ESCOLA DE GUERRA NAVAL

CC CARLOS ROBERTO BITTENCOURT DE ARAÚJO SILVA

DEFESA CIBERNÉTICA E INFRAESTRUTURAS CRÍTICAS:
Uma Análise das Vulnerabilidades dos Cabos Submarinos.

Rio de Janeiro

2024

CC CARLOS ROBERTO BITTENCOURT DE ARAÚJO SILVA

DEFESA CIBERNÉTICA E INFRAESTRUTURAS CRÍTICAS:
Uma Análise das Vulnerabilidades dos Cabos Submarinos.

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

Orientador: CC Roberto Pimenta

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.

Documento assinado digitalmente
gov.br
CARLOS ROBERTO BITTENCOURT DE ARAUJO S
Data: 12/11/2024 23:30:01-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTO

Agradeço a Deus, por Sua infinita misericórdia e por me conceder o dom da vida, além de todas as bênçãos recebidas ao longo da minha jornada.

Aos meus queridos pais, Antônio (in memoriam) e Rosalina (in memoriam), expresso minha eterna gratidão pelo amor, carinho e exemplo de vida que sempre me proporcionaram. Durante a elaboração deste trabalho, perdi minha mãe, Rosalina, cuja ausência deixou uma profunda saudade. Sua memória é um farol de coragem para mim.

Aos meus irmãos, Júnior, Rita e Luiz, agradeço profundamente pelo convívio durante nossa infância, que moldou minha formação, e pelo cuidado dedicado aos nossos pais enquanto estive ausente, servindo a Marinha do Brasil e residindo em outros estados.

Aos meus filhos, Joaquim e Diana, expresso meu eterno amor e gratidão. Vocês são a luz da minha vida e o motivo pelo qual continuo a me esforçar e crescer. Mesmo jovens, entenderam e respeitaram os momentos em que precisei me ausentar para me dedicar a este trabalho. Suas risadas, abraços e palavras carinhosas foram uma fonte constante de motivação e alegria.

À minha amada esposa, Beatriz, meu amor e gratidão sem fim. Você é a base que sustenta nossa família, minha companheira de vida e meu porto seguro. Sua presença constante e dedicação foram essenciais para que eu pudesse me concentrar neste trabalho. Seu papel em nossa família é insubstituível, e este trabalho é tanto seu quanto meu. Te amo profundamente.

Agradeço ao meu orientador, Capitão de Corveta Roberto Pimenta, por toda a ajuda e orientações valiosas ao longo deste trabalho. Sou grato por sua paciência e apoio contínuos, que me guiaram em cada etapa deste processo acadêmico.

Agradeço também à Escola de Guerra Naval pelos ensinamentos valiosos e pela oportunidade de crescimento pessoal e profissional. Sou grato a todos pelos conselhos e pelo exemplo de liderança, que serão levados comigo em minha carreira.

“AVIUM SCIENTIAM HOMINES DOCENTES”.

Autor desconhecido

RESUMO

Este estudo investiga as vulnerabilidades dos cabos submarinos no contexto das ameaças cibernéticas e seu impacto na segurança nacional do Brasil. Utilizando uma abordagem qualitativa descritiva, com revisão bibliográfica e análise documental, a pesquisa identifica que esses cabos, responsáveis por 95% das comunicações globais, são suscetíveis a danos físicos, espionagem e ataques cibernéticos. As principais vulnerabilidades incluem o uso de sistemas de gerenciamento remoto, a acessibilidade das estações de aterrissagem e a dependência de empresas privadas para reparos. Essas fragilidades comprometem a integridade das comunicações, a proteção de dados sensíveis e a estabilidade econômica, além de afetar operações militares. A crescente transmissão de dados, impulsionada pela pandemia de COVID-19, pela tecnologia 5G e pela computação em nuvem, agrava esses riscos. Conclui-se que as vulnerabilidades dos cabos submarinos podem ter consequências graves para o Brasil, incluindo interrupções nas comunicações, comprometimento de sistemas financeiros, colapsos no setor de saúde e impactos na defesa nacional, ressaltando a necessidade de uma defesa cibernética integrada e colaboração entre entidades governamentais e privadas.

Palavras-chave: Defesa Cibernética. Cabos Submarinos. Infraestrutura Crítica. Guerra Cibernética. Segurança Nacional. Brasil.

ABSTRACT

Cyber Defense and Critical infrastructure: an analysis of the vulnerabilities of submarine cables.

This study investigates the vulnerabilities of submarine cables in the context of cyber threats and their impact on Brazil's national security. Using a descriptive qualitative approach, with a literature review and documentary analysis, the research identifies that these cables, responsible for 95% of global communications, are susceptible to physical damage, espionage and cyber attacks. The main vulnerabilities include the use of remote management systems, the accessibility of landing stations and the dependence on private companies for repairs. These weaknesses compromise the integrity of communications, the protection of sensitive data and economic stability, as well as affecting military operations. Increased data transmission, driven by the COVID-19 pandemic, 5G technology and cloud computing, exacerbates these risks. It is concluded that the vulnerabilities of submarine cables can have serious consequences for Brazil, including interruptions in communications, compromise of financial systems, collapses in the health sector and impacts on national defense, highlighting the need for an integrated cyber defense and collaboration between government and private entities.

Keywords: Cyber Defense. Submarine Cables. Critical Infrastructure. Cyber Warfare. National Security. Brazil.

LISTA DE ABREVIATURAS E SIGLAS

Aç Rsp	−	Ações de Resposta
CDCiber	−	Centro de Defesa Cibernética
ComDCiber	−	Comando de Defesa Cibernética
CNUDM	−	Convenção das Nações Unidas sobre o Direito do Mar
END	−	Estratégia Nacional de Defesa
ENSIC	−	Estratégia Nacional de Segurança de Infraestruturas Críticas
ECS/Def	−	Equipe de Coordenação Setorial da Defesa
GSI/PR	−	Gabinete de Segurança Institucional da Presidência da República
GT-Ciber	−	Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica
MD	−	Ministério da Defesa
MDI	−	Medidas de Defesa Interna
PLANSIC	−	Plano Nacional de Segurança de Infraestruturas Críticas
PNCiber	−	Política Nacional de Cibersegurança
PND	−	Política Nacional de Defesa
PNSIC	−	Política Nacional de Segurança de Infraestruturas Críticas
ReGIC	−	Rede Federal de Gestão de Incidentes Cibernéticos
SIDSIC	−	Sistema Integrado de Dados de Segurança de Infraestruturas Críticas
SISMC2	−	Sistema Militar de Comando e Controle
SMDC	−	Sistema Militar de Defesa Cibernética
STIC2	−	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TI	−	Tecnologia da Informação
TIC	−	Tecnologia da Informação e Comunicações
ZEE	−	Zona Econômica Exclusiva

SUMÁRIO

1 INTRODUÇÃO

A invenção do telégrafo por Samuel Morse em 1837 revolucionou a comunicação à distância, permitindo o envio rápido de informações entre localidades distantes, inicialmente em terra e, posteriormente, entre continentes separados por oceanos. A primeira tentativa de instalação de um cabo telegráfico submarino ocorreu em agosto de 1850, conectando Dover, na Inglaterra, a Calais, na França. Este empreendimento inicial enfrentou desafios, como o corte do cabo possivelmente por pescadores, logo no dia seguinte à sua instalação, demonstrando desde cedo as vulnerabilidades dos cabos submarinos a interferências externas.

Em 1858, o pioneiro cabo telegráfico transatlântico foi lançado, conectando a América do Norte à Europa, uma conquista que permitiu a transmissão de algumas palavras por minuto. Já em 1956, o advento do TAT-1, o primeiro cabo telefônico transatlântico, marcou um avanço significativo, com a capacidade de transmitir 36 chamadas telefônicas simultâneas graças ao uso de amplificadores. Em 1988, o lançamento do TAT-8, o primeiro cabo de fibra óptica, trouxe uma capacidade exponencialmente maior, possibilitando até 40.000 chamadas simultâneas, refletindo um salto tecnológico na comunicação global.

Atualmente, cabos submarinos são responsáveis por aproximadamente 95% das comunicações globais de telefone e internet, tornando-se parte essencial da infraestrutura nacional e internacional. Essa importância estratégica também os torna alvos vulneráveis a ataques cibernéticos, que podem ser perpetrados por Estados-nação, terroristas ou agentes não estatais. No contexto das crescentes ameaças cibernéticas, onde tecnologias digitais são usadas para atacar e defender infraestruturas críticas, a segurança desses cabos se torna uma preocupação central para a segurança nacional.

A justificativa para este estudo é a crescente sofisticação e frequência dos ataques cibernéticos globalmente, aliada à dependência cada vez maior de infraestruturas críticas submarinas. A relevância deste estudo se destaca pelo papel crucial da Marinha do Brasil, como defensora dos interesses nacionais no domínio marítimo, que precisa identificar as ameaças cibernéticas e fortalecer as defesas dos cabos submarinos para prevenir interrupções, espionagem ou sabotagem que poderiam ter consequências desastrosas para o país.

Diante desse cenário, o objeto de estudo deste trabalho são as infraestruturas críticas submarinas, especificamente os cabos submarinos utilizados para telecomunicações. O objetivo deste trabalho é responder a seguinte questão: Quais são as vulnerabilidades dos cabos submarinos no contexto das ameaças cibernéticas e como essas vulnerabilidades impactam a segurança nacional do Brasil?

Para isso, o trabalho será dividido em cinco capítulos. Na sequência desta introdução, o segundo capítulo discutirá os fundamentos e as estratégias de defesa cibernética, enquanto o terceiro capítulo se concentrará nos cabos submarinos, analisando suas características e vulnerabilidades. O quarto capítulo confrontará a teoria da defesa cibernética com as vulnerabilidades dos cabos submarinos, culminando em conclusões apresentadas no quinto capítulo.

A metodologia adotada será uma abordagem descritiva qualitativa, utilizando revisão bibliográfica e análise documental, fundamentada na Doutrina de Defesa Cibernética Nacional. O próximo capítulo fornecerá uma base teórica para a análise subsequente das vulnerabilidades dos cabos submarinos Brasileiros.

2 FUNDAMENTOS DA DEFESA CIBERNÉTICA

Este capítulo teórico apresenta um panorama abrangente dos fundamentos da defesa cibernética. Dada a crescente dependência de infraestruturas críticas[1], como os cabos submarinos, e a intensificação de possíveis ameaças cibernéticas globais, torna-se essencial compreender os princípios, conceitos e diretrizes que norteiam a defesa cibernética nacional. Este capítulo explorará os conceitos básicos, princípios de emprego e características da defesa cibernética, proporcionando uma base sólida para entender as vulnerabilidades dos cabos submarinos frente a ameaça cibernética.

2.1 CIBERNÉTICA E DEFESA: CONCEITOS, EVOLUÇÃO E ESTRUTURAÇÃO

O termo "cibernética" foi introduzido por Norbert Wiener em sua obra "Cybernetics or Control and Communications in the Animal and Machine" (1948), onde é definida como a análise do controle e comunicação em sistemas mecânicos e organismos vivos. Esta disciplina inicialmente focava em sistemas de controle e *feedback*, aplicáveis tanto a mecanismos biológicos quanto a dispositivos eletrônicos (Wiener, 1948). Com o avanço tecnológico e as crescentes necessidades de segurança, o conceito de cibernética evoluiu. A Doutrina Militar de Defesa Cibernética de 2023 define cibernética como:

> [...] termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e suas interações. No campo da Defesa Nacional, inclui os recursos de Tecnologia da Informação e Comunicações (TIC) de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC²), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais. (Brasil, 2023a, p.16)

Outro conceito importante é o do espaço cibernético ou “ciberespaço”. Este termo foi popularizado por William Gibson, escritor de ficção científica, em seu romance “Neuromancer” publicado em 1984. No Glossário das Forças Armadas, o

[1]“Instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade”. (Brasil, 2018, art.1, inc.I)

espaço cibernético é definido como: “Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas” (Brasil, 2015, p.106). Esse conceito ganhou importância significativa, especialmente com a crescente interdependência das operações cibernéticas e as ações nos domínios de guerra tradicionais, como terra, mar, ar e espaço. Diante da característica do espaço cibernético, onde as ações defensivas e ofensivas podem complementar ou potencializar as ações dos outros domínios, o Brasil reconheceu esse ambiente como o quinto domínio operacional (Brasil, 2023a).

O espaço cibernético também recebeu atenção especial na Política Nacional de Defesa (PND), que destacou a necessidade de proteger o ciberespaço Brasileiro, essencial para a operação segura de sistemas de informação, administração e comunicação de importância nacional (Brasil, 2020b). A Estratégia Nacional de Defesa (END) reforçou essa importância ao destacar o setor cibernético como um dos três pilares tecnológicos essenciais para a Defesa Nacional, juntamente com os campos espacial e nuclear (Brasil, 2020a).

A END especifica que as capacidades no setor cibernético devem abranger um amplo espectro de emprego dual. Isso abrange as ferramentas de comunicação entre os diferentes setores das Forças Armadas, assegurando a interoperabilidade e a operação conjunta de forma segura. É crucial melhorar a Segurança das Comunicações e Informação, bem como a Cibersegurança com foco especial na proteção das Infraestruturas Críticas (Brasil, 2020a).

Após a implementação do setor Cibernético, definida pela END em 2008, foram criados três campos: a Guerra Cibernética, executada pelos Comandos Operacionais ativados e suas respectivas Forças Componentes; a Defesa Cibernética, gerenciada pelo Ministério da Defesa; e a Segurança Cibernética, dirigida pela Presidência da República (Brasil, 2023a).

A Doutrina Militar de Defesa Cibernética, define Defesa Cibernética como:

> [...] ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente. (Brasil, 2023a, p. 17)

No contexto da segurança cibernética, esta deve ser compreendida como a competência de assegurar a inviolabilidade do ciberespaço nacional por meio da adoção de medidas que garantam a autenticidade, integridade, confidencialidade e disponibilidade dos dados de interesse do Estado Brasileiro (Mandarino, 2010).

Em relação à Guerra Cibernética, o Glossário das Forças Armadas, definiu:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C2 [2] do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (Brasil, 2015, p. 134)

Com essas definições esclarecidas e considerando que a estrutura de cabos submarinos é uma infraestrutura crucial da defesa nacional, e que a Doutrina Militar de Defesa Cibernética estabelece que as Forças Armadas e Comando de Defesa Cibernética (ComDCiber), em conjunto com o Ministério da Defesa (MD), e o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e outros ministérios e agências, ajudarão a proteger infraestruturas críticas e recursos-chave nacionais quando necessário e aprovado (Brasil, 2023a), nossa atenção doutrinária será direcionada à Defesa Cibernética. Exploraremos sua base conceitual de emprego, princípios de atuação, características, possibilidades, peculiaridades e formas de atuação. Além disso, analisaremos os diferentes tipos de ações cibernéticas, buscando compreender suas implicações e modos de operação.

2.2 BASE CONCEITUAL DE EMPREGO E OPERAÇÕES CIBERNÉTICAS

O espaço cibernético é uma dimensão crucial que interage de forma transversal com os domínios tradicionais – aéreo, terrestre, marítimo e espacial. Ele emprega enlaces e nós situados nos domínios operacionais para gerar efeitos tanto no próprio espaço cibernético quanto em outros domínios operacionais. As operações cibernéticas, portanto, exigem um controle meticuloso dos efeitos para

[2] C2 – Comando e Controle

proporcionar liberdade de ação nas atividades em outros domínios operacionais (Brasil, 2023a).

Embora o ciberespaço faça parte do ambiente informacional, ele depende dos domínios físicos do ar, terra, mar e espaço. Assim como as operações nos domínios físicos dependem da infraestrutura física criada para aproveitar características naturais, as operações no ciberespaço dependem de infraestrutura de Tecnologia da Informação (TI) em rede, autônoma e incorporada em plataformas, além dos dados que residem e são transmitidos por esses componentes para permitir operações militares em um domínio criado pelo homem (Eua, 2018).

Consequentemente, Operações Cibernéticas são aquelas onde as ações cibernéticas são empregadas para alcançar objetivos e efeitos dentro do espaço cibernético ou através dele (Brasil, 2023a). As operações cibernéticas são conduzidas através de diferentes tipos de operações, que variam de acordo com a intenção e os objetivos do comandante. É destacável que essas operações podem ser realizadas tanto por aliados quanto por adversários, abrangendo Operações Cibernéticas Defensivas e Operações Cibernéticas Ofensivas (OTAN, 2020). Devido ao objeto de estudo deste trabalho, focaremos nossa atenção nas Operações Cibernéticas Defensivas.

As Operações Cibernéticas Defensivas, que visam neutralizar ameaças e restaurar a segurança das redes, são classificadas em Ações de Resposta (Aç Rsp) e Medidas de Defesa Interna (MDI). A maior parte dessas operações envolve MDI, que se dedicam à identificação proativa de ameaças avançadas e/ou persistentes, além da neutralização dessas ameaças e mitigação de seus efeitos por meio da implementação de respostas internas e contramedidas. As MDI ocorrem dentro do espaço cibernético defendido e incluem ações para restabelecer a segurança. Exemplos dos efeitos das MDI incluem o isolamento, que impede a interação entre o oponente e os sistemas comprometidos; a contenção, que impede a disseminação de ações maliciosas; a neutralização, que incapacita a atividade maliciosa de continuar impactando os sistemas; e a recuperação, que restaura a funcionalidade dos sistemas ao eliminar os efeitos da atividade maliciosa. Por outro lado, as Aç Rsp são realizadas externamente e podem incluir o uso da força, dependendo do contexto operacional (Brasil, 2023a).

Além de seu papel central no Sistema Militar de Defesa Cibernética (SMDC), as Operações Cibernéticas Defensivas também podem ser aplicadas para proteger

outras partes do ciberespaço nacional, incluindo infraestruturas críticas pertencentes ao setor privado e a outras agências governamentais. As Forças Armadas e o ComDCiber têm a capacidade de colaborar com o GSI/PR, o MD e outras entidades para garantir a proteção dessas infraestruturas quando necessário e autorizado, reforçando a segurança e resiliência do espaço cibernético do Brasil (Brasil, 2023a).

Diante da complexidade e importância das operações cibernéticas defensivas, é essencial entender os princípios e características que norteiam a sua implementação. No próximo item, examinaremos os princípios de emprego da defesa cibernética e suas características, que são guias para as operações militares no espaço cibernético.

2.3 PRINCÍPIOS DE EMPREGO DA DEFESA CIBERNÉTICA E CARACTERÍSTICAS DA DEFESA CIBERNÉTICA

Clausewitz, em sua obra "Da Guerra," destacou a importância de compreender e aplicar princípios fundamentais, como a concentração de forças, para alcançar a superioridade no campo de batalha (Clausewitz, 1984). De forma similar, Sun Tzu, em "A Arte da Guerra" (aproximadamente século 5 a.C.), enfatizou a importância do conhecimento do inimigo para formular estratégias eficazes (Sun Tzu, 2009).

Nesse contexto, os princípios clássicos da guerra são adaptados para a Defesa Cibernética no Espaço Cibernético. Esses princípios são fundamentais para orientar as operações cibernéticas nos níveis estratégico, operacional e tático. A aplicação desses princípios no ambiente cibernético é, portanto, essencial para a eficácia das operações de Defesa Cibernética (Brasil, 2023a).

São princípios de emprego da Defesa Cibernética:

> 1. Princípio da Adaptabilidade - consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do espaço cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis.
> 2. Princípio da Dissimulação - medidas ativas e passivas devem ser adotadas para dificultar a rastreabilidade das ações cibernéticas ofensivas. Objetiva-se, assim, mascarar a autoria e o ponto de origem dessas ações.
> 3. Princípio do Efeito- as ações no espaço cibernético devem produzir efeitos cinéticos ou não cinéticos que contribuam para a consecução dos objetivos militares.

> 4. Princípio da Rastreabilidade - medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra o próprio Espaço Cibernético Interesse (Brasil, 2023a, ed 2°, p.26)

Compreender esses princípios fornece uma base sólida para explorar as características distintas da Defesa Cibernética. As características deste campo são elementos essenciais que definem a natureza das operações cibernéticas e as diferenciam de outras formas de defesa militar. A seguir, examinaremos as principais características da Defesa Cibernética que influenciam o objeto deste estudo.

O ciberespaço possui características únicas que o diferenciam dos outros domínios clássicos da guerra, como ar, mar, espaço e a terra. Essas diferenças influenciam diretamente a forma como as operações de Defesa Cibernética são conduzidas. Conforme a Doutrina Militar de Defesa Cibernética, o ciberespaço é um domínio onde as fronteiras geográficas são irrelevantes, as ações podem ser realizadas a partir de qualquer local com acesso à rede e as consequências podem se espalhar rapidamente através das infraestruturas críticas interconectadas (Brasil, 2023a).

Nesse Cenário, a Doutrina Militar de Defesa destaca nove características[3] cruciais da Defesa Cibernética, das quais quatro serão especialmente enfatizadas neste estudo. Essas características selecionadas fornecem entendimentos valiosos sobre os desafios e estratégias fundamentais envolvidos na proteção dos sistemas cibernéticos contra ameaças emergentes.

Uma das características fundamentais da Defesa Cibernética é o alcance global das suas operações. Essa característica possibilita que operações cibernéticas ocorram em nível global concomitantemente e a partir de diferentes locais (Brasil, 2023a).

Outra característica essencial é a vulnerabilidade das fronteiras geográficas essa característica permite que as ameaças cibernéticas possam surgir de qualquer ponto do globo, tornando a defesa cibernética uma tarefa complexa e globalmente ordenada (Brasil, 2023a).

---

[3] a) Insegurança Latente; b) Alcance Global; c) Vulnerabilidade das Fronteiras Geográficas; d) Mutabilidade; e) Incerteza; f) Dualidade; g) Paradoxo Tecnológico; h) Dilema de Segurança; e i) Assimetria (Brasil, 2023a).

O paradoxo tecnológico é mais uma característica importante a ser considerada. Conforme a tecnologia continua a evoluir, aumenta a utilização da Tecnologia da Informação (TI), o que a torna mais suscetível a ameaças cibernéticas. No entanto, paradoxalmente, o alto nível de desenvolvimento tecnológico também fortalece as defesas contra-ataques cibernéticos (Brasil, 2023a). Esse paradoxo destaca a necessidade de equilibrar inovação tecnológica com medidas de segurança.

Finalmente, a assimetria surge como uma característica-chave. Baseada no desbalanceamento de forças, ela permite que atores com recursos limitados possam infligir danos significativos, desafiando as defesas tradicionais (Brasil, 2023a).

Tendo explorado as características distintas da Defesa Cibernética é crucial agora examinar as possibilidades e peculiaridades que este campo oferece. As possibilidades da Defesa Cibernética referem-se às capacidades e oportunidades que surgem do emprego de estratégias e tecnologias cibernéticas para assegurar a segurança e resiliência no Espaço Cibernético. Na próxima seção, detalharemos as principais possibilidades e peculiaridades da Defesa Cibernética.

2.4 POSSIBILIDADES DA DEFESA CIBERNÉTICA E PECULIARIDADES DA DEFESA CIBERNÉTICA

A Defesa Cibernética oferece um amplo leque de possibilidades estratégicas e operacionais, essenciais para assegurar a segurança nacional no domínio cibernético. Em relação à vulnerabilidade das infraestruturas críticas, é importante salientar as seguintes capacidades da Defesa Cibernética: "Atuar no espaço cibernético, por meio de ações ofensivas e defensivas" (Brasil, 2023a, ed. 2, p. 23). Essa característica demonstra a flexibilidade e a abrangência da Defesa Cibernética, e a exploração eficaz dessa capacidade é crucial para enfrentar os novos desafios no ciberespaço e assegurar uma postura defensiva eficaz e proativa.

Outra possibilidade importante é a de "Cooperar com a Segurança Cibernética, inclusive, de órgãos externos ao Ministério da Defesa, mediante solicitação ou no contexto de uma operação" (Brasil, 2023a, p. 23). Essa colaboração em períodos de normalidade prevista na Doutrina foi normatizada com a instituição da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), e pela

criação da Equipe de Coordenação Setorial da Defesa (ECS/Def). A ECS/Def, operada pelo ComDCiber, tem a missão de coordenar a resposta a incidentes cibernéticos, tratamento e prevenção no Setor Defesa, consolidando notificações das principais equipes das Forças Armadas e do Ministério da Defesas e de outras equipes públicas ou privadas relacionadas ao setor Defesa (Brasil, 2023b).

No entanto, apesar de suas características e capacidades, a Defesa Cibernética enfrenta desafios específicos que podem comprometer sua eficácia. Reconhecer e compreender essas particularidades é crucial para desenvolver estratégias eficazes que mitiguem seus impactos negativos. Diante disso, é essencial identificar as peculiaridades que influenciam diretamente a atuação da Defesa Cibernética.

Essas peculiaridades referem-se a características distintivas ou desafios específicos que podem influenciar a eficácia das operações de defesa cibernética. No cenário complexo da defesa cibernética, surgem diversos desafios que exigem uma abordagem estratégica e adaptativa para mitigar as ameaças em constante evolução. Entre os principais desafios enfrentados pela Defesa Cibernética estão:

> a) dificuldade para identificar o agente da ação no domínio cibernético (atribuição);
> b) constante identificação de novas vulnerabilidades nos sistemas computacionais;
> c) dificuldade de identificação e retenção de talentos humanos;
> d) grande vulnerabilidade a ações de oponentes com poder assimétrico;
> e) dificuldade de acompanhamento da evolução tecnológica; e
> f) dificuldade de identificação e mitigação das vulnerabilidades dos próprios sistemas de informação. (Brasil, 2023a, ed 2°, p.23)

Entre esses desafios, a capacidade de atribuição é particularmente crítica, pois é essencial para garantir que os responsáveis não permaneçam impunes no espaço cibernético (Maglaras, 2018). A arquitetura da Internet e seus sistemas de governança complicam significativamente a atribuição de ataques cibernéticos, pois não existem mecanismos padrão para rastreamento. Usuários habilidosos podem alterar informações dos pacotes, incluindo a falsificação de endereços de origem, o que é especialmente fácil em comunicações unidirecionais. Além disso, ataques cibernéticos sofisticados frequentemente utilizam hospedeiros intermediários comprometidos para disfarçar pacotes maliciosos, tornando ineficaz a correlação de pacotes para rastreamento (Hunker; Hutchinson; Margulies, 2008).

Para complicar ainda mais, ataques cibernéticos podem ser originados de outros países, o que complica a atribuição devido à necessidade de determinar qual nação ou agência de aplicação da lei tem a responsabilidade e a autoridade para investigar. Além disso, é necessário definir sob qual estrutura legal os responsáveis podem ser processados e quais leis são aplicáveis (Maglaras, 2018).

2.5 FORMAS DE ATUAÇÃO CIBERNÉTICA E TIPO DE AÇÕES CIBERNÉTICAS

Na área da atuação cibernética, a diversidade de abordagens varia conforme os objetivos, nível de envolvimento nacional, contexto e tecnologia empregada. A atuação cibernética política/estratégica ocorre durante tempos de estabilidade, com o propósito de alcançar objetivos políticos ou estratégicos de alto nível, muitas vezes contra ameaças à Segurança Nacional. Por outro lado, a atuação cibernética operacional/tática é comumente empregada em operações militares, contribuindo para a realização de efeitos desejados (Brasil, 2023a).

Em relação às infraestruturas críticas, embora a salvaguarda dessas instalações não seja uma obrigação direta ou exclusiva das unidades de defesa cibernética do Ministério da Defesa, ela deve, sem dúvida, contar com seu apoio. Este suporte é essencial, pois, em caso de mobilização nacional para um conflito armado, a coordenação eficaz das forças disponíveis dependerá diretamente dessa colaboração (Janczewski; Colarik, 2008).

No caso específico dos cabos submarinos, é essencial compreender as responsabilidades na proteção dessas infraestruturas. Vichi, Ayres Pinto e De Sá (2020) destacam a importância de diferenciar defesa cibernética da segurança cibernética nessa proteção. A defesa envolve a salvaguarda da autonomia estatal e de seus territórios, enquanto a segurança cibernética se concentra mais nos atores privados, que devem proteger os dados e as estações de aterragem dos cabos. A responsabilidade pela proteção dos dados é compartilhada: o Estado cuida da proteção física dos cabos, enquanto as entidades privadas garantem a criptografia e a segurança dos dados.

Quanto aos tipos de ações cibernéticas, estas se dividem em ataque, exploração e proteção cibernética. O ataque cibernético visa afetar dispositivos, redes e comunicações do oponente para causar diversos efeitos, incluindo

destruição ou degradação de equipamentos, manipulação de dados e interrupção de sistemas. Já a exploração cibernética consiste em mapear sistemas e identificar vulnerabilidades, podendo ser não-intrusiva, apenas coletando informações, ou intrusiva, com o objetivo de obter dados negados. Por fim, a proteção cibernética tem como foco garantir o funcionamento dos dispositivos e protegê-los de ataques e ações de exploração do oponente, sendo uma tarefa contínua e constante (Brasil, 2023a).

Compreender esses tipos de ações cibernéticas é crucial para entender como a Doutrina Militar de Defesa Cibernética das Forças Armadas Brasileiras é aplicada na prática. Este capítulo ofereceu um panorama abrangente sobre essa doutrina e seus fundamentos. Com essa base conceitual estabelecida, o próximo capítulo se concentrará nos cabos submarinos, analisando seu histórico, componentes essenciais, vulnerabilidades, causas de falhas, modos de ataque e as medidas de proteção implementadas no Brasil. Dessa forma, no Capítulo 4, será possível confrontar os princípios e estratégias de defesa cibernética discutidos anteriormente com a realidade específica dos cabos submarinos.

3 CABOS SUBMARINOS

Este capítulo apresenta um panorama histórico e técnico dos cabos submarinos, essenciais para a comunicação global e cada vez mais vulneráveis a ameaças cibernéticas. Ao longo do texto, serão explorados o desenvolvimento histórico desses cabos, seus principais componentes, as vulnerabilidades associadas a diferentes fatores — como causas naturais, atividades humanas e ameaças intencionais —, assim como os modos de ataque que podem comprometer essa infraestrutura. A discussão abrange também as estratégias de proteção no contexto brasileiro e o histórico de ataques, proporcionando uma base sólida para analisar as vulnerabilidades cibernéticas específicas dos cabos submarinos, tema central desta dissertação.

3.1 HISTÓRICO DOS CABOS SUBMARINOS

No século 19, cientistas e engenheiros alcançaram avanços significativos ao explorar o uso da eletricidade para transmitir mensagens, levando à criação do telégrafo elétrico, um meio de comunicação seguro e eficiente. Para a Inglaterra, esse desenvolvimento representou um desafio ainda maior. Devido ao seu caráter insular e às colônias espalhadas globalmente, era crucial dominar a habilidade de instalar cabos submersos. Essa competência era essencial para que a Inglaterra pudesse expandir sua rede telegráfica e garantir uma comunicação rápida e confiável com suas numerosas colônias ao redor do mundo (Silva, 2011).

Em 1850, foi feita a primeira tentativa organizada de lançar um cabo submarino comercial, com o objetivo de conectar Dover, na Inglaterra, a Cape Gris Nez, na França, atravessando o Estreito de Calais (Oazen; Dias, 2019). Este primeiro cabo serviu como uma experiência inicial que confirmou a viabilidade da comunicação subaquática. Apesar de ser inadequado em muitos aspectos, como seu design fino, leve e com isolamento deficiente, o cabo conseguiu transmitir algumas mensagens, embora de forma limitada (Silva, 2011).

A linha telegráfica criada tinha objetivo de conectar as bolsas de valores da Inglaterra e da França e rapidamente se tornou um sucesso comercial. A partir de 1852, essa rede se expandiu por meio de cabos submarinos, estabelecendo

conexões com diversos países europeus. No Brasil, uma linha foi instalada em 1854, ligando a capital, Rio de Janeiro, a Petrópolis, utilizando tanto segmentos terrestres quanto cabos submarinos (Kocher, 2014).

Esses cabos proporcionaram benefícios políticos e comerciais significativos. Entretanto, a tarefa de ligar a Europa às Américas apresentava um desafio imenso. A profundidade extrema do Atlântico Norte e a vasta distância entre os continentes levantaram dúvidas sobre a capacidade da engenharia da época em superar esses obstáculos (Oazen; Dias, 2019).

No entanto, esse desafio monumental não intimidou os visionários da época. A integração entre os interesses científicos, políticos e financeiros foi plenamente demonstrada no ambicioso projeto do primeiro cabo transatlântico. Em 1854, o financista americano Cyrus Field concebeu a ideia de conectar a Escócia a Terra Nova, no Canadá, estendendo-se para ligar os Estados Unidos à Grã-Bretanha. O objetivo era melhorar a rapidez na transmissão de informações comerciais cruciais, como a cotação de grãos e algodão, entre as bolsas de valores desses países. As várias tentativas frustradas de lançar o cabo em 1857, 1858 e 1865 não desencorajaram os investidores, que continuaram a levantar enormes quantias de capital. O sucesso finalmente veio em 1866, refletindo a confiança inabalável no potencial revolucionário dessa tecnologia (Kocher, 2014).

Em relação ao Brasil, o barão do Rio Branco, em 1871, solicitou ao barão de Mauá que estabelecesse a comunicação telegráfica entre o Brasil e a Europa. Mauá aceitou a tarefa sob a condição de não utilizar seu próprio capital e, caso o projeto fosse bem-sucedido, ele não obteria lucro pessoal. Este empreendimento seria um esforço dedicado ao benefício da nação (Oazen; Dias, 2019).

Após a superação dos desafios tecnológicos iniciais, os cabos telegráficos submarinos se espalharam por todos os continentes, integrando-se eficientemente às redes terrestres de telegrafia. Este avanço tecnológico, ocorrido por volta da década de 1880, facilitou a conexão das diferentes zonas econômicas ao redor do mundo, contribuindo significativamente para a formação de um sistema econômico global (Kocher, 2014).

A introdução do telefone comercial por rádio entre os Estados Unidos e a Inglaterra em 1927 marcou o declínio da telegrafia e dos cabos submarinos de longa distância, que perderam parte significativa de seu mercado. Durante esse período, a telegrafia enfrentou uma concorrência crescente da tecnologia sem fio, sinalizando o

fim da era dos grandes cabos telegráficos. No entanto, os cabos submarinos voltaram a superar a tecnologia sem fio em 1956, com o lançamento do Cabo Transatlântico TAT-1. Este avanço foi possível graças à combinação de cabos coaxiais e repetidores (Oazen; Dias, 2019).

O TAT-1 foi responsável por 707 chamadas entre Londres e a América do Norte apenas no seu primeiro dia de operação. Este marco deu início à era das comunicações telefônicas submarinas utilizando cabos coaxiais (Carter, 2009), representando um salto tecnológico substancial.

Contudo, à medida que avançava a tecnologia, os cabos coaxiais submarinos na década de 1970 e início dos anos 1980 enfrentaram limitações. Devido à baixa largura de banda e ao alto custo, eles eram viáveis principalmente em rotas de alta densidade de comunicação. Com a crescente demanda por maior capacidade de transmissão a custos mais baixos, iniciou-se, em meados dos anos 1970, o desenvolvimento da tecnologia de fibra óptica para cabos submarinos. Esta inovação marcou o começo de uma nova era nas comunicações submarinas, oferecendo uma solução mais eficiente e econômica para o aumento exponencial do tráfego de dados globais (Carter, 2009).

A introdução das fibras ópticas revolucionou o campo das comunicações globais, oferecendo a capacidade de transmitir até 12.000 canais, significativamente mais do que os 5.500 canais suportados pelos cabos coaxiais mais avançados da época. Apesar de inicialmente parecer improvável que essa tecnologia pudesse ser a base de uma rede global, o lançamento do TAT-8 em 1988 — o primeiro cabo transoceânico de fibra óptica — ligou os Estados Unidos, o Reino Unido e a França. Este cabo não só ultrapassou os satélites em termos de custo, rapidez e capacidade nas comunicações de dados e voz, mas também inaugurou uma nova fase nas telecomunicações mundiais (Carter, 2009).

Nesse período, a internet começava a emergir como uma força revolucionária. A implementação de cabos de fibra óptica, com sua maior capacidade e custos reduzidos, ofereceu a base econômica essencial para o crescimento acelerado da internet. Essas duas tecnologias se complementaram de maneira notável: os cabos de fibra óptica permitiram a transmissão segura e rápida de grandes volumes de dados, enquanto a internet possibilitou o acesso e uso desses dados de forma diversificada. Tal combinação transformou profundamente o cenário das

comunicações, gerando mudanças substanciais nos negócios, no comércio, na educação e no entretenimento global (Carter, 2009).

Atualmente, os cabos submarinos são uma parte essencial e muitas vezes negligenciada da infraestrutura global de Internet. Estima-se que eles sejam responsáveis por transportar mais de 95% do tráfego intercontinental da Internet. Sem essa rede de cabos submersos, a Internet moderna, como a conhecemos, não seria viável. Estes cabos são fundamentais para a continuidade e eficiência da comunicação global, e sua importância na geopolítica e na segurança cibernética está se tornando cada vez mais evidente à medida que os riscos de ataques físicos e cibernéticos aumentam (Sherman,2021). Estima-se que existam aproximadamente 1,4 milhão de quilômetros desses cabos em operação ao redor do mundo, formando uma vasta e complexa rede que sustenta a conectividade internacional (Telegeography, 2024).

Desde 2012, a dinâmica do uso dos cabos submarinos mudou significativamente. Anteriormente dominada por provedores de infraestrutura de Internet e de trânsito de dados, a capacidade desses cabos passou a ser cada vez mais utilizada por grandes empresas de serviços de nuvem e provedores de conteúdo, como *Google*, *Facebook*, *Amazon* e *Microsoft*. A partir de 2016, essas empresas começaram a investir massivamente em cabos submarinos. Hoje, elas controlam ou alugam mais de metade da capacidade global desses cabos, demonstrando sua crescente influência na infraestrutura mundial de comunicações (Brake, 2019).

Essa transformação global também se reflete no Brasil, que é conectado ao restante do mundo por meio de 15 cabos submarinos, fundamentais para a conectividade com a América do Norte, África e Europa (Telegeography, 2024). Além disso, o Brasil está prestes a reforçar essas conexões com a construção do cabo FIRMINA pela Google. Este novo cabo, com aproximadamente 13.500 quilômetros, conectará diretamente os Estados Unidos à Argentina, passando pelo Uruguai e Brasil, ampliando significativamente a capacidade de comunicação e integração do país com outros continentes (Baladron; Riviero, 2022).

Essa infraestrutura submarina no Brasil é suportada por quatro pontos de aterrissagem de cabos submarinos, conhecidos como *landing points*. Dentre eles, Fortaleza destaca-se como um importante hub intercontinental localizado na Praia do Futuro. Este ponto é reconhecido pela comunidade global de cabos submarinos

devido à sua capacidade de conectar diversas rotas submarinas. Além de Fortaleza, outros pontos de aterrissagem incluem Rio de Janeiro, Santos e Salvador. Embora todos desempenhem papéis cruciais na interconectividade do Brasil com o resto do mundo, Fortaleza é visto como o mais significativo em termos de conectividade intercontinental (Mariano, 2020).

3.2 COMPONENTES ESSENCIAIS DOS CABOS SUBMARINOS

Para compreender como surgem as ameaças decorrentes de ataques deliberados à infraestrutura de cabos submarinos, é fundamental examinar detalhadamente sua arquitetura e os componentes essenciais. Esses elementos principais incluem: Infraestrutura de Cabos, Estações de aterrissagem e a Capacidade de reparo.

Primeiramente, a vulnerabilidade dos cabos submarinos varia significativamente com base em sua localização. Em águas costeiras e rasas, as posições dos cabos são geralmente divulgadas publicamente para evitar acidentes, como ancoragem e dragagem, e são indicadas em cartas náuticas. No entanto, em alto-mar, as localizações exatas não são publicadas, tornando a identificação e o reparo dos cabos mais desafiadores. Além disso, a profundidade do fundo marinho em alto-mar complica os reparos, resultando em impactos potencialmente mais graves em caso de ruptura (Buerger; Liebetrau; Franken, 2022).

Além das questões técnicas, do ponto de vista jurídico, os cabos submarinos estão sujeitos a diferentes regras dependendo da zona legal estabelecida pela Convenção das Nações Unidas sobre o Direito do Mar (CNUDM). Nas águas territoriais (até 12 milhas náuticas da costa), os Estados têm jurisdição completa sobre os cabos. Na zona contígua (até 24 milhas náuticas), os Estados têm responsabilidades adicionais de aplicação da lei. Fora dessas áreas, em alto-mar e nas Zonas Econômicas Exclusivas (ZEE) (até 200 milhas náuticas), a jurisdição e as responsabilidades para a proteção dos cabos tornam-se mais ambíguas (Buerger; Liebetrau; Franken, 2022).

Outro componente essencial são as estações de aterrissagem, que são pontos críticos onde os cabos submarinos se conectam à infraestrutura terrestre. Localizadas geralmente próximas à costa, essas estações muitas vezes

compartilham espaço com outras infraestruturas essenciais, como redes de eletricidade submarina (Courtois; Bardelay, 2016). Equipadas com servidores e tecnologias de roteamento, elas garantem a transição dos dados da rede submarina para a terrestre. Para segurança, são protegidas por cercas, arame farpado e sistemas de vigilância como câmeras e sensores. Embora suas localizações exatas não sejam amplamente divulgadas, existem mapas e comunidades dedicadas a identificar esses locais (Buerger; Liebetrau; Franken, 2022).

A segurança e a integridade operacional das estações de aterrissagem são ainda complementadas pelas tecnologias avançadas de monitoramento incorporadas nos sistemas de cabos modernos. Entre essas tecnologias, destaca-se o Sensoriamento Acústico Distribuído, que utiliza a própria fibra óptica dos cabos para detectar sinais acústicos ao longo de toda a sua extensão. Esse sistema permite identificar rapidamente qualquer dano ou ruptura nos cabos, facilitando a execução de reparos rápidos e fornecendo dados cruciais em processos legais sobre danos (Buerger; Liebetrau; Franken, 2022).

Por fim, a manutenção e o reparo dos cabos submarinos são gerenciados quase que exclusivamente por empresas privadas especializadas. Os operadores e proprietários firmam contratos com empresas de manutenção marítima que possuem depósitos de armazenamento de cabos e equipamentos, além de navios de reparo estrategicamente posicionados em todo o mundo. Os navios ficam em prontidão 24 horas por dia, 7 dias por semana, para responder a falhas nos cabos. A organização da manutenção dos cabos é feita por meio de zonas globais e acordos cooperativos sem fins lucrativos (Buerger; Liebetrau; Franken, 2022).

De fato, o setor privado desempenha um papel fundamental em várias atividades relacionadas aos cabos submarinos, desde a coleta de informações até a reparação de danos. Quando cidadãos, empresas e órgãos governamentais precisam restaurar o acesso à Internet após danos aos cabos submarinos, o setor privado é acionado para realizar reparos e restabelecer a conectividade. Essas empresas geralmente têm controle direto e profundo conhecimento da infraestrutura crítica. Isso é particularmente relevante nas democracias, onde o setor privado tem uma longa história de envolvimento significativo, especialmente com cabos de telecomunicações (Sherman, 2021).

3.3 VULNERABILIDADE E CAUSAS DE FALHAS NOS CABOS SUBMARINOS

Nas discussões contemporâneas sobre a segurança da Internet, o foco de muitos especialistas tem se voltado para as tecnologias de ponta, como a infraestrutura de computação em nuvem, as redes de telecomunicações 5G e as novas gerações de satélites. No entanto, é fundamental reconhecer que a maior parte do tráfego internacional de dados, que inclui desde videoconferências até transações financeiras e informações militares confidenciais, ainda transita majoritariamente por uma tecnologia mais antiga e menos glamorosa: os cabos submarinos. Esses cabos, embora não atraiam a mesma atenção que as tecnologias emergentes, permanecem cruciais para a conectividade global, transportando diariamente vastas quantidades de dados entre os continentes (Sherman, 2021).

Os cabos de dados submarinos enfrentam uma série de ameaças que podem comprometer sua funcionalidade. Anualmente, ocorrem cerca de 100 rupturas desses cabos, mas a maioria dos usuários finais não percebe essas falhas, pois o tráfego de dados é redirecionado por rotas alternativas. Interrupções completas da internet são raras e geralmente ocorrem somente quando não há redundância disponível para substituir o cabo danificado. As causas dessas falhas podem ser classificadas em três categorias principais: causas naturais, como eventos sísmicos; causas humanas, que podem ser intencionais ou acidentais, como danos causados por atividades marítimas; e causas externas, relacionadas a falhas na infraestrutura de suporte (Buerger; Liebetrau; Franken, 2022).

Entre as causas naturais, desastres como terremotos submarinos, tsunamis e tempestades severas representam riscos significativos para os cabos, enquanto fatores de longo prazo, como corrosão e correntes marítimas, contribuem para o desgaste das camadas protetoras dos cabos. Embora menos frequentes do que os danos causados por atividades humanas, os incidentes naturais representam aproximadamente um quinto das falhas de cabos. A complexidade desses eventos é que eles podem causar múltiplas falhas simultâneas, como ocorreu após o terremoto de Tōhoku, em 2011, quando quatro cabos para o Japão foram danificados ao mesmo tempo, afetando significativamente o tráfego de internet na região. Em lugares com menor redundância de cabos, essas falhas múltiplas podem resultar em apagões completos da internet (Buerger; Liebetrau; Franken, 2022).

As falhas dos cabos submarinos também são influenciadas por fatores externos, particularmente infraestruturas e serviços dos quais dependem. Cabos de fibra óptica com extensão superior a 150 km necessitam de energia elétrica para operar eficientemente, devido à necessidade de repetidores para manter a integridade do sinal ao longo de grandes distâncias (Agrawal, 2016). Normalmente, a energia é fornecida pelas estações de aterrissagem em cada extremidade do cabo, minimizando o risco de uma interrupção total. Contudo, apagões significativos que afetam simultaneamente ambas as estações podem causar a perda de conectividade (Buerger; Liebetrau; Franken, 2022).

Além disso, a perda de infraestruturas regionais em terra, como cabos, centros de dados e pontos de troca de internet, seja por destruição física ou falhas de roteamento, pode inutilizar os cabos submarinos internacionais. Outro aspecto crítico é a segurança dos operadores de cabos. Se as empresas que operam esses cabos ou seus funcionários não tiverem segurança, a falta de manutenção pode comprometer a funcionalidade dos cabos a longo prazo. Essa situação também é relevante em casos de falência dessas empresas, o que poderia levar a interrupções prolongadas na operação dos cabos (Buerger; Liebetrau; Franken, 2022).

Por fim, os danos aos cabos submarinos causados por atividades humanas podem ocorrer de forma intencional ou não. A maior parte desses incidentes resulta de atividades marítimas cotidianas, como pesca, ancoragem e dragagem, que são as causas mais comuns de danos (Buerger; Liebetrau; Franken, 2022). De fato, danos aos cabos, principalmente não intencionais e decorrentes de atividades comerciais marítimas, representam em média mais de 70% dos incidentes anuais (Martinage, 2015).

Apesar de a maioria dos danos aos cabos submarinos ser causada por atividades diárias e acidentais, como pesca de arrasto, ancoragem de embarcações e fenômenos naturais, é crucial reconhecer que também existem riscos associados a danos intencionais. Atos de sabotagem, espionagem ou até mesmo ataques físicos diretos contra as infraestruturas vitais dos cabos submarinos, embora menos frequentes, representam ameaças significativas. Por isso, tornam-se objeto de estudo detalhado na próxima seção, intitulada Modos de Ataque aos Cabos Submarinos.

3.4 MODOS DE ATAQUE AOS CABOS SUBMARINOS

Nesta seção, analisaremos os principais tipos de ataques intencionais que representam ameaças significativas à segurança dos cabos submarinos. Abordaremos os ataques físicos, o roubo de dados e inteligência, além dos ataques cibernéticos.

Ataques físicos aos cabos submarinos podem assumir diversas formas, com potencial para causar interrupções significativas na conectividade. Navios civis, como embarcações de pesca ou de lazer, podem ser equipados com dispositivos improvisados para cortar cabos, aproveitando-se do tráfego marítimo comum para se esconderem. Outra ameaça vem dos explosivos submarinos, como minas navais ou dispositivos explosivos improvisados, que são baratos e simples de fabricar, mas eficazes em interromper conexões de cabos (Truver, 2009).

Além disso, veículos submersíveis, incluindo submarinos e drones, podem ser usados para colocar explosivos ou operar armas sofisticadas, e essa tecnologia está cada vez mais acessível, não se limitando às forças militares. Esses métodos de ataque são especialmente preocupantes para as estações de aterrissagem e infraestruturas de reparo, que são vitais para a conexão de cabos submarinos à rede terrestre e para a manutenção dos cabos. A destruição ou danos a essas instalações podem resultar em interrupções prolongadas, especialmente em áreas com poucas alternativas de conexão (Buerger; Liebetrau; Franken, 2022).

O roubo de dados e a espionagem sobre cabos submarinos também representam riscos importantes, embora tecnicamente complexos e desafiadores. De acordo com especialistas, não há informações públicas confirmando que algum país possui a capacidade de realizar tal interceptação no mar. Isso sugere que a ameaça pode ser exagerada e que é improvável que qualquer tentativa de manipulação dos cabos passe despercebida, dado que a maioria dos cabos modernos possui sistemas de vigilância integrados para detectar interrupções. Assim, a espionagem direta sobre cabos submarinos no oceano é considerada pouco provável (Buerger; Liebetrau; Franken, 2022).

Apesar de Burger, Liebetrau e Franken afirmarem que a espionagem através da interceptação de cabos no mar seja pouco provável, outros autores afirmam o contrário. Segundo analistas de inteligência, submarinos como o USS Jimmy Carter

dos EUA e a embarcação russa Yantar podem interceptar dados de cabos submarinos sem rompê-los (Barker, 2018).

Além da interceptação de cabos, outras várias vulnerabilidades podem surgir em diferentes partes da cadeia de suprimentos dos cabos submarinos. Empresas que constroem esses cabos podem inserir porta de entradas ou equipamentos de vigilância antes da instalação. Além disso, as estações de aterrissagem em terra, onde os cabos se conectam à rede terrestre, são mais acessíveis e, portanto, alvos mais vulneráveis para operações de espionagem e inteligência (Buerger; Liebetrau; Franken, 2022).

Em relação às estações de aterrissagem, o Departamento de Estado dos EUA classificou esses locais ao redor do mundo como uma das infraestruturas mais críticas para o país. Essa classificação se justifica pelo fato de que, ao obter acesso aos terminais situados nesses locais ou ao controlar os sistemas que gerenciam os comprimentos de onda da fibra óptica, um hacker poderia assumir o controle de partes significativas do tráfego internacional de dados e voz. Isso conferiria a capacidade de perturbar ou degradar consideravelmente as infraestruturas cibernéticas (Sechrist, 2012).

Um cenário significativo para ataques à infraestrutura de cabos submarinos envolve o uso de ações cibernéticas para comprometer sua operabilidade técnica. Os sistemas de gerenciamento remoto de redes, que frequentemente estão conectados à internet e baseados em protocolos HTTP e TCP/IP [4], são especialmente vulneráveis (Sechrist, 2012).

Esses sistemas de gerenciamento de redes controláveis à distância permitem o monitoramento e a alteração de sinais de fibra ótica de forma remota, sem a necessidade de pessoal no local. No entanto, essa conveniência e economia de custo trazem novos riscos de cibersegurança. A camada virtualizada de controle, conectada à Internet, expõe os cabos a possíveis invasões, permitindo que hackers interrompam ou degradem os sinais transmitidos. Além disso, as más práticas de segurança de alguns fornecedores de software e a falta de diversidade entre eles aumentam o risco, pois uma falha pode ter efeitos amplos. Muitos desses sistemas utilizam sistemas operacionais comuns, como *Linux* ou *Microsoft Windows*,

[4] Os protocolos de Internet foram desenvolvidos para permitir a comunicação entre dois pontos da rede, ou dispositivos, garantindo sempre uma conexão uniforme, segura e eficiente (HOSTMIDIA, 2024).

conhecidos pelos agentes maliciosos, facilitando possíveis explorações. Além da interrupção dos sinais, a pirataria desses sistemas pode permitir a interceptação de dados nas estações de aterragem (Sherman, 2021).

A centralização dos fornecedores de software de gerenciamento remoto é um ponto crítico, amplificando os riscos. Os desenvolvedores desses sistemas podem não priorizar a segurança devido a incentivos de mercado inadequados. Semelhante a muitos sistemas de controle industrial, essas tecnologias frequentemente são projetadas com foco na conveniência e funcionalidade, em detrimento da cibersegurança. A falta de diversidade entre os fornecedores pode levar ao comprometimento de toda a tecnologia caso uma nova vulnerabilidade seja descoberta (Sherman, 2021).

Para agravar a situação, a transmissão de dados por cabos submarinos tem aumentado diariamente e se tornado mais sensível. A pandemia de COVID-19 acelerou essa tendência ao transferir atividades para o ambiente online, aumentando o tráfego na infraestrutura da Internet. A tecnologia 5G também contribuirá para um crescimento significativo no volume de dados transmitidos (Sherman, 2021).

Além disso, a computação em nuvem desempenha um papel central no aumento da sensibilidade dos dados transmitidos. Empresas de vários setores, como saúde, comércio, defesa e logística, estão transferindo funções críticas e dados anteriormente mantidos offline para plataformas de nuvem, que operam em escala global. Esta dependência crescente significa que dados mais sensíveis estão sendo continuamente enviados através da infraestrutura de cabos submarinos. Consequentemente, as falhas e interrupções nesse tráfego se tornam mais perturbadoras para a sociedade em geral, causando prejuízos a indivíduos e organizações públicas e privadas (Sherman, 2021).

Além dos sistemas de gerenciamento remoto, centros de operações de rede, portais de acesso remoto e outros sistemas necessários para o funcionamento dos cabos, como fontes de energia elétrica, roteadores, sistemas de aquecimento, ventilação e ar-condicionado, também são vetores potenciais para ataques cibernéticos (Buerger; Liebetrau; Franken, 2022).

Para enfrentar essas ameaças, é essencial adotar medidas de proteção adequadas, conforme exploraremos na próxima seção sobre a proteção dos cabos submarinos no Brasil.

3.5 PROTEÇÃO DOS CABOS SUBMARINOS NO BRASIL

A preocupação com a segurança de infraestruturas críticas se tornou um movimento global após os ataques terroristas em Nova York em 2001. No Brasil, esse tema ganhou força desde 2006, quando investidas realizados por um grupo criminoso em São Paulo impulsionaram o Governo a identificar e proteger prioritariamente infraestruturas essenciais do país em caso de novas ocorrências semelhantes (Brasil, 2022). Em resposta a essa necessidade crescente, foi estabelecido a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), a qual descreve a segurança das infraestruturas críticas como um conjunto de ações preventivas e reativas, focadas em manter ou restaurar os serviços essenciais (Brasil, 2018).

Para a execução da PNSIC, três instrumentos principais importantes foram estabelecidos: a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) que aponta desafios e estabelece diretrizes e metas estratégicas para prever ameaças e aprimorar a segurança; o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC), que coordena a atuação de diversos órgãos, promove parcerias, atribui responsabilidades e destaca a gestão de riscos e interdependências; e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (SIDSIC) (Brasil, 2022).

Complementando essas iniciativas, a homologação do Regulamento de Proteção Cibernética para o Setor de Telecomunicações pela Anatel marca um progresso importante e significativo na proteção dos cabos submarinos. Este regulamento estabelece diretrizes e práticas para fortalecer a proteção das infraestruturas e serviços de telecomunicações, além de criar o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) para assegurar a governança. Adicionalmente, a Política Nacional de Cibersegurança (PNCiber), que ainda está em fase de elaboração e desenvolvimento, tem como objetivo direcionar a segurança cibernética no Brasil, com foco na prevenção de incidentes e ataques contra infraestruturas e serviços essenciais (Freire; Aquino, 2023).

Para aprimorar ainda mais a segurança dos cabos submarinos, Freire e Aquino recomendaram que o Brasil siga as normativas vigentes e as melhores práticas globais. Eles sugeriram a implementação de medidas estratégicas com a

colaboração de diferentes entidades governamentais e empresas do segmento para reforçar a proteção da infraestrutura de cabos submarinos, principalmente as mencionadas a seguir:

> 1. Vigilância e Patrulha Marítima: reforçar a vigilância marítima para detectar e prevenir potenciais ameaças aos cabos submarinos;
>
> 2. Cooperação Internacional: promover a colaboração com outras nações e operadoras de cabo para compartilhar informações e recursos na proteção de cabos submarinos;
>
> 3. Parcerias Público-Privadas: envolver-se com empresas privadas que operam cabos submarinos para promover práticas de segurança e investir em tecnologias avançadas de monitoramento, aprimorando a qualidade das informações sobre capacidade e quantidade de dados trafegados nos cabos submarinos no Brasil;
>
> 4. Auditorias de segurança e monitoramento contínuo: realizar auditorias regulares para avaliar a eficácia das medidas de segurança e identificar áreas que precisam de maior atenção, além de estabelecer sistemas de monitoramento contínuo para identificar e responder rapidamente a ameaças potenciais;
>
> 5. Medidas de segurança cibernética: implementar medidas robustas de segurança cibernética para proteger contra-ataques cibernéticos que comprometam a integridade dos cabos;
>
> 6. Criptografia de dados: garantir criptografia robusta para proteger os dados transmitidos por cabos, propiciando uma comunicação segura;
>
> 7. Firewalls e proteção contra malware: utilizar firewalls e software para proteger os sistemas contra ameaças cibernéticas;
>
> 8. Estudos de resiliência: fundamental para garantir a segurança e a estabilidade da infraestrutura crítica de comunicações no Brasil, salvaguardando a integridade dos serviços essenciais e contribuindo para o desenvolvimento sustentável do país;
>
> 9. Diversificação e redundância de rotas: investir em rotas alternativas e em redundâncias para minimizar o impacto das interrupções de cabos;
>
> 10. Isolamento de rede: segmentar as redes para limitar o acesso, evitando que o comprometimento de uma parte afete todo o sistema;
>
> 11. Resposta rápida a incidentes: desenvolver protocolos de resposta rápida a incidentes para prontamente mitigar danos ou interrupções;
>
> 12. Educação e conscientização: promover a conscientização sobre a importância estratégica dos cabos submarinos tanto para o público em geral como para o corpo técnico envolvido em sua operação;
>
> 13. Revisão da Legislação: atualizar e fortalecer regularmente a legislação relacionada à proteção de cabos submarinos, impondo penalidades rigorosas para atividades ilícitas, sem prejuízos de outras medidas não sancionatórias de cunho responsivo; e
>
> 14. Indústria nacional: avaliar a viabilidade em se estimular a entrada do Brasil no mercado de cabos submarinos de longa distância. (Freire; Aquino, 2023)

3.6 HISTÓRICO DE ATAQUES CIBERNÉTICOS A CABOS SUBMARINOS

Não existem casos comprovados e publicados de ataques cibernéticos deliberados à rede de cabos submarinos por atores estatais ou grupos não estatais. A maioria das discussões sobre ameaças de perda total de conectividade baseia-se em avaliações geopolíticas gerais, e não em eventos anteriores, sugerindo que esses cenários de ameaça podem ser exagerados e promover um medo infundado. No entanto, muitos países e agentes não estatais têm a capacidade de danificar esses cabos, e a aquisição dessa capacidade é relativamente barata, tornando plausíveis ataques menores para demonstrar capacidade e intenção. Diversos motivos podem levar a ataques deliberados, como tensões geopolíticas, ações de organizações terroristas para manter transações financeiras como reféns, ou redes criminosas transnacionais explorando vulnerabilidades na rede (Buerger; Liebetrau; Franken, 2022).

A grande preocupação com um ataque cibernético a cabos submarinos é que a guerra cibernética, estrategicamente, visa atacar sistemas essenciais das infraestruturas sociais, de energia e financeiros, prejudicando a habilidade dos Estados de preservar sua defesa e resposta (Silva, 2014). Além disso, Ayres Pinto e Grassi (2020) argumentam que as guerras cibernéticas têm o potencial de danificar ou eliminar essas infraestruturas essenciais, colocando em perigo os sistemas de segurança e ameaçando a soberania e atingindo alvos civis. Devido a essa vulnerabilidade estratégica, os cabos submarinos se tornam alvos prioritários em conflitos cibernéticos, dada sua importância para a conectividade e o funcionamento global.

Essa preocupação se tornou ainda mais relevante com o surgimento do *malware* Stuxnet[5], considerado um ponto de inflexão nos ataques cibernéticos. Stuxnet foi o primeiro a visar uma infraestrutura crítica de um país, particularmente as usinas nucleares iranianas além de ter afetado outras nações como Estados Unidos, Paquistão, Malásia, Índia, Indonésia, Austrália e Reino Unido. O uso dessas tecnologias como armas cibernéticas contra infraestruturas essenciais ou para

[5] Stuxnet foi um vírus sofisticado lançado contra as instalações de enriquecimento de urânio do Irã em Natanz, em junho de 2009, visando prejudicar o programa nuclear iraniano e impedir a construção de uma bomba nuclear pelo presidente Mahmoud Ahmadinejad. (ZETTER, 2017)

colocar em risco a soberania dos Estados é uma preocupação significativa em relação à evolução da guerra cibernética (Ayres Pinto; Grassi, 2020).

Após explorar detalhadamente o histórico dos cabos submarinos, seus componentes essenciais, as diversas vulnerabilidades, as causas de falhas e os modos de ataque que podem comprometer essa infraestrutura, é possível compreender a complexidade e a criticidade desses sistemas no contexto da segurança global. Cada uma dessas análises permite visualizar como esses cabos podem se tornar alvos estratégicos, seja por sua importância para a comunicação intercontinental, seja pela interdependência crescente com as atividades econômicas, sociais e de defesa. Assim, no próximo capítulo, confrontaremos esses elementos com os princípios e estratégias de defesa cibernética discutidos anteriormente. O Capítulo 4 se concentrará na aplicação prática da teoria da Defesa Cibernética em relação às vulnerabilidades cibernéticas dos cabos submarinos.

4 ANÁLISE DAS VULNERABILIDAD ES DOS CABOS SUBMARINOS A LUZ DA DOUTRINA MILITAR DE DEFESA CIBERNÉTICA

Neste capítulo, faremos uma conexão entre os conceitos teóricos de defesa cibernética apresentados no Capítulo 2, que incluem Operações Defensivas, Princípios de Emprego, Características, Possibilidades, Peculiaridades e Formas de Atuação, além dos Tipos de Ações Cibernéticas, com a análise das vulnerabilidades dos cabos submarinos abordada no Capítulo 3. Devido à ausência de dados históricos sobre ataques cibernéticos a cabos submarinos, não realizaremos uma análise de ataques passados.

4.1 ANÁLISE DAS OPERAÇÕES CIBERNÉTICAS DEFENSIVAS

As Operações Cibernéticas Defensivas são fundamentais para neutralizar ataques cibernéticos e recuperar a rede ao seu estado original após uma invasão. No contexto dos cabos submarinos, essas medidas incluem a identificação proativa de ameaças e a implementação de estratégias para mitigar possíveis danos antes que possam causar interrupções significativas nos serviços de comunicação e transmissão de dados.

Uma das estratégias que podem ser aplicadas aos cabos submarinos é o Sensoriamento Acústico Distribuído, uma técnica que detecta sinais acústicos nos cabos, permitindo a rápida identificação de danos ou rupturas e facilitando reparos imediatos.

No que diz respeito às Medidas de Defesa Interna (MDI) voltadas para a restauração do funcionamento dos cabos submarinos após um ataque, é crucial destacar o papel significativo do setor privado na recuperação. Em situações em que os cabos submarinos são danificados e o acesso à Internet precisa ser restabelecido, as empresas privadas geralmente assumem a responsabilidade pelos reparos necessários e pela reconexão da rede

A teoria das Operações Cibernéticas Defensivas mostra aderência com a realidade dos cabos submarinos, especialmente na importância da identificação proativa de ameaças e na recuperação pós-ataque. No entanto, a dependência do

setor privado para a reparação de cabos evidencia uma vulnerabilidade prática que necessita de maior atenção e ação coordenada.

4.2 ANÁLISE DOS PRINCÍPIOS DE EMPREGO DA DEFESA CIBERNÉTICA

Entre os quatro pilares do emprego da defesa cibernética - rastreabilidade, o efeito, a dissimulação e a adaptabilidade - o princípio da adaptabilidade se destaca como especialmente relevante para a proteção de infraestruturas críticas, como os cabos submarinos. Esse princípio destaca a importância de uma capacidade de resposta flexível e rápida às mudanças no ambiente de ameaças.

Os cabos submarinos são particularmente vulneráveis devido à interconexão de seus sistemas de gerenciamento remoto com a internet, utilizando protocolos comuns como HTTP e TCP/IP. Essa conectividade facilita a operação e manutenção, mas também aumenta a exposição a riscos cibernéticos, permitindo que atacantes explorem falhas nos sistemas para causar danos ou interromper serviços.

Além disso, a camada de controle desses sistemas, que é frequentemente virtualizada e acessível online, cria um ponto de vulnerabilidade significativo. Hackers podem explorar essa camada para invadir a infraestrutura dos cabos, interrompendo ou degradando a qualidade dos sinais transmitidos. Essas invasões não apenas afetam a integridade dos dados, mas também podem levar a perdas financeiras significativas e impactos na comunicação global.

A adaptabilidade, nesse contexto, se manifesta na capacidade das defesas cibernéticas de ajustarem-se rapidamente a novas ameaças e de desenvolverem contramedidas eficazes. Sem essa adaptabilidade, as defesas podem se tornar obsoletas rapidamente, deixando a infraestrutura crítica exposta a ataques que comprometam a segurança e a funcionalidade dos sistemas.

O princípio da adaptabilidade, conforme discutido na teoria, se alinha bem com a realidade enfrentada pelos cabos submarinos. A capacidade de resposta flexível é crucial para enfrentar as vulnerabilidades criadas pela conectividade com a internet. A teoria e a prática demonstram que sem essa adaptabilidade, as defesas cibernéticas se tornam insuficientes para proteger essa infraestrutura crítica.

4.3 ANÁLISE DAS CARACTERÍSTICAS DA DEFESA CIBERNÉTICA

As operações de defesa cibernética são definidas por características únicas do ciberespaço, que se distinguem dos domínios tradicionais de guerra, como terrestre, marítimo, aéreo e espacial. Essas particularidades são fundamentais para a proteção de infraestruturas críticas, como os cabos submarinos, que desempenham um papel essencial na comunicação global.

Uma característica distintiva da defesa cibernética é o alcance global das operações no ciberespaço. Ao contrário dos domínios físicos, onde as atividades são limitadas pela distância e espaço, no ciberespaço as operações de ataque ou defesa podem ser iniciadas de qualquer lugar do mundo e simultaneamente. Isso significa que ameaças cibernéticas podem surgir de qualquer ponto do globo e podem ser integradas, exigindo uma resposta defensiva que também seja global e coordenada. No caso dos cabos submarinos, que se estendem por mais de 1 milhão de quilômetros em todo o planeta, essa característica se torna ainda mais relevante. A vasta rede de cabos submarinos interconecta continentes, tornando a proteção dessas infraestruturas críticas uma tarefa complexa.

Para a proteção dos cabos submarinos, essa característica destaca a necessidade de uma cooperação internacional abrangente, envolvendo tanto governos quanto o setor privado. Nos últimos anos, a crescente participação de grandes empresas de serviços de nuvem e provedores de conteúdo na utilização e controle da capacidade dos cabos submarinos reforça a importância dessa colaboração.

Outra característica relevante é a questão das vulnerabilidades relacionadas às fronteiras geográficas. No ciberespaço, essas fronteiras se tornam irrelevantes, permitindo que ameaças cibernéticas se originem de qualquer lugar e se espalhem rapidamente por infraestruturas críticas interconectadas. No caso dos cabos submarinos, que transportam cerca de 95% do tráfego global de internet isso implica que um ataque cibernético pode ser lançado de qualquer parte do mundo, sem a necessidade de presença física. A vasta e complexa rede de cabos, com inúmeros pontos de conexão espalhados globalmente, torna a defesa ainda mais desafiadora.

O paradoxo tecnológico é uma característica central na defesa cibernética. Com o avanço tecnológico, a dependência dos sistemas de TI aumenta, elevando a vulnerabilidade a ataques cibernéticos. No entanto, esse progresso também

proporciona ferramentas de defesa mais avançadas, como sistemas sofisticados de monitoramento e tecnologias de segurança. No contexto dos cabos submarinos, o uso de sistemas de gestão remota permite o monitoramento e a alteração de sinais de fibra ótica de forma remota, facilitando uma resposta mais eficiente em caso de incidentes. Contudo, essa mesma capacidade expõe a infraestrutura a riscos significativos. A possibilidade de monitorar e controlar os cabos à distância pode ser explorada por agentes mal-intencionados, ampliando a superfície de ataque e aumentando a vulnerabilidade a invasões cibernéticas.

A assimetria na defesa cibernética refere-se à capacidade de atores com recursos limitados causarem danos significativos. No caso dos cabos submarinos, as estações de aterrissagem são pontos estratégicos particularmente vulneráveis para esse tipo de ação. Estas estações são consideradas uma das infraestruturas mais críticas para os Estados Unidos, de acordo com o seu Departamento de Estado, devido à sua importância estratégica. A preocupação central é que, se atacantes conseguirem acesso a esses terminais ou aos sistemas que controlam os comprimentos de onda da fibra óptica, eles poderiam potencialmente dominar uma parte significativa do tráfego internacional de dados e voz. Isso poderia resultar em interrupções graves ou na degradação das infraestruturas cibernéticas.

Com isso, podemos observar que as características da defesa cibernética descritas na teoria correspondem claramente à realidade dos cabos submarinos. A teoria oferece uma base sólida para compreender os desafios práticos enfrentados na defesa desses cabos contra ameaças cibernéticas.

4.4 ANÁLISE DAS POSSIBILIDADES DA DEFESA CIBERNÉTICA

A defesa cibernética oferece possibilidades estratégicas e operacionais para proteger infraestruturas críticas, como os cabos submarinos, que são essenciais para a comunicação global. No Brasil, a segurança dessas infraestruturas tem sido reforçada por meio de políticas e medidas coordenadas que abordam tanto a prevenção quanto a resposta a incidentes cibernéticos.

Para proteção dos dados transmitidos por cabos submarinos, são necessárias medidas defensivas, incluindo criptografia avançada, uso de firewalls[6] e software anti-malware[7]. A segmentação das redes é crucial para restringir o acesso e evitar que a falha de um segmento comprometa o sistema inteiro. Além disso, o desenvolvimento de protocolos para uma resposta ágil a incidentes é necessário para minimizar prejuízos ou paralisações de forma eficaz. No Brasil, a adoção dessas práticas foi fortalecida pelo Regulamento de Segurança Cibernética Aplicado ao Setor de Telecomunicações, estabelecido pela Anatel, que define diretrizes para a segurança das redes e serviços de telecomunicações.

A colaboração com órgãos externos ao Ministério da Defesa, como previsto na Doutrina Militar de Defesa Cibernética, é uma possibilidade essencial para a segurança cibernética. No Brasil, isso é exemplificado pela criação da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) e da Equipe de Coordenação Setorial da Defesa (ECS/Def), além do Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC). Essas iniciativas coordenam respostas a incidentes e promovem a integração de diferentes setores na defesa cibernética.

Sendo assim, a teoria das possibilidades da defesa cibernética demonstra uma clara conexão à realidade dos cabos submarinos. Isso evidencia que as medidas técnicas de proteção e a colaboração institucional são fundamentais para a defesa eficaz desses cabos contra ameaças cibernéticas.

4.5 ANÁLISE DAS PECULIARIDADES DA DEFESA CIBERNÉTICA

A defesa cibernética enfrenta uma série de peculiaridades e desafios específicos que afetam a eficácia das operações de proteção de infraestruturas críticas, como os cabos submarinos. Esses desafios exigem uma abordagem estratégica e adaptativa para lidar com ameaças em constante evolução.

Um dos principais desafios é a dificuldade de atribuição, que envolve identificar os responsáveis por ataques cibernéticos. A estrutura da Internet e a falta de mecanismos padrão de rastreamento tornam esse processo complexo. Atacantes

---

[6] Este sistema dedicado de hardware-software controla o tráfego de dados, bloqueando ou permitindo pacotes para prevenir atividades mal-intencionadas e ações não autorizadas na rede (KASPERSKY, 2024).

[7] Anti-malware é um software que monitora e remove ameaças virtuais em computadores e redes. (LAC Blog, 2024).

podem falsificar endereços de origem nos pacotes, dificultando a identificação de sua localização real. Além disso, muitos ataques utilizam intermediários comprometidos para ocultar o ponto de origem, complicando a correlação de pacotes para rastreamento. Esse desafio é exacerbado pela jurisdição internacional, onde ataques podem ser originados de outros países, levantando questões sobre qual nação ou agência deve investigar e sob quais leis os responsáveis podem ser processados.

Outro aspecto crítico é a constante identificação de novas vulnerabilidades, especialmente com o uso dos sistemas de gerenciamento remoto de cabos submarinos. Esses sistemas, conectados à Internet para monitoramento e controle, são atraentes devido à eficiência e custo-benefício, mas também expõem os cabos a riscos de invasão. Hackers que comprometem esses sistemas podem obter direitos administrativos, acessando dados sensíveis e até mesmo controlando o fluxo de dados. Esse cenário é particularmente perigoso, pois invasores podem manipular ou interromper o tráfego de dados, comprometendo a proteção e resiliência da infraestrutura mundial de comunicação.

A dificuldade de identificar e mitigar vulnerabilidades nos próprios sistemas de informação, frequentemente conectados à Internet, é agravada pelo uso de sistemas operacionais amplamente conhecidos, como *Linux* e *Windows*. Isso facilita o trabalho de agentes mal-intencionados familiarizados com essas plataformas, que podem explorar falhas de segurança para acessar ou comprometer sistemas críticos.

A vulnerabilidade a ações de oponentes assimétricos é outro desafio significativo. Pequenos grupos com recursos limitados podem causar danos desproporcionais, especialmente em pontos críticos como as estações de aterrissagem de cabos submarinos. Esses pontos, onde os cabos são mais acessíveis, são alvos fáceis para sabotagem, espionagem e outros tipos de ataques. A facilidade de acesso físico e a importância estratégica dessas estações tornam-nas vulneráveis, necessitando de vigilância constante e medidas de segurança reforçadas.

Além disso, a própria evolução tecnológica representa um desafio, pois exige uma adaptação contínua das defesas cibernéticas para acompanhar novas ameaças. A evolução que possibilitou o surgimento dos sistemas de gerenciamento remoto também criou oportunidades para ataques cibernéticos. Esses avanços tecnológicos, enquanto melhoram a eficiência operacional, simultaneamente aumentam a

superfície de ataque, expondo a infraestrutura a novos riscos e exigindo uma constante atualização das medidas de segurança.

Concluímos que a teoria das peculiaridades da Defesa Cibernética demonstra uma clara aderência à realidade dos cabos submarinos, evidenciando desafios complexos como a dificuldade de atribuição, a constante identificação de novas vulnerabilidades, a vulnerabilidade a ações de oponentes assimétricos, e a necessidade de adaptação contínua das defesas cibernéticas frente às evoluções tecnológicas.

4.6 ANÁLISE DAS FORMAS DE ATUAÇÃO E TIPOS DE AÇÕES CIBERNÉTICAS

A proteção dos cabos submarinos é conduzida em níveis político e estratégico, dada a sua classificação como infraestrutura crítica. Em tempos de estabilidade, essas atividades visam atingir objetivos políticos e estratégicos de alto nível, muitas vezes focados em responder a ameaças à segurança nacional. Essa estratégia no Brasil foi oficializada com a criação do Plano Nacional de Segurança de Infraestruturas Críticas, além da autorização para que as Forças Armadas e o ComDCiber colaborem com o GSI/PR, o MD e outras entidades, garantindo a proteção dessas infraestruturas críticas quando necessário.

No que tange à proteção dos cabos submarinos contra ameaças cibernéticas, essas ações são classificadas como medidas de proteção cibernética. Tais medidas incluem a implementação de criptografia para assegurar que os dados transmitidos sejam protegidos, proporcionando uma comunicação segura. Além disso, a utilização de firewalls e software de a defesa contra malware é fundamental para proteger os sistemas frente a riscos cibernéticos.

A segmentação de redes, ou isolamento de rede, é vital para restringir o acesso e prevenir que a vulnerabilidade de um setor comprometa toda a infraestrutura. A diversificação e redundância de rotas é outra prática crucial, pois o investimento em rotas alternativas e redundantes minimiza o impacto de possíveis interrupções nos cabos submarinos. Na prática, essa proteção contínua é essencial para prevenir interrupções significativas que possam impactar a soberania Brasileira.

É importante destacar que essas ações de proteção devem ser realizadas tanto pelo Estado Brasileiro quanto pelas empresas privadas, que são as principais

detentoras desses cabos. Dado o caráter crítico e a propriedade majoritariamente privada dessa infraestrutura, a colaboração entre as esferas governamental e empresarial é fundamental para garantir a proteção e a resiliência das comunicações.

Em resumo, as formas de atuação e tipos de ações cibernéticas teorizadas na defesa cibernética para a proteção dos cabos submarinos mostram-se bem alinhadas com as práticas reais, reforçando a importância de uma abordagem integrada que envolva tanto o Estado quanto o setor privado para salvaguardar estas infraestruturas críticas.

Ao final desse capítulo concluímos que há uma significativa aderência entre diversos pontos da Doutrina de Defesa Cibernética e a realidade das vulnerabilidades enfrentadas pelos cabos submarinos no contexto da ameaça cibernética. A análise realizada ao longo deste capítulo revelou que os conceitos teóricos de Operações Defensivas, Princípios de Emprego, Características, Possibilidades, Peculiaridades, Formas de Atuação, e Tipos de Ações Cibernéticas, se alinham estreitamente com os desafios e vulnerabilidades observados na proteção dos cabos submarinos. Essa aderência confirma a relevância dos princípios doutrinários no estudo das vulnerabilidades dos cabos submarinos as ameaças cibernéticas. No próximo capítulo, concluiremos este estudo abordando a questão: Quais são as vulnerabilidades dos cabos submarinos no contexto das ameaças cibernéticas e como essas vulnerabilidades impactam a segurança nacional do Brasil?

5 CONCLUSÃO

Este trabalho explorou as vulnerabilidades dos cabos submarinos no contexto das ameaças cibernéticas e como elas impactam a segurança nacional do Brasil. A pesquisa revelou que a segurança desses cabos, essenciais para a infraestrutura crítica de telecomunicações, é uma questão vital para o país. Destacamos a interseção entre a Doutrina de Defesa Cibernética e a aplicação prática de seus conceitos básicos, evidenciando a importância estratégica desses cabos.

No Capítulo 1, discutimos a relevância dos cabos submarinos para a economia e a segurança do Brasil, sendo responsáveis por 95% das comunicações globais. Eles se tornam alvos atraentes para ataques cibernéticos por diversos atores mal-intencionados. Utilizamos uma metodologia qualitativa descritiva, com revisão bibliográfica e análise documental, para fornecer uma compreensão abrangente do problema.

O Capítulo 2 abordou os conceitos e princípios fundamentais da defesa cibernética, com a Doutrina Militar de Defesa Cibernética de 2023, que reconhece o ciberespaço como o quinto campo de operações, sendo fundamental para a proteção de infraestruturas críticas.

No Capítulo 3, analisamos o histórico, os componentes essenciais e as vulnerabilidades dos cabos submarinos, identificando ameaças como eventos naturais, atividades humanas e falhas na infraestrutura de suporte. A dependência do setor privado para a reparação desses cabos foi destacada como uma vulnerabilidade significativa. Além disso, o uso de sistemas de gerenciamento remoto, que permite o monitoramento e controle dos cabos a distância, aumenta a exposição a riscos cibernéticos. As estações de aterrissagem, por sua facilidade de acesso, também representam pontos críticos de vulnerabilidade.

No Capítulo 4, conectamos os conceitos teóricos de defesa cibernética com as vulnerabilidades dos cabos submarinos, enfatizando a importância das Medidas de Defesa Interna (MDI), como o Sensoriamento Acústico Distribuído, para a identificação proativa de ameaças. A análise ressaltou o paradoxo tecnológico, onde o avanço tecnológico, ao mesmo tempo em que aumenta a eficiência e capacidade de defesa, também expande as superfícies de ataque e as vulnerabilidades. A questão das fronteiras geográficas tornou-se irrelevante no ciberespaço, permitindo

que ameaças cibernéticas se originem de qualquer lugar e se espalhem rapidamente por infraestruturas críticas interconectadas.

Após dessas discussões, torna-se fundamental responder à pergunta central deste estudo: Quais são as vulnerabilidades dos cabos submarinos no contexto das ameaças cibernéticas e como essas vulnerabilidades impactam a segurança nacional do Brasil? Os resultados indicam que as infraestruturas críticas submarinas Brasileiras são vulneráveis às ameaças cibernéticas devido ao uso de sistemas de gerenciamento remoto, à acessibilidade das estações de aterrissagem e à dependência de empresas privadas para reparos. Essas fragilidades afetam profundamente a integridade das comunicações, a proteção de dados sensíveis e a estabilidade econômica, além de comprometer operações militares.

Para agravar a situação, a transmissão de dados por cabos submarinos tem aumentado significativamente, com os dados tornando-se mais sensíveis. A pandemia de COVID-19 acelerou a transição para atividades online, aumentando o tráfego na infraestrutura da Internet. A tecnologia 5G, com seu aumento previsto no volume de dados, também contribui para esse crescimento. Além disso, a computação em nuvem desempenha um papel central nesse contexto, com empresas de setores críticos transferindo funções e dados para plataformas de nuvem, aumentando a quantidade e a sensibilidade dos dados transmitidos por cabos submarinos. As falhas e interrupções nesse tráfego são, portanto, mais prejudiciais, afetando negativamente indivíduos e organizações públicas e privadas em setores como saúde, comércio, defesa e logística.

Com a evolução tecnológica e o aumento da sensibilidade dos dados, ataques cibernéticos aos cabos submarinos Brasileiros podem ter consequências catastróficas, incluindo interrupções nas comunicações, comprometimento de sistemas financeiros, colapsos no setor de saúde e impactos na defesa nacional. A ameaça de armas cibernéticas, como evidenciado pelo malware Stuxnet, que visou infraestrutura crítica e afetou diversos países, destaca a seriedade dessas vulnerabilidades.

Concluímos assim que o objetivo do trabalho foi alcançado, fornecendo uma análise detalhada das vulnerabilidades dos cabos submarinos no contexto das ameaças cibernéticas e suas implicações para a segurança nacional do Brasil. A pesquisa confirma a necessidade de uma defesa cibernética integrada, alinhada com as doutrinas e estratégias nacionais, para proteger essas infraestruturas críticas

de ameaças cibernéticas cada vez mais sofisticadas. Medidas estratégicas e colaboração entre entidades governamentais e privadas são essenciais para garantir a integridade e resiliência desses sistemas, contribuindo para a estabilidade e o desenvolvimento equilibrado do país.

REFERÊNCIAS

AGRAWAL, Govind. Optical communication: its history and recent progress. **Optics in our time**, p. 177-199, 2016.

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, 2021. Disponível em: https://rbed.abedef.org/rbed/article/view/75178. Acesso em: 10 jun. 2024.

BALADRON, Mariela; RIVERO, Ezequiel**.** Los cables de la Red, en unas pocas manos. **Hipertextos**, v. 10, n. 18, p. 061-061, 2022.

BARKER, Pete. Undersea Cables and the Challenges of Protecting Seabed Lines of Communication. **Center for International Maritime Security** (CIMSEC), 2018. Disponível em: https://cimsec.org/tag/sloc/. Acesso em: 25 jun. 2024.

BRAKE, Doug. **Submarine cables: Critical infrastructure for global communications.** Washington, DC: Information Technology & Innovation Foundation, 2019.

BRASIL. Gabinete de Segurança Institucional. **Segurança de Infraestruturas Críticas (SIC)**. Brasília, DF: Gabinete de Segurança Institucional, 2022. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic. Acesso em: 12 jul. 2024.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética. MD31-M-07**. Brasília, DF: Ministério da Defesa, 2023a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 25 jul. 2024.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2020a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/estrategia-nacional-de-defesa. Acesso em: 01 jul. 2024.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas. MD35-G-01**. Brasília, DF: Ministério da Defesa, 2015. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/141. Acesso em: 22 jul. 2024.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2020b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/politica-nacional-de-defesa. Acesso em: 22 jul. 2024.

BRASIL. Presidência da República. Secretaria-Geral. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas

Críticas. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 01 jul. 2024.

BRASIL. Ministério da Defesa. **Portaria GM-MD nº 4.138, de 14 de agosto de 2023b**. Institui a Equipe de Coordenação Setorial da Defesa (ECS/Def). Diário Oficial da União: Seção 1, Brasília, DF, 15 ago. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gm-md-n-4.138-de-14-de-agosto-de-2023-503286617. Acesso em: 27 jun. 2024.

BUEGER, Christian; LIEBETRAU, Tobias; FRANKEN, Jonas. **Security threats to undersea communications cables and infrastructure–consequences for the EU**. SEDE Committee of the European Parliament, PE702, v. 557, 2022.

CARTER, Lionel. **Submarine cables and the oceans: connecting the world**. Cambrigde: UNEP/Earthprint, 2009.

CLAUSEWITZ, Carl von. **Da Guerra**. Tradução de Michael Howard e Peter Paret. Tradução do inglês para o português por CMG (RRm) Luiz Carlos Nascimento e Silva do Valle. 1. ed. Brasília, DF: Ministério da Defesa, 1984.

COURTOIS, Olivier; BARDELAY-GUYOT, Caroline. **Undersea Fiber Communication Systems**. Cambridge: Academic Press, 2016.

EUA. Joint Chiefs of Staff. **Cyberspace Operations**. Washington, DC: Department of Defense, 2018. Disponível em: https://irp.fas.org/doddir/dod/jp3_12.pdf. Acesso em: 21 jul. 2024.

FREIRE, Alexandre; AQUINO, Vicente. Por uma política de Segurança Nacional para a infraestrutura de cabos submarinos. **Teletime**. 04 dez. 2023. Disponível em: https://teletime.com.br/04/12/2023/por-uma-politica-de-seguranca-nacional-para-a-infraestrutura-de-cabos-submarinos/. Acesso em: 27 jun. 2024.

HOSTMIDIA. **O que são protocolos de Internet e quais os mais usados?** Disponível em: https://www.hostmidia.com.br/blog/protocolos-de-internet/#:~:text=Resumidamente,%20protocolos%20s%C3%A3o%20regras%20definidas. Acesso em: 24 jul. 2024.

HUNKER, Jeffrey; HUTCHINSON, Robert; MARGULIES, Jonathan. Attribution of cyber attacks on process control systems. In: **Critical Infrastructure Protection II 2**. Springer US, 2008. p. 87-99.

JANCZEWSKI, Lech; COLARIK, Andrew. **Cyber Warfare and Cyber Terrorism**. Nova Iorque, EUA: Information Science Reference, 2008.

KASPERSKY. **O que é um Firewall?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/firewall. Acesso em: 24 jul. 2024.

KOCHER, José Mauro. **Cabos submarinos no século XIX: considerações técnicas e econômicas**. Anais Eletrônicos do 14º Seminário Nacional de História da Ciência e da Tecnologia–14º SNHCT, 2014.

LAC BLOG. **Anti-malware: o que é, como funciona e quais são os tipos de detecção de ameaças**. Disponível em: https://blog-pt.lac.tdsynnex.com/anti-malware-o-que-e-como-funciona-e-quais-sao-os-tipos-de-deteccao-de-ameacas. Acesso em: 24 jul. 2024.

MAGLARAS, Leandros. Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures**. ICST Transactions on Security and Safety**, v. 18, n. 6, p. 1-10, 2018.

MANDARINO Junior, Raphael. **Segurança e defesa do espaço cibernético Brasileiro**, Cubzac Editora, Recife, 2010.

MARIANO, Rogério. **Panorama de cabos submarinos no Brasil: passado, presente e futuro**. IX Fórum de cabos submarinos. Rio de Janeiro, 2020. Disponível em: https://forum.ix.br/files/apresentacao/arquivo/985/IX%20Forum%202020%20-%20Panorama%20Cabos%20Submarinos%20no%20Brasil%20-%20v0.3.pdf. Acesso em: 12 jun. 2024.

MARTINAGE, Robert. Under the sea: The vulnerability of the commons. **Foreign Affairs**, v. 94, p. 117, 2015.

OAZEN, Eduardo Valente; DIAS, Marco Antônio Schwingel. **História antiga das linhas submarinas**. Rio de Janeiro: Petrobras, 2019.

OTAN. Ministry of Defense. **AJP-3.20 Doctrine for Cyberspace Operations**. UK: OTAN/NATO, 2020. Disponível em: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf. Acesso em: 21 jun. 2024.

SECHRIST, Michael. **New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems**. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2012. Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/sechrist-dp-2012-03-march-5-2012-final.pdf. Acesso em: 27 jun. 2024.

SHERMAN, Justin. **Cyber Defense across the Ocean Floor**. Atlantic Council, 2021. Disponível em: https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf. Acesso em: 13 jun. 2024.

SILVA, Júlio Cezar. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. **Revista da Escola de Guerra Naval**, v. 20, n. 1, p. 193-211, 2014.

SILVA, Mauro Costa da. **Os primeiros cabos submarinos: ciência e tecnologia a serviço do poder**. Anais Scientiarum História IV, v.1., p. 263-269, 2011.

TELEGEOGRAPHY. **Submarine Cable Frequently Asked Questions.** Disponível em: https://www2.telegeography.com/submarinecable-faqs-frequently-asked-questions. Acesso em: 19 jun. 2024.

TRUVER, Scott. Mines and underwater IEDs in US ports and waterways: Context, threats, challenges, and solutions. **Naval War College Review**, v. 61, n. 1, p. 106-127, 2008.

TZU, Sun. **A Arte da Guerra**. 2. ed. São Paulo: Editora Martins Fontes, 2009.

VICHI, Leonardo Perin; AYRES PINTO, Danielle Jacon; DE SÁ, André Luiz Nery. A Defesa da Infraestrutura de Cabos Submarinos: por uma interface entre a Defesa Cibernética ea Segurança Marítima no Brasil. **Revista da Escola de Guerra Naval**, v. 26, n. 2, 2020.

WIENER, Norbert. **Cybernetics or Control and Communications in the Animal and Machine**. Cambridge: MIT Press, 1948.

ZETTER, Kim. **Contagem regressiva até zero day: stuxnet e o lançamento da primeira arma digital do mundo**. Tradução de Alan de Sá, Davidson Boccardo, Fabian Martins, Lucila Bento. 1. ed. Rio de Janeiro: Brasport, 2017. 432 p.