas direcionadas a instalações de cabos e seus *landing-points* ou pontos de aterragem (locais onde os cabos submarinos se conectam a estrutura terrestre). No mar, isso abrange incidentes reportados de atividades suspeitas nas águas territoriais ou na zona econômica exclusiva de diversos Estados (Kavanagh, 2023).

Há relatos de sabotagem intencional de cabos, possivelmente apoiada por Estados (ainda são poucos e não comprovados), bem como preocupações sobre os potenciais efeitos de tal atividade nas operações militares. Presume-se que quanto mais distante da costa ocorrer uma avaria, maior a probabilidade do envolvimento de uma grande potência, uma vez que são necessários capacidades e recursos tecnológicos significativos para localizar e alcançar os cabos em maiores profundidades. Este seria o caso das escutas de cabos em alto-mar, em que potências tecnológicas teriam a capacidade de monitorar os dados que passam pelos cabos e até mesmo *hackeá-los*, embora os desenvolvimentos nas técnicas de encriptação tornem mais difícil o acesso a esses dados, prevenindo tal atividade (Kavanagh, 2023).

Essas ameaças físicas e cibernéticas – que ocorrem num contexto de crescente concorrência tecnológica entre Estados – são, por sua vez, cada vez mais referenciadas ou inferidas em políticas e estratégias nacionais e regionais, e em acordos de cooperação bilaterais entre Estados. São crescentes as despesas de investigação e desenvolvimento de capacidades navais e tecnologias estratégicas para permitir monitorar e dissuadir atividades que possam afetar os sistemas de cabos submarinos, ou conferir uma vantagem sobre outros Estados nesta área. Tais ameaças estão levando a decisões governamentais para aumentar os investimentos em capacidades de reparo de cabos, em investigação e desenvolvimento de tecnologias e redes de cabos confiáveis para comunicações militares/de defesa (Kavanagh, 2023).

Além disso, muitos Estados estão atuando mais ativamente em projetos de cabos para influenciar as escolhas sobre sua tecnologia e autorizações de operadoras por razões de segurança nacional. Em alguns casos, os Estados bloqueiam projetos específicos se certas empresas, consideradas suspeitas de atividade de espionagem, estiverem envolvidas, ou se os cabos aterrarem ou se

ligarem a determinadas jurisdições. (Kavanagh, 2023). A exemplo da não concessão de permissão de alguns Estados na instalação de cabos submarinos por empresas chinesas (Wroe, 2017).

3 - VULNERABILIDADES E AMEAÇAS ÀS INFRAESTRUTURAS CRÍTICAS DO PODER MARÍTIMO NO REINO UNIDO, NORUEGA E UNIÃO EUROPEIA

O propósito desse capítulo é conhecer a infraestrutura de cabos submarinos de alguns países da Europa, principalmente o Reino Unido, Noruega e de forma mais genérica a UE, sem a pretensão de detalhar seus países-membros, entretanto buscando conhecer suas vulnerabilidades e as ameaças mais latentes que têm enfrentado nesse ambiente.

Após o início do conflito Rússia Ucrânia em 2022, a comunidade internacional, principalmente a Europa, passou a conviver com diversas vulnerabilidades em diferentes espectros, que até então não eram tão visíveis ou lembrados no cotidiano do continente. Após a eclosão do conflito, termos como: segurança alimentar, segurança energética passaram a estar presentes nos noticiários e influenciando diretamente a vida das pessoas.

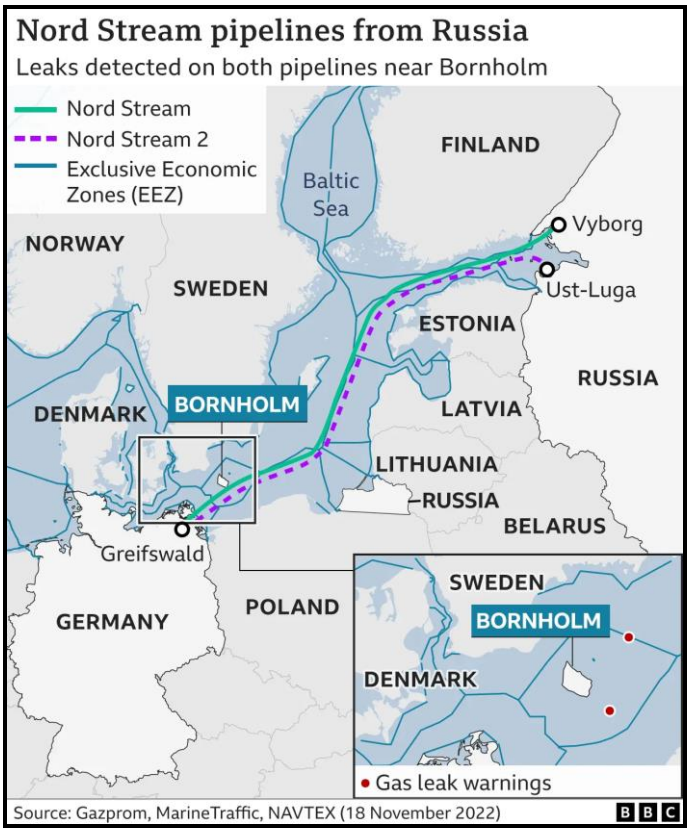
Da mesma forma que houve o crescimento nas preocupações com esses tópicos, pretende-se demonstrar nesse capítulo que é uma questão crescente em vários países europeus a preocupação em incrementar a proteção das infraestruturas críticas, que estão intimamente ligadas ao setor energético, no caso de gasodutos, oleodutos e fazendas eólicas, mas também na conectividade de comunicação e internet por meio dos cabos submarinos. Essas estruturas garantem o fluxo de comunicações eficiente e seguro no mundo e como vimos, podem ser alvo de ataques visando a interrupção dos seus serviços ou sofrerem ações de espionagem e ciberataques. Veremos que a gestão de cabos submarinos na Europa possui particularidades de acordo com o país responsável, há uma diferença de tratamento na gestão de vigilância e proteção desses ativos, responsáveis pela conexão mundial de dados.

Em um passado recente, ações adversas sobre infraestruturas consideradas como críticas mostraram ao mundo suas vulnerabilidades frente a ameaças de diferentes naturezas. A exemplo do ocorrido em setembro de 2022 com os gasodutos NordStream 1 e 2 entre a Rússia e a Alemanha, dentro do contexto temporal do conflito entre Rússia e Ucrânia. Esses gasodutos transportavam gás natural através do mar Báltico da Rússia para a Alemanha (figura 4), país fortemente dependente daquela matriz energética. Os gasodutos foram danificados após

explosões ocorrerem em suas proximidades, impedindo assim, a transferência de gás para a Alemanha. No período em questão, vários países europeus e EUA estavam empregando sanções econômicas contra a Rússia devido a invasão da Ucrânia (Gozzy,2024).

Em janeiro de 2024 a Dinamarca divulgou o encerramento de uma investigação sobre a explosão do referido oleoduto. No documento foi relatado que vazamentos foram descobertos em três das quatro linhas de gás ao leste da ilha dinamarquesa de Bornholm, no Mar Báltico, de acordo com a Figura 4. Pouco depois, autoridades suecas encontraram traços de explosivos no local, sugerindo sabotagem.

Figura 4 – Mapa do gasoduto NordStream



Fonte: Gozzy (2024).

Os gasodutos eram de propriedade da Empresa Russa Gazprom. O Nord Stream 1 operou de 2011 até 2022 e o Nord Stream 2 nunca havia sido utilizado devido à interrupção do projeto pela Alemanha após a invasão russa à Ucrânia. A polícia dinamarquesa conduziu uma investigação detalhada com sua agência de

inteligência, mas não divulgou mais detalhes sobre o caso. As autoridades concluíram que os gasodutos Nord Stream 1 e 2 foram sabotados em setembro de 2022, mas também disseram que não havia base para iniciar um processo criminal. A responsabilidade pela suspeita de sabotagem ainda é desconhecida (Gozzy, 2024).

Outra ocorrência em infraestrutura crítica ocorrido na Europa, anterior ao evento da NordStream, aconteceu na Noruega. Um cabo submarino que ligava uma estação terrestre satelital da ilha de Svalbard, no Oceano Ártico, ao continente norueguês, foi cortado em janeiro de 2022, há suspeitas do governo norueguês de ter sido resultado da ação humana (Humpert, 2022). A estação de Satélite Svalbard (SvalSat), pertencente a KSAT, *Kongsberg Satellite Services*, é a maior estação satelital privada do mundo, que oferece serviços para diversas empresas e governos. O SvalSat está localizado no topo de uma cordilheira montanhosa em Svalbard e consiste em mais de 100 antenas vitais para satélites em órbita polar (Figura 5).

Figura 5 – Arquipélago Norueguês de Svalbard e estação satelital Svalsat

Fonte: Averre (2022)

A falha no cabo, que liga a estação situada em Longyearbyen (cidade em Svalbard), até Andoeya, na costa norte da Noruega, foi detectada entre 80 e 140 milhas da ilha.

A estação representa uma das duas únicas estações terrestres das quais podem ser baixados dados desses tipos de satélites em cada uma das rotações da

terra, sendo, desta forma, um ativo valioso. A comunicação não foi interrompida pois o sistema de conexão prevê a ambiguidade de cabos, assim, um segundo cabo submarino absorveu o fluxo de comunicação de dados entre o arquipélago e o continente. Entretanto o evento contribuiu para aumentar o alerta sobre a vulnerabilidade dessas estruturas e suas ameaças (Humpert, 2022).

No ano anterior, ainda na Noruega, ocorreu um corte de cabos que fazem parte de uma rede de monitoramento submarino. Uma rede de sensores na costa do norte do país, operados pela empresa IMR, *Institute of Marine Research,* que é um dos maiores institutos de pesquisa marinha da Europa. Esse sistema consiste numa rede de cabos e sensores subaquáticos localizados na plataforma continental norueguesa, uma área de interesse estratégico tanto para a Noruega como para a Rússia. Esse sistema usa sensores para monitorar os efeitos das mudanças climáticas, das emissões de metano e dos estoques pesqueiros, fornecendo aos cientistas uma transmissão ao vivo de imagens, sons e outros dados. Entretanto, são capazes também de coletar dados sobre a passagem de submarinos nas proximidades. Estranhamente e de forma desconhecida, o sistema foi interrompido e parte dos cabos foram subtraídos, ao total foram 4,3 km de cabos submarinos que desapareceram sem vestígios. O fato levantou suspeitas sobre sabotagem deliberada, e possivelmente, realizadas pelo governo russo, que supostamente poderia estar incomodado com a capacidade do país vizinho em realizar esse tipo de monitoramento e coleta de dados. A desconfiança foi canalizada para a Rússia pois teoricamente seria o país com os meios e tecnologia para execução desse tipo de ação. Entretanto nenhuma responsabilidade foi apontada de forma comprovada e contundente (Newdick, 2021).

Em ambos os casos, as autoridades explicaram que as rupturas foram provavelmente causadas pela atividade humana e que nenhum fenômeno natural poderia ter causado tais danos.

Os episódios que envolveram os cabos submarinos da Noruega elevaram a consciência situacional do país para a segurança de suas infraestruturas críticas submersas, tanto que, por ocasião do ocorrido nos gasodutos NordStream, houve então uma resposta a esta ameaça emergente pelo governo norueguês, que anunciou um maior reforço das medidas de segurança, incluindo o destacamento

das suas forças armadas, para além das já implementadas pelas empresas petrolíferas e operadores de oleodutos. Adicionalmente o presidente da Noruega solicitou apoio dos países aliados da Organização do Tratado do Atlântico Norte (OTAN) na patrulha e vigilância dessas infraestruturas submarinas. A resposta norueguesa foi motivo de pronunciamento e apoio *do First Sea Lord* inglês:

> "Há uma vulnerabilidade em torno de tudo o que se encontra no fundo do mar, sejam gasodutos, sejam cabos de dados, que impõe a organizações como a Royal Navy – mas não somente ela – da obrigação de ter meios de monitorar e fornecer segurança no entorno dessas infraestruturas" (Borger, 2022)

Mais recentemente, em fevereiro de 2023, responsáveis pela inteligência militar nos Países Baixos emitiram um aviso indicando que a Rússia tinha iniciado atividades de espionagem e parecia estar preparando operações para perturbação e sabotagem de cabos submarinos no Mar do Norte, além de parques eólicos e gasodutos (Hancock e Sheppard, 2023 *apud* NATO, 2023). Estes incidentes e outros ilustram que a infraestrutura dos aliados permanece vulnerável a ataques e que atribuir ações maliciosas no fundo do mar e sob ele continua extremamente difícil (Machi, 2023 *apud* NATO, 2023).

Em outubro de 2023 o governo da Finlândia reportou danos em um gasoduto submarino e em um cabo de telecomunicações que liga o país à Estônia. Segundo o relatório os danos foram intencionais, entretanto não há definição do responsável pela avaria. Autoridades estônios e finlandeses realizaram investigações conjuntas para verificarem os navios que estavam na área no início daquele mês, período provável do ocorrido das avarias. Preliminarmente foi relatado um histórico de navio com bandeira russa e outro de propriedade chinesa na área, entretanto o estudo não foi conclusivo. Posteriormente, autoridades finlandesas encontraram uma âncora nas proximidades do gasoduto, acreditando que o arrastamento desta poderia ter sido a causa dos danos. Eles sugeriram que um porta-contêineres de propriedade chinesa e bandeira de Hong Kong seria o principal suspeito (Chiappa; Ngendakumana, 2023).

As avarias foram descobertas quando operadores finlandeses e estônios notaram uma queda invulgar na pressão no gasoduto Balticconnector no dia 8 de Outubro de 2023 e subsequentemente interromperam o fluxo de gás . Dois dias depois, o governo finlandês afirmou que houve danos tanto no gasoduto como no

cabo de telecomunicações entre os dois países. As avarias no cabo foram parciais (Chiappa; Ngendakumana, 2023).

Mais um fato indicando a necessidade de monitoramento mais efetivo das águas de jurisdição dos países que possuem infraestruturas a serem protegidas e de uma estrutura para investigação e vigilância dos ativos submersos.

Assim sendo, torna-se importante saber como dissuadir as ameaças, reduzir as vulnerabilidades e minimizar as consequências que poderão ocorrer em função de ações adversas sobre uma ICPM.

Em abril de 2023, o navio russo Almirante Vladimirsky foi acusado de navegar nas proximidades da costa do Reino Unido a fim de mapear as infraestruturas submarinas no Mar do Norte. Embora seja oficialmente classificado como um navio de pesquisa oceânica, supostamente faz parte de uma frota que examina as infraestruturas dos países do mar do norte mapeando suas vulnerabilidades. Há suspeitas de ter navegado em águas escocesas a fim de investigar alguns dos parques eólicos *offshore*, como o parque eólico *Seagreen*, nos arredores de Aberdeen (Osborne, 2023).

O sítio da Royal Navy relata diversas matérias sobre a necessidade de interceptação pela Marinha Real e eventualmente com apoio da Royal Air Force (RAF) no acompanhamento de meios de superfície ou submarinos russos, sejam navios de guerra ou navios de pesquisa, nas proximidades de suas águas jurisdicionais. A aproximação desses navios é uma preocupação constante da Marinha Real. Medidas de incremento de patrulha e dissuasão estão sendo implementadas pelo Reino Unido e a busca de cooperação com países vizinhos, com o objetivo de maximizar esforços contra as ameaças às infraestruturas críticas na região (Royal Navy, 2023).

Em maio de 2023 o Reino Unido e Noruega assinaram um tratado de cooperação em uma parceria estratégica para combater ameaças partilhadas no domínio submarino, incluindo ameaças à infraestrutura submarina. E foram incrementados os exercícios entre os participantes da OTAN e Joint Expedictionary Force (JEF) a fim se oporem a estas visitas cada vez mais indesejadas na área do Alto Norte (Reino Unido, 2023).

Após conhecer alguns eventos ocorridos em sistemas de cabos submarinos, estudou-se porque alguns países são considerados mais ameaças às ICPM do que outros. Considerando relatórios de países europeus publicados recentemente:

A Rússia é frequentemente mencionada como uma ameaça significativa devido às suas capacidades militares submarinas avançadas e ao histórico de envolvimento em atividades cibernéticas que poderiam visar infraestruturas críticas; e

A China, devido à proximidade de cabos submarinos em regiões sensíveis como o Estreito de Luzon, perto de Taiwan, Japão, e outras áreas, coloca o país como potencial ameaça, especialmente em cenários de tensão geopolítica na região.

Entretanto, na literatura consultada, a Rússia é a principal ameaça considerada pelos países estudados devido a sua estrutura tecnológica além de inclinação para guerra híbrida. Essa pesquisa procurou verificar quais são essas capacidades. Verificou-se em relatório da OTAN publicado em dezembro de 2023*, NATO's Role in Protecting Critical Undersea Infrastructure*, que a própria OTAN não se considera preparada para mitigar a agressão russa cada vez mais prevalente contra as infraestruturas submarinas críticas (CUI – *Critical underwater infrstructure*) europeias. Apesar das suas forças terrestres esgotadas e da sua base industrial militar tensa, as táticas híbridas russas continuam a ser a ameaça mais premente à CUI no norte da Europa. Apesar das suas atuais limitações, a OTAN é o principal ator capaz de dissuadir e prevenir ataques híbridos aos seus aliados e acelerou a sua abordagem à proteção da CUI, estabelecendo novas organizações para esse objetivo (NATO, 2023).

Segundo o mesmo relatório da OTAN, a Rússia utiliza táticas híbridas para ameaçar ou danificar infraestruturas submersas a fim de desestabilizar e intimidar países europeus e a OTAN, operando abaixo do limiar de guerra aberta, o que dificulta a atribuição e a resposta efetiva. A frota submarina russa, baseada na Península de Kola, inclui submarinos nucleares e convencionais capazes de operar em profundidades críticas, permitindo monitorar e interferir em cabos submarinos (NATO, 2023).

A Rússia possui em sua estrutura subordinada diretamente ao Ministério da Defesa a Diretoria Principal de Pesquisa em Águas Profundas (GUGI) que é uma unidade especializada que opera submarinos e veículos subaquáticos projetados para missões críticas no fundo do mar, como o BS-64 Podmoskovye e o AS-31 Losharik, capazes de realizar operações clandestinas de corte de cabos. As bases navais em Kaliningrado e a capacidade de operar em várias frentes permitem à

Rússia projetar poder e ameaçar infraestruturas críticas de maneira estratégica. A doutrina militar russa inclui o uso de ataques a infraestruturas críticas para impor custos econômicos e dissuadir intervenções externas em conflitos regionais. Esses fatores combinados fazem da Rússia uma ameaça significativa, exigindo uma resposta coordenada da OTAN e de seus aliados para proteger esses ativos vitais (Kaushal, 2023).

Além de submarinos, a GUGI opera também diversos navios considerados espiões. Uma das classes são os navios da classe Yantar, que são navios de pesquisa e inteligência. Esta classe inclui os navios Yantar, Almaz e o futuro navio Veliky Novgorod. Esses navios são equipados com submarinos de resgate e pesquisa autônomos, que podem operar a profundidades significativas e são capazes de realizar uma variedade de tarefas submarinas, incluindo a manipulação de objetos no fundo do mar, a realização de pesquisas oceanográficas e a intercepção de comunicações submarinas (Hendriks e Halem, 2024).

Esses navios são projetados para apoiar a operação de minissubmarinos que podem realizar missões complexas no fundo do mar, como a exploração de cabos submarinos. As capacidades desses navios incluem a realização de operações de busca e salvamento submarino, bem como a instalação e a manutenção de infraestruturas submarinas. Eles também possuem avançados equipamentos de comunicação e inteligência, permitindo a intercepção e monitoramento de sinais subaquáticos (Hendriks e Halem, 2024).

Em termos de capacidades técnicas, os navios da classe Yantar possuem equipamentos de sonar e sistemas de navegação que lhes permitem operar em condições de mar desfavoráveis. A combinação de suas capacidades técnicas e a integração com submarinos autônomos tornam esses navios altamente versáteis para uma ampla gama de operações submarinas, incluindo potencialmente a interferência em cabos submarinos críticos (Policy Exchange, 2024).

Essas capacidades tornam os submarinos da GUGI e os navios da classe Yantar preocupações significativas para as infraestruturas críticas submersas, especialmente no contexto de tensões geopolíticas e de segurança internacional.

É claro que a literatura consultada lista países de viés autoritários como, Rússia e China, como potenciais ameaças às ICPM. Esses países além da questão geopolítica, são aqueles que possuem tecnologia avançada e orçamento para

desenvolvimento de novos meios com esse propósito. Contudo há de considerar que diversos países desenvolvidos e empresas de tecnologia submarina também possuem essa capacidade.

4 - ESTRATÉGIAS DE ENFRENTAMENTO DAS AMEAÇAS ÀS ICPM NO REINO UNIDO, NORUEGA E EU

Como descrito no capítulo anterior, a segurança dos cabos submarinos representa uma grande vulnerabilidade para as comunicações mundiais. A ocorrência de diversos eventos em que essas estruturas foram danificadas, além de outras estruturas críticas submersas, alertou diversos países a tomarem medidas para incrementar a segurança desses ativos com o objetivo de prevenir ou mitigar tais vulnerabilidades. O objetivo deste capítulo é descrever como os países internalizam a problemática da proteção das ICPM e as ações implementadas e respectivos planejamentos dos países estudados, Reino Unido, Noruega e União Europeia, para a proteção das suas redes de cabos submarinos.

4.1 - REINO UNIDO

O estudo observou que o Reino Unido é um dos países com maiores preocupações no monitoramento e proteção de suas infraestruturas críticas, tendo em vista sua condição insular, possuidor de interesses globais, com territórios ultramarinos e 99% das comunicações internacionais do Reino Unido realizadas por meio de cabos submarinos de fibra óptica. Tais características justificam a forte inclinação do país em incrementar suas capacidades na proteção dessas infraestruturas e promover ações internas e com seus aliados e parceiros para garantir os interesses do país (Reino Unido, 2022).

A promulgação em 2021 da grande estratégia do Reino Unido, a *Integrated Review*, a Revisão Integrada da Segurança, Defesa, Desenvolvimento e Política Externa do país, apresenta os objetivos estratégicos no pós-Brexit. Já na introdução do documento é colocado:

> “O cerne da Revisão Integrada é um maior compromisso com a segurança e a resiliência, para que o povo britânico esteja protegido contra ameaças. Isto começa em casa, defendendo o nosso povo, o nosso território, as **infraestruturas nacionais críticas,** as instituições democráticas e o modo de vida – e reduzindo a nossa vulnerabilidade à ameaça dos Estados, do terrorismo e do crime grave e organizado (SOC).” (Reino Unido, 2021, p.11, grifo nosso).

A citação das infraestruturas nacionais críticas demonstra o reconhecimento da importância desses sistemas para o bem-estar do país e sua vulnerabilidade. O *Integrated Review* foi revisado em 2023. O foco da revisão foi uma mudança estratégica em ampliar a segurança euro-atlântica a despeito do documento de 2021 ter focado na ampliação de domínios e influência na região do indo-pacífico. A revisão, ocorre após a deflagração do conflito na Ucrânia, reforçando a necessidade de proteção do entorno estratégico do Reino Unido.

Em 2022, seguindo as diretrizes da *Integrated Review* 2021, foi publicada a estratégia marítima de defesa do Reino Unido. A publicação é crucial devido à sua abordagem abrangente na proteção das infraestruturas críticas e dos cabos submarinos, que são essenciais para a segurança nacional e a economia global. A estratégia destaca que, como uma nação insular com interesses globais significativos, o Reino Unido depende fortemente de suas rotas de navegação e infraestrutura subaquática. A proteção dessas infraestruturas garante o fluxo livre de mercadorias e informações, sustentando a economia do país. Há um capítulo exclusivo para a proteção das infraestruturas críticas abaixo d´água, com várias citações para a importância dos cabos submarinos para o mundo e em particular para o Reino Unido e seus domínios ultramarinos.

> “Os cabos submarinos são essenciais para o nosso modo de vida moderno, fornecendo comunicações que suportam a Internet e a conectividade energética que distribui eletricidade entre os mercados. Ambas as funções essenciais apoiam as nossas indústrias modernas e a conectividade global e contribuem para o Net Zero. £545 bilhões de Valor Agregado Bruto (VAB) por ano estão associados às exportações do Reino Unido que dependem de cabos submarinos.” (Reino Unido, 2022, p.66).

O documento aponta uma característica dos cabos submarinos semelhante de outros países, que é a propriedade e operação privada deles. Apontado em diversos estudos como um desafio para a gestão de monitoramento, reparo e proteção. Entretanto, o governo considera os cabos ligados ao Reino Unido como parte da conectividade e infraestrutura internacional crítica do país. A importância dos cabos para o padrão de vida do Reino Unido também exige consciência de segurança contra danos acidentais e potenciais perturbações por parte de atores mal-intencionados. Uma perda significativa de cabos submarinos poderá ser sentida por

todos no Reino Unido. O impacto afetaria diretamente as comunicações e os serviços baseados na Internet, bem como o tráfego financeiro.

Para garantir que o país esteja bem-posicionado para ser um HUB seguro para cabos de dados submarinos e reter conhecimentos especializados para apoiar a economia digital moderna, o governo avalia gestões para o apoio na segurança, resiliência e integridade desse sistema crítico. Dessa forma, algumas ações foram tomadas pelo governo britânico para incrementar a segurança e resiliências das infraestruturas críticas, dentre elas a proteção dos seus cabos submarinos, a citar:

- Reforço nas capacidades de segurança marítima do Reino Unido ao estabelecer o Centro Conjunto de Segurança Marítima (JMSC) em 2019.

O Centro Conjunto de Segurança Marítima é uma organização interagências responsável por garantir que o Reino Unido mantém a sua compreensão do domínio marítimo ao redor do país e desenvolve quadros de coordenação intergovernamental para responder às ameaças à segurança, à lei e à ordem e ao ambiente marinho (Reino Unido, 2022).

O JMSC incorpora o Centro Nacional de Informações Marítimas (NMIC), que desde 2010 fornece um mecanismo para as organizações civis e militares marítimas e de aplicação da lei e compartilhamento de inteligência, dados e capacidades. Isso maximiza o impacto operacional no país e no exterior (Reino Unido, 2022).

O Centro de Operações do JMSC utiliza tecnologia para fornecer monitoramento 24 horas por dia, 7 dias por semana nas águas do Reino Unido. O centro utiliza equipes proveniente de todo o governo em caráter interagências, pode identificar rapidamente incidentes de segurança marítima e permitir a coordenação eficaz de meios aéreos e marítimos do Reino Unido para pronta resposta (Reino Unido, 2022).

O JMSC oferece aos departamentos e agências governamentais um ponto central para consciência situacional marítima do Reino Unido para auxiliar na política e na tomada de decisões. O JMSC coopera internacionalmente com estados e com organizações internacionais, na partilha de informações, incrementando o relacionamento interestatais e nos esforços de capacitação.

A coordenação principal do Centro Conjunto de Segurança Marítima é liderada pelo *Border Control* (Força de Fronteira, equivalente a Polícia Federal), da Marinha Real e do Ministério da Defesa.

Além disso, o JMSC é apoiado pela Polícia Antiterrorista, pelo Departamento de Transportes, pelo *Foreign Commonwealth and Development Office*, pelo *Home Office*, pela *HM Coastguard*, *pela HM Revenue and Customs* e pela *National Crime Agency*, pela *Marine Management Organization* e pela *Marine Scotland* (agência de segurança marítima da Escócia) (Reino Unido, 2022).

Ou seja, o caráter interagências permite uma consciência situacional marítima de diversos órgãos e entidades que contribuem mais facilmente para uma tomada de decisão e uma melhor reação a situações que necessitem de pronta resposta. Ao analisar a proteção de infraestruturas críticas marítimas, em particular os cabos submarinos que possuem controle privado e responsabilidades compartilhadas em diferentes níveis e agências, tal modelo de trabalho interagências no JMSC contribui para um efetivo controle e assessoria na tomada de decisões.

- Instalação do novo centro de monitoramento da OTAN, *NATO's Maritime Centre for the Security of Critical Undersea Infrastructure* nas instalações da *NATO's Maritime Command* (MARCOM) em Northwood, em 2024.

A proteção das infraestruturas críticas marítimas é um assunto que a OTAN vem perseguindo e efetuando gestões nos países membro para criar maior resiliência e permitir maior proteção. Em 2024 foi inaugurado um novo centro de monitoramento em Northwood- Reino Unido, local onde já existia o Comando Marítimo Aliado da OTAN (MARCOM) (Monaghan, Svendsen, Darrah, 2023).

O novo centro operacional, operando juntamente com um centro estratégico baseado na sede da OTAN em Bruxelas, para coordenar esforços entre aliados da OTAN, parceiros e o setor privado para proteger a infraestrutura submarina (Monaghan, Svendsen, Darrah, 2023).

A OTAN vem trabalhando para aumentar a segurança da infraestrutura crítica há anos. A infraestrutura subaquática crítica sempre foi um foco para a segurança marítima e a consciência situacional marítima, de acordo com a aliança, e agora está seguindo com um programa de contribuição ativa para a proteção das infraestruturas críticas submarinas.

Os esforços incluem sensores submersos para monitorar a infraestrutura e sinalizar rastros de responsabilidade para impedir que prováveis agentes envolvidos em ataques a cabos submarinos possam negar suas ações e, em última análise,

serem responsabilizados. As nações contribuintes são: Dinamarca, Alemanha, Noruega, Polônia, Turquia, Reino Unido e EUA. Há a previsão na contribuição também da Grécia, Portugal e Suécia (Monaghan, Svendsen, Darrah, 2023).

- Aquisição de meio específico para monitoramento e proteção de infraestruturas submersas, *Multi-Role Ocean Surveillance Ship* (MROSS).

O programa MROSS do Ministério da Defesa do Reino Unido (MoD) e da Marinha Real britânica, desempenhará um papel de relevância e versátil na proteção da integridade das zonas marítimas e da infraestrutura submarina crítica do Reino Unido. Sistemas pilotados remotamente instalados no navio irão proporcionar flexibilidade ao meio, fundamental na gestão dos desafios submarinos modernos, que continua a ser coordenada a nível intergovernamental (Royal Navy, 2024).

O *Royal Fleet Auxiliary* (RFA) Proteus (Figura 6) se dedicará à salvaguarda de infraestruturas críticas do fundo marinho e atuará como um “navio-mãe”, operando sistemas externos remotos e autônomos para vigilância subaquática e guerra no fundo marinho. O navio de 6.000 toneladas foi construído em 2019 e adquirido pelo Ministério da Defesa por £ 70 milhões da Topaz Marine, uma subsidiária da P&O Maritime (Royal Navy, 2024).

A aquisição do navio foi anunciada em janeiro de 2023, quando iniciou processo de modificações e adaptações para instalação de novos equipamentos de monitoramento abaixo d´água (Royal Navy, 2024).

Essa aquisição é um exemplo de como a Royal Navy trabalhou no dimensionamento da força influenciado por uma lacuna de sua capacidade estratégica. A necessidade de possuir uma capacidade de monitorar e vigiar as infraestruturas críticas submarinas de forma mais efetiva tornou-se mais latente nos últimos anos, após fatos abordados neste trabalho como os acidentes ocorridos nos cabos submarinos na Europa. O acidente nos gasodutos Nordstream e a constante visita de navios russos nas águas britânicas e de países aliados são exemplo. Tal cenário corroborou para a decisão da incorporação de meios navais com a capacidade de monitoramento e proteção das infraestruturas críticas submersas. Adicionalmente ao programa MROSS, foi incorporado no mesmo período outro navio padrão *off-shore* para, da mesma forma, ser convertido e atuar pela RFA como navio-mãe nas ações de contramedidas de minagem, utilizando sistemas não

tripulados. Essas duas recentes aquisições do Reino Unido indicam a preocupação do país em preencher lacunas de capacitação no ambiente submarino na proteção de infraestruturas críticas marítimas (Royal Navy, 2024).

Figura 6 – Royal Fleet Auxiliary Proteus

Fonte: Navylookout, (2023).

- Ampliação de cooperação com países vizinhos com o propósito específico de monitorar e proteger infraestruturas críticas;

No fim de 2023, o Ministério da Defesa do Reino Unido (MoD) anunciou a mobilização de uma Força Tarefa para patrulhar áreas com infraestruturas críticas submarinas vulneráveis, em cooperação com outras nações. Tal cooperação foi acordada no fórum de defesa das nações componentes da Força Expedicionária Conjunta do inglês *Joint Expeditionary Force* (JEF), que concordaram em ativar uma Força Tarefa liderada pela Marinha Real Britânica para reforçar a segurança da infraestrutura submarina e dissuadir ameaças híbridas. Desde a destruição do gasoduto NordStream em setembro de 2022 e o ataque ao gasoduto Baltic Connector em outubro de 2023, tem havido uma preocupação crescente com a atividade subaquática russa no alto norte e báltico. (NAVYLOOKOUT, 2023).

A JEF é uma parceria militar multinacional do norte da Europa liderada pelo Reino Unido, projetada para resposta rápida e operações expedicionárias. Além do Reino Unido, que iniciou o estabelecimento da força em 2012, ela consiste nos

países nórdicos (Dinamarca, Finlândia, Islândia, Noruega, Suécia), os Estados bálticos (Estônia, Letônia, Lituânia) e os Países Baixos. A JEF pode atuar de forma independente, entretanto pode ser implantada em apoio à OTAN ou outras missões de cooperação. Não possui forças permanentes, como aquela organização, porém existe um diálogo constante entre os membros e são realizados exercícios militares regulares utilizando os padrões e a doutrina da OTAN como referência (NAVYLOOKOUT, 2023).

A Rússia é inevitavelmente a principal ameaça às nações do JEF e impedir a interferência em infraestruturas críticas é o tipo de cenário para o qual foi concebida. Os membros concordaram em junho de 2023 em partilhar ativamente dados de inteligência operacional, vigilância e reconhecimento, bem como reunir e partilhar capacidades neste domínio (NAVYLOOKOUT, 2023).

A tarefa principal da Força Tarefa será cobrir uma grande área, incluindo o Atlântico Norte, o Mar do Norte e o Báltico. O monitoramento das atividades no mar é um trabalho de rotina e a vigilância dos navios russos tem sido uma tarefa contínua das marinhas europeias desde o final da Segunda Guerra Mundial. Até certo ponto, este é um exercício político e de sinalização, concebido para demonstrar a unidade das nações do JEF e ações concretas em resposta aos ataques aos oleodutos. As nações do JEF reconheceram o carácter cada vez mais híbrido dos conflitos e a necessidade de adaptação para serem capazes de responder eficazmente às ameaças que operam no espaço abaixo do limiar do conflito convencional (NAVYLOOKOUT, 2023).

Entretanto a grande questão sobre esses exercícios do JEF é saber como funcionará a missão caso algum navio de guerra encontrar um navio (russo ou não) em águas internacionais, parado e agindo de forma suspeita sobre cabos ou oleodutos conhecidos, que medidas pode tomar? Pode ser muito difícil discernir ou provar que está em curso uma atividade ilegal contra infraestruturas submersas.

A interferência a ativos submarinos pode potencialmente ser realizada a partir de embarcações pequenas com equipes de mergulhadores em partes mais rasas do Báltico. Os russos têm uma vasta gama de opções, desde navios de superfície dedicados da classe do *Russian Research Vessel Yantar* que utilizam submersíveis, até submarinos nucleares especializados , como o Belgorod, equipados com minissubmarinos para operações totalmente secretas.

Mesmo que os navios da força-tarefa um veículo subaquático não tripulado que possam ser implantados para inspecionar o fundo do mar nas imediações, pode não ser simples descobrir se o navio de interesse está tomando alguma ação contra as instalações, seja algum tipo de ataque cibernético ou se preparando para danificá-las. Supondo que possam ser obtidas provas concretas de interferência, então isso irá se tornar um assunto para autoridades superiores, uma vez que é pouco provável que as regras de engajamento permitam tentativas de embarque ou o uso da força em um navio em águas internacionais. Torna-se, a princípio, uma questão de recolhimento de informações e provas para que pelo menos a atividade não seja negada pelo antagonista.

No mesmo contexto de cooperação, seis países que fazem fronteira com o Mar do Norte assinaram um acordo em 2024 para proteção da infraestrutura subaquática crítica contra sabotagens e ataques estrangeiros. O acordo envolvendo Bélgica, Holanda, Alemanha, Noruega, Reino Unido e Dinamarca, visa fortalecer a cooperação para proteger a infraestrutura de energia e aumentar a segurança na região. Tais países consideram que o Mar do Norte é detentor de força motriz que impulsiona as ambições de fontes renováveis da Europa, ajudando a reforçar a segurança energética no continente (Kar-Gupta, 2024).

Como parte do novo acordo de segurança do Mar do Norte, que é complementar ao trabalho da OTAN, os países do norte da Europa revisarão as medidas atuais de proteção e segurança, compartilharão informações e conhecimentos e relatarão informações relevantes em nível operacional. O acordo se concentra principalmente em resiliência e prevenção (Kar-Gupta, 2024).

A resposta às ameaças híbridas que tem como alvo as infraestruturas críticas europeias é a formação de zonas de cooperação entre países. Seja na troca de informações de inteligência operacional, no monitoramento de áreas comuns de interesse e na execução de patrulha naval e marítima envolvendo meios de suas Forças Armadas. Nesse exemplo de cooperação entre os países componentes do JEF e a execução das patrulhas conjuntas, percebe-se um dos grandes desafios para salvaguarda das infraestruturas críticas. O ambiente submarino onde ocorrem as interações dificulta a determinação de uma ação ilegal. Adicionalmente, a legislação do alto-mar, não permite uma ação mais contundente contra um meio suspeito em ter deliberado alguma ação contra alguma ICPM, mesmo que seja efetivamente flagrado em tal atividade a ação no alto-mar deverá ser muito bem

planejada pela nação que estiver em patrulha, tendo em vista os dispositivos legais atuais. Embora a guerra híbrida procure explorar os limites e lacunas legais, os países devem garantir que as suas respostas contra ameaças híbridas permaneçam dentro dos limites do estado de direito e da transparência.

Dois anos depois e coincidentemente após o conflito Russia x Ucrânia, o governo britânico publicou a revisão de sua Estratégia de Defesa Nacional (Reino Unido 2023). Na primeira versão percebe-se que o Reino Unido expandiu objetivos estratégicos para a região do Indo-Pacífico, trabalhando uma parceria com os EUA em uma estratégia de contenção da China (Reino Unido, 2021). Na revisão de 2023, percebe-se que a segurança Euro-Atlântica foi colocada como prioridade. Entretanto, para isso, outros mecanismos estratégicos foram tomados pelo Reino Unido e aliados, principalmente com os EUA, para o monitoramento da contenção da China. Cito o acordo AUKUS[1] de apoio à Austrália para operar submarinos nucleares em um futuro próximo. Adiciona-se a esse evento, outros em que o Reino Unido e EUA conseguem ampliar suas influências na região, como Five Eyes[2] e o Quad[3].

Todas as ações anteriores descritas permitem ao Reino Unido manter influência na Região do indo-pacífico por meio de seus aliados e parceiros estratégicos e deste modo, atuar mais ativamente no seu entorno estratégico euro-atlântico e alto norte em cooperação regional.

O conflito Russia x Ucrânia reascendeu as vulnerabilidades no continente Europeu, expondo as fragilidades na segurança energética, segurança alimentar e ameaças às infraestruturas críticas dos países europeus. Assim, percebe-se a nítida retomada de preocupação do Reino Unido no entorno estratégico euro-atlântico.

---

[1] AUKUS – Parceria de segurança anunciada em setembro de 2021 entre Austrália, o Reino Unido e os Estados Unidos que apoiará a Austrália na aquisição de submarinos de armas convencionais movidos a energia nuclear (SSNs). https://www.pm.gov.au/media/joint-leaders-statement-aukus.

[2] Five Eyes Intelligence Oversight and Review Council - é um acordo entre Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos que visava a cooperação entre as inteligências dessas nações.https://www.dni.gov/index.php/who-we-are/organizations/enterprise-capacity/chco/chco-related-menus/chco-related-links/recruitment-and-outreach/217-about/organization/icig-pages/2660-icig-fiorc

[3] Quad - Diálogo de Segurança Quadrilateral (em inglês: *Quadrilateral Security Dialogue*), é um fórum estratégico informal entre Estados Unidos da América, Japão, Austrália e Índia que é mantido por meio de cúpulas semirregulares, trocas de informações e exercícios militares entre os países membros. https://www.dfat.gov.au/international-relations/regional-architecture/quad

A revisão da estratégia Marítima em 2022 e do *Integrated Review* de 2023 destacam a importância de proteger as infraestruturas críticas nacionais, reconhecendo seu papel essencial no funcionamento do Estado e da economia. Ele aborda ameaças à ICPM (usando aqui o termo em português em nossa doutrina para citar as CNI) – *Critical National infrastructure*, como ciberataques, ataques físicos e outras formas de interrupção, e delineia estratégias para aumentar a resiliência e a segurança nessas áreas. Isso inclui medidas para melhorar a cibersegurança, aumentar a coordenação entre o governo e o setor privado e investir em tecnologias e capacidades para salvaguardar a ICPM (Reino Unido, 2022).

Do mesmo modo o incremento nas cooperações internacionais denota a preocupação do Reino Unido e de seus aliados na Europa, principalmente os vizinhos Euro-Atlânticos, na patrulha e contenção de ameaças às infraestruturas críticas submarinas. Entretanto, no exercício de patrulhas em águas internacionais expõe a dificuldade de ações contra possíveis meios sabotadores ou espiões, devido à dificuldade de comprovação da atividade ilegal e da legislação internacional para navios em águas internacionais. Contudo a presença de meios capazes de efetuar tal dissuasão ainda é, sem dúvida, o meio mais efetivo de proteger as ICPM.

4.2 – NORUEGA

A Noruega foi um dos países que em passado recente sofreu efetivamente com danos à sua infraestrutura de cabos submarinos, conforme apresentado previamente neste trabalho (cabo que liga o continente a Svalbard e o cabo de monitoramento ambiental). Possui fronteira terrestre e marítima com a Rússia, país que é tido como potencial responsável pelos danos ocorridos, tanto aos cabos submarinos mencionados como à infraestrutura do gasoduto NordStream, porém nada comprovado até o momento.

Diversas ações tomadas pelo país já foram listadas, considerando o país ser um aliado histórico do Reino Unido e membro da OTAN e JEF. No âmbito dessas parcerias, o país está envolvido ativamente nas medidas de monitoramento, contribuindo no *NATO's Maritime Centre for the Security of Critical Undersea Infrastructure* em Northwood Reino Unido e participa das missões combinadas de

patrulha naval e marítima com os demais países do JEF, tendo como principais áreas de patrulha o Alto Norte, em águas jurisdicionais norueguesas e adjacentes.

Em questões normativas a Noruega promulgou sua nova Lei de Segurança que entrou em vigor em 1º de janeiro de 2019 (Godzimirski apud Ministério da Defesa, 2021); (Godzimirski apud Stortinget, 2021). A lei trata os elementos da infraestrutura como dignos de proteção se as funções nacionais fundamentais puderem ser prejudicadas, se sua funcionalidade for reduzida ou se forem submetidos a vandalismo, dano ou apreensão ilegal (Godzimirski apud Stortinget, 2021).

No documento de 2016 sobre objetivos e meios de longo prazo na política de defesa (Godzimirski apud Ministério da Defesa, 2016), a infraestrutura crítica é mencionada e prover a proteção dessas infraestruturas é uma prioridade para garantir a continuidade dos serviços essenciais e a segurança da população

Em 2024, foi lançado um novo plano de longo prazo para o setor de defesa *The Norwegian Defence Pledge Long-term Defence Plan 2025–2036*, onde prevê a ampliação das capacidades de comando e controle das áreas marítimas, da força naval e de sistemas não tripulados. O documento enfatiza que a Noruega é uma nação com interesses marítimos consideráveis. E a proximidade com a força de submarinos nucleares da Rússia, faz-se mister manter a consciência situacional no alto norte e no atlântico norte (Noruega, 2024).

O plano também prevê uma futura capacidade de contramedidas para minas marítimas, consistindo em sistemas autônomos de contramedidas em um conceito de uso de navio mãe.

Adicionalmente, assim como o Reino Unido a Noruega mantém um centro de comando e controle conjunto, o *Norwegian Joint Headquarters* (NJHQ), situado no norte do país (Bodo), para monitorar continuamente a atividade nos territórios terrestres e marítimos da Noruega. A sede reúne todas as informações e faz um panorama completo da situação. Essa imagem é partilhada com outros departamentos das Forças Armadas Norueguesas, agências e com a OTAN. O chefe do NJHQ é considerado o conselheiro mais importante do Chefe da Defesa em questões relativas a operações e atividades militares.

4.3 - UNIÃO EUROPEIA

O Parlamento da União Europeia por meio do Departamento de Política para Relações Externas encomendou um relatório sobre ameaças à segurança das infraestruturas de comunicações submarinas e as consequências para a UE que foi publicado em abril de 2022 (Bueger; Liebetrau; Franken, 2022).

O presente trabalho se utilizou desse relatório para apresentar de forma resumida um panorama dos estados membro da UE em relação as suas posturas em relação ao tema de proteção dos cabos submarinos. Veremos como há diferenças relevantes e como o relatório criticou e formulou sugestões ao parlamento europeu.

Segundo o relatório, seu objetivo era triplo. Primeiramente, fornecer ao Parlamento Europeu e ao público interessado uma análise sistemática da vulnerabilidade dos Estados europeus a falhas de cabos submarinos devido a ataques deliberados. Isso incluiu uma avaliação dos intervenientes estatais e não estatais das ameaças. Em segundo lugar, o estudo mostra quais os cenários que poderiam afetar os Estados-Membros da UE. Critica a forma como alguns estados internalizaram a problemática. Finalmente, o último objetivo do estudo é apresentar recomendações para melhorar a resiliência da infraestrutura de cabos submarinos da UE (Bueger; Liebetrau; Franken, 2022).

O estudo foi dirigido em duas dimensões: a) Sensibilização e respostas estratégicas: que indicações existem sobre o nível de sensibilização nos Estados-Membros da UE e nos seus processos estratégicos. b) Monitoramento e governança: como são atualmente os modelos de governança na proteção dos cabos e como é organizada a relação entre os diferentes membros.

Há uma diferença significativa na percepção de vulnerabilidade e nas estratégias dos Estados-Membros à proteção dos cabos submarinos. Em alguns Estados-Membros, existe uma consciência política considerável refletida nos debates públicos e traduzida nas estratégias nacionais de segurança e defesa, predominantemente aquelas que se concentram na segurança marítima e cibernética. Em outros Estados-Membros, a sensibilização pública e política é mais tímida por diversos motivos e a proteção dos cabos de dados está ausente das estratégias e políticas de segurança nacionais, limitando-se a ser abordada como uma questão técnica ou de autorregulação.

Países que tiveram experiências de atividade naval ou submarina russa em suas águas jurisdicionais tendem a expressar uma maior consciência para proteção de suas infraestruturas críticas, em particular aos cabos submarinos e a identificar a proteção dos cabos como uma questão principalmente militar. Três Estados-Membros da EU documentam uma compreensão na responsabilidade militar a esse respeito: França, Irlanda e Portugal. Nos três estados, a liderança militar tornou públicas as questões, ou foi discutida nos meios de comunicação nacionais, com a questão dos cabos submarinos em particular.

No caso particular da França, país com vários domínios ultramarinos e com a segunda maior ZEE do mundo, o Ministério da Defesa publicou em 2022 uma estratégia nacional específica para controle dos fundos marinhos.

> "Confrontados com modos de ação diversos, evolutivos e duais, garantir a liberdade de ação das nossas forças armadas significa, acima de tudo, estender o controle do espaço marítimo ao fundo do mar. Devemos demonstrar a nossa determinação em **desenvolver conhecimento, monitorar e agir**. Estas três atividades serão desenvolvidas principalmente nas águas territoriais, na Zona Económica Exclusiva (ZEE) francesa e em qualquer área de relevância operacional. Neste quadro, será necessário aumentar as nossas capacidades de vigilância e ação até uma profundidade de 6.000 metros". (França, 2022, grifo nosso).

De forma pioneira a França publica uma estratégia integrando a relevância do domínio dos fundos marinhos à estratégia de defesa. O país buscará envolver sistemas capazes de operar por conta própria ou dentro de uma rede (com Sistemas não tripulados e Inteligência Artificial - IA), as operações de guerra no fundo do mar serão estruturadas em torno de três funções: desenvolver conhecimento, monitorar e agir.

No caso de Portugal, o país detectou atividades navais russas pelo menos desde 2014, quando um navio hidrográfico russo foi interceptado ao sul do porto de Faro (Bueger; Liebetrau; Franken, 2022).

A Irlanda não possui capacidades significativas de vigilância submarina, porém as atividades submarinas e de inteligência da Rússia foram divulgadas várias vezes nos meios de comunicação nacionais e internacionais, criando uma consciência e criticidade no país sobre a ameaça. Sobretudo a sua condição insular

traz uma preocupação maior quanto a proteção de suas infraestruturas críticas do poder marítimo (Bueger; Liebetrau; Franken, 2022).

Contudo, uma situação diferente surge no que diz respeito aos países mediterrâneos. No debate público na Itália, Espanha e Malta, as ameaças aos cabos de dados não têm tido um lugar de destaque, o problema da imigração irregular toma a principal atenção da mídia e das autoridades nas questões de segurança marítima.

Assim os estados-membros da UE desenvolveram quadros nacionais bastante diferentes para a resiliência dos cabos submarinos. Três modelos principais de governança são verificados. Em primeiro lugar, os mecanismos orientados para a segurança nacional, observado nos casos de França e Portugal; em segundo lugar, acordos e ações liderados por organizações civis, visualizados de forma mais proeminente no caso de Malta, a despeito de sua condição insular. Em terceiro lugar, os acordos de autorregulação conduzidos pela indústria são mais evidentes no caso da Dinamarca. Países como a Itália e Espanha indicam uma consciência governamental básica sobre a questão, a infraestrutura de cabos submarinos é mencionada nos documentos relevantes de segurança nacional e de política oceânica, colocando responsabilidades nas suas marinhas, entretanto sem ações mais contundentes de proteção (Bueger; Liebetrau; Franken, 2022).

Os Estados que priorizam as ameaças interestatais tendem a favorecer a segurança nacional e adotar modelos liderados pela marinha, como é o caso de França e Portugal.

Como apresentado, a conscientização para a proteção dos cabos submarinos, em particular, é bastante heterogênea entre os estados-membros da EU. Dois domínios de segurança estão bem formatados na UE, a segurança marítima e a segurança cibernética, o que colabora para que a segurança dos cabos submarinos seja abarcada nesses domínios. Contudo, mesmo com uma expressiva mentalidade de segurança marítima presente em quase todos os países, a atenção é dada a diferentes expressões do crime no mar, especialmente na pirataria e no contrabando de seres humanos, porém não diretamente com os cabos submarinos.

Outro domínio importante, que a UE está bastante focada, é com a segurança cibernética, e que possui bastante aderência com os cabos submarinos. A Agência da União Europeia para a Cibersegurança (ENISA) é a responsável, entretanto a

proteção dos cabos submarinos não está em sua competência (Bueger; Liebetrau; Franken, 2022).

A UE possui em sua estrutura as seguintes agências marítimas: Agência Europeia de Controle de Pesca (EFCA), a Agência Europeia de Segurança Marítima (EMSA) e a Agência Europeia da Guarda Costeira e de Fronteiras (Frontex). Essas organizações são agências técnicas essenciais na segurança marítima da EU. O produto dessa interação é fundamental, fornecem funções de vigilância, partilha de informações e coordenação da aplicação das normas de segurança marítima.

A EFCA é responsável pela regulamentação das pescas e apoia os estados-membros da UE na vigilância das atividades de pesca, inspeções, conformidade e partilha de informações. O relatório indica que há um elevado nível de consciência na EFCA de que a pesca é um fator central na prevenção de acidentes em cabos submarinos. No entanto, foi salientado que a proteção e vigilância dos cabos não são explicitamente um elemento das políticas pesqueiras e das medidas de conformidade da pesca (Bueger; Liebetrau; Franken, 2022).

A EMSA é a autoridade da UE para ajudar os estados-membros em questões de segurança marítima. Por um lado, isto envolve apoio para garantir o cumprimento dos regulamentos de segurança internacionais e europeus nos portos e nos navios. Isso inclui medidas diretamente relacionadas com a segurança, como o Código Internacional de Segurança de Navios e Instalações Portuárias (ISPS), que foi introduzido como parte da resposta ao terrorismo internacional. A segunda função principal da EMSA é monitorar a atividade marítima com foco nas águas europeias, mas com capacidades globais (Bueger; Liebetrau; Franken, 2022).

A EMSA desenvolve um quadro de situação marítima para os Estados-Membros da UE e outras agências técnicas. A imagem é baseada no Sistema de Identificação Automatizada (AIS) que permite identificar a posição e rota dos navios, bem como em imagens de satélite derivadas do sistema Copernicus[4]. A EMSA funde esses dados espaciais e fornece algoritmos que permitem a identificação de comportamentos suspeitos e não conformes que são utilizados em operações de aplicação da lei marítima. A EMSA é também a agência líder no desenvolvimento do Ambiente Comum de Partilha de Informações, que se pretende tornar a ferramenta

[4] O Copernicus é o Programa de Observação da Terra da União Europeia, que analisa o nosso planeta e o seu ambiente em benefício de todos os cidadãos europeus. Oferece serviços de informação baseados na observação da Terra por satélite e dados in situ (não espaciais). https://www.copernicus.eu/pt-pt/acerca-do-copernicus

chave para a partilha de informações de vigilância marítima em toda a UE (Bueger; Liebetrau; Franken, 2022).

A principal atenção da Frontex é a prevenção da migração irregular e dos crimes marítimos, como o contrabando. É a única agência marítima da UE que dispõe de capacidades substanciais de aplicação da lei. Até agora, estas capacidades estão totalmente centradas na proteção das fronteiras. A Frontex é responsável pelo Sistema Europeu de Vigilância das Fronteiras (EUROSUR). O EUROSUR integra diferentes meios (drones, aeronaves, radares etc.) para desenvolver uma imagem marítima partilhada para prevenir a criminalidade transfronteiriça e a migração irregular. Cada estado-membro da UE contribui para o sistema por meio de um centro nacional dedicado, sendo a Frontex responsável na fusão desses dados, incluindo fontes fornecidas pela EMSA (Bueger; Liebetrau; Franken, 2022).

A Frontex também opera uma rede de Comunidade de Inteligência Marítima e Análise de Risco. Criada em 2018, é uma rede para o intercâmbio de informações, inteligência, estatísticas de criminalidade transfronteiriça e a divulgação dos seus produtos de análise de risco. A rede foi concebida para apoiar: alertas precoces operacionais/estratégicos, alertas de risco, perfis de risco, relatórios gerais, análise de áreas/portos e mapeamento de riscos marítimos regionais/da UE. Uma vez que pretende prevenir e monitorar ameaças transnacionais, esta capacidade também poderia ser utilizada para abordar a resiliência dos cabos. Estudo indicam que a consciência de proteção dos cabos é baixa na organização e que a proteção de infraestruturas críticas é interpretada como estando fora das competências da agência (Bueger; Liebetrau; Franken, 2022).

Os fóruns da guarda costeira são outras ferramentas vitais na promoção de segurança marítima, na partilha de informações e na coordenação entre os órgãos da UE e os estados-membros. O *European Coast Guard Functions Forum* - Fórum Europeu das Funções da Guarda Costeira (ECGFF) é a entidade chave na UE na coordenação com os vizinhos marítimos. Isto inclui o Fórum de Cooperação da Guarda Costeira do Mediterrâneo, a Cooperação no Controle Fronteiriço da Região do Mar Báltico, o Fórum da Guarda Costeira do Atlântico Norte (NACGF) e o Fórum de Guardas Costeira do Ártico (ACGF). Esses fóruns regionais, que não são formalmente entidades da UE, discutiram a questão da segurança dos cabos (Bueger; Liebetrau; Franken, 2022).

O ECGFF, com sua capilaridade envolvendo um elevado número de intervenientes, é uma ferramenta fértil identificada no relatório anterior descrito para proporcionar a conscientização dos estados-membro na proteção e resiliência dos cabos submarinos na UE.

A proteção de infraestruturas críticas na UE enfrenta vários desafios, particularmente no contexto de cabos de comunicação submarinos. Existe uma disparidade significativa na conscientização e nas estratégias de proteção entre os estados-membros da UE. Alguns países, expostos a atividades submarinas russas, demonstram maior conscientização e tratam a proteção de cabos como uma questão militar. Outros países, porém, têm consciência pública e política limitada sobre o assunto, o que impacta negativamente a coordenação e a implementação de estratégias eficazes. A Cooperação e Coordenação são palavras chaves: A criação do *European Coast Guard Functions Forum* (ECGFF) é uma medida importante. Este fórum informal de coordenação reúne autoridades de guarda costeira de países da UE e do espaço Schengen para facilitar o compartilhamento de informações, segurança cibernética e análise de riscos no mar. Além disso, a *European Maritime Safety Agency* (EMSA) e a Frontex estão sendo avaliadas para incluir a vigilância de cabos em seus mandatos (Bueger; Liebetrau; Franken, 2022).

Dentro da ótica da cooperação, o compartilhamento de informações é essencial. Incentivar o relato de incidentes e o compartilhamento de informações entre a indústria e as autoridades policiais é vital para prevenir ataques criminosos e melhorar a resiliência geral.

Essas medidas refletem um esforço contínuo da UE para mitigar os riscos e fortalecer a segurança das suas infraestruturas críticas, garantindo uma resposta coordenada e eficaz frente às ameaças emergentes. Contudo ainda é um desafio tendo em vista as diferentes prioridades no campo da segurança marítima decorrente de outros problemas latentes como a imigração ilegal. Adicionalmente o fato de os cabos cruzarem diferentes mandatos, responsabilidades e jurisdições representa mais um desafio significativo.

5 - ANÁLISE DAS ESTRATÉGIAS ADOTADAS PARA PROTEÇÃO DAS ICPM NO REINO UNIDO, UNIÃO EUROPEIA E NORUEGA

Após conhecer como foi internalizado o assunto proteção de infraestruturas críticas do poder marítimo no Reino Unido, Noruega e UE, particularmente em atenção aos cabos submarinos e as respectivas medidas tomadas, percebe-se que há uma diferença de postura, principalmente entre os países do Atlântico Norte e os países mediterrâneos. Tanto na sensibilização, quanto na importância dada para um melhor monitoramento e proteção e governança.

Verificou-se que o assunto foi alvo de discussão e compartilhado em diversos fóruns de segurança marítima. Os acidentes ocorridos nas ICPM foram amplamente divulgados pela mídia, expondo a vulnerabilidade dos sistemas e a necessidade de ações coordenadas para mitigação das ameaças. Entretanto percebe-se diferentes posturas dos países.

Observou-se que os países que priorizaram medidas de proteção aos sistemas de cabos submarinos são aqueles que se enquadram em pelo menos uma das características a seguir:

a) Países que possuem maior dependência da infraestrutura submarina para sua sobrevivência (energética, comunicações);
b) Países que tiveram avarias em seus sistemas de ICPM ou a visita de navios considerados ameaças e essas estruturas;
c) Países que são grandes HUB de cabos submarinos;
d) Países vizinhos de países considerados ameaças (Rússia);

Podemos listar o Reino Unido, Noruega, França, Portugal assim como os países componentes da JEF.

Por outro lado, percebeu-se que outros países tiveram uma sensibilização modesta, a ponto de não tomarem medidas robustas de proteção das ICPM. Avalia-se que tais países ou não se enquadram nas condições anteriores, ou possuem uma realidade com desafios que os impedem de se voltarem ao assunto das ICPM no momento, como por exemplo, enfrentamento a entrada de imigrantes ilegais. Seria o caso de países como Espanha e Itália.

Essa pesquisa identificou, entretanto que países como a Alemanha, não tomaram medidas contundentes na proteção de suas ICPM, mesmo tendo sido um

dos protagonistas do acidente no *NordStream*. Percebe-se que a prioridade na proteção das ICPM na Alemanha não era elevada até aquele momento. O país possui uma estratégia nacional para proteção de infraestruturas críticas publicada em 2009, que não menciona diversos domínios de vulnerabilidades atuais. Tal documento já merece uma atualização quando comparado a alguns vizinhos europeus. Adicionalmente, sua condição como país detentor de rede de comunicação predominante terrestre, corrobora com essa postura em relação aos cabos submarinos.

Dentro da ótica de que outras vulnerabilidades podem ter demandado as preocupações da Alemanha, destaca-se o comprometimento de sua segurança energética no âmbito das sanções envolvendo o conflito na Ucrânia e com as consequências do próprio acidente do *NordStream*. O país teve que buscar outras fontes de fornecimento de gás, decorrente da forte dependência da Rússia para fornecimento.

E com certeza o suporte da OTAN para assumir tais preocupações, faz com que países não tão afetados com acidentes em ICPM nem com uma vizinhança que ofereça ameaça iminente, permitam-se se concentrar em outras prioridades e contar com o esforço dos aliados da organização para assumirem tais tarefas.

É o que se observa nas medidas tomadas principalmente pelo Reino Unido, Noruega e países membros do JEF. O Reino Unido que possui a condição insular, ou seja, totalmente dependente de ICPM, e no caso dos cabos submarinos, um grande HUB europeu e intercontinental bem como detentor de domínios ultramarinos, está entre os países europeus mais engajados em proteger suas infraestruturas críticas.

Esse capítulo passará a avaliar as ações adotadas pelos países que tiveram maior grau de conscientização na proteção dos cabos submarinos, como Reino Unido e Noruega e outros países europeus, como França e ações no âmbito da OTAN e União Europeia.

Algumas medidas buscaram objetivos similares de elevar a conscientização de segurança às agências governamentais e setores privados, seja atualizando suas estratégias de defesa e segurança nacional e planos decorrentes seja atualizando outras normas e estratégias setoriais com o mesmo objetivo.

A atualização de documentos de alto nível, no caso da Estratégia de Segurança traz diversos benefícios como a melhor percepção e visualização das

ameaças, pois essas estão em constante evolução, tornando-se mais sofisticadas, diversificadas e acompanhando as evoluções tecnológicas. Nesse processo de atualização, os estudos de alto nível necessários podem identificar novas lacunas de capacitação que necessitam ser preenchidas para mitigar essas ameaças. Atualizar as estratégias permite que os países estejam preparados para enfrentá-las de forma eficaz.

Além disso, o avanço tecnológico traz tanto oportunidades quanto novos riscos. A integração de tecnologias como a Internet das Coisas (IoT), IA e sistemas não tripulados exige novas abordagens de segurança para proteger infraestruturas críticas contra falhas e ataques.

Estratégias atualizadas incluem planos de resposta rápida e recuperação em caso de incidentes, garantindo que as infraestruturas críticas possam continuar operando ou se recuperar rapidamente após um ataque ou desastre natural. A cooperação internacional também é facilitada com a atualização dessas estratégias, uma vez que muitas infraestruturas críticas, como cabos submarinos e rotas de transporte, têm uma dimensão global, exigindo coordenação entre países para protegê-las contra ameaças.

Manter as estratégias de segurança atualizadas garante conformidade com regulamentações e padrões internacionais em constante mudança, evitando sanções e promovendo a confiança internacional. A segurança das infraestruturas críticas está diretamente ligada à estabilidade econômica, e falhas ou ataques a esses sistemas podem causar enormes prejuízos econômicos e sociais. Estratégias de segurança atualizadas ajudam a mitigar esses riscos e garantir a continuidade dos negócios e serviços.

Entre as infraestruturas críticas incluem-se redes de eletricidade e gás que fornecem energia, cabos submarinos e redes de comunicação para conectividade global, portos, aeroportos, ferrovias e estradas essenciais para o transporte, sistemas de abastecimento de água e tratamento de esgoto para a saúde pública, além de hospitais e redes de saúde que prestam serviços médicos essenciais. A atualização das estratégias nacionais de segurança é essencial para proteger essas infraestruturas contra uma ampla gama de ameaças modernas, garantindo a continuidade dos serviços essenciais e protegendo a economia e a segurança nacional. Os países devem adotar uma abordagem proativa, integrando avanços

tecnológicos e promovendo a cooperação internacional para fortalecer a resiliência de suas infraestruturas críticas.

Desafio adicional a ser superado na escrituração dessas estratégias é encontrar a divisão de responsabilidades tendo em vista que a maioria dos cabos submarinos é propriedade de empresas privadas de telecomunicações. Isso significa que a responsabilidade primária pela proteção e manutenção desses cabos recai sobre essas empresas, e não sobre os governos nacionais. Assim, definir com maior clareza as responsabilidades entre o setor público e privado na proteção das infraestruturas críticas e a criação de uma cadeia de comando clara para respostas a incidente é um desafio nas estratégias dos países estudados e no contexto da UE.

Destaca-se outra relevante medida implementada, o incremento do monitoramento em proveito da segurança marítima. No caso do Reino Unido temos o exemplo do Centro Conjunto de Segurança Marítima (JMSC) em 2019, e ainda no país, mas na esfera da OTAN, citamos a criação do *NATO's Maritime Centre for the Security of Critical Undersea Infrastructure* nas instalações da *NATO's Maritime Command* (MARCOM) em Northwood, em 2024. Ambos os centros irão permitir uma maior consciência situacional marítima empregando tecnologias de detecção que possam identificar atividades suspeitas ou danos potenciais em tempo real, permitindo assim melhor reação a ameaças e contribuindo com dados de inteligência operacional no planejamento de missões de dissuasão. Essas medidas são mais efetivas devido ao caráter interagências, no caso do JMSC e do caráter de cooperação internacional no caso da OTAN.

Como citado anteriormente, a questão da propriedade dos cabos submarinos é uma de suas peculiaridades, pois quase todos pertencem a empresas não estatais. Tal fato mostra ser um desafio adicional na coordenação de sua gestão e proteção. A troca de informações entre países e suas agências minimiza esse obstáculo, demonstrando que a cooperação é outro pilar importante a ser explorado para reagir aos desafios de proteção às vulnerabilidades das ICPM, em especial aos cabos submarinos.

No âmbito da UE, o relatório encomendado pelo Parlamento Europeu demonstra que embora haja uma grande preocupação nos domínios da segurança marítima e segurança cibernética, a proteção de cabos submarinos é considerada uma vulnerabilidade, pois o assunto é tangenciado por algumas agências de segurança, mas não é compromisso de nenhuma efetivamente. O Relatório propõe

que a UE poderia encorajar as instituições que lideram o processo de elaboração da nova estratégia de segurança marítima a priorizar a proteção dos cabos submarinos e coordenar com as agências técnicas relevantes (EFCA, EMSA, ENISA, Frontex) sobre potenciais ações. Outra sugestão, rever o mandato da EMSA, para inclusão da segurança dos cabos submarinos no rol de suas responsabilidades (Bueger; Liebetrau; Franken, 2022).

Percebe-se então que na UE o assunto da proteção dos cabos submarinos está em processo de maturação para definição de responsabilidades entre as agências do bloco, e assim, refinar uma gestão coesa sobre o assunto. A revisão da estratégia e a preocupação do Parlamento Europeu demonstram ações em andamento para uma regulação que aproveitará a estrutura das agências já existentes, com suas diversas capacidades. Adicionalmente, verifica-se que o fator cooperação já é uma realidade no bloco e nas respectivas agências, o que facilita a troca de informações entre elas. Resolvendo a questão da regulamentação das responsabilidades a gestão será aperfeiçoada e o ambiente de cooperação existente será otimizado e funcionará de forma mais eficaz.

O relatório estudado sugere também que a Agência da União Europeia para a Cibersegurança (ENISA) fizesse uma avaliação envolvendo a segurança dos cabos de dados submarinos. Tal estudo foi realizado pela agência em 2023 e apresentou algumas observações e recomendações com a dificuldade de identificar de forma clara, quais autoridades nacionais devem ter o poder de supervisionar os cabos submarinos e receber relatórios de incidentes. E que os estados-membros da UE devam esclarecer a nível nacional quem tem a responsabilidade e o mandato pela proteção e segurança dos cabos submarinos (ENISA. 2023). Ou seja, tanto a estrutura da UE, quanto seus estados, necessitam definir claramente a responsabilidade na proteção dos cabos submarinos, para que a troca de informação seja efetiva e útil para minimizar as vulnerabilidades e dissuadir possíveis interferências.

Das experiências anteriores, conclui-se que o conhecimento das vulnerabilidades, o monitoramento e cooperação são essenciais para uma boa gestão do conhecimento.

Nos parágrafos anteriores apresentou-se como os conceitos de conhecimento das vulnerabilidades e ameaças, traduzido na atualização das estratégias de segurança marítimas, o monitoramento das áreas, exemplificado nos centros de

vigilância e monitoramento, que nos remete a outro conceito essencial e recomendado que é a cooperação, refletido nas trocas de informações interagências e entre agências dos países envolvidos, são primordiais para um eficiente sistema de proteção de ICPM.

Adicionalmente, como exemplo de cooperação, os exercícios navais programados entre nações do JEF e OTAN exploram a presença de meios para a dissuasão de ameaças e encontro de soluções comuns para respostas rápidas a essas ameaças. A exemplo do Reino Unido e Noruega, estados não membros da UE e focados na região euro-atlântica e mar do norte, e a cooperação entre eles e mais alguns países da UE já é uma realidade mais contundente. Esses exercícios entre aliados e parceiros se torna essencial para que haja um compartilhamento de informações e recursos. Principalmente nessa região estudada, onde as fronteiras são bem próximas, navios russos trafegam constantemente, existe grande atividade pesqueira e diversos países possuem estruturas críticas associadas a indústria de óleo e gás, fazendas eólicas *off-shore* e de comunicações. Assim, atividades suspeitas e informações de acidentes ocorridos podem ser compartilhados e ferramentas de acompanhamento e meios de dissuasão possam ser empregados para afastar as ameaças ou minimizar as ocorrências indesejáveis de possíveis navios sabotadores ou espiões. Mesmo atividades que possam causar avarias não intencionais, como atividade pesqueira, visto anteriormente, possam ser monitoradas e orientadas a não causarem danos às ICPM.

O planejamento de exercícios combinados pela OTAN e JEF com diferentes marinhas para missão específica de proteção à ICPM demonstra o alto grau de cooperação entre esses países e a prioridade para o assunto. Em resumo, a proteção das infraestruturas críticas submersas depende cada vez mais da cooperação internacional, envolvendo o compartilhamento de inteligência, a coordenação de patrulhas e a utilização de tecnologias avançadas para detectar e neutralizar ameaças. A mobilização da Royal Navy e os exercícios da OTAN são passos significativos nesse esforço colaborativo para garantir a segurança dessas instalações vitais.

Por fim, outra medida robusta verificada, foi a incorporação de novo meio naval ao inventário das forças armadas do Reino Unido. O que indica como um processo de análise de risco das ICPM do país, dentro de um contexto de vulnerabilidade e novas ameaças, foi entendido pelas autoridades do Reino Unido como uma lacuna de capacidade a ser coberto e com uma razoável celeridade.

Como apresentado no início desse capítulo, o Reino Unido foi o único país entre os estudados que incorporou meios navais com o objetivo específico de contribuir para monitorar e proteger suas ICPM em especial os cabos submarinos.

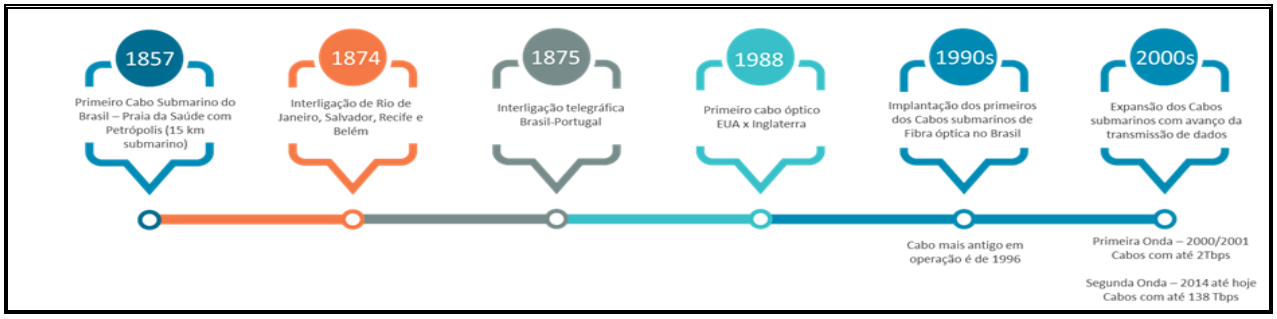
Concluindo, a proteção dos cabos submarinos é uma tarefa complexa que exige uma abordagem multifacetada, combinando tecnologia avançada, cooperação interagências e internacional e estratégias de resposta eficazes. Melhoria nas capacidades de monitoramento, resposta rápida, e integração de esforços na segurança cibernética e marítima, passos essenciais para fortalecer a resiliência das infraestruturas críticas do poder marítimo. A colaboração entre os países e a harmonização de normas e legislações também são fundamentais para garantir a segurança contínua dessas infraestruturas vitais.

6 - GESTÃO DE PROTEÇÃO DE CABOS SUBMARINOS NO BRASIL

No Brasil, os cabos submarinos são utilizados em sistemas de telecomunicações desde 1857, com a inauguração da primeira de uma linha de comunicações telegráfica no Estado do Rio de Janeiro. Entre 1870 e 1880 foram implantadas linhas telegráficas interligando cidades na costa brasileira e, também, um ponto de conexão com Portugal (ANATEL, 2022).

Na década de 1990, foram inaugurados os primeiros cabos submarinos de fibra óptica no Brasil, como indica a Figura 7.

Figura 7 - Histórico de implantação de cabos submarinos no país

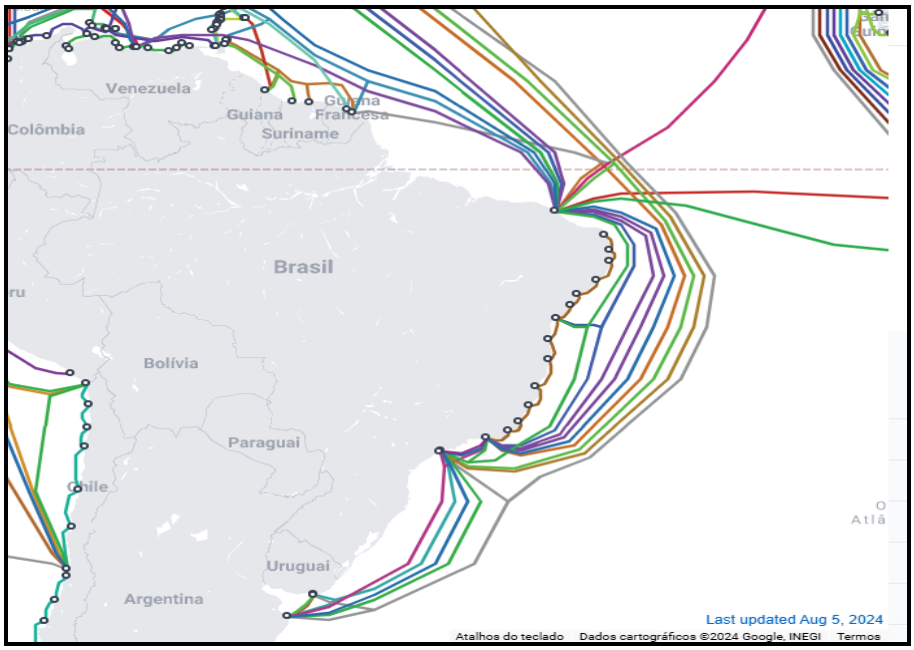


Fonte: ANATEL (2022).

Os cabos submarinos ancorados na costa brasileira atendem as necessidades do sistema de telecomunicações nacional e viabilizam a interconexão de qualquer sistema de telecomunicações e internet da América Latina com os demais continentes do mundo, como indicado na Figura 8.

No total, o Brasil é servido por 22 cabos submarinos que chegam ao país, cada um avaliado em cerca de seis bilhões de dólares. O país possui quatro pontos de chegada de cabos submarinos em terra, conhecidos como *landing points*, que desempenham um papel estratégico na conectividade do país com o mundo. Esses pontos estão localizados em Fortaleza (CE), Salvador (BA), Rio de Janeiro (RJ) e Santos (SP) A cidade de Fortaleza se destaca como um importante hub internacional, com dezessete cabos em operação, tornando-se uma ligação entre a América do Norte, África e Europa (Telegeography, 2023).

Figura 8 - Situação dos cabos submarinos no Brasil



Fonte: Telegeography (2023)

O propósito desse capítulo é conhecer as medidas tomadas no Brasil para a proteção das ICPM, em particular dos cabos submarinos, analisando o arcabouço legal existente, os níveis de prioridade que foram dispendidos ao tema, a fim de verificar a sensibilização e respostas estratégicas dadas pelo Brasil, verificando tanto o contexto normativo quanto sua gestão. Adicionalmente, identificar os modelos de governança na proteção dos cabos e qual o grau de monitoramento das áreas onde são posicionados e o nível de cooperação existente entre as instituições que possuem interesses nos cabos submarinos.

6.1 – SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

A segurança de infraestruturas críticas passou a ser uma tendência mundial logo após os atentados terroristas ocorridos nos Estados Unidos da América, em 11 de setembro de 2001. O governo estadunidense, à época, publicou uma série de diretrizes de segurança interna, entre as quais havia a elaboração de um plano nacional abrangente para garantir a segurança de infraestruturas críticas, por meio de cooperação das autoridades e das agências federais, regionais e locais, além do setor privado e de outras entidades (Brasil, 2020a).

No Brasil, o tema teve impulso a partir de 2006, após os ataques perpetrados por uma organização criminosa a várias instalações sediadas no Estado de São Paulo. Esses eventos levaram o Governo brasileiro a tomar a iniciativa de identificar quais infraestruturas do País deveriam ser prioritariamente protegidas, no caso de novas ocorrências daquela natureza (Brasil, 2020b).

Entretanto o tema ganhou vulto e necessidade de maior proatividade na proteção de infraestrutura crítica (IC) no país, graças a realização de grandes eventos, iniciando com os Jogos Pan-americanos de 2007, no Rio de Janeiro, e em seguida com a Jornada Mundial da Juventude (2013), Copa das Confederações (2013), Copa do Mundo de Futebol (2014) e Olimpíadas (2016).

6.1.1 – Documentos Regulatórios

Os documentos centrais da defesa brasileira em suas versões de 2020, a Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END), já trataram da questão das infraestruturas críticas e da necessidade da manutenção e proteção desses ativos.

A PND em seu capítulo 4 estabelece como um dos objetivos nacionais de defesa: Assegurar a capacidade de Defesa para o cumprimento das missões constitucionais das Forças Armadas.

Os documentos de forma ampla outorgam às Forças Armadas as capacidades necessárias para realizar a vigilância, o controle e a defesa do território, das águas jurisdicionais e dos espaços aéreos para proverem a segurança das linhas de comunicação marítimas de interesse. Acrescenta a importância das infraestruturas críticas, tais como transporte, energia e comunicação, entre outros para o cumprimento da missão de proteção. Leva em conta a necessidade de contínuo aperfeiçoamento das técnicas e da doutrina de emprego das Forças, de forma singular e conjunta, com foco na interoperabilidade (Brasil, 2020a, b).

Na END, o tema foi inserido no contexto das capacidades nacionais de defesa de proteção, de forma mais particular imputando à Marinha do Brasil, em seu subitem 3.6.2, a capacidade para controlar áreas marítimas, negar o uso do mar e projetar o Poder Naval terão por foco incrementar a segurança e a habilitação para defender as infraestruturas críticas marítimas, os arquipélagos e as ilhas oceânicas nas águas jurisdicionais brasileiras ou onde houver interesses nacionais, assim

como responder prontamente a qualquer ameaça às vias marítimas de comércio (Brasil, 2020a).

Ao analisar esses arcabouços normativos, conclui-se que o Brasil adota uma gestão de proteção de suas infraestruturas securitizada em suas Forças Armadas, assim como observamos em alguns países da Europa como: Reino Unido, Noruega, França, Portugal entre outros. Como aqueles países, o setor privado é o detentor dos ativos possuindo suas responsabilidades e atribuições, bem como os respectivos ministérios correlatos. Entretanto, a capacidade para proteção em termos de dissuasão de certas ameaças e mitigação de vulnerabilidades fica a cargo das Forças Armadas. Para isso, um arcabouço legal com divisão de responsabilidades é essencial para uma boa gestão desses ativos.

A norma de alto nível no Brasil sobre o assunto é a Política Nacional de Segurança de Infraestruturas Críticas – PNSIC (regulamentada pelo Decreto nº 9.573/2018), estabelecendo os seguintes instrumentos para sua efetivação: I – a Estratégia Nacional de Segurança de Infraestruturas Críticas; II – o Plano Nacional de Segurança de Infraestruturas Críticas; e III – o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. A Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222/2020) foi um passo importante com o estabelecimento do objetivo estratégico de elevar o nível de proteção das Infraestruturas Críticas Nacionais (Freire; Aquino, 2023).

A Estratégia Nacional de Segurança das Infraestruturas Críticas (ENSIC) foi o documento base para que em 2022 fosse publicado o Plano Nacional de Segurança das Infraestruturas Críticas (PlanSIC). O documento, embora normatize questões relevantes sofre infraestruturas críticas, possui uma abordagem ampla, citando os cabos submarinos apenas uma vez e não abordando especificidades já mencionadas sobre os cabos submarinos (Serrano; Porchéra, 2023).

Adicionalmente, a aprovação do Regulamento de Segurança Cibernética Aplicado ao Setor de Telecomunicações (Resolução nº 740/2020) foi um passo a mais para enfrentar os desafios de segurança associados aos cabos submarinos. Imputando atribuições à Anatel relacionadas à Infraestrutura Crítica de Comunicações, pois fornece um quadro de conduta e procedimentos para melhorar a segurança nas redes e serviços de telecomunicações, inclusive a proteção dos cabos submarinos. O Regulamento estabelece, ainda, um modelo de governança

por meio do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) (Freire; Aquino, 2023).

De acordo com a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), compete ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) o acompanhamento dos assuntos pertinentes às infraestruturas críticas no âmbito da administração pública federal. Desta forma, o GSI/PR coordena, junto aos diversos setores, os inúmeros Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC), responsáveis por estudar e propor a implementação de medidas e de ações relacionadas com a segurança das infraestruturas críticas nas suas respectivas áreas de atuação, como energia elétrica, petróleo e gás, transportes, telecomunicações, entre outros (Brasil, 2018).

Os Grupos Técnicos de Segurança de Infraestruturas Críticas, que são compostos por representantes dos setores público e privado, onde, de acordo com a metodologia aplicada, realizam estudos para levantamento das infraestruturas críticas do setor de telecomunicações; identificação de ameaças, vulnerabilidades e medidas de controle; gerenciamento de riscos; além da confecção de um diagnóstico nacional para o setor e análise de interdependências. Além disso, o GSI passará a coordenar o Comitê Nacional de Segurança de Infraestruturas Críticas (CNSIC) em fase de implantação no período desse trabalho, de acordo com o apêndice A. Adicionalmente, a atualização do PLANSIC que está ocorrendo devido à reestruturação Ministerial contempla esta alteração. O CNSIC será composto por Ministérios e Órgãos da Administração Pública Federal com aderência ao tema, assim como é feita a composição dos GTSIC. Essas atualizações possivelmente permitirão aumentar a integração entre órgãos públicos e privados envolvidos no tema, um grande desafio, como observado nesse estudo.

Assim, o Brasil tem publicado normas para favorecer a segurança e a resiliência das infraestruturas críticas do País e a manutenção de seus serviços. Entretanto, o grande desafio é cumprir o que está disposto nesses normativos.

Cabe mencionar que o PlanSIC imputa ao Ministério das Comunicações a responsabilidade pela elaboração de um plano setorial para a área prioritária de comunicações, onde o assunto da proteção dos cabos submarinos deveria ser mais detalhado e responsabilidades serem definidas, entretanto o documento ainda não foi promulgado. Exatamente um dos problemas estudados sobre o tema, a dificuldade de definir responsabilidades, tendo em vista o caráter privado dos cabos.

Da mesma forma o PlanSIC atribui ao Ministério da Defesa a edição de um plano setorial, o que também ainda não foi publicado. A falta dos planos setoriais pode constituir um desafio para uma melhor gestão desses ativos, além de indicar ainda a necessidade de uma maior conscientização sobre o tema em algumas esferas da administração pública e privada.

No contexto da Marinha do Brasil, a instituição tem conduzido atualizações normativas decorrentes das orientações oriundas dos documentos de alto nível, o que resultou na publicação de algumas normas em que a segurança das ICPM está inserida, como na Estratégia de Defesa Marítima (EDM). A atualização de conceitos doutrinários também ocorreu, o que se fez por meio da publicação Fundamentos Doutrinários da Marinha (FDM), base para a atualização da Doutrina Militar Naval (DMN) (BRASIL, 2023a, b)

Consultando as normas recém atualizadas percebe-se que, embora foi dada uma boa abordagem para as ICPM, entretanto, a proteção dos cabos submarinos não foi detalhada, mesmo sendo uma ICPM com características bastante específicas, merecendo uma abordagem maior.

Na EDM foram listados diversos Objetivos Estratégicos (OBE), é importante ressaltar que os OBE abrangem todos os Campos de Atuação do Poder Naval (CAPN), quais sejam: Defesa Naval, Segurança Marítima, Diplomacia Naval e Apoio às Ações do Estado. Outra característica relevante a ser ressaltada é o caráter permanente dos OBE intrínseco a cada um deles. Isto posto, foram elaborados onze OBE. Dentre esses, o terceiro OBE retrata a importância de “Proteger as Infraestruturas Críticas do Poder Marítimo (ICPM) (Brasil, 2023a).

> 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, 2023a p. 1-2)

Ainda na EDM, foram definidas as Prioridades Estratégicas que derivam de análises que levam em conta o diagnóstico do Poder Naval e a missão da MB. São escolhas que permitem direcionar os esforços empreendidos pela MB na busca de um Poder Naval compatível com os desafios, coadunando o cumprimento da Missão com uma aplicação eficaz de recursos toda ordem (Brasil, 2023a).

Elas foram divididas por Campos de Atuação e/ou ambientes operacionais de atuação da MB. E dentro do campo de atuação Defesa Naval, destaca-se nesse estudo a seguinte Prioridade Estratégica:

Incrementar a capacidade de defender as ICPM consideradas prioritárias. E foi inserida no documento a seguinte nota de rodapé sobre essa prioridade estratégica referindo-se a ICPM:

> "Principais plataformas de petróleo e gás responsáveis diretamente pelo abastecimento interno do País e estruturas portuárias prioritárias, de acordo com o Plano de Configuração de Força (PCF)." (Brasil, 2023a p.1-8).

Sem dúvida as plataformas de petróleo e gás são ICPM que devem ter a máxima prioridade estratégica e a MB está de forma bastante lúcida, envidando esforços no cumprimento dessa missão e de forma transparente na EDM, buscando uma configuração da Força mais adequada e capacitada para a defesa dessas ICPM. Entretanto, carece de uma revisão, tendo em vista a ausência dos cabos submarinos no contexto das ICPM. Devido a sua importância estratégica, peculiaridades que demandam uma gestão em diferentes esforços, responsabilidades e o desafio que representa a sua proteção.

Depreende-se que o modelo de governança de proteção às ICPM, comparado com o que foi estudado anteriormente para alguns países, aproxima o Brasil do modelo orientado para a segurança nacional, ou seja, assim como os modelos apresentados para França, Portugal, Reino Unido e Noruega. A despeito das ICPM terem seus ativos pertencentes a empresas privadas, sua proteção está intrinsecamente dependente de uma capacitação do Estado em cooperação com o setor privado.

Embora mais uma vez os cabos submarinos não foram citados nos campos de atuação do FDM, novamente esse trabalho sugere que é válida uma ponderação para a revisão e sua inclusão. Pois, não sendo diferentes dos outros ativos das ICPM, como plataformas de petróleo de gás e instalações portuárias, já que muitas dessas, também são pertencentes ao setor privado, os cabos submarinos merecem a mesma proteção.

Ao analisar o arcabouço normativo do Brasil, percebemos que, da mesma forma que a maioria dos países estudados, a revisão de normas é de suma importância para mapear as vulnerabilidades, identificar ameaças e definir objetivos

estratégicos. Os cenários são dinâmicos e a evolução tecnológica e configuração geopolítica exigem que os estados estejam atualizados em suas políticas e estratégias de defesa.

Considerando o quesito monitorar, verificamos que o Brasil persegue uma maior efetividade nesta questão. Na EDM foram destacadas as seguintes prioridades estratégicas (BRASIL, 2023a):

No Campo de atuação de Defesa Naval:

I) DEF1 - Ampliar a consciência situacional marítima e fluvial na Amazônia Azul e nas bacias Amazônica e Platina;

V) DEF5 - Ampliar o comando e controle da Força Naval;

VI) DEF6 - Ampliar a cooperação com a Força Aérea Brasileira (FAB) e o Centro Gestor e Operacional do Sistema de Proteção da Amazônia (CENSIPAM) com foco na Inteligência, Vigilância e Reconhecimento (IVR) e Defesa Aeroespacial;

No campo de atuação da Segurança Marítima (SMA):

I) SMA1 - Ampliar a consciência situacional nas Linhas de Comunicação Fluvial (LCF) da Bacia Amazônica;

II) SMA2 - Ampliar as capacidades logística e de inteligência das Organizações Militares do Sistema de Segurança do Tráfego Aquaviário na Bacia Amazônica;

III) SMA3 - Ampliar a consciência situacional na Amazônia Azul, incluindo as Ilhas Oceânicas;

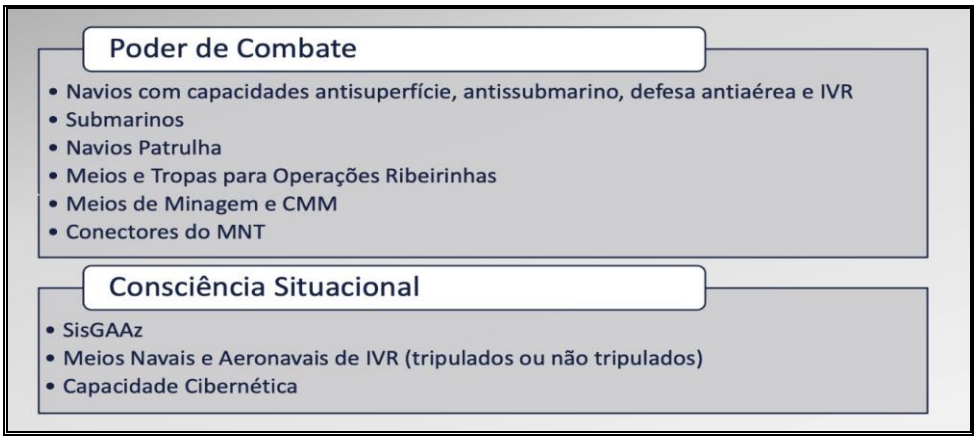
IV) SMA4 - Ampliar a cooperação com a FAB com foco em IVR e Patrulha Marítima;

V) SMA5 - Otimizar os meios empregados na Patrulha Marítima;

VI) SMA6 - Ampliar a consciência situacional nas LCF da Bacia Platina;

Todas essas prioridades reconhecidas na EDM possuem aderência ao incremento do monitoramento e ampliação da consciência situacional. A publicação expõe que o preparo do poder naval está pautado em duas linhas de esforço principais, cada uma calcada em uma Capacidade Estratégica. Uma tem por objetivo incrementar o Poder de Combate, de forma contextualizada com as ameaças, e outra visa aumentar a Consciência Situacional da MB nas áreas marítimas e fluviais prioritárias identificadas na EDM. Cada linha de esforço é composta pelos eixos temáticos, conforme apresentado na Figura 9.

Figura 9: Eixos Temáticos do preparo do Poder Naval



Fonte: Brasil (2023a).

Em relação a Linha de Esforço de ampliar a Consciência Situacional a MB deve primeiramente ampliar a Consciência Situacional Marítima nas áreas referentes ao Projeto Piloto do Sistema de Gerenciamento da Amazônia Azul (SisGAAz), buscando o gradualismo que permita a expansão da Consciência Situacional, sequencialmente, para a Elevação do Rio Grande, Ilhas Oceânicas, Foz do Rio Amazonas, Bacia de Santos, Margem Equatorial brasileira e para o Arquipélago de São Pedro e São Paulo (Brasil, 2023a).

O principal órgão responsável pelo monitoramento e contribuinte para a manutenção da consciência situacional e segurança marítima é o Comando de Operações Marítimas e Proteção da Amazônia Azul (COMPAAz), que tem o propósito de contribuir para o aprestamento e emprego das Forças Navais, Aeronavais e de Fuzileiros Navais subordinadas ao ComOpNav; para a segurança do tráfego marítimo e fluvial de interesse do Brasil; para o desenvolvimento da Segurança Marítima; e para o desenvolvimento da Consciência Situacional Marítima (MB, 2024).

6.1.2 - O SisGAAz

A Marinha do Brasil, em parceria com agências e órgãos governamentais, coordena a implementação e o aperfeiçoamento do Sistema de Gerenciamento da Amazônia Azul, cuja missão está em monitorar e proteger, continuamente, as áreas marítimas de interesse e as águas interiores, bem como seus recursos vivos e não

vivos, seus portos, embarcações e infraestruturas, mediante ameaças, emergências, desastres ambientais, hostilidades ou ilegalidades, com o objetivo de contribuir para a segurança e a defesa da Amazônia Azul e para o desenvolvimento nacional (Lampert, 2024).

Quando estiver operacional, o SIsGAAz terá como objetivo permitir monitorar e proteger as águas jurisdicionais brasileiras (AJB). Sabe-se o quanto de possibilidade há nos campos do pré-sal (petróleo e gás) e em outros tipos de recursos minerais, os quais irão demandar maior segurança na Amazônia Azul. O projeto SIsGAAz é um exemplo da estrutura dual, civil e militar, para permitir a presença do Estado brasileiro na segurança e na defesa de interesses vitais e estratégicos.

O projeto SisGAAz prevê a integração de equipamentos e sistemas compostos por radares localizados em terra e embarcações, além de câmeras de alta resolução e capacidades como o fusionamento de informações recebidas de sistemas colaborativos, destacando o Sistema de Monitoramento Marítimo de Apoio às Atividades de Petróleo (SIMMAP), o Sistema de Identificação e Acompanhamento de Navios a Longa Distância (LRIT), o Sistema de Informação Sobre o Tráfego Marítimo (SISTRAM) e o Programa Nacional de Rastreamento de Embarcações Pesqueiras por Satélite (PREPS), todos baseados em rastreamento de posição por via satélite. Os dados captados por sistema de posicionamento global (GPS) são transmitidos por meio de comunicação satelital para centrais de rastreamento e, no futuro, haverá a incorporação de sensores acústicos aos sites de monitoramento. Há também a previsão de incorporar o monitoramento de longo alcance, até cerca de 200 milhas (pouco mais de 320 km) da costa brasileira, com radares *Over The Horizon* (OTH) (Lampert, 2024).

Ademais, o SisGAAz busca integração e conexão com outros sistemas, como, por exemplo, com as redes da Polícia Federal, do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis, da Receita Federal, da Petrobrás, entre outros órgãos e empresas capacitadas a compartilhar e analisar dados e informações indispensáveis à proteção da Amazônia Azul. Sua implementação reduzirá custos de operações de vigilância e patrulha, bem como outras atividades que envolvam deslocamentos de pessoal e, principalmente, a salvaguarda da vida humana no mar (CEMBRA, 2022).

6.2 - HISTÓRICO DE AMEAÇAS NO BRASIL

No início de 2020 a Marinha do Brasil monitorou durante uma semana o navio russo Yantar, suspeito de espionagem, após sua entrada na (ZEE) do Brasil. O Yantar, conhecido por sua avançada tecnologia de sensores e capacidade de rastrear comunicações submarinas, desapareceu dos sistemas de acompanhamento, levantando suspeitas de que seu sistema de identificação tenha sido desligado intencionalmente. Posteriormente, a embarcação foi localizada a 80 quilômetros das praias do Rio de Janeiro, próximo a cabos submarinos de internet que conectam o Brasil a outros países. A tripulação russa deu respostas evasivas sobre suas atividades, aumentando as suspeitas de espionagem. O incidente ocorre em um contexto de crescente preocupação global com a segurança dos cabos submarinos. A Rússia já foi alvo de suspeitas semelhantes, com o Yantar sendo escoltado pela Força Aérea britânica no Canal da Mancha e monitorado pelos EUA e Irlanda em incidentes anteriores (Monteiro, 2020).

7 - COMPARAÇÃO DAS MEDIDAS PARA PROTEÇÃO DOS CABOS SUBMARINOS DOS PAÍSES ESTUDADOS E DAS REALIDADES DO BRASIL NA ÁREA, PROPOSTAS PARA INCREMENTO DA RESILIÊNCIA DO MODELO BRASILEIRO

Neste capítulo, faremos uma análise comparativa das estratégias adotadas pelo Reino Unido, Noruega e União Europeia na proteção de suas infraestruturas críticas de cabos submarinos, relacionando-as com a realidade brasileira. O objetivo é identificar as melhores práticas internacionais e adaptá-las ao contexto nacional, propondo medidas que possam aumentar a resiliência do modelo brasileiro.

A abordagem começa com a revisão das medidas específicas de cada país estudado nos capítulos anteriores. O Reino Unido, sendo um HUB crucial para a conectividade na Europa, possui um dos modelos mais robustos de proteção de cabos submarinos. A insularidade e a dependência de cabos para comunicação externa forçaram o Reino Unido a desenvolver uma estratégia integrada que inclui monitoramento contínuo, colaboração com aliados, e uma legislação forte para proteção das ICPM. O país atualizou suas estratégias, identificou suas vulnerabilidades e ampliou a cooperação interna e externa, bem como seu sistema de monitoramento, principalmente no contexto OTAN, tendo sido criado um centro de monitoramento combinado. Dos países estudados, foi o único que investiu na aquisição de navios especializados na vigilância de cabos submarinos.

A Noruega, por sua vez, tem focado na proteção de suas ICPM devido à sua dependência do setor energético e às ameaças emergentes no Ártico, tendo sido um dos países que mais tiveram avarias em seus cabos submarinos sem identificação de responsáveis, entretanto, com indícios de terem sido causados por fatores humanos. O País adota medidas que incluem tanto vigilância, quanto a cooperação internacional, especialmente no contexto da OTAN e países componentes do JEF, sendo o Reino Unido um dos que mais contribui nessa cooperação.

A União Europeia, ao contrário, possui a realidade de uma abordagem mais fragmentada, com cada Estado-membro implementando suas próprias políticas. No entanto, a crescente conscientização sobre as vulnerabilidades na infraestrutura digital tem levado a um aumento da cooperação entre os países-membros e a implementação de diretrizes comuns para a proteção dos cabos submarinos. Exemplo dessa crescente conscientização é o próprio Parlamento Europeu ter se

preocupado em encomendar o estudo para verificar o grau de resiliência dos cabos submarinos do bloco. E embora exista a fragmentação nos países membro com medidas isoladas, algumas ferramentas institucionais e fóruns de segurança marítima já existentes poderão ser otimizados para uma melhor gestão e incluírem o tema de segurança dos cabos submarinos na UE.

Outro fator em comum a diversos países europeus é a proximidade do que eles consideram como ameaça, a Rússia, especialmente os que compartilham fronteiras terrestres ou marítimas com ela, tendo uma influência significativa no incremento dos sistemas de proteção marítima na Europa. Essa proximidade geopolítica, combinada com a postura assertiva da Rússia em questões de segurança e defesa, tem levado muitos países europeus a reforçarem suas infraestruturas de segurança marítima, incluindo a proteção de cabos submarinos.

Primeiramente, a Rússia é vista por muitos países europeus como uma potência que pode representar uma ameaça potencial, seja por meio de ações militares convencionais ou de estratégias de guerra híbrida, que incluem ciberataques e sabotagem de infraestruturas críticas. A anexação da Crimeia em 2014 e a intervenção militar na Ucrânia, por exemplo, reforçaram essas preocupações, levando a uma intensificação das medidas de segurança na Europa.

Os cabos submarinos, sendo vitais para a comunicação e economia global, são particularmente vulneráveis a essas ameaças. A Rússia tem investido significativamente em capacidades submarinas, incluindo submarinos especializados em operações de fundo do mar, que poderiam teoricamente ser usados para interceptar ou cortar cabos submarinos em caso de conflito. A presença dessas capacidades russas nas proximidades das águas europeias impulsionou a necessidade de incrementar as defesas desses ativos críticos.

Em resposta, países europeus, especialmente os do norte da Europa e os membros da OTAN, têm reforçado seus sistemas de vigilância e proteção marítima. Isso inclui o aumento das patrulhas navais, a instalação de sensores submarinos para detectar movimentos suspeitos, e o desenvolvimento de novas tecnologias para monitorar a integridade dos cabos submarinos. Além disso, a cooperação entre países europeus e a OTAN foi intensificada, resultando em exercícios conjuntos e em uma maior troca de informações de inteligência.

Quando comparadas com o Brasil, as medidas adotadas na Europa revelam uma série de desafios e oportunidades. O Brasil, com sua vasta extensão territorial e

litoral, depende fortemente dos cabos submarinos para a sua conectividade com o resto do mundo. Entretanto, a proteção dessas infraestruturas no país ainda é insuficiente. O arcabouço legal e as políticas de defesa para ICPM no Brasil, estão estruturadas principalmente para o setor energético, óleo e gás, mesmo assim ainda em crescimento, pois carecem de uma maior sensibilização dos diversos atores envolvidos ao tema.

A dificuldade inerente à propriedade dos cabos é praticamente a mesma aqui e nos países estudados. O modelo de propriedade dos cabos foi uma herança dos primeiros cabos telegráficos, o setor privado domina a gestão de instalação e uso dos cabos submarinos de fibra ótica. Entretanto sua resiliência e proteção transborda para os governos, que em sua maioria, identificaram a necessidade de uma política de proteção dos mesmos.

Diante desse cenário, propõe-se um conjunto de medidas para aumentar a resiliência do modelo brasileiro. Primeiramente, é essencial que o Brasil adote uma legislação específica para a proteção de cabos submarinos. Embora o Brasil tenha editado uma política, uma estratégia e um plano nacional de segurança das infraestruturas críticas, o que pode ser considerado um grande avanço no sentido de criar uma mentalidade da proteção, o grande desafio é cumprir o que já está disposto nesses normativos. Como por exemplo, promulgar os documentos decorrentes, como os planos setoriais, previstos no PLANSIC, que até o momento não foram expedidos.

Além disso, o estabelecimento de parcerias internacionais e o fortalecimento da cooperação regional no âmbito sul-americano são fundamentais para garantir uma resposta rápida e eficaz a incidentes. Por exemplo, alguns cabos submarinos da Argentina e Uruguai passam pelo HUB no Brasil para sua conexão com outros continentes, assim, incentivar a cooperação e troca de informações entre esses parceiros é fundamental.

Outro elemento bastante fomentado na Europa é a capacidade de monitoramento em proveito da segurança marítima e de forma particular em proveito das ICPM. A exemplo da instalação de novo centro da OTAN no Reino Unido em Nothwood, e a iniciativa da EU em estudos para inclusão do tema de segurança dos cabos submarinos nos mandatos da European Maritime Safety Agency (EMSA) e da Frontex, aproveitando assim, suas respectivas infraestruturas de vigilância e monitoramento.

O paralelo no Brasil é o SISGAAZ, que foi projetado para integrar uma ampla gama de sensores, radares, sistemas de vigilância e plataformas navais, aéreas e espaciais, permitindo uma visão abrangente e em tempo real das atividades na ZEE do Brasil. Ao ser plenamente implementado, poderá desempenhar um papel crucial contribuindo no monitoramento de ameaças aos cabos submarinos que cruzam as águas jurisdicionais brasileiras.

Ao analisarmos o conceito estratégico do SISGAAZ, com arquitetura para integrar diversos sistemas colaborativos e sensores que irão obter dados não colaborativos, ampliando assim, a consciência situacional da MB e melhorando a gestão da segurança marítima nas AJB. Adicionalmente, seu conceito de integração e conexão com outros órgãos corrobora com a mesma visão estratégica dos países estudados, buscar monitorar as áreas de interesse e a cooperação para uma melhor efetividade nas ações mitigadoras às ameaças, reduzindo assim as vulnerabilidades.

No conceito do sistema, é nítida a preocupação da cooperação com órgãos também responsáveis com ICPM, principalmente no setor de óleo e gás. E como visto na EDM, as áreas com prioridade para serem beneficiadas com a instalação de sistemas ativos de monitoramento são aquelas com maiores ICPM instaladas ou com potencial para uma futura instalação, como já comentado a exemplo da Bacia de Santos, margem equatorial e elevação do Rio Grande.

A despeito dos obstáculos que a implantação do sistema vem encontrando ao longo dos anos, existe o planejamento de instalação de sensores de forma faseada priorizando algumas áreas ao longo do litoral. Para uma contribuição mais efetiva à proteção dos cabos submarinos, o ideal é que sua cobertura alcance as áreas críticas, como os HUB existentes no litoral do Brasil como Rio de Janeiro, Santos, Salvador e Fortaleza, sendo este último o mais importante da rede.

Tendo em vista o já estudado nesse trabalho, é válido reconhecer que as áreas com elevada concentração de cabos submarinos nas AJB sejam também priorizadas para um incremento da vigilância. Como contribuição desse trabalho, sugere-se que essas áreas sejam também incluídas no planejamento de ampliação de cobertura do sistema. Tal medida poderá visualizar as atividades anômalas e contribuir na segurança marítima dos cabos submarinos.

Entretanto é relevante ressaltar a importância desse projeto estratégico e como sua arquitetura e conceito de integração e cooperação estão alinhados com as boas práticas de segurança marítima em diversos países, muitos deles também em

processo de implementação e melhoria de gestão para otimizar seus recursos e melhor resposta aos usuários.

A sensibilização para o assunto é algo verificado com o nível de cooperação entre instituições. Como verificado em outros países, é essencial a cooperação entre instituições e empresas privadas, que geralmente são donas e operadoras dos cabos submarinos. Assim, governo e empresas precisam trabalhar em conjunto para garantir a segurança física e cibernética desses ativos. A colaboração permite o desenvolvimento de padrões de segurança, práticas de mitigação de riscos e respostas coordenadas a emergências.

No sentido de sensibilização e cooperação entre instituições, aqui no Brasil a MB recentemente deu um grande passo quando planejou e executou um exercício de proteção de cabos no litoral do Rio de Janeiro. Em seu planejamento diversos níveis de cooperação foram trabalhados, contribuindo para um incremento da mentalidade de proteção desses ativos e reflexão das possibilidades de melhoria no tema. O exercício ocorreu em maio do corrente ano. De forma inédita, navios, mergulhadores escafandristas, tropas de operações especiais, navios e embarcações do Comando em Chefe da Esquadra, realizaram um treinamento de defesa desses ativos. Além do foco nas infraestruturas críticas submarinas, a Força-Tarefa também aprestou as ações voltadas às estações terrestres de cabos submarinos, no litoral do Rio de Janeiro, inclusive com a utilização de drone de superfície (NOMAR ONLINE, 2024).

O treinamento foi coordenado pelo Comando Naval de Operações Especiais a bordo de um Navio de Socorro Submarino e contou com a participação de diversas organizações da Marinha do Brasil. Adicionalmente, participaram da missão: Gabinete de Segurança Institucional, Agência Nacional de Telecomunicações, Agência Nacional de Comunicações – Portugal, Empresa de Telecomunicações Claro, Instituto Chico Mendes de Conservação de Biodiversidade e o Comando de Defesa Cibernética.

Essa iniciativa demonstra um incremento no grau de sensibilização para o tema de proteção dos cabos submarinos. Embora diversas ações ainda devam ser tomadas, foi um marco para que normas e procedimentos sejam aperfeiçoados e a interoperabilidade e cooperação entre instituições seja uma realidade para esse tema e diversos outros relativos à segurança marítima. E com certeza foi uma

oportunidade para identificarem processos a serem melhorados e vulnerabilidades a serem mitigadas.

Uma diferença latente entre os países estudados e o Brasil, é a sensação de ameaça aos cabos submarinos. A presença de navios e submarinos russos em suas águas jurisdicionais ou próximo delas faz com que os países europeus tomem medidas mais contundentes de proteção como visto anteriormente. A capacidade tecnológica que a Rússia possui para afetar esses ativos submarinos e seu protagonismo no ambiente submarino, inteligência naval e mais recentemente em guerra híbrida e cibernética a qualifica como a grande ameaça na Europa, principalmente nesse ambiente submarino. Mas vale ressaltar que qualquer país com capacidade tecnológica e com intenções antagônicas pode se tornar uma ameaça.

Entretanto, mesmo estando distante do Mar do Norte, o Brasil é um *player* internacional em diversas áreas em um mundo conectado, e proteger as ICPM já se mostrou extremamente importante. Podemos relembrar a presença em águas jurisdicionais brasileiras do navio oceanográfico russo Yantar em 2020, que gerou cuidados e reações das autoridades como estudado anteriormente.

O Brasil possui uma grande rede de ICPM instalada na área de petróleo e gás, com potencial para expansão, considerando sua área da margem equatorial. Além disso, possui projetos de instalação de fazendas eólicas off-shore, com consequente instalação de novas infraestruturas críticas, tornando o país cada vez mais um protagonista em segurança energética no mundo.

A elevação do Rio Grande possui potencial para, em breve, ser uma referência mundial na exploração mineral e consequentemente instalação de novas ICPM. Soma-se a vocação do país para continuar sendo uma referência mundial em segurança alimentar, assim, continuar nos holofotes das grandes potências.

Todas essas infraestruturas *in-shore* e *off-shore*, estão conectadas com os interesses de parceiros estratégicos por meio dessa imensa rede global em que os cabos submarinos são as estruturas vitais. O Brasil deve desenvolver cada vez mais estratégias de segurança marítima à sua realidade geopolítica e econômica, garantindo a segurança e a resiliência de suas infraestruturas críticas submarinas.

Assim, mesmo distante das ameaças consideradas pelos países estudados, verificamos que o Brasil desperta interesse internacional. A natural vocação do país para os setores alimentar e energético, somada as áreas de nossa Amazônia Azul

com potencial para crescimento e exploração de riquezas e consequente instalação de novas ICPM, qualifica o Brasil a se dedicar ainda mais à proteção de suas infraestruturas críticas. E, não menos importante, incluir os cabos submarinos como ativos a serem também protegidos.

8 – CONCLUSÃO

Após a revisão da literatura e conceitualização dos cabos submarinos enquanto objeto de atenção da segurança marítima, percebe-se que estes são parte sensível das ICPM e desempenham um papel vital na infraestrutura global de comunicação e economia. Esses cabos são responsáveis por cerca de 99% das comunicações transoceânicas, incluindo a transmissão de dados da internet, chamadas telefônicas e transações financeiras internacionais. A ameaça aos cabos submarinos é de caráter estratégico, sendo alvos potenciais de acidentes e de ataques físico ou cibernético.

Ao examinar as estratégias de alguns países na busca por uma maior resiliência e proteção dos cabos submarinos, podemos depreender que há uma busca para estender o controle marítimo ao ambiente submarino e para isso, há uma determinação nas seguintes atividades: desenvolver conhecimento, monitorar, agir e cooperar. Ou seja, conhecer suas vulnerabilidades e ameaças, monitorar seu funcionamento e estruturas componentes, tomar medidas de proteção e reparo necessárias para a manutenção do seu funcionamento pleno, em um ambiente cooperativo de troca de informações e divisão de responsabilidades.

Ainda sobre desenvolvimento de conhecimento, após verificar as melhores práticas nos países estudados e nas boas iniciativas no Brasil, observamos que a implementação e atualização de legislações nacionais para a proteção de cabos submarinos é de vital importância, pois permitirá conhecer melhor as vulnerabilidades do sistema, as principais ameaças e assim definir responsabilidades para todos os atores envolvidos. Isso facilita uma resposta mais rápida e eficaz a incidentes, como ataques cibernéticos ou ações maliciosas.

Como estudado, embora as legislações internacionais forneçam uma base para a proteção e o uso de cabos submarinos, essas leis são insuficientes para lidar com desafios específicos que variam de acordo com a jurisdição e os interesses de cada país. Portanto, a legislação nacional permite que os países adaptem as diretrizes internacionais às suas necessidades e contextos específicos.

O desenvolvimento de conhecimento também é permeado com o uso de novas tecnologias e meios para permitir a segunda atividade, o monitoramento. O correto monitoramento é essencial para a manutenção da segurança marítima, proteção da soberania, e promoção do desenvolvimento econômico sustentável. Ao

garantir a vigilância contínua das áreas de interesse, pode-se prevenir e mitigar ameaças, proteger seus recursos e infraestruturas críticas.

O programa estratégico de consciência situacional marítima da MB, o SisGAAz, foi concebido como um sistema de monitoramento e controle relacionado ao conceito internacional de segurança marítima para a proteção do litoral brasileiro, projetado para se tornar o principal sistema de comando e controle da Marinha, possibilitando a gestão das atividades ligadas ao mar que envolvam vigilância, monitoramento, prevenção da poluição, recursos naturais, entre outras. Ainda em implantação, merece receber implementações em seu projeto para cobrir áreas onde os principais HUB de cabos submarinos estejam instalados. Devido a sua arquitetura, será um sistema em que irá colaborar com a outra importante atividade, a cooperação.

A cooperação internacional e interagências é essencial para a gestão e proteção eficaz dos cabos submarinos. A colaboração entre países permite uma abordagem coordenada para proteger uma infraestrutura crítica que transcende fronteiras, enquanto a cooperação interagências garante que as diversas capacidades e expertise dentro de um país sejam utilizadas de forma integrada.

No Brasil o GSI-PR, órgão competente para acompanhamento dos assuntos pertinentes às infraestruturas críticas no âmbito da administração pública federal, coordena Grupos Técnicos de Segurança de Infraestruturas Críticas, que são compostos por representantes dos setores público e privado. Adicionalmente, é o órgão responsável pelo Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, cujas informações contidas ainda são geridas exclusivamente internamente naquele órgão. Futuramente, existe a previsão de acesso seletivo pelos representantes de outros órgãos de acordo com a necessidade de conhecimento. Ampliando assim, a integração e cooperação no tema. essas formas de cooperação fortalecem a resiliência dos cabos submarinos, assegurando a continuidade das comunicações globais.

Por fim, ao mencionarmos as ações para aumentar a resiliência e segurança dos cabos, estão envolvidas desde atividades de monitoramento, patrulha naval e marítima, exercícios de proteção até ações de manutenção e reparos.

A iniciativa da MB em realizar o primeiro exercício de proteção de cabos submarinos em 2024, constitui-se em um marco na busca de cooperação com demais Órgãos e Agências nacionais para o aumento do conhecimento sobre o

tema e para contribuir para a proteção dos cabos submarinos brasileiros. Criar no nível operacional e tático Procedimentos Operativos Padronizados, desenvolver Táticas técnicas e Procedimentos para a contraposição de ameaças, permitindo assim, a toda estrutura de proteção a essas infraestruturas críticas, rever a legislação vigente e planos decorrentes, criar procedimentos, contribuindo assim para uma mentalidade de proteção.

Concluindo, o ambiente submarino é uma área estratégica crucial, tanto para operações militares quanto para atividades econômicas. Ele inclui tudo o que está abaixo da superfície do mar, desde águas costeiras até as profundezas oceânicas, e abriga recursos naturais valiosos como petróleo, gás e minerais, além de ser a rota por onde passam os cabos submarinos de comunicação. Esses ativos no fundo do oceano sustentam as comunicações digitais que definem a nossa era, são hoje fundamentais para o tráfego de dados global em um mundo cada vez mais conectado. Conhecê-lo bem, monitorá-lo e protegê-lo são desafios para os estados costeiros que não podem ser negligenciados.

REFERÊNCIAS

ANATEL - Agência Nacional de Telecomunicações, **Cabos Submarinos,** 2022. Disponível em: https://www.gov.br/anatel/pt-br/dados/infraestrutura/cabos-submarinos. Acessado em 07 de junho de 2024.

AUSTRÁLIA, **The Quad.** 2024.Disponível em: https://www.dfat.gov.au/international-relations/regional-architecture/quad. Acessado em 10 de julho de 2024.

AVERRE, D. **Undersea cable connecting Norway and Arctic satellite station is mysteriously damaged**, Mail Online, 2022. Disponível em: https://www.dailymail.co.uk/news/article-10390555/Undersea-cable-connecting-Norway-Arctic-satellite-station-mysteriously-damaged.html . Acessado em 10 de junho de 2024.

BORGER, J. **Nord Stream attacks highlight vulnerability of undersea pipelines in west,** The Guardian, 29 de setembro 2022. Disponível em: https://www.theguardian.com/business/2022/sep/29/nord-stream-attacks-highlight-vulnerability-undersea-pipelines-west. Acessado em: 20/04/2023.

BOYD, A. **The security of subsea cables: an enduring naval challenge**. 2022. Disponível em : https://www.maritimefoundation.uk/publications/maritime-2023/the-security-of-subsea-cables-an-enduring-naval-challenge/. Acessado em 18 de julho de 2024.

BRASIL. Decreto nº 10.569, de 09 de dezembro de 2020. **Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas**, 2020b.

BRASIL. Decreto nº 11.200, de 15 de setembro de 2022. **Aprova o Plano Nacional de Segurança de Infraestruturas Críticas**. 2022

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. **Aprova a Política Nacional de Segurança de Infraestruturas Críticas.** 2018

BRASIL., **Estratégia De Defesa Marítima.** Brasília, DF: Ministério da Defesa, 2023a

BRASIL., **Fundamentos de Doutrina Marítima.** Brasília, DF: Ministério da Defesa, 2023b

BRASIL., **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2020a

BUEGER, C.; LIEBETRAU, T.; FRANKEN, J. **Security threats to undersea communications cables and infrastructure – consequences for the EU**. IN-DEPTH ANALYSIS, Brussels European Union, 2022.

CEMBRA-Centro de Excelência para o Mar Brasileiro**, O Brasil e o mar no século XXI: Relatório aos tomadores de decisão do País**, 3ªedição, Quiteriense Serviços gráficos e editoriais. Rio de Janeiro, 2022.

CHIAPPA, C., NGENDAKUMANA, P. **Everything indicates Chinese ship damaged Baltic pipeline on purpose, Finland says,** POLITICO, 2023. Disponível em: https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/. Acessado em 30 de julho de 2024.

ENISA- The European Union Agency for Cybersecurity. ***Subsea Cables - What is at Stake?*** **European Union Agency for Cybersecurity,** 2023. Disponível em: https://www.enisa.europa.eu/publications/subsea-cables-what-is-at-stake. Acessado em: 06 ago. 2024.

FREIRE, A.; AQUINO, V., **Por uma política de Segurança Nacional para a infraestrutura de cabos submarinos**, 2023. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/conselheiros-da-anatel-publicam-artigo-sobre-politica-de-seguranca-nacional-para-a-infraestrutura-de-cabos-submarinos. Acessado em 06 de agosto de 2024.

GODZIMIRSKI, J.M., **Protection of critical infrastructure in Norway – factors, actors and systems**, Security and Defence, vol. 39, 2022. Disponível em: https://securityanddefence.pl/. Acessado em 07 de julho de 2024.

GOZZI, L. **Nord Stream: Denmark closes investigation into pipeline blast**, BBC News, 26 February 2024. Disponível em: https://www.bbc.com/news/world-europe-68401870. Acessado em 10 de junho de 2024.

HENDRIKS, M. S.; HALEM, H. **From space to seabed, Protecting the UK's undersea cables from hostile actors**, Policy Exchange 2024, Disponível em :www.policyexchange.org.uk. Acessado em 11/05/2024.

HUMPERT, M., **Nord Stream Pipeline Sabotage Mirrors Svalbard Cable Incident,** ICPC - INTERNATIONAL CABLE PROTECTION COMMITTEE. Disponível em: https://www.iscpc.org/. Acessado em: 18 ago. 2024.

KAR-GUPTA, S**. European states sign pledge to protect North Sea infrastructure.** Reuters, 2024. Disponível em: https://www.reuters.com/world/europe/european-states-sign-pledge-protect-north-sea-infrastructure-2024-04-09/. Acessado em: 12 de maio de 2024.

KAUSHAL, S. **Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure**. RUSI. 2023. Disponível em https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure. Acessado em 30 de julho de 2024.

KAVANAGH, C. **Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour**. Geneva, Switzerland: UNIDIR, 2023.

LAMPERT, J.A.A. **Sistema de Gerenciamento da Amazônia Azul: A importância estratégica e o aprimoramento**, 2024. Disponível em: https://www.marinha.mil.br/sisgaaz-protecao-e-monitoramento-das-aguas-jurisdicionais-

brasileiras#:~:text=O%20SisGAAz%20%C3%A9%20um%20Programa,para%20a%20gera%C3%A7%C3%A3o%20de%20empregos. Acessado em 15 de julho de 2024.

MB - Marinha do Brasil, **COMPAAz – Comando de Operações Marítimas e Proteção da Amazônia Azul,** 2024, Disponível em: https://www.marinha.mil.br/compaaz/?q=node/156. Acessado em 10 de julho de 2024.

MONAGHAN, S.; SVENDSEN, O.; DARRAH, M. **NATO's Role in Protecting Critical Undersea Infrastructure**, Center for Strategic and International Studies (CSIS) 2023. Disponível em: https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure. Acessado em 10 de junho de 2024.

MONTEIRO, T. **Navio russo suspeito de espionagem coloca Marinha brasileira em alerta**, O Estado de São Paulo, 21 de fevereiro de 2020.

NATO- North Atlantic Treaty Organization Parliamentary Assembly, **Protecting Critical Maritime Infrastructure – The Role Of Technology** Science and technology committee, 2023.

NATO- North Atlantic Treaty Organization. **NATO's Role in Protecting Critical Undersea Infrastructure**. Communications and Information Agency, 2023.

NAVYLOOKOUT, **Analysis: Royal Navy deploys seven ships on underwater infrastructure patrols**. 2023. Disponível em: https://www.navylookout.com/analysis-royal-navy-deploys-seven-ships-on-underwater-infrastructure-patrols/. Acessado em 11 de maio de 2024.

NEWDICK T. **Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut.** The War Zone News & Features, High North News, 29 setembro de 2022. Disponível em: https://www.twz.com/43094/norwegian-undersea-surveillance-network-had-its-cables-mysteriously-cut. Acessado em 01 de julho de 2024.

NOMAR ONLINE, **Marinha realiza exercício de proteção aos cabos submarinos brasileiros na área do Rio de Janeiro**, 2024. Disponível em: https://www.marinha.mil.br/sites/all/modules/nomarn957/book.html. Acessado em 25 de julho de 2024.

NORUEGA. Ministry of Defence. ***The Norwegian Defence Pledge: Long-term Defence Plan 2025–2036***. Disponível em: https://www.regjeringen.no/en/dokumenter/the-norwegian-defence-pledge/id3032809/?ch=1\ Acesso em: 05 de julho 2024.

ODNI - OFFICE *of the* DIRECTOR *of* NATIONAL INTELLIGENCE, **Five Eyes Intelligence Oversight and Review Council (FIORC)**, 2024. Disponível em: https://www.dni.gov/index.php/who-we-are/organizations/enterprise-capacity/chco/chco-related-menus/chco-related-links/recruitment-and-outreach/217-about/organization/icig-pages/2660-icig-fiorc . Acessado em: 20 de julho de 2024.

OSBORNE S. **Russian ship 'spying' around wind farms off UK coast in possible sabotage plot**. SKY NEWS. Dsiponível em: https://news.sky.com/story/russian-ship-spying-around-wind-farms-off-uk-coast-in-possible-sabotage-plot-12861217. Acessado em 10 de junho de 2024.

PAPAPAVLOU, C.; PAXIMADIS, K.; UZUNIDIS, D.; TOMKOS, I. **Toward SDM-Based Submarine Optical Networks: A Review of Their Evolution and Upcoming Trends**, Telecom, 2022

REINO UNIDO, **Joint statement by Joint Expeditionary Force ministers**, November 2023, Disponível em: https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-november-2023. Acessado em 06 de maio de 2024.

REINO UNIDO, **National Strategy for Maritime Security**, 2022. Disponível em: www.gov.uk/official-documents . Acessado em: 04 de abril de 2024.

REINO UNIDO. Prime Minister. ***Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*.** London: 2021. Disponível em: www.gov.uk/official-documents. Acessado em: 04/04/2024.

ROYAL NAVY NEWS, **Royal Navy and RAF track Russian vessels in waters close to the UK**, 2023. Disponível em: https://www.royalnavy.mod.uk/news/2023/august/31/230831-portland-and-tyne-track-russian-ships Acessado em 05 de maio de 2024.

ROYAL NAVY, **RFA Proteus is the first of a new generation of survey and surveillance ships harnessing leading-edge technology and dedicated to monitoring underwater in areas of UK sovereign interest**. 2024. Disponível em: https://www.royalnavy.mod.uk/organisation/units-and-squadrons/support-ships/rfa-proteus. Acessado em: 05 de agosto de 2024.

SERRANO, E.; PORCHÉRA, P., **Infraestruturas Críticas de Comunicações: Uma Análise Sobre Cabos Submarinos no Brasil**, Trabalho de Conclusão de Curso, Escola Superior de Defesa, 2023.

SUNAK, R., Undersea Cables: Indispensable, insecure, Policy Exchange, 2017, Disponível em: www.policyexchange.org.uk, acessado em 11/05/2024.

TELEGEOGRAPHY. **Submarine Cable Map**, 2023. Disponível em: https://www.submarinecablemap.com/#/submarine-cable/south-atlantic-cable-system-sacs. Acessado em: 29 maio 2024.

WROE, D. **Australia refuses to connect to undersea cable built by Chinese company**. The Sydney Morning Herald, 2017. Disponível em: https://www.smh.com.au/politics/federal/australia-refuses-to-connect-to-undersea-cable-built-by-chinese-company-20170726-gxj9bf.html. Acessado em 29 de julho de 2024.

APÊNDICE A - ENTREVISTA COM OFICIAL ASSESSOR MILITAR DO GABINETE DE SEGURANÇA INSTITUCIONAL – GSI.

Perguntas referente a alguns itens das normas: Estratégia Nacional de Segurança de Infraestruturas Críticas e Plano Nacional de Segurança de Infraestruturas Críticas

ESTRATÉGIA NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

3.1.2. Estimular a elaboração de planos de prevenção e resposta coordenadas das infraestruturas críticas.

Pergunta: Existe plano de prevenção e resposta coordenada?

Resposta: Hoje, as Normas existentes na temática de SIC são a PNSIC, ENSIC e PLANSIC que não possuem esse nível de atuação. Futuramente, após a criação do CNSIC, serão confeccionados pelos Ministérios Responsáveis, conforme preconizado pelo PLANSIC, os planos setoriais para cada setor. O GSI-PR é responsável, de acordo com o art. 2 do PNSIC, pelo acompanhamento dos assuntos pertinentes às infraestruturas críticas no âmbito da Administração Pública Federal.

3.4.1. Estabelecer no Plano Nacional de Segurança de Infraestruturas Críticas a previsão de elaboração de Planos Setoriais de segurança de infraestruturas críticas, sob responsabilidade dos órgãos e das entidades envolvidos....

(...PLANO NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS)

DISTRIBUIÇÃO DAS RESPONSABILIDADES ENTRE OS MINISTÉRIOS PARA A ELABORAÇÃO DOS PLANOS SETORIAIS DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

ÁREA PRIORITÁRIA	SETOR	MINISTÉRIO RESPONSÁVEL*
Comunicações	Telecomunicações	Ministério das Comunicações
	Radiodifusão	
	Serviços Postais	
Defesa	Defesa	Ministério da Defesa

Pergunta: Existe plano setorial do Ministério das comunicações que aborde o tema cabos submarinos? Existe plano setorial do ministério da Defesa? Caso sejam ostensivos, consulto possibilidade disponibilizar.

Resposta: Hoje não possuímos nenhum plano setorial que aborde proteção à cabos submarinos pois os planos setoriais não foram confeccionados pelos Ministérios

Responsáveis. Recentemente, no final do mês de maio, a Marinha do Brasil realizou o primeiro exercício de proteção a cabos submarinos com a finalidade de estabelecer doutrinas e protocolos de proteção a esta importante infraestrutura crítica.

4.1. Promover, no âmbito da administração pública e do setor privado, a geração, a disponibilização e a atualização periódica de dados íntegros, consistentes e padronizados sobre infraestruturas críticas e ameaças.

Pergunta: Quais ações para estreitar a cooperação entre o setor público e privado (proprietários das ICPM, como cabos submarinos)?

Resposta: Hoje, o GSI-PR coordena Grupos Técnicos de Segurança de Infraestruturas Críticas, que são compostos por representantes dos setores público e privado, onde, de acordo com a metodologia aplicada, ocorre o estudo para levantamento das infraestruturas críticas do setor de telecomunicações; identificação de ameaças, vulnerabilidades e medidas de controle; gerenciamento de riscos; além da confecção de um Diagnóstico Nacional para o setor e análise de interdependências. Além disso, através do Grupo Técnico da qual fazem parte, entre outros, o Ministérios das Comunicações, a Anatel e a Conexis (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal) é estabelecida uma rede de contato que é utilizada como uma ferramenta facilitadora para trâmite de informações e demandas ao GSI-PR, que faz o papel de articulação com os demais Órgãos e Instituições de Governo.

Cabe salientar que, apesar do SIDSIC ainda não estar funcionando em sua plenitude, existe a perspectiva de que, no futuro, ele seja uma ferramenta de integração de dados subsidiando o acompanhamento e monitoramento permanente da Segurança das Infraestruturas Críticas do País, como auxílio à tomada de decisão pelos Órgãos aderentes.

PLANO NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

“Assim, o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas será a estrutura operacional que irá subsidiar o acompanhamento e monitoramento permanente da Segurança das Infraestruturas Críticas do País, identificadas nos diversos setores. Como órgão articulador da atividade de Segurança de Infraestruturas Críticas, o Gabinete de Segurança Institucional da Presidência da República orientará o desenvolvimento e a implantação desse Sistema, ...”

Pergunta: Qual a estrutura do Sistema Integrado de Dados de Segurança de Infraestruturas Críticas? Quais órgãos fazem uso do sistema para troca de informações e cooperação interagência?

Resposta: O SIDSIC é um sistema que atua como um banco de dados acerca das informações das infraestruturas críticas dos 14 setores aderentes ao tema de Segurança de Infraestruturas Críticas. A estrutura contempla o conteúdo mínimo previsto conforme art. 11° do PNSIC.

As informações contidas no aludido sistema são consideradas sensíveis e estão restritas aos assessores do GSI. Futuramente, existe a previsão de ocorrer acesso seletivo dos representantes dos Órgãos de acordo com a necessidade de conhecimento.

Para a governança das atividades de Segurança de Infraestruturas Críticas no âmbito da administração pública federal e com vistas a atender ao objetivo estratégico da Estratégia Nacional de Segurança de Infraestruturas Críticas de estabelecer uma estrutura de governança, será criado o Comitê Gestor de Segurança de Infraestruturas Críticas. Esse Comitê Gestor será composto por um conjunto de órgãos responsáveis por articular, orientar, propor e gerir a implementação de ações relacionadas à Segurança das Infraestruturas Críticas, o qual buscará, inclusive, assegurar o cumprimento das metas estabelecidas neste Plano

Pergunta: Como se constitui o Comitê Gestor de Segurança de Infraestruturas Críticas?

Resposta: Esse Comitê Gestor de Segurança de Infraestruturas Críticas será chamado por outro nome, Comitê Nacional de Segurança de Infraestruturas Críticas (CNSIC). A atualização do PLANSIC que está ocorrendo devido à reestruturação Ministerial contempla esta alteração.

O CNSIC será composto por Ministérios e Órgãos da Administração Pública Federal com aderência ao tema, assim como é feita a composição dos GTSIC. O CNSIC ainda está em fase de aprovação.

Nome: CF Marcelo Pereira da Rocha Gonçalves

Função: Assessor Militar no GSI-PR

(encarregado pelas respostas)