UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

EDSON DE OLIVEIRA PEIXOTO NETO

AS AMEAÇAS HÍBRIDAS E CIBERNÉTICAS AOS CABOS SUBMARINOS DE COMUNICAÇÃO E AS LIMITAÇÕES DA CNUDM: UMA ANÁLISE DOS INCIDENTES NO MAR BÁLTICO (2023–2024)

São Cristóvão/SE
2026

EDSON DE OLIVEIRA PEIXOTO NETO

AS AMEAÇAS HÍBRIDAS E CIBERNÉTICAS AOS CABOS SUBMARINOS DE COMUNICAÇÃO E AS LIMITAÇÕES DA CNUDM: UMA ANÁLISE DOS INCIDENTES NO MAR BÁLTICO (2023–2024)

Trabalho apresentado como requisito para aprovação na disciplina de TCC 2 do curso de Relações Internacionais da Universidade Federal de Sergipe.

Orientadora: Prof.ª Dra. Flávia de Ávila.

São Cristóvão/SE

2026

Às mulheres que me moldaram, em especial à minha mãe, cuja dedicação incansável ampliou o horizonte das minhas possibilidades.

AGRADECIMENTOS

Finalizar este ciclo é compreender que esta conquista é coletiva. Agradeço à minha família, meu porto seguro, pelo amparo que sustentou cada etapa dessa trajetória. Obrigado pelo apoio incondicional, pela compreensão nos momentos de ausência e pelo incentivo constante para que eu seguisse firme na construção do caminho que escolhi trilhar. Morar longe de quem se ama é aprender a viver com um pedaço de si em outro lugar; nestes três anos e meio de distância, a saudade foi uma constante, mas o cuidado atravessou quilômetros.

À minha mãe, o grande amor da minha vida, agradeço por ter me ensinado sobre o poder transformador da educação. Obrigado por cada ligação diária que, mais do que rotina, me trazia de volta para casa todos os dias. O som da sua voz e as perguntas "você já almoçou? está tudo bem? como foi na escola?" me mantiveram firme nos dias mais difíceis, lembrando-me de que, não importa a distância, eu nunca estive sozinho.

Ao meu pai, agradeço por me ensinar que o verdadeiro saber vai muito além dos livros e que jamais devemos esquecer as nossas raízes. À minha irmã, pela amizade de uma vida inteira e por ser meu lugar de escuta, ensinando-me diariamente o valor da paciência. À minha tia, pelas histórias que me abriram os olhos para o poder infinito da cultura e da fé. À minha avó, que, no auge dos seus 95 anos e enfrentando o Alzheimer, ainda teima em me guardar na memória. Às vezes a lembrança demora a chegar, mas ela sempre me encontra.

Minha gratidão se estende também à minha orientadora, Prof.ª Dra. Flávia de Ávila, pela confiança e pela orientação, fundamentais para o amadurecimento deste trabalho. Aos membros da banca examinadora, Prof. Dr. Cairo Junqueira e Prof. Dr. Rodrigo de Albuquerque, registro meu agradecimento pela disponibilidade, pelas críticas e observações que elevaram o nível desta pesquisa. À Universidade Federal de Sergipe, agradeço por me receber e proporcionar o ambiente que tornou possível esta jornada; estendo este reconhecimento aos demais docentes que, ao longo destes anos, contribuíram não apenas para meu crescimento acadêmico, mas para minha formação humana.

Por fim, não poderia deixar de agradecer aos meus amigos, Luisa, Mariana, Leonardo, Geovanna e Manuela, que dividiram comigo os altos e baixos deste caminho e se fizeram família enquanto estive longe da minha. A vocês, deixo minha gratidão sincera.

A todos que, direta ou indiretamente, fizeram parte desta jornada, deixo este trabalho como um pequeno gesto de retribuição ao investimento, ao tempo e, acima de tudo, ao amor que depositaram em mim. No fim das contas, são as conexões que cultivamos ao longo do caminho que nos lembram que ninguém chega a lugar algum sozinho.

RESUMO

O presente estudo analisa a vulnerabilidade da infraestrutura de cabos submarinos, essencial para a conectividade global, diante de ameaças híbridas e cibernéticas. A pesquisa formula o seguinte problema: como tais ameaças evidenciam os limites do regime normativo da Convenção das Nações Unidas sobre o Direito do Mar (CNUDM) na proteção dessas infraestruturas críticas? O referencial teórico baseia-se na teoria das Infraestruturas Críticas e na governança global, enquanto a metodologia adota uma abordagem qualitativa, pautada em pesquisa bibliográfica, análise documental e no exame empírico de incidentes paradigmáticos ocorridos no Mar Báltico (2023–2024). Os principais achados revelam que a CNUDM padece de anacronismo normativo ao focar apenas no dano material, ignorando agressões lógicas e ataques cibernéticos. Identifica-se uma crise de imputabilidade jurídica exacerbada pelo uso de frotas fantasmas e táticas de negação plausível em zonas cinzentas, as quais desafiam os critérios clássicos de atribuição. Conclui-se pela necessidade de adoção de um Protocolo Adicional ou de instrumento internacional vinculante específico, apto a superar a lógica estritamente civil da responsabilização e a instituir mecanismos ampliados de jurisdição internacional voltados à proteção das infraestruturas que sustentam a conectividade digital global.

Palavras-chave: direito internacional; infraestruturas críticas; governança global; segurança marítima.

ABSTRACT

This study examines the vulnerability of submarine cable infrastructure, essential to global connectivity, in the face of hybrid and cyber threats. It addresses the following research question: how do such threats reveal the limits of the normative regime established by the United Nations Convention on the Law of the Sea (UNCLOS) in protecting these critical infrastructures? The theoretical framework is grounded in Critical Infrastructure theory and global governance approaches, while the methodology adopts a qualitative design based on bibliographic research, documentary analysis, and the empirical examination of paradigmatic incidents that occurred in the Baltic Sea (2023–2024). The main findings indicate that UNCLOS suffers from normative anachronism by focusing exclusively on material damage while disregarding logical intrusions and cyberattacks. The study identifies a crisis of legal attribution, exacerbated by the use of shadow fleets and plausible-deniability tactics in gray-zone operations, which challenge classical standards of attribution. It concludes that there is a need for the adoption of an Additional Protocol or a specific binding international instrument capable of overcoming the strictly civil logic of liability and establishing expanded mechanisms of international jurisdiction aimed at protecting the infrastructures that sustain global digital connectivity.

Keywords: international law; critical infrastructures; global governance; maritime security.

LISTA DE ABREVIATURAS E SIGLAS

A2/AD - *Anti-Access/Area Denial*

AI - Inteligência Artificial

AIS - *Automatic Identification System*

AWS - *Amazon Web Services*

BBNJ - *Biodiversity Beyond National Jurisdiction*

CAGR - Taxa de Crescimento Anual Composta

CDI - Comissão de Direito Internacional

CHS - Convenção sobre o Alto Mar

CIA - Confidencialidade, Integridade e Disponibilidade

CIJ - Corte Internacional de Justiça

CIP - Proteção De Infraestrutura Crítica

CISA - *Cybersecurity and Infrastructure Security Agency*

CLP - Controlador Lógico Programável

CLS - *Cable Landing Stations*

CNUDM - Convenção das Nações Unidas sobre o Direito do Mar

C-OTDR - *Coherent Optical Time Domain Reflectometry*

CPZ - *Cable Protection Zone*

DAS - *Distributed Acoustic Sensing*

DDoS - Negação de Serviço Distribuída

DLT - *Distributed Ledger Technology*

DoS - Negação de Serviço

ENISA - *European Union Agency for Cybersecurity*

EUA - Estados Unidos da América

FAO - Organização das Nações Unidas para a Alimentação e a Agricultura

FCC - *Federal Communications Commission*

FOC - Bandeiras de Conveniência

FOD - *Flags of Deceit*

GCP - *Google Cloud Platform*

GPS - *Global Positioning System*

HEIST - *Hybrid Space and Submarine Architecture*

IC - Infraestruturas Críticas

ICPC - Comitê Internacional de Proteção de Cabos

ICS - Sistema de Controle Industrial

ILA - *International Law Association*

IOC - *Initial Operational Capability*

ISO - *International Organization for Standardization*

ITLOS - Tribunal Internacional do Direito do Mar

IU - *Interrogator Unit*

JEF - *Joint Expeditionary Force*

JRO - *JEF Response Option*

LEO - *Low Earth Orbit*

MARCOM - *Allied Maritime Command*

MDO - *Multi-Domain Operations*

MEO - *Medium Earth Orbit*

MSA - *Maritime Situational Awareness*

NBI - *National Bureau of Investigation*

NETCONF - *Network Configuration Protocol*

NMCSCUI - *NATO Maritime Centre for Security of Critical Undersea Infrastructure*

NMS - Sistema de Gerenciamento de Rede

NOAA - *National Oceanic and Atmospheric Administration*

ONU - Organização das Nações Unidas

OSI - *Open Systems Interconnection*

OTAN - Organização do Tratado do Atlântico Norte

PCCIP - *President's Commission on Critical Infrastructure Protection*

PFE - *Power Feeding Equipment*

PSMA - *Port State Measures Agreement*

S3A - *Seabed-to-Space Situational Awareness*

SAR - *Synthetic Aperture Radar*

SCL - *Smart Contracting Layer*

SNMP - *Simple Network Management Protocol*

SPS - *Science for Peace and Security*

SUA - *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*

SWIFT - *Society for Worldwide Interbank Financial Telecommunication*

TIC - Tecnologia da Informação e Comunicação

UAV - Veículo Aéreo Não Tripulado

UE - União Europeia

UIT - União Internacional de Telecomunicações

UIT-T - Setor de Normatização das Telecomunicações da União Internacional de Telecomunicações

USV - Veículo de Superfície Não Tripulado

UUV - Veículo Subaquático Não Tripulado

YANG - *Yet Another Next Generation*

ZEE - Zona Econômica Exclusiva

SUMÁRIO

1 INTRODUÇÃO

A infraestrutura de cabos submarinos constitui, hoje, um dos elementos mais críticos e paradoxalmente invisíveis da economia global e da arquitetura da conectividade digital contemporânea. Responsáveis pela transmissão de mais de 95% do tráfego internacional de dados, esses sistemas físicos sustentam desde comunicações governamentais e transações financeiras até o funcionamento de redes sociais e serviços em nuvem (Carter *et al*., 2009). Apesar de sua relevância estratégica, o tema permanece pouco explorado na literatura de Relações Internacionais, dos Estudos de Segurança e da Governança Global, ao mesmo tempo em que, no campo do Direito Internacional, apresenta omissões significativas e uma abordagem fragmentada. Bueger e Liebetrau (2021) atribuem essa escassez analítica à chamada "tripla invisibilidade" (p. 393) que caracteriza essa infraestrutura. A primeira camada decorre de sua própria natureza. Operando em segundo plano, os cabos submarinos acabam por ser naturalizados e esquecidos, característica constitutiva das tecnologias modernas, que tendem a desaparecer do campo da atenção à medida que se consolidam como arranjos sociotécnicos maduros, funcionando de modo aparentemente automático e contínuo (Edwards, 2003).

Em segundo lugar, a invisibilidade é reforçada por sua localização física, que, ao se encontrarem submersos, causa pouca interferência visível no cotidiano, tornando-os uma das formas mais ocultas de infraestrutura (Starosielski, 2012). Por fim, a terceira camada revela-se ainda mais profunda, pois esses sistemas não se encontram apenas ocultos sob a superfície terrestre, mas inseridos no ambiente marítimo, um espaço historicamente concebido como vazio ou periférico, afastado da experiência cotidiana da maioria das populações em terra e frequentemente reduzido a uma simples via de passagem (Steinberg, 2001), fenômeno associado à persistente "cegueira marítima" (Bueger; Edmunds, 2017, p. 1294).

Embora o termo tenha sido originalmente cunhado para criticar a negligência política e pública em relação à dependência estratégica do mar, a formulação contemporânea do conceito evoluiu para diagnosticar uma lacuna epistemológica estrutural nas Relações Internacionais. Nesse enquadramento, identifica-se a persistência de uma "armadilha territorial" (*territorial trap*) (Agnew, 1994, p. 53), responsável por tratar historicamente o oceano como um vazio social ou mero pano de fundo logístico para a projeção de poder continental, e não como um espaço dotado de dinâmicas políticas próprias (Agnew, 1994; Bueger; Edmunds, 2017). A superação dessa cegueira requer o reconhecimento do domínio marítimo como um complexo de segurança denso e interligado, marcado por sua

“liminaridade” (*liminality*) (Bueger; Edmunds, 2017, p. 1300), entendida como a condição em que as distinções entre terra e mar tornam-se porosas, e estruturado pela intersecção indissociável de quatro dimensões: segurança nacional, economia azul, segurança humana e ambiente marinho (Bueger; Edmunds, 2017).

Mais recentemente, essa crítica foi aprofundada mediante a formulação do conceito de “afasia marítima” (*maritime aphasia*) (Sowden-Carvalho; Valença, 2025, p. 1), utilizado para indicar que o problema não se limita à invisibilidade perceptiva, mas envolve também uma insuficiência ontológica da própria linguagem disciplinar, ainda fortemente estruturada por categorias territoriais herdadas do paradigma vestfaliano (Sowden-Carvalho; Valença, 2025). Sob essa perspectiva, o espaço oceânico tende a ser filtrado por noções de soberania, fronteira e controle espacial que obscurecem sua ontologia fluida e conectiva (Sowden-Carvalho; Valença, 2025), contribuindo para a naturalização de infraestruturas como os cabos submarinos enquanto meros suportes técnicos. A vulnerabilidade desses sistemas, portanto, não decorre apenas de sua exposição física, mas também de uma limitação cognitiva persistente, conforme apontam Bueger e Edmunds (2017), que dificulta a formulação de arranjos de governança compatíveis com sua natureza transjurisdicional.

Essa invisibilidade técnica, espacial e, sobretudo, epistemológica torna-se particularmente problemática em um contexto geopolítico no qual os cabos submarinos deixaram de ser meros meios de telecomunicação para assumir a condição de instrumentos estratégicos de poder. Integrados ao núcleo da infraestrutura digital, esses sistemas expõem, de forma crescente, a ausência de mecanismos eficazes de governança global voltados à sua proteção, segurança e resiliência. Nesse contexto, a intensificação da interdependência digital entre Estados, empresas e indivíduos transforma os cabos submarinos em alvos potenciais de disputas geopolíticas e operações hostis de natureza híbrida e cibernética, que combinam estratégias convencionais, desinformação e ataques digitais, com impactos diretos sobre a estabilidade das comunicações globais. A opacidade que envolve essas infraestruturas tem favorecido a ocorrência de casos recentes de sabotagens, ataques cibernéticos e incidentes não atribuídos a atores específicos, evidenciando sua vulnerabilidade sistêmica e suscitando questionamentos quanto à suficiência do regime jurídico internacional atualmente aplicável.

No âmbito desse arcabouço normativo, a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), adotada em 1982 e frequentemente qualificada pela doutrina como a “constituição dos oceanos”, continua sendo o principal instrumento normativo que disciplina a instalação, manutenção e proteção dos cabos submarinos (ONU, 1982; Carter *et al*., 2009; Keating-Bitonti, 2023). Entretanto, concebida em um período anterior à revolução

digital, a Convenção não contemplou as dimensões tecnológicas e estratégicas associadas à segurança cibernética e à proteção de dados, limitando-se, em seus artigos 112 a 115[1], a regular aspectos técnicos e responsabilidades por danos físicos aos cabos. Este anacronismo normativo ilustra um déficit mais amplo de governança global, em que a arquitetura jurídica internacional não acompanha a velocidade e a singularidade das transformações tecnológicas que caracterizam a era digital moderna.

Essa lacuna normativa torna-se ainda mais evidente quando se observa que as ameaças contemporâneas não se restringem ao rompimento material dos cabos, mas abrangem também a interceptação de informações, a manipulação de sinais ópticos e a exploração de vulnerabilidades digitais, práticas que escapam à lógica tradicional de dano físico e à estrutura jurídica concebida pela CNUDM (Davenport, 2015). Essa insuficiência da Convenção diante das novas ameaças revela, na ótica da governança global, um desafio jurídico mais amplo: o descompasso entre o ritmo acelerado das transformações tecnológicas e a capacidade adaptativa do Direito Internacional Público. A ausência de disposições específicas sobre ataques cibernéticos, operações híbridas e responsabilidades compartilhadas em zonas marítimas complexas cria um vácuo normativo que fragiliza a governança global das infraestruturas digitais críticas. Como observa Davenport (2015), embora a CNUDM tenha consolidado um marco robusto de direitos e deveres para a exploração dos mares, sua eficácia depende de interpretações dinâmicas e de uma constante atualização institucional, especialmente em temas que emergiram após sua adoção, como a proteção de fluxos de dados e a cibersegurança marítima. A análise das ameaças híbridas e cibernéticas dirigidas aos cabos submarinos insere-se em uma reflexão mais ampla sobre a capacidade do Direito Internacional de responder às novas configurações de poder e vulnerabilidade próprias da era digital.

O presente estudo formula, portanto, o seguinte problema de pesquisa: como as ameaças híbridas e cibernéticas dirigidas aos cabos submarinos de comunicação evidenciam as limitações do regime normativo previsto na Convenção das Nações Unidas sobre o Direito do Mar (CNUDM) no que tange à proteção dessas infraestruturas críticas? Busca-se, assim, examinar se o arcabouço jurídico internacional vigente é adequado para responder aos desafios contemporâneos da segurança digital global e, caso não o seja, em que medida se

[1] Em síntese, o escopo normativo dos artigos 112 a 115 da CNUDM estrutura um regime de tutela eminentemente material. O artigo 112 consagra a liberdade de instalação de cabos no leito marinho; o artigo 113 impõe aos Estados o dever de adotar leis e regulamentos que estabeleçam sanções para a ruptura ou danificação intencional ou culposa dos cabos; enquanto os artigos 114 e 115 concentram-se na disciplina da responsabilidade civil e compensatória entre operadores por danos operacionais ou sacrifício de equipamentos (BRASIL, 1990).

mostra necessária a atualização ou complementação desse regime, de modo a fortalecer a proteção dessa infraestrutura crítica.

A relevância teórica da pesquisa decorre, primeiramente, de sua dupla dimensão: por um lado, busca-se contribuir para o debate emergente sobre a governança global das infraestruturas digitais críticas, em um contexto marcado pela crescente militarização e instrumentalização política do ciberespaço; por outro, pretende-se analisar os descompassos estruturais e a adaptabilidade do Direito Internacional clássico, historicamente fundado na centralidade do Estado e na materialidade do território, diante da natureza difusa, interconectada e desmaterializada das ameaças digitais. A questão assume também relevância jurídica e estratégica, uma vez que a integridade dos cabos submarinos está diretamente vinculada à soberania digital dos Estados, à continuidade de serviços essenciais e à estabilidade das comunicações globais. Compreender a exiguidade da CNUDM significa, sob esse prisma, refletir sobre a capacidade do Direito Internacional contemporâneo de garantir a segurança das democracias diante de novas modalidades de conflito que transcendem as fronteiras tradicionais e extrapolam o escopo originalmente concebido pela norma.

O objetivo geral deste estudo consiste em analisar de que maneira as ameaças híbridas e cibernéticas dirigidas aos cabos submarinos de comunicação evidenciam as limitações do regime normativo previsto na CNUDM no que diz respeito à proteção dessas infraestruturas críticas. Para alcançar esse propósito, são perseguidos objetivos específicos integrados ao percurso analítico: (i) contextualizar a importância estratégica dos cabos submarinos na era digital, analisando a tipologia das ameaças contemporâneas; (ii) analisar as disposições da CNUDM aplicáveis à proteção dos cabos, identificando suas limitações estruturais, os desafios de responsabilização e as possibilidades e limites da interpretação funcional frente às novas ameaças; e (iii) examinar as limitações das disposições da CNUDM na proteção de infraestruturas submarinas frente às ameaças híbridas e cibernéticas, tomando como referência os incidentes ocorridos no Mar Báltico entre 2023 e 2024.

No que se refere à metodologia, a pesquisa adota uma abordagem qualitativa, de natureza exploratória e analítico-descritiva, fundamentada na análise de fontes primárias e secundárias do Direito Internacional Público e das Relações Internacionais. O estudo combina revisão bibliográfica especializada, com ênfase na doutrina jurídica, na literatura de segurança cibernética e governança global, à análise documental de instrumentos normativos relevantes. Nesse sentido, examinam-se de forma articulada a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM) e a Convenção Internacional para a Proteção dos Cabos Submarinos, de 1884, consideradas marcos centrais do regime jurídico aplicável à instalação,

manutenção e proteção dessas infraestruturas. A análise histórico-normativa desses instrumentos permite identificar a herança legal, as continuidades, bem como as lacunas e os limites estruturais de um arcabouço normativo concebido em contextos tecnológicos distintos. Complementarmente, recorre-se ao exame de incidentes documentados envolvendo redes de infraestrutura submarina no Mar Báltico entre 2023 e 2024, selecionados por sua relevância empírica e capacidade ilustrativa, com o objetivo de evidenciar, na prática, as limitações do regime jurídico vigente diante de ameaças híbridas e cibernéticas. A partir dessa triangulação metodológica, busca-se articular o plano normativo, o contexto geopolítico e a dimensão tecnológica, permitindo avaliar a suficiência do Direito Internacional contemporâneo frente às transformações da era digital.

Cumpre ressaltar, sob o prisma metodológico, uma limitação inerente ao recorte temporal e à natureza empírica do objeto de estudo. Os incidentes analisados no Mar Báltico, a exemplo das diligências envolvendo as embarcações *Yi Peng 3* e *Eagle S*, constituem eventos geopolíticos extremamente recentes, cujos desdobramentos fáticos e processuais permanecem juridicamente indeterminados. Enquanto o inquérito do primeiro esbarra em entraves diplomáticos e na exclusividade jurisdicional do Estado de bandeira, o segundo encontra-se em fase recursal após o declínio de jurisdição em primeira instância (Andersson *et al*., 2025; SUBMARINE NETWORKS, 2025). Consequentemente, a reconstrução fática elaborada neste estudo apoia-se majoritariamente em relatórios preliminares, declarações governamentais e fontes abertas, conferindo caráter provisório às conclusões factuais sobre a autoria dos ataques. Não obstante, essa contingência empírica não compromete a validade da análise jurídica e estratégica. Pelo contrário, a opacidade informacional, a morosidade probatória e a impossibilidade de atribuição imediata constituem os traços definidores das operações em zona cinzenta, funcionando, nesta pesquisa, como evidência empírica da insuficiência do regime de responsabilização previsto na CNUDM.

No plano empírico, embora a fundamentação teórica abarque tanto vulnerabilidades físicas quanto lógicas, incluindo sistemas de gestão de rede (*Network Management Systems* – NMS), os incidentes recentes no Mar Báltico evidenciam a predominância tática da sabotagem material dos cabos. A pesquisa adota, portanto, uma perspectiva integrada da segurança cibernética, compreendendo-a a partir de sua dimensão infraestrutural. No estágio atual da guerra híbrida, a interrupção cinética por meio de âncoras e arrasto revela-se o vetor preferencial de ataque à conectividade digital, sobretudo por explorar as lacunas de atribuição jurídica da CNUDM relativas aos acidentes de navegação, cenário no qual a negação plausível se mostra particularmente eficaz.

A sistematização contemporânea do campo analítico sobre cabos submarinos organiza-se, de modo geral, em três abordagens principais. A primeira corresponde ao eixo securitário, voltado à proteção dessa infraestrutura frente a ameaças associadas a guerras híbridas, disputas geopolíticas e ações terroristas. A segunda adota uma perspectiva técnico-operacional, voltada aos riscos, falhas e danos operacionais, bem como às estratégias de manutenção, redundância e resiliência da rede. Por fim, a terceira vertente é de natureza jurídico-institucional, direcionada à análise dos marcos regulatórios vigentes, sobretudo no plano internacional, e às possibilidades de seu aprimoramento diante das lacunas normativas existentes (Bueger; Liebetrau, 2021). Em conjunto, essas perspectivas oferecem um arcabouço analítico integrado, permitindo mapear vulnerabilidades, identificar assimetrias de poder e avaliar os limites da governança global dessas infraestruturas, justificando a organização do presente trabalho.

Seguindo as abordagens identificadas na literatura, o trabalho está organizado em três capítulos, além desta introdução e das considerações finais. O primeiro capítulo dedica-se à contextualização da infraestrutura digital submarina, examinando a evolução e a centralidade dos cabos submarinos para a conectividade e para a economia global, sua progressiva elevação ao status de infraestrutura crítica e a tipologia das ameaças contemporâneas que incidem sobre esses sistemas. O segundo capítulo desloca a análise para o plano jurídico-institucional, desenvolvendo uma contextualização teórica e conceitual da governança global e investigando o regime de proteção dos cabos submarinos, com ênfase nas disposições da Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), em suas lacunas normativas diante das novas ameaças e no desafio estrutural da atribuição e da responsabilização internacional. O terceiro capítulo desenvolve uma análise empírica centrada nos incidentes ocorridos no Mar Báltico entre 2023 e 2024, examinando o contexto estratégico e geopolítico da região, as reações estatais observadas e, por meio desse cenário concreto, a confirmação empírica das inadequações da CNUDM para responder adequadamente às ameaças híbridas e cibernéticas dirigidas aos cabos submarinos de comunicação. Por fim, a conclusão apresenta a síntese dos resultados obtidos e indica, com base na literatura especializada, a necessidade de desenvolvimento de novos instrumentos normativos internacionais, diante das deficiências estruturais do regime atualmente aplicável à proteção dos cabos submarinos.

2 A INFRAESTRUTURA DIGITAL SUBMARINA: CONTEXTO, DEPENDÊNCIA E AMEAÇAS

A desmistificação da chamada "nuvem" digital exige, primordialmente, o reconhecimento da infraestrutura material que sustenta a circulação global de dados e informa a própria arquitetura do poder contemporâneo. Longe de constituírem meros artefatos técnico-comerciais, os cabos submarinos de fibra óptica consolidaram-se como o alicerce físico da economia digital e da conectividade transoceânica, tornando-se progressivamente centrais para o funcionamento das sociedades modernas. Essa centralidade, forjada ao longo de uma trajetória tecnológica marcada pela intensificação da interdependência sociotécnica, converteu a dependência informacional em uma vulnerabilidade de natureza soberana, deslocando o leito marinho para o núcleo das preocupações estratégicas e geopolíticas.

Nesse sentido, a compreensão da materialidade dos cabos submarinos é indissociável da definição de espaço cibernético. Este não deve ser compreendido apenas como um ambiente virtual abstrato, mas como um domínio global dentro do ambiente de informações composto por uma rede interdependente de infraestruturas de tecnologia da informação (JOINT CHIEFS OF STAFF, 2018). Conforme definido por Singer e Friedman (2014), o ciberespaço abrange o domínio das redes de computadores em que as informações são armazenadas, compartilhadas e comunicadas, incluindo não apenas a dimensão virtual, mas os sistemas físicos e infraestruturas, a exemplo dos cabos de fibra óptica[2], que permitem o fluxo desses dados. É importante ressaltar que, embora frequentemente associados, ciberespaço e Internet não são sinônimos: o primeiro constitui o domínio caracterizado pelo uso de eletrônicos e do espectro eletromagnético, enquanto a segunda, rede central baseada em computadores, surgiu décadas depois; assim, o ciberespaço pode existir sem a Internet, mas esta só existe graças a ele (Kuehl, 2009; Cepik *et al*., 2014). Sob a ótica normativa brasileira, o Ministério da Defesa o caracteriza como o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, no qual as informações digitais transitam, são processadas e/ou armazenadas (BRASIL, 2015, p. 106). Portanto, a infraestrutura de cabos

[2] Os cabos submarinos de comunicações são compostos por fibras ópticas, um condutor elétrico, um elemento interno de reforço em aço e uma capa protetora de polipropileno de qualidade marítima, projetados para suportar condições ambientais adversas por até 25 anos. Dependendo do local de assentamento, o cabo pode receber uma blindagem protetora (utilizada na plataforma continental) composta por fios de aço. Cabos sem blindagem protetora são geralmente instalados em águas oceânicas profundas e possuem diâmetro típico de 17 a 20 milímetros, enquanto cabos de fibra óptica blindados podem atingir até 50 milímetros de diâmetro. As seções de cabos e os amplificadores, responsáveis por reforçar os sinais luminosos transportados pelas fibras, são montados quase integralmente em fábrica, acondicionados em tanques e posteriormente carregados em navios especializados para instalação (Burnett *et al*., 2015, p. 10, tradução nossa).

submarinos de comunicação funciona como a sustentação material essencial para a existência e funcionalidade desse domínio.

É nesse contexto que se inscreve o presente capítulo, dedicado a compreender como sistemas historicamente invisibilizados foram progressivamente reconfigurados como infraestruturas críticas, passando a integrar agendas de segurança nacional, governança global e resiliência sistêmica. O processo de securitização dos cabos submarinos revela uma inflexão teórica e política na qual se observa a convergência entre a exposição estrutural e sistêmica do suporte físico e a volatilidade do espaço cibernético, inaugurando uma ecologia de riscos marcada pela articulação entre ameaças físicas, cibernéticas e híbridas que, ao explorarem as interdependências do sistema, desafiam a resiliência das redes e a soberania dos Estados.

2.1 CABOS SUBMARINOS COMO ESPINHA DORSAL DA CONECTIVIDADE GLOBAL E ECONOMIA DIGITAL

A proeminência contemporânea dessa rede, consolidada como o alicerce físico do ciberespaço, é o resultado de um processo histórico de longa duração que remonta ao século XIX, quando a instalação dos primeiros cabos telegráficos transatlânticos inaugurou uma nova era de comunicação quase instantânea entre potências políticas e centros econômicos, sobretudo entre a Europa e a América do Norte. O cabo de 1866, o primeiro cabo telegráfico[3] transatlântico a operar de forma estável, não representou apenas um marco tecnológico ao reduzir drasticamente o tempo de transmissão de mensagens entre os dois continentes, mas também criou um novo regime de circulação de informação, permitindo o intercâmbio de formas inéditas de coordenação diplomática, financeira e jornalística. Como argumenta Standage (1999), esse sistema telegráfico inaugurou uma lógica sociotécnica comparável, em seus efeitos estruturantes, ao advento da internet.

Assim, ao longo do século XX, as redes telegráficas submarinas passaram por uma rápida expansão e profunda transformação, mas o salto qualitativo que consolidou sua relevância geoeconômica ocorreu apenas a partir da década de 1980, com a introdução da fibra óptica. Essa inovação transformou as capacidades de transmissão ao permitir fluxos de dados exponencialmente maiores, maior segurança e menor interferência. Paralelamente, uma profunda reconfiguração organizacional ocorreu no setor: o modelo tradicional, baseado predominantemente em consórcios estatais ou operadoras públicas, deu lugar a uma

[3] O primeiro cabo telegráfico submarino bem-sucedido foi instalado em 1850, conectando Dover (Inglaterra) a Calais (França), ainda com tecnologia rudimentar (Carter *et al*., 2009, p. 5, tradução nossa).

governança composta por empresas privadas, consórcios internacionais e, mais recentemente e de forma crescente, grandes provedores de conteúdo e *hyperscalers*[4], que passaram a financiar e, em muitos casos, controlar diretamente segmentos inteiros de cabos transoceânicos, buscando otimizar latência, capacidade e controle sobre rotas estratégicas (Martino, 2024; Sunak, 2017; Bueger; Liebetrau, 2021). Essa reconfiguração institucional modificou profundamente a geopolítica da infraestrutura digital, pois transferiu o poder decisório para corporações transnacionais capazes de moldar rotas, *hubs* e redundâncias segundo interesses comerciais próprios, fenômeno esse que deslocou a governança para fora das estruturas estatais e fragilizou os mecanismos internacionais de responsabilização, coordenação e resposta a incidentes.

A materialidade dessa rede revela sua importância estratégica: estima-se que aproximadamente 95% das comunicações intercontinentais transitem atualmente por cabos submarinos (Carter *et al*., 2009), os quais movimentam, diariamente, cerca de 10 trilhões de dólares apenas no setor financeiro (Johnson, 2017). Com mais de 1,48 milhão de quilômetros de cabos ópticos assentados no leito oceânico[5], essa malha global constitui o suporte físico da economia digital, da administração pública, dos sistemas financeiros, das redes de defesa e, de forma mais ampla, do exercício da soberania digital pelos Estados. A tendência é que tal dependência se intensifique exponencialmente nos próximos anos, impulsionada pela rápida expansão das redes 5G e pela consolidação de serviços baseados em nuvem (Morcos; Wall, 2021)[6].

Essa importância se acentua quando comparada às alternativas via satélite, uma vez que os cabos submarinos oferecem vantagens substanciais, como maior capacidade de transmissão, menor latência, maior confiabilidade e custos operacionais reduzidos. Esses atributos os posicionam como infraestruturas estruturalmente indispensáveis à conectividade global (NOAA, 2024). Como reflexo direto desse cenário, projeta-se que a demanda por

[4] São grandes provedores globais de serviços em nuvem, como Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP), reconhecidos como os três principais provedores de *hyperscalers* do mundo, responsáveis pela operação de vastas infraestruturas de *data centers* interconectados e pela oferta de capacidade de armazenamento e processamento em grande escala (Montevirgen, s.d.; Blancato; Carr, 2024).

[5] Em agosto de 2025, contabilizavam-se 597 cabos submarinos em operação ou em fase de construção, representando um aumento notável em relação aos 559 registrados no ano anterior, de acordo com dados da TeleGeography.

[6] Segundo relatórios compilados de mercado (MARKETSANDMARKETS, 2025; OPENPR, 2025; PERSISTENCE MARKET RESEARCH, 2025), o mercado global de sistemas de cabos submarinos demonstra um crescimento robusto. Em 2024, o tamanho do mercado foi estimado em US$ 18,16 bilhões, com projeções de aumento para aproximadamente US$ 33,75 bilhões até 2030, o que representa uma Taxa de Crescimento Anual Composta (CAGR) de 11,1% de 2025 a 2030. Projeções mais amplas indicam que o mercado geral de cabos submarinos poderá alcançar US$ 56,9 bilhões até 2035, com um CAGR de 6,3% ao longo da década. Especificamente para o mercado de cabos de fibra óptica submarinos, a expectativa é que atinja US$ 59,3 bilhões em 2032, com um CAGR de cerca de 12,6% entre 2025 e 2032.

largura de banda praticamente dobre nos próximos quatro anos (SUBTEL FORUM, 2023). Esse conjunto de fatores evidencia que os cabos submarinos deixaram de ser apenas uma infraestrutura tecnológica de suporte para assumir o papel de elemento estruturante da economia digital e da própria ordem internacional contemporânea.

A crescente dependência global de fluxos massivos de dados, somada à concentração geográfica de rotas e pontos de amarração, transformou os cabos submarinos em elementos cuja importância ultrapassa o domínio técnico das telecomunicações. A robustez tecnológica contrasta com vulnerabilidades operacionais e normativas que tornam esses sistemas suscetíveis a falhas acidentais, interferências geopolíticas e operações maliciosas, sobretudo em um cenário marcado por disputas estratégicas no domínio digital. Esse conjunto de fatores desencadeou um processo de reconceitualização dos cabos submarinos no plano político e securitário, levando Estados, organizações internacionais e pesquisadores a classificá-los como parte integrante das infraestruturas críticas modernas, categorização fundamental para compreender tanto sua centralidade quanto os desafios de segurança que a cercam.

2.2 A EVOLUÇÃO ESTRATÉGICA DOS CABOS SUBMARINOS COMO INFRAESTRUTURA CRÍTICA

A transformação histórica e tecnológica dos cabos submarinos criou as condições para que essa infraestrutura fosse progressivamente reconfigurada como um ativo crítico de segurança nacional e internacional. À medida que a conectividade global passou a depender quase integralmente de redes ópticas transoceânicas, sua proteção deixou de ser apenas uma questão técnica para se tornar tema de *high politics*[7], inserido no centro das agendas de defesa, governança digital e resiliência sistêmica. Essa elevação dos cabos submarinos ao estatuto de ativo estratégico não constitui um fenômeno isolado, mas expressa uma inflexão mais ampla na forma como sistemas técnicos essenciais passaram a ser compreendidos no pensamento de segurança contemporâneo. A centralidade atribuída à conectividade global insere-se, assim, no processo histórico de consolidação do arcabouço teórico das Infraestruturas Críticas (IC),

[7] Refere-se às questões de importância existencial para o Estado, concernentes à sua própria sobrevivência e segurança contínua. Fundamentado na tradição realista e neorealista das Relações Internacionais, este termo estabelece uma hierarquia de prioridades na qual a segurança militar e a defesa nacional dominam, subordinando questões sociais, econômicas e humanitárias à categoria de *Low Politics* (Keohane; Nye, 2011). De acordo com Jeremy Youde (2016), classificar um tema como *High Politics* implica operar sob uma "mentalidade de crise", exigindo respostas imediatas e justificando, muitas vezes, a suspensão dos processos políticos normais em favor de medidas extraordinárias de segurança.

que passou a interpretar a segurança não mais a partir de ativos individuais, mas da vulnerabilidade estrutural de redes interdependentes.

A emergência desse enquadramento analítico não se deu de forma súbita, mas resultou de uma evolução histórica conceitual, na qual distintas tradições analíticas, de natureza militar, sistêmica, tecnológica e de gestão de riscos, convergiram para redefinir a relação entre segurança, desenvolvimento e interdependência sociotécnica. A vulnerabilidade de sistemas vitais constitui uma preocupação anterior à própria formalização do conceito de IC, tendo suas raízes na teoria do bombardeio estratégico[8] e na percepção de que sociedades industrializadas dependem do funcionamento contínuo de redes interligadas de produção, transporte e comunicação (Collier; Lakoff, 2008). No pós-Segunda Guerra Mundial e, de modo mais sistemático, durante a Guerra Fria, esse raciocínio foi aprofundado por meio da defesa civil e da análise de sistemas, que passaram a empregar modelos quantitativos e simulações para estimar os efeitos sistêmicos de ataques sobre a capacidade de recuperação econômica e institucional dos Estados. Esse deslocamento analítico marcou a transição da proteção de ativos isolados para a preocupação com a resiliência de sistemas complexos, estabelecendo as bases conceituais que, décadas mais tarde, permitiriam a consolidação do arcabouço das IC no campo da segurança internacional.

Esse conjunto de bases conceituais encontrou seu momento de consolidação na década de 1990, quando transformações simultâneas no ambiente estratégico internacional e na base tecnológica das economias avançadas conferiram proeminência política à noção de Infraestruturas Críticas. A institucionalização desse enquadramento foi impulsionada, em especial, por dois vetores complementares: de um lado, a reorientação das agendas de segurança nacional no pós-Guerra Fria, marcada pelo declínio da ameaça militar convencional e pela busca de novos referenciais capazes de justificar e orientar os aparatos de defesa diante de riscos difusos, assimétricos e frequentemente não estatais; de outro, a intensificação da dependência de infraestruturas informacionais, cuja rápida expansão passou a converter a superioridade tecnológica das sociedades avançadas em fonte paradoxal de vulnerabilidade estrutural (Cavelty, 2007). A crescente interconexão entre sistemas ampliou a percepção de que a própria vantagem tecnológica produzia vulnerabilidades desproporcionais, passíveis de serem exploradas por atores incapazes de enfrentar o poder militar convencional, mas capazes

[8] A teoria do bombardeio estratégico, formulada no período entre as Guerras Mundiais, constitui uma doutrina militar que redefiniu a condução da guerra ao deslocar o foco do confronto direto entre forças armadas para o ataque sistemático aos centros vitais das sociedades industrializadas. Associada inicialmente a Giulio Douhet e posteriormente desenvolvida nos Estados Unidos, essa abordagem, ancorada na noção de "guerra total", sustentava que a destruição seletiva de "nós" industriais e infraestruturais essenciais poderia comprometer simultaneamente a capacidade material e a coesão política do adversário (Collier; Lakoff, 2008).

de gerar efeitos sistêmicos por meio de ataques a pontos vitais do território e da economia. Redefine-se, assim, a própria segurança nacional como gestão de riscos associados à dependência de redes interdependentes, deslocando-se da defesa territorial clássica para um paradigma orientado à resiliência sistêmica e à governança de infraestruturas críticas.

A cristalização do arcabouço teórico das ICs no plano político-institucional ocorreu nos Estados Unidos entre meados da década de 1990 e o final da administração Clinton, em resposta a eventos e dinâmicas que tornaram visível a interdependência entre sistemas físicos e informacionais. O atentado de Oklahoma City[9], em 1995, é recorrentemente apontado como fator catalisador desse processo, ao demonstrar que um ataque localizado podia produzir efeitos em cascata sobre processos administrativos, econômicos e institucionais distantes do local do evento, em razão da interconexão sistêmica. O episódio converteu-se, pragmaticamente, em um dos primeiros marcos empíricos a estabelecer um nexo entre ameaças físicas e vulnerabilidades de infraestruturas informacionais, ao revelar que a destruição de ativos materiais era capaz de comprometer fluxos de dados e funções estatais essenciais.

Ao tornar visível a articulação entre terrorismo, dependência informacional e vulnerabilidades assimétricas, o evento revelou os limites do paradigma tradicional de segurança nacional, deslocando o foco analítico para a gestão de riscos associados à interrupção de infraestruturas interdependentes. Essa reconfiguração do enquadramento da ameaça na agenda de segurança norte-americana passou a incorporar, de forma integrada, terrorismo, ciberameaças, infraestruturas e, progressivamente, segurança interna. Como resposta institucional, a administração Clinton instituiu, em 1996, a *President's Commission on Critical Infrastructure Protection* (PCCIP), cujo relatório *Critical Foundations*, publicado em 1997, estabeleceu de modo explícito que a segurança nacional, a prosperidade econômica e o modo de vida da sociedade estadunidense dependiam da resiliência de infraestruturas físicas e cibernéticas interligadas. Tal orientação foi posteriormente formalizada por meio das Diretivas de Decisão Presidencial 62 e 63, em 1998, que converteram o arcabouço teórico emergente em política de Estado, formalizando a proteção de Infraestruturas Críticas como responsabilidade compartilhada entre governo e setor privado (Cavelty, 2007).

Inicialmente consolidada no contexto doméstico norte-americano, essa matriz interpretativa não permaneceu circunscrita à política de segurança dos Estados Unidos, mas

[9] O atentado de Oklahoma City consistiu na detonação de um caminhão-bomba diante do *Alfred P. Murrah Federal Building*, resultando em 168 mortos e 853 feridos, além do colapso parcial da estrutura e de danos extensos no entorno (UNITED STATES. Department of Justice, 2000).

foi progressivamente difundida e internalizada por instâncias centrais da governança internacional. Organizações como a União Europeia (UE) e a Organização do Tratado do Atlântico Norte (OTAN) passaram a adotar definições convergentes de infraestruturas críticas, incorporando a noção de interdependência sistêmica e de vulnerabilidade transversal como elementos estruturantes de suas agendas de segurança. A Diretiva (UE) 2022/2557 materializa essa convergência ao definir infraestruturas críticas como "um ativo, instalação, equipamento, rede ou sistema, ou parte destes, necessário para a prestação de um serviço essencial"[10] (EUROPEAN UNION, 2022, art. 2.º, § 4, tradução nossa). No mesmo movimento de difusão normativa, os cabos submarinos foram formalmente incorporados ao rol de componentes críticos da infraestrutura global de comunicações. As Nações Unidas, já em 2010, classificaram-nos como "infraestrutura crítica de comunicações" (UNITED NATIONS, 2010), advertindo que falhas técnicas ou ataques deliberados poderiam produzir efeitos sistêmicos, desde a paralisação de fluxos financeiros internacionais até a interrupção de serviços públicos essenciais. Essa classificação permite compreender que a criticidade dos cabos submarinos não decorre apenas do volume de dados que transportam, mas de seu papel estrutural na sustentação da conectividade global, da soberania digital dos Estados e do funcionamento integrado das demais infraestruturas essenciais da economia contemporânea.

Subjacente à difusão desse arcabouço normativo, as ICs são entendidas como sistemas, ativos ou serviços essenciais à continuidade das funções vitais do Estado e da sociedade, cuja interrupção ou destruição gera efeitos sistêmicos em larga escala, afetando economias, soberania e bem-estar social. A criticidade não se baseia apenas em características isoladas dos ativos, mas, sobretudo, em sua inserção em sistemas sociotécnicos altamente interdependentes, tornando essa interdependência o elemento central para compreender a vulnerabilidade e o valor estratégico dessas infraestruturas (Collier; Lakoff, 2008; Cavelty, 2007; De Bruijne; Van Eeten, 2007; Aven, 2015). A partir desse enquadramento, impõe-se o aprofundamento da noção de criticidade propriamente dita, cuja evolução teórica é marcada por interpretações divergentes acerca dos elementos que conferem centralidade e vulnerabilidade a uma infraestrutura. Metzger (2004) propõe uma distinção analítica entre duas dimensões complementares: a primeira refere-se à criticidade como conceito simbólico, pelo qual determinadas infraestruturas são inerentemente críticas devido ao seu papel ou função na sociedade; a segunda compreende a criticidade como conceito sistêmico, segundo o

[10] No original: "'critical infrastructure' means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service."

qual um componente se torna crítico em razão de sua posição estrutural dentro de um sistema interdependente, de modo que sua falha compromete o funcionamento do conjunto. Dessa forma, a combinação dessas dimensões amplia significativamente o espectro de elementos classificados como críticos, sobretudo em sistemas altamente acoplados, nos quais disfunções aparentemente periféricas podem desencadear efeitos em cascata com elevado grau de imprevisibilidade (Cavelty, 2007).

A análise é refinada pela distinção entre a criticidade baseada na vulnerabilidade, referente àquelas infraestruturas cujo colapso gera consequências severas independentemente da probabilidade de o evento ocorrer, da criticidade baseada no risco, que decorre da interação entre a severidade dos efeitos e a probabilidade de ocorrência, seja por falha técnica, acidente ou ataque intencional (Aven, 2015). A criticidade é um atributo relacional e dinâmico, dependente das interdependências sociotécnicas que conectam setores como energia, comunicações, finanças e segurança pública (Collier; Lakoff, 2008; De Bruijne; Van Eeten, 2007). Sob essa chave analítica compreende-se a criticidade das infraestruturas de informação e comunicação (TIC), em especial dos cabos submarinos. A centralidade desses sistemas não decorre apenas de sua função estrutural enquanto infraestrutura nodal de transmissão de dados, mas de sua função sistêmica ampliada, ao integrar, sustentar e viabilizar a operação de praticamente todas as demais infraestruturas críticas contemporâneas. Infere-se, por conseguinte, uma forma de criticidade composta, na qual vulnerabilidade, risco, interdependência e significado estratégico convergem, elevando os ativos subaquáticos à condição de componentes vitais na arquitetura global de conectividade. Tais vulnerabilidades adquirem, hoje, relevância estratégica em um ambiente internacional marcado por tensões geopolíticas, expansão do ciberespaço como domínio de conflito e crescente recorrência de ameaças híbridas.

2.3 TIPOLOGIA DAS AMEAÇAS CONTEMPORÂNEAS: FÍSICAS, CIBERNÉTICAS E HÍBRIDAS

A partir da consolidação dos cabos submarinos como infraestrutura crítica de alta interdependência, a identificação das ameaças que incidem sobre esse sistema torna-se elemento indispensável para compreender sua vulnerabilidade estrutural no ambiente internacional contemporâneo. Em sistemas sociotécnicos complexos e fortemente acoplados, os riscos não decorrem apenas da fragilidade material, mas da interação de múltiplos vetores físicos, digitais e político-estratégicos (Collier; Lakoff, 2008; De Bruijne; Van Eeten, 2007).

Assim, as ameaças aos cabos submarinos não podem ser analisadas como eventos isolados, mas como manifestações de uma ecologia de riscos que se retroalimentam e podem produzir efeitos sistêmicos. Para fins analíticos, é útil classificá-las em três macrodomínios: físicos, cibernéticos e híbridos, permitindo identificar tanto suas especificidades quanto as interações que moldam a lógica contemporânea de risco e potencializam os impactos.

Entre os três macrodomínios, a dimensão física constitui a face historicamente mais visível e documentada das vulnerabilidades dessa infraestrutura, permanecendo até hoje como a principal causa de interrupções globais de conectividade[11]. Embora a discussão contemporânea reconheça a crescente relevância das operações híbridas e do espectro cibernético, estudos técnicos e estatísticos realizados por entidades governamentais, centros de pesquisa estratégica e organizações industriais indicam que a esmagadora maioria dos incidentes ainda decorre de danos acidentais ou ambientais. Esses eventos refletem uma combinação de fragilidades estruturais, pressões operacionais crescentes e restrições intrínsecas à condição material dessa malha global. Nesse contexto, para fins analíticos, as ameaças físicas podem ser agrupadas em duas subcategorias analíticas: (i) danos acidentais decorrentes de atividades humanas; e (ii) eventos de origem natural.

Dentro da dimensão física, os cabos submarinos foram historicamente concebidos para operar em um ambiente hostil, sujeito a pressões elevadas, corrosão marinha, abrasão sedimentar e perturbações geológicas. Apesar das evoluções tecnológicas, como blindagem multicamadas, materiais sintéticos mais resistentes, instalação em profundidade e ampliação dos padrões de redundância, a infraestrutura permanece sensível a riscos físicos de múltiplas naturezas. Os danos decorrentes da atividade humana constituem o fator mais recorrente de interrupções físicas. Análises de registros de falhas indicam que entre 80% e 90% dos incidentes estão associados a atividades marítimas, especialmente pesca e ancoragens mal posicionadas em águas rasas, isto é, em profundidades inferiores a 200 metros (Qiu, 2025; RECORDED FUTURE, 2025). Nessas áreas a intensa presença humana com baixa redundância operacional aumenta a probabilidade de contato involuntário, fricção mecânica e consequente dano acidental aos sistemas.

Além dos riscos decorrentes de atividades humanas, os cabos submarinos também estão sujeitos a ameaças de origem natural, como terremotos submarinos, erupções vulcânicas e deslizamentos sedimentares, capazes de provocar rupturas simultâneas em múltiplos

[11] Segundo a União Internacional de Telecomunicações (2024), com base em dados do International Cable Protection Committee (ICPC), ocorrem anualmente entre 150 e 200 falhas em cabos submarinos, exigindo em média três reparos por semana.

segmentos de rede. Episódios como os registrados no Estreito de Luzon[12], em 2006, e no Mediterrâneo Oriental[13], em 2008, demonstram a magnitude potencial desses eventos e sua capacidade de gerar interrupções generalizadas de conectividade. Em termos globais, as falhas decorrentes de perigos naturais correspondem a uma parcela relativamente reduzida das ocorrências totais, situando-se entre 10% e 20%. (Clare, 2025; RECORDED FUTURE, 2025). No conjunto, esses dados revelam que, embora estatisticamente minoritárias, essas ameaças possuem elevado potencial disruptivo[14] e tendem a se tornar particularmente críticas em sistemas que operam com baixa redundância ou alto grau de interdependência estrutural, condições que amplificam o risco de efeitos em cascata sobre a conectividade global.

Paralelamente, análises específicas para o período de 2024–2025 indicam que cerca de 31% dos danos relatados publicamente permanecem classificados como de causa não identificada (RECORDED FUTURE, 2025), ou seja, não há evidências conclusivas que permitam determinar sua origem, como fragmentos de equipamentos, marcas de arrasto ou sulcos no fundo marinho associados a ancoragens. Essa categoria residual revela não apenas obstáculos à capacidade de investigação em ambientes submarinos, mas também o caráter intrincado dos processos de diagnóstico operacional em redes transoceânicas de grande escala.

Para além dessas vulnerabilidades materiais, surge um segundo eixo de ameaças associado ao domínio cibernético. A crescente digitalização dos sistemas de telecomunicações ampliou a superfície de ataque, expondo centros de controle, redes corporativas, sistemas de telemetria e softwares especializados a tentativas de intrusão, manipulação ou interrupção. Diferentemente dos domínios tradicionais (terrestre, naval e aéreo), o ciberespaço caracteriza-se pela baixa barreira de entrada, forte assimetria entre atacantes e defensores e, sobretudo, pela dificuldade de atribuição, fator que limita respostas políticas e militares (Nye, 2011).

---

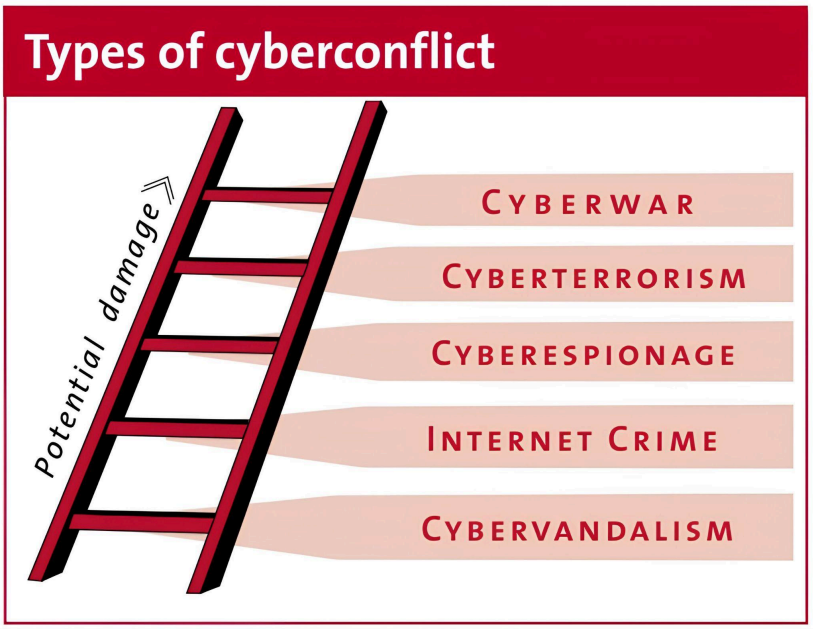
[12] O terremoto de Hengchun, de magnitude 7,1, ocorrido no fundo marinho ao sul de Taiwan em dezembro de 2006, desencadeou um grande deslizamento de sedimentos que rompeu pelo menos nove cabos submarinos no Estreito de Luzon, entre Taiwan e as Filipinas. Essa ruptura gerou uma interrupção severa na conectividade da Ásia-Pacífico, comprometendo serviços essenciais, incluindo comunicação corporativa, operações financeiras e tráfego de Internet, em países como China, Singapura, Taiwan, Japão e Filipinas. Foram registradas 21 falhas nos cabos, exigindo o envio de 11 navios especializados e 49 dias para a completa restauração dos serviços (INTERNATIONAL CABLE PROTECTION COMMITTEE, 2007).

[13] Em janeiro-fevereiro de 2008, dois cabos submarinos foram danificados no mar Mediterrâneo, próximo de Alexandria (Egito), causando uma interrupção de até 70% da conectividade de internet no Egito e impactos em outros países da Ásia-Pacífico (SUBMARINENETWORKS, 2008; ABC NEWS, 2008).

[14] Projeções indicam que o aquecimento atmosférico alterará os padrões de precipitação e a descarga fluvial, aumentando o volume de sedimentos instáveis nas plataformas continentais. Com a aceleração de tempestades intensas devido às mudanças climáticas, espera-se que riscos geológicos, como correntes de turbidez e deslizamentos submarinos, se tornem ainda mais recorrentes nas próximas décadas (Carter *et al*., 2009; Bueger; Liebetrau, 2021).

A complexidade intrínseca ao domínio cibernético, marcada pela assimetria operacional e pela opacidade dos atores, impõe a necessidade de instrumentos analíticos capazes de distinguir a gravidade, a intencionalidade e os efeitos das ações hostis. Nesse esforço de sistematização, o modelo da escada cibernética (*cyberladder*), desenvolvido por Cavelty (2010), organiza as operações no ciberespaço ao longo de um *continuum* de intensidade, considerando tanto o dano potencial quanto a motivação política subjacente. Essa estrutura é particularmente útil para enquadrar incidentes situados na chamada "zona cinzenta", ao evidenciar o ponto em que interferências de baixo impacto passam a assumir relevância estratégica para a segurança nacional e para a proteção de infraestruturas críticas.

Figura 1 – Tipos de conflitos na escada cibernética (*Cyberladder*)



Fonte: Cavelty (2010).

Como ilustrado na figura, o modelo pauta-se na premissa de que o perigo concreto de um incidente é proporcional à sua ascensão nos níveis de hostilidade. No patamar inferior, situa-se o cibervandalismo ou ciber-hacktivismo, focado na modificação ou destruição virtual de conteúdos com efeitos limitados e transitórios. Os níveis intermediários compreendem o crime na internet e a ciberespionagem[15], eventos que ocorrem rotineiramente voltados ao lucro ou à coleta de dados e que, embora graves, muitas vezes operam de forma independente de conflitos estatais declarados. No topo da estrutura, situam-se o ciberterrorismo, que

[15] Como pontua Cavelty (2010), a convergência entre o crime na internet e a ciberespionagem constitui, na atualidade, o desafio de maior gravidade enfrentado pela comunidade internacional, em virtude da recorrência de incidentes e da magnitude dos prejuízos, estimados em US$ 1 trilhão anualmente, que vitimam sobretudo o setor corporativo.

envolve ataques ilegais de atores não estatais para intimidar ou coagir populações e governos, exigindo violência física ou a geração de temor considerável, e a ciberguerra, que foca em conflitos bélicos no espaço virtual visando influenciar a vontade e as capacidades de decisão das lideranças políticas e militares do oponente estratégico (Cavelty, 2010).

O enfrentamento desse espectro de ameaças exige, portanto, um arcabouço de cibersegurança que transcenda o âmbito estritamente técnico. Embora o termo ainda careça de uma definição universalmente aceita no âmbito acadêmico (Belli *et al*., 2023), a ausência de um conceito oficial e taxativo não deve ser compreendida como sinal de fragilidade conceitual, mas, antes, como expressão da natureza intrinsecamente dinâmica e multifacetada do ciberespaço. Tal característica impõe que qualquer formulação seja dotada de flexibilidade e adaptabilidade, de modo a abarcar as múltiplas dimensões que a estruturam, sejam elas técnicas, humanas, jurídicas ou políticas. Não obstante, a definição de maior reconhecimento institucional no sistema internacional foi estabelecida pelo Setor de Normatização das Telecomunicações da União Internacional de Telecomunicações (UIT-T), órgão das Nações Unidas, segundo a qual:

> Cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de riscos, ações, treinamentos, boas práticas, garantias e tecnologias que podem ser utilizados para proteger o ciberespaço e os ativos da organização e dos usuários. Os ativos da organização e dos usuários incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações e a totalidade das informações transmitidas e/ou armazenadas no ciberespaço. A cibersegurança busca assegurar a conquista e a manutenção das propriedades de segurança da organização e dos ativos dos usuários contra riscos de segurança relevantes no ciberespaço. Os objetivos gerais de segurança compreendem: Disponibilidade; Integridade — que pode incluir autenticidade e não repúdio; e Confidencialidade[16] (UIT-T, 2008, p. 2, tradução nossa).

A análise de incidentes nesse domínio deve partir da estrutura fundamental da segurança da informação, tradicionalmente sintetizada pela "Tríade CIA", composta por Confidencialidade, Integridade e Disponibilidade[17]. Esse modelo orienta tanto a avaliação de riscos quanto a seleção de contramedidas técnicas e organizacionais, deslocando a atenção do

[16] No original: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality."

[17] No original: "Confidentiality, Integrity, Availability."

mero ato de intrusão para os efeitos que ele provoca sobre objetivos estratégicos e operacionais (Whitman; Mattord, 2021). Nesse cenário, ataques cibernéticos tendem a buscar o comprometimento de sistemas computacionais e das informações neles contidas, afetando qualquer um dos três pilares da segurança da informação (Singer; Friedman, 2014), frequentemente como meio para a consecução de finalidades políticas, econômicas ou militares mais amplas.

No que se refere à Confidencialidade, busca-se garantir que a informação seja acessível apenas a usuários autorizados. Uma violação desse princípio ocorre quando há acesso não autorizado a redes de computadores, permitindo monitoramento de atividades e extração de dados sensíveis, prática frequentemente associada à espionagem cibernética. A Integridade, por sua vez, assegura que dados e sistemas operem sem alterações não autorizadas. Ataques direcionados a esse pilar nem sempre têm como finalidade obter informações, mas sim modificá-las sem detecção, o que permite manipular dados no ambiente virtual e influenciar sistemas e pessoas que deles dependem no mundo real, podendo constituir estratégias sofisticadas de sabotagem ou subversão de dispositivos físicos. Por fim, a Disponibilidade garante que serviços e sistemas estejam acessíveis sempre que necessário. Seu comprometimento consiste em impedir o acesso legítimo a uma rede ou serviço, seja por sobrecarga de tráfego, como nos ataques de negação de serviço distribuída (DDoS), seja pela paralisação de processos digitais ou físicos que dependem do sistema afetado (Singer; Friedman, 2014).

Para sistematizar a análise do impacto dessas violações sobre a arquitetura da rede, recorre-se ao Modelo de Referência OSI (*Open Systems Interconnection*), desenvolvido pela Organização Internacional de Padronização (ISO) para padronizar a comunicação entre sistemas computacionais (INTERNATIONAL TELECOMMUNICATION UNION, 1994). O modelo organiza o processo comunicacional em sete camadas hierarquicamente articuladas, que se estendem desde a camada física (*Layer 1*), responsável pela transmissão de sinais, até as interfaces de aplicação utilizadas pelos usuários (Muhamad; Abdulmonim, 2024). Ao decompor a rede em níveis funcionais, essa arquitetura evidencia uma relação de dependência estrutural entre as camadas: embora operem com relativa autonomia lógica, o funcionamento das camadas superiores pressupõe a integridade da infraestrutura material que viabiliza o transporte dos dados (Muhamad; Abdulmonim, 2024). Para a análise da segurança internacional, essa constatação é central, pois demonstra que a interrupção física ou cinética da infraestrutura correspondente à camada física não constitui mero dano infraestrutural, mas mecanismo capaz de produzir efeitos sistêmicos comparáveis aos de ataques conduzidos

exclusivamente no domínio lógico, configurando, na prática, uma forma de negação de serviço (*Denial of Service* – DoS) mediante o comprometimento do substrato material da conectividade (Obaid; Abeed, 2020).

É justamente essa dualidade entre o domínio lógico e o substrato material da conectividade que faz com que, no caso dos cabos submarinos, a cibersegurança ultrapasse o âmbito estritamente técnico, envolvendo implicações estratégicas para a teoria da segurança e para as práticas de governança internacional (Bueger; Liebetrau, 2021). Isso significa que a proteção dessa infraestrutura crítica não se esgota em medidas tecnológicas, implicando a necessidade de mecanismos políticos e jurídicos, capazes de assegurar uma tutela integrada e coordenada, que a engenharia, por si só, não tem condições de prover.

A transposição dessa arquitetura técnica para a proteção de infraestruturas críticas permite converter a abstração dos vetores de ataque em danos mensuráveis à funcionalidade sistêmica. Nesse contexto, o plano jurídico exerce função complementar ao esforço técnico-analítico, buscando enquadrar normativamente os ataques cibernéticos. Referencial central nesse debate, o *Manual de Tallinn 2.0* apresenta a seguinte definição de ciberataque: "uma operação cibernética, ofensiva ou defensiva, que se espera razoavelmente que cause lesão ou morte a pessoas, ou dano ou destruição a objetos"[18] (Schmitt, 2017, p. 415, tradução nossa). Ao incluir expressamente a possibilidade de dano ou destruição de objetos físicos, essa formulação reconhece a dimensão material das operações cibernéticas e conecta o debate jurídico sobre o uso da força às dinâmicas das operações híbridas, nas quais ataques cibernéticos podem ser parte integral de ofensivas híbridas mais amplas, destinadas a desativar defesas ou provocar caos operacional antes de uma ação cinética[19].

Na prática, essa interferência na funcionalidade materializa-se, sobretudo, através da exploração dos sistemas de gestão de rede (NMS)[20], que atuam como o "cérebro" operacional

[18] No original: "A cyber attack is a cyber operation, whether offensive or defensive,that is reasonably expected to cause injury or death to persons or damage or destruction to objects."

[19] Segundo o Glossário das Forças Armadas, ações cinéticas "são aquelas desencadeadas no interior da Área de Operações, que envolvem movimentos (fogos, voos, deslocamento de tropas e de blindados) e produzem resultados tangíveis, como destruição, captura e conquista". Já as ações não cinéticas "são aquelas desencadeadas no interior da Área de Operações, que não envolvem movimentos — como ações de guerra eletrônica, operações psicológicas, ações de assuntos civis ou no ciberespaço — e produzem resultados intangíveis, tais como interferências eletromagnéticas, bloqueio ou a percepção positiva da população sobre as forças amigas e suas operações, mas que contribuem para o sucesso da operação" (BRASIL, 2015, p. 17-19).

[20] Os *Network Management Systems* (NMS) são plataformas integradas concebidas para assegurar a operação, a administração e a manutenção de infraestruturas de comunicações. Em termos operacionais, um NMS "é o processo e a plataforma que permite configurar, monitorar e gerir o desempenho de uma rede" (CISCO, s.d.). Operam a partir da coleta de telemetria de elementos gerenciados (roteadores, transmissores ópticos, repetidores, PFE) por protocolos como SNMP e NETCONF/YANG, consolidando estados, diagnosticando falhas e acionando automações. No contexto dos cabos submarinos, constituem centros de comando para a gestão remota de estações de aterrissagem (*Cable Landing Stations* – CLS), dos equipamentos de transmissão óptica e dos

dessas conexões. A integração desses sistemas de gestão remota introduz uma camada de controle virtualizada na arquitetura de cabos submarinos que, segundo a Agência da União Europeia para a Cibersegurança (ENISA, 2023), amplia o espectro de vetores de ataque lógico incidentes sobre a infraestrutura física. Nesse cenário, atores maliciosos exploram vulnerabilidades em sistemas corporativos para realizar movimentação lateral (*lateral movement*) e comprometer redes operacionais, visando o acesso a sistemas de vigilância e gestão sem necessidade de presença física (FCC, 2025). Esse acesso administrativo ilegítimo permite não apenas a interceptação silenciosa e o redirecionamento de tráfego para jurisdições adversárias, alterando a topologia lógica da rede para fins de espionagem (Sherman, 2021), mas também a sabotagem direta. O cenário mais crítico, descrito na literatura como *kill click*, envolve a manipulação de NMS para deletar remotamente os comprimentos de onda (*wavelengths*) que transportam dados ou desabilitar componentes ativos, causando uma interrupção de serviço comparável a cortes físicos, mas executada via *software*, evidenciando a letalidade das novas formas de hostilidade híbrida (Morcos; Wall, 2021; Papapavlou *et al.*, 2022).

Assim, o paradigma das ameaças desloca-se progressivamente de rupturas acidentais para interrupções, manipulações e interceptações deliberadas, nas quais o alvo prioritário deixa de ser necessariamente o cabo físico, cuja reparação, embora logisticamente complexa, segue protocolos operacionalmente estabelecidos, para concentrar-se no sistema digital que o torna funcional. A gravidade desse deslocamento reside no fato de que um ataque cibernético bem-sucedido e coordenado contra os NMS de múltiplos consórcios poderia conceder a um invasor o controle simultâneo sobre diversas rotas transoceânicas. As consequências seriam sistêmicas e abrangeriam desde a paralisação de sistemas de liquidação financeira global, como o sistema *SWIFT* (*Society for Worldwide Interbank Financial Telecommunication*), que dependem de latência mínima, até a cegueira de sistemas de comando e controle militares que utilizam essa infraestrutura para operar drones e transmitir inteligência em tempo real.

Em resposta a essa vulnerabilidade sistêmica, observa-se, notadamente nos Estados Unidos, um fortalecimento institucional e normativo do setor. A promulgação do *Cybersecurity and Infrastructure Security Agency Act of 2018* constituiu um marco nesse processo, formalizando a CISA (*Cybersecurity and Infrastructure Security Agency*) como órgão central de coordenação da proteção de infraestruturas críticas. A missão da agência evoluiu para incluir a colaboração proativa com o setor privado e parceiros internacionais,

subsistemas de alimentação (*Power Feeding Equipment* – PFE) que sustentam os repetidores submarinos, sendo essenciais para a continuidade e segurança operacional da transmissão (Ford-Ramsden; Davenport, 2014).

com o objetivo de mitigar riscos na cadeia de suprimentos de cabos submarinos e em seus sistemas de gestão. Mais recentemente, a Comissão Federal de Comunicações (FCC) avançou na adoção de medidas regulatórias de caráter vinculante que condicionam o licenciamento de cabos a certificações rigorosas de segurança cibernética, visando assegurar que operadores implementem controles efetivos contra ameaças lógicas e físicas (Ribeiro, 2025). Esse movimento consolida a percepção de que a integridade dos cabos transcende a esfera comercial, afirmando-se como dimensão estratégica da segurança nacional.

Essa mobilização estatal reflete o fato de que a consolidação do ciberespaço como novo domínio estratégico alterou profundamente a lógica da competição interestatal e a natureza da segurança internacional. Se no século XX a disputa geopolítica concentrava-se predominantemente na projeção militar, econômica e tecnológica tradicional, no século XXI o código, entendido como *software*, protocolos, sistemas digitais e algoritmos, passou a constituir uma arena autônoma de disputa política e de instrumento de poder. Nesse sentido, ele atua como regulador, estruturando e condicionando comportamentos no ambiente digital, gerando assimetrias de acesso, governança e controle (Lessig, 2006). Assim, a arquitetura técnica da *internet* e das redes privadas deixou de ser apenas um conjunto de meios operacionais para se tornar um instrumento de política internacional e de extensão da soberania estatal sobre os fluxos de informação.

Essa transformação repercute diretamente na compreensão das infraestruturas críticas, em especial os cabos submarinos. A ascensão de disputas geopolíticas, guerras híbridas e ameaças cibernéticas reconfigurou esses cabos em ativos críticos de natureza geoestratégica, cuja estrutura global de conectividade produz interdependências complexas e vulnerabilidades sistêmicas que podem ser exploradas deliberadamente em cenários de tensão ou conflito, como forma de coerção ou projeção de influência (Bueger; Liebetrau, 2021). Nesse contexto, o código adquire densidade política ao definir as fronteiras do que pode ser acessado, protegido, modificado ou violado. Esse controle, exercido por Estados, empresas ou atores não estatais, configura uma nova forma de poder estrutural, associada à centralidade da infraestrutura digital no funcionamento das sociedades contemporâneas.

A compreensão plena das vulnerabilidades dos cabos submarinos requer ir além da distinção técnica entre vetores físicos e cibernéticos. Na realidade operacional, esses dois domínios não atuam de forma isolada; constituem instrumentos mobilizados dentro de um padrão mais amplo de competição interestatal. É nesse ponto que emerge o conceito de ameaças híbridas, associado a formas de guerra que combinam meios convencionais, operações encobertas, desinformação, pressões econômicas, sabotagem física e intrusão

digital, de forma coordenada e calibrada para explorar vulnerabilidades sistêmicas. Sob essa ótica, os ataques físicos aos cabos, as ações de espionagem digital conduzidas por meio de sistemas de gestão (como os NMS) e a manipulação de fluxos de informação passam a ser entendidos não como eventos dissociados, mas como componentes integrados de estratégias híbridas voltadas à obtenção de vantagem estratégica sem recorrer necessariamente a um confronto direto e declarado.

Essa dinâmica insere-se em uma tradição analítica que antecede a própria consolidação do termo híbrido. Já na década de 1990, Arquilla e Ronfeldt (2001) introduziram o conceito de "guerra em rede" (*netwar*) para descrever formas emergentes de conflito distribuído, indireto e de baixa intensidade, situados fora dos marcos da guerra militar tradicional e caracterizados por estruturas organizacionais descentralizadas e fortemente dependentes de fluxos de informação. A arquitetura do ciberespaço, marcada por interconexões difusas e pela possibilidade de ações encobertas de difícil atribuição, ampliou exponencialmente a viabilidade desse padrão de enfrentamento.

A partir dessa base teórica, o conceito evoluiu para sua formulação moderna, introduzida por Frank Hoffman em 2007. Essa evolução ocorreu diante das transformações dos conflitos do início do século XXI, período em que as fronteiras tradicionalmente estabelecidas entre guerra e paz, combatentes e não combatentes, e entre o espaço físico e o virtual, tornaram-se progressivamente mais difusas. Nessa perspectiva, a guerra híbrida pode ser entendida como a mudança no caráter dos conflitos armados, nos quais adversários violentos combinam, de forma coordenada, diferentes modalidades de combate e meios não militares, com o objetivo de neutralizar o poder militar convencional (Monaghan, 2019). Essa transição expressa a atuação de oponentes que rejeitam as regras e limites historicamente impostos à condução dos conflitos, seja por não se enquadrarem como atores estatais, seja por recorrerem a métodos de pressão e coerção situados abaixo do limiar de uma guerra formalmente declarada. É nesse contexto que, no campo dos estudos estratégicos contemporâneos, o conceito de guerra híbrida consolidou-se como um dos eixos centrais de análise, emergindo com força a partir da década de 2010 em estreita relação com as crescentes

tensões geopolíticas e militares ligadas à política externa da Federação Russa[21] (Bueger; Liebetrau, 2021).

Complementarmente, a expressão "ameaça híbrida" emergiu paralelamente como um conceito polissêmico, sendo objeto de múltiplas definições por parte de acadêmicos e organizações internacionais. O termo designa um desafio de natureza abrangente, caracterizado pelo uso deliberado de meios ambíguos no contexto de uma grande estratégia revisionista predominantemente não violenta. Tais ações exploram a "zona cinzenta" entre a paz e a guerra, empregando de forma coordenada instrumentos políticos, econômicos, civis e informacionais para influenciar a vontade da população e comprometer a capacidade decisória do governo, visando atingir vulnerabilidades estruturais da sociedade sem provocar uma reação típica de um estado formal de guerra (Monaghan, 2019).

Essa compreensão consolidou a percepção de que forças armadas concebidas para missões específicas não seriam suficientes para enfrentar esse padrão de ameaça, tornando indispensáveis capacidades flexíveis e de múltiplo emprego, bem como a integração com outros instrumentos do poder nacional. Como ressalta Monaghan (2019), distinguir ameaça híbrida de guerra híbrida é fundamental para a formulação de políticas de defesa e segurança, na medida em que envolve limiares jurídicos e militares distintos para a resposta estatal. Além disso, tal diferenciação também revela que os atores operam em um espectro contínuo de coerção, no qual a violência formal constitui apenas uma entre diversas ferramentas disponíveis. No caso dos cabos submarinos, esse arcabouço é particularmente útil, uma vez que essas ameaças podem materializar-se tanto por operações de coleta de inteligência e espionagem quanto por sabotagem física ou digital de pontos estratégicos (Davenport, 2015). A combinação entre vetores físicos e cibernéticos permite gerar efeitos ampliados, reduzir a possibilidade de atribuição e explorar a interdependência estrutural do sistema global de conectividade.

Essa lógica não se restringe ao plano teórico. Nos últimos anos, episódios concretos demonstraram como a competição interestatal tem-se materializado na infraestrutura dos cabos submarinos. Regiões estratégicas como o Mar Báltico, o Mar Vermelho e o entorno de

[21] A expressão guerra híbrida ganhou projeção internacional após a anexação da Crimeia pela Federação Russa, em 2014, quando a combinação de forças especiais de atuação "negável", milícias locais por procuração, pressão econômica, campanhas de desinformação e exploração de divisões sociais impôs à Ucrânia e ao Ocidente um *fait accompli*, expressão francesa que significa "fato consumado", isto é, uma situação consolidada antes que a parte adversária possa reagir de forma eficaz. Apesar de associada majoritariamente às ações russas, a noção de guerra híbrida constitui esforço conceitual mais amplo e duradouro para descrever a transformação do caráter da guerra, marcado pela integração de instrumentos militares e não militares visando vantagens assimétricas (Monaghan, 2019).

Taiwan[22] tornaram-se palco de cortes e avarias em cabos submarinos sob circunstâncias envoltas em ambiguidades e dificuldades de atribuição, sinalizando a crescente plausibilidade de ações hostis conduzidas por atores estatais ou paraestatais. Esses episódios exemplificam a operacionalização da chamada "zona cinzenta" entre paz e conflito, caracterizada por operações ofensivas conduzidas abaixo do limiar da guerra declarada e associadas a diferentes graus de negabilidade plausível (Monaghan, 2019). Nesse marco interpretativo, as vulnerabilidades dos cabos submarinos deixam de ser fenômenos isolados para integrar um ecossistema de competição interestatal, no qual a exploração coordenada de fragilidades técnicas, informacionais e operacionais converte-se em instrumento central de projeção de poder.

[22] O Insikt Group identificou quatro incidentes no Mar Báltico envolvendo oito danos distintos a cabos submarinos e cinco incidentes ao redor de Taiwan envolvendo cinco danos distintos a cabos submarinos, ocorridos em 2024 e 2025, dos quais quatro envolveram embarcações ligadas à China ou à Rússia, com propriedade opaca ou manobras suspeitas nas proximidades dos cabos danificados (RECORDED FUTURE, 2025).

3 A PROTEÇÃO DOS CABOS SUBMARINOS NA GOVERNANÇA GLOBAL: REGIME JURÍDICO, LACUNAS NORMATIVAS E O DESAFIO DA ATRIBUIÇÃO

O domínio marítimo encontra-se, na conjuntura presente, em um ponto de inflexão entre a estabilidade normativa herdada do século XX e as vulnerabilidades sistêmicas próprias do século XXI. Sob a ótica da governança global, a investigação interroga a aptidão dos mecanismos de coordenação e dos padrões normativos de conduta vigentes para assegurar a resiliência das redes globais de dados. Partindo da premissa de que a ordem marítima é produto de intencionalidades históricas específicas, examina-se o esgotamento da racionalidade funcional da CNUDM, tradicionalmente orientada à tutela da materialidade do dano físico, frente às ameaças híbridas e progressivamente desmaterializadas. Ainda que se observem iniciativas recentes voltadas ao fortalecimento da governança marinha, tais esforços permanecem estruturados em torno de agendas que não contemplam a dimensão estratégica da segurança informacional, perpetuando lacunas relevantes nos planos penal e civil. Evidencia-se, assim, o descompasso ontológico entre a normatividade e a transformação das formas contemporâneas de agressão, cenário que precipita a crise de imputabilidade em um ambiente marcado pela opacidade operacional e pela erosão dos critérios clássicos de responsabilidade estatal no nexo marítimo-digital.

3.1 A TUTELA NORMATIVA DA CNUDM: FUNDAMENTOS DE GOVERNANÇA E ALCANCE JURISDICIONAL

A governança dos espaços oceânicos constitui, na contemporaneidade, um dos mais sofisticados e desafiadores campos de aplicação do Direito Internacional Público. A multiplicidade de usos do mar, que abrange navegação, exploração de recursos naturais, proteção ambiental e instalação de infraestruturas críticas, projeta os oceanos como um espaço paradigmático de interação entre soberania estatal, interesses econômicos globais e bens públicos internacionais. A governança global afirma-se, aqui, como a categoria analítica central para compreender as respostas normativas e institucionais formuladas pela comunidade internacional diante de problemáticas transnacionais que ultrapassam os limites tradicionais da jurisdição estatal.

No âmbito desta reflexão, amparada nas categorias de James Rosenau (1992), a governança distingue-se de estruturas hierárquicas e estatais formalizadas, dotadas de capacidade coercitiva institucional, ao se referir a um conjunto mais amplo de mecanismos

formais e informais, estatais e não estatais, por meio dos quais atores diversos coordenam comportamentos, estabelecem expectativas normativas e produzem padrões relativamente estáveis de ordem. Essa dinâmica opera fundamentalmente a partir de objetivos compartilhados, significados intersubjetivos e níveis variáveis de aceitação social e política (Rosenau, 1992); trata-se, assim, de um sistema de regras que regula atividades humanas em múltiplos níveis, operando frequentemente como uma "ordem sem governo", especialmente em contextos nos quais a autoridade central se mostra ausente ou difusa. Essa perspectiva permite compreender como a governança articula a ordem e a intencionalidade no sistema internacional, fornecendo a fundamentação para a análise de sua dimensão deliberada e normativa.

Essa distinção assume relevância particular no plano internacional, caracterizado estruturalmente pela ausência de uma autoridade governamental suprema. Em um sistema descentralizado, a governança global não se funda na imposição vertical de normas, configurando-se antes como a produção de uma ordem funcional cuja eficácia depende menos da coerção e mais da deferência reflexiva, da partilha de significados intersubjetivos e da convergência de interesses, operando apenas na medida em que é aceita pela maioria ou pelos atores dotados de maior capacidade de poder e sendo reforçada pela formação de regimes e pelo emaranhamento normativo dos Estados na gestão de problemas transnacionais (Rosenau, 1992; Keohane, 2003; Zürn, 2018). A noção de ordem refere-se aos padrões de comportamento relativamente previsíveis e recorrentes de interação, expressos em arranjos rotinizados que estruturam o funcionamento cotidiano do sistema internacional, podendo emergir de forma espontânea, sem um propósito consciente ou autoridade central, enquanto a governança pode ser entendida como uma "ordem acrescida de intencionalidade", correspondente às ações deliberadas, orientadas por objetivos compartilhados, que incidem sobre esses padrões, buscando mantê-los, regulá-los ou transformá-los (Rosenau, 1992). O termo traduz, portanto, o esforço consciente de conferir direção normativa e funcionalidade ao sistema, assegurando sua estabilidade e adaptação mesmo na inexistência de um governo formal.

A partir desse referencial, a noção de governança revela-se fundamental para compreender a forma pela qual a ordem internacional contemporânea busca responder à crescente complexidade dos espaços comuns globais, entre os quais se insere o domínio marítimo. Ao deslocar o foco exclusivo da autoridade estatal para arranjos normativos mais difusos, baseados na coordenação entre múltiplos atores e na internalização de padrões compartilhados de conduta, a governança explicita tanto o potencial quanto os limites da

regulação em contextos marcados pela ausência de um poder centralizado. A intencionalidade que caracteriza esse modelo não se manifesta por meio de comandos hierárquicos, mas pela estruturação progressiva de expectativas normativas aptas a orientar comportamentos estatais e privados, conferindo previsibilidade e estabilidade às interações internacionais. Mais do que um mecanismo de resposta a oscilações conjunturais, a governança atua, portanto, como uma arquitetura institucional voltada à organização de condutas ao longo do tempo. É precisamente essa noção de intencionalidade que permite diagnosticar a assimetria do regime jurídico vigente: ao examinar a forma como tais princípios se materializam na CNUDM, observa-se uma governança historicamente concebida para pacificar fronteiras e assegurar as liberdades de navegação, mas que, por não ter sido originalmente projetada para regular a segurança das infraestruturas digitais, contribuiu para conformação de um vácuo normativo que hoje vulnerabiliza os cabos submarinos.

Aplicada ao regime jurídico dos oceanos, essa lente teórica situa a CNUDM como um dos exemplos mais bem-sucedidos de produção de ordem no sistema internacional. Ao balizar limites marítimos precisos e codificar as liberdades de navegação e sobrevoo, o tratado mitigou drasticamente a incerteza e a instabilidade que caracterizavam o direito do mar pré-1982. Essa previsibilidade normativa constitui, hoje, o lastro indispensável para empreendimentos de elevado investimento, notadamente a malha de cabos submarinos, cuja operação repousa na expectativa de estrito cumprimento das liberdades consagradas no texto convencional.

Todavia, embora a CNUDM tenha sido notavelmente eficaz na criação de ordem e previsibilidade no uso dos espaços marítimos, sua arquitetura institucional reflete sobretudo as prioridades políticas e econômicas do contexto histórico em que foi concebida. Como observa Oxman (1996), a estrutura da Convenção foi moldada pelo desencanto dos Estados recém-independentes em relação ao direito do mar tradicional e por sua demanda por novos arranjos institucionais que refletissem sua plena participação, o que contribuiu para a centralidade conferida a regimes de exploração, navegação e utilização funcional dos mares. Nesse desenho normativo, as infraestruturas submarinas são reduzidas a uma lógica estritamente técnica e comercial, integrando um regime circunscrito às liberdades de instalação e à responsabilidade civil por danos. O modelo de governança resultante privilegia, assim, a organização procedimental de atividades, em detrimento da formulação de políticas públicas internacionais voltadas à proteção ativa de ativos estratégicos.

No plano normativo, a disciplina jurídica dos cabos submarinos encontra-se dispersa em diversos dispositivos da CNUDM, cuja estrutura reverbera a herança consolidada em

instrumentos pretéritos, como a Convenção para a Proteção de Cabos Telegráficos Submarinos de 1884 e a Convenção de Genebra sobre o Alto-Mar (CHS) de 1958[23]. Esses antecedentes revelam uma lógica regulatória centrada na garantia da liberdade de comunicação e na funcionalidade dos espaços marítimos, orientação que permeia o regime contemporâneo e fundamenta a consagração expressa da liberdade de instalação e manutenção de cabos como prerrogativa tradicional do alto-mar[24], extensiva à Zona Econômica Exclusiva (ZEE)[25] e à plataforma continental[26].

Esse legado normativo, inaugurado em 1884, estabeleceu o reconhecimento internacional de que a danificação voluntária ou decorrente de negligência culpável de cabos submarinos é passível de punição, ao mesmo tempo em que consolidou uma arquitetura jurídica fundada na primazia da jurisdição do Estado de bandeira e na ausência de mecanismos executórios diretos. Um dispositivo dessa Convenção, de renovada relevância contemporânea para o debate sobre a segurança de infraestruturas críticas, é o artigo X[27], que confere aos navios de guerra dos Estados signatários o direito de abordar embarcações mercantes suspeitas de causar danos a cabos em alto-mar (Agnorelli, 2025).

---

[23] A Convenção das Nações Unidas sobre o Alto-Mar (1958) trata especificamente das liberdades do alto-mar; do direito de um Estado de ter navios arvorando sua bandeira, sob condições por ele fixadas, incluindo a controversa exigência de um vínculo genuíno (*genuine link*); dos direitos e obrigações do Estado de bandeira; da pirataria; do direito de visita; da perseguição em alto-mar; e do lançamento de cabos e oleodutos submarinos. Contém, ainda, duas disposições pioneiras sobre a poluição por descarga de petróleo e de resíduos radioativos.

[24] Art. 87, § 1º, alínea c, da Convenção das Nações Unidas sobre o Direito do Mar (1982): "A liberdade do alto-mar compreende, inter alia, para os Estados quer costeiros quer sem litoral, a liberdade de colocar cabos e dutos submarinos, nos termos da Parte VI" (BRASIL, 1990).

[25] Art. 58, § 1º, da Convenção das Nações Unidas sobre o Direito do Mar (1982): "Na zona econômica exclusiva, todos os Estados, quer costeiros quer sem litoral, gozam, nos termos das disposições da presente Convenção, das liberdades de navegação e de sobrevôo e de colocação de cabos e dutos submarinos, a que se refere o artigo 87, bem como de outros usos do mar internacionalmente lícitos, relacionados com as referidas liberdades, tais como os ligados à operação de navios, aeronaves, cabos e dutos submarinos e compatíveis com as demais disposições da presente Convenção" (BRASIL, 1990).

[26] Art. 79 da Convenção das Nações Unidas sobre o Direito do Mar (1982): "Todos os Estados têm o direito de colocar cabos e dutos submarinos na plataforma continental, em conformidade com as disposições do presente artigo. O Estado costeiro não pode impedir a colocação ou manutenção desses cabos ou dutos, ressalvado o seu direito de adotar medidas razoáveis para a exploração da plataforma continental, o aproveitamento de seus recursos naturais e a prevenção, redução e controle da poluição causada por dutos. O traçado das linhas para a colocação de tais dutos fica sujeito ao consentimento do Estado costeiro, permanecendo assegurada sua jurisdição sobre os cabos e dutos que penetrem em seu território ou mar territorial, bem como sobre aqueles relacionados à exploração da plataforma continental ou ao funcionamento de instalações e estruturas sob sua jurisdição" (BRASIL, 1990).

[27] Tradução livre do autor do artigo X da Convenção para a Proteção de Cabos Telegráficos Submarinos (1884): "As infrações à Convenção podem ser comprovadas por todos os meios de prova admitidos pela legislação do Estado do tribunal competente. Quando os comandantes de navios de guerra tiverem razões para acreditar que uma infração foi cometida *(has been committed*) por uma embarcação mercante, podem exigir do capitão ou mestre a apresentação dos documentos oficiais que comprovem a nacionalidade da embarcação. [...] Além disso, os referidos oficiais podem lavrar relatórios formais dos fatos, independentemente da nacionalidade do navio, os quais deverão ser redigidos na forma e na língua do Estado a que pertençam" (CONVENTION FOR THE PROTECTION OF SUBMARINE TELEGRAPH CABLES, 1884).

Tal prerrogativa, contudo, é estritamente delimitada, restringindo-se à verificação da nacionalidade da embarcação e à lavratura de um auto de infração, sem autorizar a prisão da tripulação, o confisco do navio ou o desvio compulsório de sua rota (Ringbom, 2025). Ao preservar a jurisdição penal exclusiva do Estado de bandeira, a Convenção de 1884 institucionalizou uma baixa capacidade de pronta-resposta que a CNUDM viria a mimetizar quase um século depois. Embora a CNUDM não tenha incorporado formalmente o artigo X em seu texto, o tratado de 1884 permanece aplicável entre seus Estados-partes, de modo que o direito de abordagem ali previsto subsiste no plano convencional, ainda que externo à arquitetura normativa da Convenção de 1982 (Agnorelli, 2025).

A aplicabilidade contemporânea desse dispositivo enfrenta, adicionalmente, obstáculos geopolíticos centrais, uma vez que importantes potências marítimas atuais não figuram entre os Estados signatários do tratado original. Nesse cenário, emerge um dissenso interpretativo que tensiona a eficácia dessa herança jurídica. Enquanto os Estados Unidos com respaldo em parcela da doutrina, sustentam que a Convenção de 1884 e, por extensão, o direito de abordagem previsto em seu artigo X teriam se consolidado como norma de Direito Internacional Consuetudinário[28], o que implicaria a validade universal do poder de fiscalização sobre navios suspeitos de dano intencional, independentemente da ratificação formal do tratado pelo Estado de bandeira (Agnorelli, 2025), o Comitê da *International Law Association* (ILA) conclui que tal entendimento não encontra respaldo suficiente na prática estatal contemporânea, permanecendo a aplicação da regra restrita aos Estados partes do tratado de 1884 (Azaria, 2025).

A fragilidade dessa solução normativa é agravada por duas limitações estruturais destacadas pela doutrina especializada. Primeiro, o escopo material da regra de 1884 restringe-se exclusivamente a cabos telegráficos, deixando desprotegidos os modernos sistemas de fibra óptica, redes de transmissão de energia e gasodutos que compõem o leito marinho atual. Segundo, o dispositivo autoriza medidas de execução apenas após a ocorrência do dano consumado, carecendo de eficácia para legitimar as ações preventivas de interdição e interrupção necessárias ao enfrentamento de ameaças híbridas e operações em zona cinzenta (Azaria, 2025).

Sob essa mesma lógica de restrição jurisdicional, a disciplina jurídica dos cabos submarinos na CNUDM estrutura-se, de modo mais específico, nos artigos 112 a 115, que

[28] Essa posição dos Estados Unidos é tradicionalmente fundamentada no *Restatement (Third) of the Foreign Relations of the United States*, § 521 (1986), conforme mencionado no relatório do Comitê da *International Law Association* (2024).

compõem o núcleo regulatório específico aplicável à sua instalação, manutenção e proteção. Esses dispositivos consagram um regime essencialmente funcional, voltado à garantia da liberdade de colocação e conservação de cabos no alto-mar e nas zonas sob jurisdição limitada dos Estados costeiros, ao mesmo tempo em que estabelecem deveres mínimos de diligência e cooperação entre os sujeitos envolvidos. O exame sistemático desse arcabouço revela a dualidade do sistema: evidencia tanto a racionalidade funcional que o orienta quanto as insuficiências estruturais que comprometem sua adequação aos desafios contemporâneos do ambiente marítimo.

Na sequência do regime inaugurado pelo artigo 112, que consagra a liberdade de instalação e impõe o dever de respeito às infraestruturas já existentes, o artigo 113, que trata da ruptura ou lesão de um cabo ou duto submarino, estabelece seu contraponto defensivo. O dispositivo constitui o núcleo da tutela penal dessa infraestrutura, ao estabelecer a obrigação dos Estados de adotarem medidas legislativas e regulamentares nos seguintes termos:

> Todo Estado deve adotar as leis e regulamentos necessários para que constituam infrações passíveis de sanções a ruptura ou danificação, por um navio arvorando a sua bandeira ou por uma pessoa submetida à sua jurisdição, de um cabo submarino no alto mar, causadas intencionalmente ou por negligência culposa, de modo que possam interromper ou dificultar as comunicações telegráficas ou telefônicas, bem como a ruptura ou danificação, nas mesmas condições, de um cabo de alta tensão ou de um duto submarino. Esta disposição aplica-se também aos atos que tenham por objeto causar essas rupturas ou danificações ou que possa ter esse efeito. Contudo, esta disposição não se aplica às rupturas ou às danificações cujos autores apenas atuaram com o propósito legítimo de proteger a própria vida ou a segurança dos seus navios, depois de terem tomado todas as precauções necessárias para evitar tal ruptura ou danificação (BRASIL, 1990, art. 113).

Contudo, a norma não tipifica um crime internacional autônomo; institui, antes, um dever de incriminação no plano doméstico, em estrita consonância com a lógica descentralizada que permeia a Convenção. Ao preservar a exclusividade da jurisdição estatal, tal modelo configura o regime não como um sistema penal de aplicação direta, mas como uma engrenagem de coordenação normativa entre ordens jurídicas nacionais, visando assegurar um padrão mínimo de repressão a condutas lesivas.

Complementam esse arcabouço os artigos 114 e 115, voltados à disciplina da responsabilidade civil por danos causados a infraestruturas já instaladas no leito marinho (BRASIL, 1990). O artigo 114, ao impor o custeio de reparos por prejuízos decorrentes de negligência ou por falta de diligência razoável, institui um regime de alocação de riscos adaptado à crescente densidade de ocupação do fundo oceânico. Tal mecanismo transcende a mera sanção patrimonial, operando como incentivo econômico à cautela na interação entre

atividades conflitantes, como pesca, navegação e instalação de infraestruturas. Em contrapartida, o artigo 115 regula a tensão inversa, assegurando indenização àquele que sacrifica equipamentos, como âncoras ou redes, para preservar a integridade de um cabo e evitar prejuízos mais graves. A norma harmoniza interesses concorrentes por meio de uma lógica compensatória: reconhece a primazia da segurança da navegação, mas distribui os ônus econômicos de modo a fomentar soluções cooperativas entre os diferentes usuários do mar.

Não obstante a aparente funcionalidade desse mecanismo compensatório, a doutrina recente aponta contradições estruturais na arquitetura do artigo 114. A redação do dispositivo revela o que Kwan (2025) define como uma "lógica desajustada" (*awkward logic*). Ao concentrar-se na disciplina da responsabilidade civil entre operadores de cabos e dutos, obrigação que em grande medida já decorreria de princípios gerais do direito, a CNUDM permanece silente quanto à responsabilização de terceiros perpetradores de danos, como embarcações mercantes ou pesqueiras que não operam infraestruturas submarinas. O resultado é a formação de um vácuo de responsabilização em áreas além da jurisdição nacional, pois, ao não prever um regime jurisdicional residual para a reparação de danos causados por atores externos ao setor, a Convenção deixa os operadores dependentes da eventual disposição do Estado da bandeira[29]. Como efeito adicional, o autor destaca que a própria estrutura do artigo pode produzir incentivos contraproducentes ao concentrar riscos financeiros sobre as operadoras responsáveis pela manutenção, especialmente diante do risco de danos acidentais a cabos adjacentes durante os reparos. Cria-se, assim, um cenário no qual se impõem passivos econômicos relevantes sem oferecer, em contrapartida, um regime jurídico eficaz para a proteção da estabilidade sistêmica das redes (Kwan, 2025).

Em conjunto, esses dispositivos consolidam uma lógica predominantemente reparatória que permeia o tratamento conferido pela CNUDM às infraestruturas submarinas, reforçando o caráter eminentemente civil e patrimonial da tutela jurídica estabelecida. Esse enquadramento mostra-se limitado diante da centralidade estratégica das redes contemporâneas, cujas rupturas geram efeitos sistêmicos irredutíveis à mera esfera dos prejuízos individuais. Essa percepção de incompletude torna-se ainda mais evidente com a entrada em vigor, em janeiro de 2026, do Acordo sobre a Biodiversidade Marinha Além da Jurisdição Nacional (*Biodiversity Beyond National Jurisdiction* – BBNJ)[30], que, embora

[29] Na sistemática do Direito do Mar, o Estado da bandeira corresponde ao Estado de registro da embarcação, cuja nacionalidade ela ostenta, exercendo sobre ela jurisdição e controle em alto-mar, nos termos do princípio da exclusividade jurisdicional, o que implica que eventuais medidas sancionatórias e reparatórias dependem, em regra, da atuação desse Estado (BRASIL, 1990, arts. 91 e 92).

[30] Trata-se do tratado, formalmente denominado Acordo no âmbito da Convenção das Nações Unidas sobre o Direito do Mar relativo à Conservação e ao Uso Sustentável da Biodiversidade Marinha em Áreas Além da

represente um avanço relevante na governança oceânica, mantém seu escopo circunscrito à conservação da biodiversidade marinha, deixando a proteção das instalações submarinas em alto-mar majoritariamente submetida ao arcabouço normativo de 1982. Essa escolha reflete, na chave analítica de Rosenau, uma intencionalidade predominantemente preservacionista, que relega a segundo plano a formulação de respostas jurídicas específicas voltadas à segurança física e cibernética da conectividade global, evidenciando a persistência das lacunas estruturais do regime vigente.

3.2 AS LACUNAS DA CNUDM DIANTE DAS NOVAS AMEAÇAS E A CRISE DE IMPUTABILIDADE

A insuficiência do regime anteriormente descrito revela-se no descompasso entre a literalidade do artigo 113 da CNUDM e a tipologia das ameaças cibernéticas contemporâneas. Desse contraste emerge uma incongruência estrutural entre o formalismo da norma, ainda ancorado em uma concepção eminentemente material que condiciona a infração à ocorrência de "ruptura ou lesão", e as dinâmicas imateriais do ciberespaço. Ao restringir a tutela jurídica ao suporte material do cabo, o arcabouço de 1982 deixa à margem a violência lógica que, sem deteriorar a fibra óptica, compromete gravemente sua operacionalidade, confiabilidade e disponibilidade, abrangendo desde intrusões em sistemas de gerenciamento (NMS) e desvio de tráfego de dados até ataques de negação de serviço (DoS) (Davenport, 2015). Essa insuficiência é corroborada pela doutrina especializada, que identifica um vácuo de proteção decorrente da resistência jurídica tradicional em equiparar a perda de funcionalidade a danos materiais tangíveis (Schmitt, 2017). Consequentemente, consolida-se uma "lacuna de segurança" (*security gap*) na qual ações estatais ou não estatais capazes de paralisar fluxos de dados vitais permanecem em uma zona de impunidade, não sendo classificadas nem como crimes nos termos do artigo 113, nem como atos de guerra, o que perpetua a vulnerabilidade sistêmica dessa infraestrutura crítica (Beckman, 2014).

Frente a esse vácuo normativo, o *Tallinn Manual 2.0* surge como um esforço doutrinário para adaptar o Direito Internacional à era digital. Embora desprovido de força jurídica vinculante, o Manual sistematiza o entendimento de especialistas acerca da aplicação

Jurisdição Nacional. O instrumento alcançou o quórum necessário de 60 ratificações em 19 de setembro de 2025 (ONU News, 2025), durante a Assembleia Geral das Nações Unidas, fato que deu início à contagem do prazo de 120 dias para sua entrada em vigor, nos termos do artigo 68 do próprio Acordo (ONU, 2023).

de normas vigentes, transpondo-as a um novo domínio de operações[31] no ciberespaço. Mais do que uma orientação técnica, a obra serve de referencial para as situações que a CNUDM não previu, estipulando critérios para identificar quando uma ação digital ultrapassa os limites da legalidade internacional. A relevância dessa transposição reside, primordialmente, na reinterpretação de dois conceitos basilares: a soberania e o uso da força no ambiente digital.

No que tange à Soberania (Regra 4), o Manual estende o princípio da integridade territorial para abarcar não apenas o espaço físico, mas a infraestrutura cibernética nele situada e as funções que ela sustenta. Para os cabos submarinos, isso implica que a violação da soberania independe de dano material, configurando-se também quando uma operação estrangeira usurpa "funções governamentais inerentes" (Schmitt, 2017). Dessa forma, intrusões digitais que paralisem serviços essenciais, como a defesa nacional, a arrecadação tributária ou processos eleitorais, constituem afronta direta ao Estado, independentemente da integridade física do cabo. Esse entendimento representa um salto qualitativo frente à CNUDM, ao deslocar o eixo da tutela jurídica do objeto para a função estratégica que ele desempenha.

Em contrapartida, a caracterização de um incidente como uso da força (Regra 69) demanda um patamar de gravidade significativamente superior, ancorado no artigo 2º, § 4º[32], da Carta das Nações Unidas. O Manual estipula que a operação deve projetar escala e efeitos análogos aos de ações militares cinéticas, aferição que se pauta no referido "Schmitt Criteria" (Ziolkowski, 2012). Essa matriz analítica pondera oito vetores para mensurar a agressividade do ato: gravidade, imediatidade, diretividade causal, invasividade, mensurabilidade dos efeitos, caráter militar, envolvimento estatal e legalidade presumida (Schmitt, 2017). Essa distinção é vital para a governança dos cabos: enquanto a sabotagem física ou lógica destrutiva (como um *kill switch*) enquadra-se prontamente como uso da força, a espionagem e a coerção econômica situam-se em uma zona de "legalidade presumida" (Schmitt, 2017), ou seja, embora nocivas, elas raramente atingem o limiar do uso da força, permanecendo impunes sob a ótica dos mecanismos clássicos de defesa coletiva da ONU. Ademais, a eficácia de todo esse arcabouço colide com um obstáculo prático anterior à própria qualificação do ato: a imperatividade de identificar o agressor. É nesse nexo que a governança global esbarra no que a doutrina define como "crise de imputabilidade".

---

[31] Conforme registrado no *Tallinn Manual 2.0*, "destina-se a ser uma reafirmação objetiva da *lex lata*. Por conseguinte, os especialistas envolvidos em ambos os projetos evitaram incluir declarações que refletissem *lex ferenda*" (Schmitt, 2017, p. 3, tradução nossa).

[32] Art. 2º, § 4º, da Carta das Nações Unidas: "Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas."

Ocorre que a efetividade da ordem internacional repousa na capacidade de imputar condutas ilícitas a sujeitos determinados. No domínio dos cabos submarinos, essa premissa é corroída pelo hiato entre o anonimato das operações híbridas e a rigidez dos critérios de responsabilidade estatal. Por conseguinte, a noção de atribuição assume centralidade absoluta, operando como o elo que transmuta um fato material em dever jurídico. Nesse sentido, a atribuição corresponde ao processo pelo qual o direito internacional estabelece se a conduta de uma pessoa física ou de outro intermediário pode ser considerada um "ato de Estado" e, assim, gerar responsabilidade estatal (Crawford, 2013, p. 113, tradução nossa)[33]. Sem a comprovação desse vínculo estruturante, tornam-se inócuos os regimes de reparação e responsabilização previstos no Direito Internacional.

A operacionalização desse conceito, contudo, demanda discernir duas dimensões fundamentais: a fática e a jurídica, cujas assimetrias operacionais constituem um dos núcleos da impunidade no ambiente marítimo-digital. A atribuição fática opera no plano da causalidade material, enfrentando o desafio probatório de rastrear a autoria física ou o nexo técnico do dano em um ambiente marcado tanto pela opacidade oceânica quanto pelo mascaramento cibernético (Davenport, 2023). Todavia, o êxito na identificação do agente não garante a responsabilização: o principal entrave encontra-se na complexidade da etapa subsequente, a atribuição jurídica. Trata-se do processo normativo que busca vincular a conduta individual à esfera de soberania de um Estado, qualificando-a como "ato de Estado" (Davenport, 2023). Essa imputação constitui o pressuposto indispensável para a incidência dos Artigos sobre Responsabilidade dos Estados por Atos Internacionalmente Ilícitos, elaborados pela Comissão de Direito Internacional (CDI) (Crawford, 2002). A conjugação desses elementos expõe o caráter anacrônico do regime jurídico da CNUDM, concebido sob a premissa da visibilidade imediata dos agressores e de uma correspondência estatal direta, pressupostos que já não se sustentam diante das dinâmicas contemporâneas de atuação encoberta, indireta e mediada por intermediários.

O quadro de impunidade é agravado pela própria arquitetura da CNUDM, alicerçada na primazia da jurisdição do Estado da bandeira. Consagrada desde a Convenção de 1884 e reafirmada nos artigos 91 e 92 do atual tratado[34], essa regra confere ao país de registro da embarcação a competência exclusiva para legislar e exercer poder de polícia sobre navios em

[33] No original: "'Attribution' is the process by which international law establishes whether the conduct of a natural person or other such intermediary can be considered an 'act of state', and thus be capable of giving rise to state responsibility."

[34] Art. 92, §1º: "Os navios devem navegar sob a bandeira de um só Estado e, salvo nos casos excepcionais previstos expressamente em tratados internacionais ou na presente Convenção, devem submeter-se, no alto mar, à jurisdição exclusiva desse Estado" (BRASIL, 1990).

alto-mar (Burnett *et al*., 2014). Essa lógica projeta-se sobre o artigo 113, delegando primordialmente ao Estado da bandeira, ou ao Estado de nacionalidade do infrator, a obrigação de criminalizar e punir a ruptura dessas instalações. Correlatamente, veda-se que navios de guerra de terceiros Estados abordem ou detenham embarcações suspeitas sem consentimento prévio, salvo nas hipóteses excepcionais de pirataria (Beckman, 2014). O modelo pressupõe, em tese, que o Estado de registro detenha não apenas capacidade jurídica, mas também interesse político efetivo em investigar e processar seus próprios nacionais ou agentes. Na prática, contudo, o monopólio jurisdicional atua como mecanismo de blindagem: a inércia legislativa ou a falta de *enforcement* interno geram situações nas quais ataques em águas internacionais ou na ZEE frequentemente não configuram crime em nenhuma jurisdição nacional. Consolida-se, assim, um vácuo estrutural de responsabilização que esvazia a função dissuasória do regime internacional (Beckman, 2014; Davenport, 2023).

Esse esvaziamento não se limita a uma falha procedimental pontual, mas reflete um descompasso ontológico entre uma norma concebida para um ambiente estratégico estático e a dinâmica contemporânea das ameaças híbridas e cibernéticas. O diagnóstico de esgotamento do modelo vigente é reiteradamente corroborado pela literatura especializada, que identifica no arcabouço normativo fundado na simbiose entre a Convenção de 1884 e a CNUDM de 1982 uma arquitetura desenhada para um contexto histórico no qual tais modalidades de ameaça eram inexistentes e que, por isso, permanece desatualizada e inadequada para enfrentar os desafios contemporâneos de segurança (Chang, 2025). Essa inércia normativa materializa o que Ringbom (2025) conceitua como o dilema das *New Threats—Old Rules*, no qual a rigidez jurisdicional e a centralidade do Estado da bandeira operam como barreiras estruturais à ação preventiva dos Estados costeiros. Consequentemente, o cenário atual não apenas perpetua as "lacunas de segurança" (*security gaps*) originalmente identificadas por Beckman (2014), mas aprofunda as "brechas legais" (*legal loopholes*) posteriormente examinadas por Lott (2025), que garantem uma zona de impunidade funcional para operações de sabotagem em zona cinzenta.

A vulnerabilidade sistêmica não se esgota na figura do Estado da bandeira, mas reverbera também sobre as prerrogativas do Estado costeiro. No âmbito da ZEE e da plataforma continental, a CNUDM institui uma tensão normativa: ao passo que os artigos 56 e 79 asseguram direitos soberanos sobre recursos naturais e meio ambiente, o artigo 58 preserva a liberdade de terceiros para a instalação e manutenção de cabos (Burnett *et al*., 2014). Esse arranjo gera um limbo jurisdicional, pois a Convenção não autoriza expressamente a criação de zonas de segurança ou o exercício de poder de polícia para a proteção de cabos,

instrumentos assegurados apenas para ilhas artificiais e estruturas extrativas (Burnett, 2014). Emerge, assim, um paradoxo operacional: embora o Estado costeiro possua interesse estratégico na integridade da rede que cruza sua zona marítima, suas competências permanecem funcionalmente atadas. Essa restrição inviabiliza a adoção de medidas preventivas robustas e compromete, na base, qualquer esforço de repressão a atos hostis.

Resta, por fim, a jurisdição do Estado do porto como alternativa de *enforcement*. Ancorada na soberania territorial do Estado sobre suas águas internas e portos, essa competência permite exercer jurisdição sobre embarcações estrangeiras quando estas se encontram voluntariamente em seu território, alcançando inclusive infrações cometidas em alto-mar ou na ZEE de terceiros. Contudo, a transposição desse modelo, exitoso no combate à pesca ilegal e à poluição, para a proteção de cabos esbarra em um vácuo institucional e probatório. A inexistência de um instrumento multilateral análogo ao *Port State Measures Agreement* (PSMA), adotado no âmbito da Organização das Nações Unidas para a Alimentação e a Agricultura (FAO) (Ye, 2015), inviabiliza a padronização global de protocolos de inspeção e coleta de provas. Sem essa arquitetura cooperativa, a jurisdição portuária permanece como uma potencialidade latente, juridicamente válida mas operacionalmente estéril para compensar as falhas estruturais da exclusividade da bandeira (Beckman, 2014).

Diante dos entraves jurisdicionais do direito do mar, o vácuo estrutural de responsabilização é explorado estrategicamente por meio da "negação plausível" (*plausible deniability*). Elemento central das guerras híbridas e operações em zona cinzenta, essa tática permite a atores estatais conduzirem hostilidades abaixo do limiar do conflito armado, dificultando respostas internacionais decisivas ou a ativação de mecanismos de defesa coletiva (Monaghan, 2019). A estratégia opera mediante a exploração da ambiguidade, valendo-se do emprego de forças *proxy*, milícias não identificadas ou vetores cibernéticos para obscurecer o vínculo direto entre o Estado agressor e a conduta ilícita, gerando incertezas suficientes quanto à autoria dos eventos para evitar a atribuição jurídica imediata e a imposição de sanções subsequentes (Sunak, 2017).

Esse *modus operandi* incide diretamente sobre o hiato entre a realidade fática da agressão e o rigor normativo do critério do controle efetivo, consolidado pela Corte Internacional de Justiça (CIJ) no caso *Nicarágua vs. Estados Unidos* (1986). Segundo a jurisprudência da Corte, a imputação de condutas a um Estado exige não apenas a comprovação de apoio logístico ou financiamento a grupos terceiros, mas a demonstração de que o Estado exerceu direção e controle sobre cada operação específica. No domínio

cibernético, tal exigência probatória, somada à dificuldade técnica de rastreamento forense, revela a insuficiência dos parâmetros clássicos de atribuição. O resultado é a consolidação de um déficit estrutural de imputabilidade, uma vez que o direito internacional carece de ferramentas flexíveis para vincular juridicamente as dinâmicas contemporâneas de agressão indireta aos seus verdadeiros autores estatais.

Diante das restrições da atribuição direta, o princípio da devida diligência (*due diligence*) projeta-se como um dos poucos vetores normativos capazes de mitigar os efeitos do déficit de imputabilidade. Consagrado na jurisprudência da CIJ, notadamente no caso do *Estreito de Corfu* (1949), o postulado estabelece que o Estado tem a obrigação de não permitir conscientemente que seu território ou infraestrutura sob controle governamental exclusivo sejam utilizados para atos lesivos a direitos de terceiros (Schmitt, 2017). No contexto da segurança marítimo-digital, tal dever configura-se não como uma obrigação de resultado, que exigiria sucesso absoluto na prevenção, mas como uma obrigação de conduta. Exige-se, portanto, que o Estado empregue seus melhores esforços e adote medidas viáveis dentro de sua capacidade técnica e financeira para cessar atividades maliciosas, uma vez configurado o conhecimento efetivo ou construtivo delas (Schmitt, 2017). Sob essa perspectiva, a devida diligência atua como mecanismo de contenção da negação plausível, visto que a ausência de prova cabal quanto à autoria não afasta a responsabilidade decorrente da tolerância ou inércia estatal. Desloca-se, assim, o eixo da responsabilização: da difícil prova do ato comissivo para a verificação da omissão juridicamente relevante.

Em última análise, o exame do regime jurídico oceânico evidencia um anacronismo normativo. Ao passo que a governança global, compreendida sob a lente de Rosenau como ordem dotada de intencionalidade, logrou êxito em consolidar as liberdades de navegação, permanece omissa diante da vulnerabilidade das infraestruturas que sustentam a conectividade digital contemporânea. O hiato entre a tutela do objeto material e a proteção do fluxo (dados e funcionalidade) expõe a fragilidade de um modelo que condiciona a reparação à ruptura física, transformando critérios rígidos de atribuição em fatores de blindagem para operações conduzidas em zonas cinzentas. Contudo, a constatação desse descompasso não deve conduzir a um diagnóstico de inércia absoluta. Diante da insuficiência da literalidade normativa, a doutrina contemporânea tem apontado para a necessidade de explorar as margens interpretativas do regime vigente. A preservação da relevância da Convenção passa, portanto, pela investigação de abordagens jurídicas não convencionais que, ancoradas em uma hermenêutica funcional e sistêmica, busquem extrair do texto da CNUDM instrumentos aptos

a mitigar o vácuo de segurança identificado e a restaurar, ainda que de forma limitada, a capacidade de resposta dos Estados.

3.3 A HERMENÊUTICA FUNCIONAL DA CNUDM: ABORDAGENS JURÍDICAS NÃO CONVENCIONAIS NA PROTEÇÃO DE INFRAESTRUTURAS SUBMARINAS

A constatação das lacunas estruturais da CNUDM face à sofisticação das ameaças híbridas contemporâneas conduz, inevitavelmente, ao debate sobre a pertinência de um novo tratado internacional dedicado exclusivamente à proteção da infraestrutura submarina. Contudo, dada a inércia diplomática e a fragmentação geopolítica que inviabilizam consensos amplos para a codificação de novos instrumentos ou emendas estruturais, a doutrina especializada tem apontado para a conveniência de explorar as potencialidades interpretativas do arcabouço normativo existente e do direito internacional costumeiro. Nesse quadro, esta seção adota uma abordagem baseada na porosidade normativa da Convenção, concebendo-a não como um texto estático, mas como um instrumento vivo, cuja interpretação, orientada pela boa-fé, por seu objeto e finalidade e por mecanismos de integração sistêmica, permite a absorção de regras externas sem subversão de sua arquitetura convencional. Essa metodologia hermenêutica foi recentemente chancelada na jurisprudência do Tribunal Internacional do Direito do Mar (ITLOS), que reconheceu a imperatividade de harmonização com outros regimes jurídicos como condição para evitar o isolamento da Convenção[35] (Mello Filho, 2025; ITLOS, 2024). Essa perspectiva visa assegurar a efetividade do regime diante de riscos não antecipados em 1982, sem incorrer em ativismo judicial ou revisionismo teleológico.

Sob essa ótica, o escopo da análise centra-se na mobilização não convencional de institutos jurídicos consolidados (Lott, 2025), notadamente a vedação ao abuso de direito, a cláusula de devida consideração (*due regard*), as obrigações de devida diligência ambiental e a recalibragem funcional do instituto da pirataria, para mitigar o vácuo de proteção que vulnerabiliza as infraestruturas críticas, especialmente nos espaços situados além do mar territorial, como a ZEE e o alto-mar, nos quais a jurisdição do Estado costeiro é mais limitada. Trata-se de um esforço hermenêutico para conferir exequibilidade à postura política que a literatura denomina "ambiguidade construtiva" (*constructive ambiguity*) (Azaria, 2025). Não

[35] No parecer consultivo, o Tribunal ressaltou a necessidade de coordenação da CNUDM com normas externas, a fim de preservar sua função como um instrumento vivo. Nesse contexto, identificou a presença de regras de referência na Parte XII da Convenção e recorreu à interpretação sistêmica prevista no Art. 31, § 3º, alínea c) da Convenção de Viena sobre o Direito dos Tratados, de modo a permitir que o tratado seja interpretado em consonância com o conjunto do sistema jurídico internacional vigente (*ITLOS*, *Advisory Opinion*, Case No. 31, 21 May 2024).

obstante, esse movimento preserva a cautela quanto ao dilema estratégico central: a aplicação extensiva dessas categorias deve ser calibrada para evitar a criação de precedentes de reciprocidade indesejada, passíveis de instrumentalização por potências rivais para restringir liberdades de navegação essenciais sob pretexto de segurança (Azaria, 2025).

A ancoragem dogmática dessa reorientação hermenêutica reside no artigo 300 da CNUDM, que impõe aos Estados o dever de exercer os direitos nela previstos de boa-fé e veda o seu uso abusivo (BRASIL, 1990). A proibição do abuso de direito atua como uma cláusula de *renvoi* (reenvio) aos princípios gerais do Direito Internacional, operando como um mecanismo de integração sistêmica que permite interpretar a Convenção segundo critérios de razoabilidade, proporcionalidade e necessidade, conferindo atualização funcional ao conteúdo de suas normas marítimas (Mello Filho, 2025). A jurisprudência internacional reconhece essa abertura normativa; no caso *Duzgit Integrity* (2016), o tribunal arbitral assentou que o exercício de poderes de polícia por Estados costeiros está sujeito a limites de princípios gerais integrados via os artigos 293, § 1º e 300 da CNUDM (CORTE PERMANENTE DE ARBITRAGEM, 2016). De igual modo, no caso *Saiga (No. 2)* (1999), o ITLOS incorporou considerações extrínsecas de humanidade e a proibição do uso excessivo da força como parâmetros vinculantes, evidenciando que o Direito do Mar não opera em isolamento (ITLOS, 1999).

Essa construção jurisprudencial conduz à conclusão de que a liberdade de navegação não possui caráter absoluto, encontrando limites claros na vedação ao abuso de direito. A aplicação prática dessa restrição materializa-se pela obrigação de devida consideração (*due regard*), prevista no artigo 87, § 2º, a qual exige que o exercício de liberdades no mar respeite os interesses legítimos de outros Estados. Sob essa ótica, a liberdade de colocar cabos e dutos (artigos 87 e 112) não pode ser lida de forma estática, mas deve ser compreendida de forma extensiva para incluir a "liberdade de operar" e manter tais infraestruturas (Azaria, 2025). Nessa perspectiva, atos intencionais de dano constituem uma interferência material nessa liberdade e violam a obrigação negativa de não interferência. Consequentemente, manobras como o arrasto deliberado de âncoras sobre eixos estratégicos de conectividade em tempo de paz não se enquadram como meros "incidentes de navegação" sob o escopo do artigo 97, mas configuram uma instrumentalização abusiva da liberdade marítima, desnaturando-a para fins ilícitos (ILA, 2024; Hartmann; Lott, 2025). Tal conduta rompe o nexo de boa-fé, afasta a presunção de proteção jurídica associada ao exercício regular da liberdade de navegação, enfraquece a invocação da jurisdição exclusiva do Estado de bandeira e legitima, em tese, a

adoção de medidas proporcionais de fiscalização e controle pelo Estado costeiro, nos limites do direito internacional aplicável.

No mesmo horizonte interpretativo, assume centralidade a discussão acerca da possibilidade de expansão funcional das zonas de segurança previstas na CNUDM, cuja interpretação tradicional do artigo 60, § 4º, restringiria sua aplicação exclusiva a ilhas artificiais e instalações e estruturas, excluindo, numa análise exegética, os cabos e dutos submarinos (ILA, 2024). Todavia, a vitalidade estratégica dessas conexões para a estabilidade econômica e para a segurança nacional impõe um tratamento funcional que as equipare a estruturas passíveis de proteção na ZEE (Lott, 2025). Essa hermenêutica encontra respaldo na prática estatal contemporânea; países como Austrália, Nova Zelândia e Dinamarca legislaram para estabelecer Zonas de Proteção de Cabos (*Cable Protection Zones* – CPZs) em suas jurisdições, restringindo atividades de risco, como ancoragem e pesca de arrasto, em corredores definidos (Lott, 2025). Destaca-se o modelo australiano, o qual estendeu essa tutela a profundidades que atingem os 2.000 metros, consolidando a jurisdição preventiva do Estado costeiro sobre o leito marinho mesmo em águas profundas (Carter *et al*., 2009). Embora a doutrina majoritária ainda resista a qualificar cabos como estruturas nos termos do artigo 60, a crescente pressão geopolítica tem fomentado o uso de uma leitura dinâmica, permitindo ao Estado costeiro adotar medidas preventivas e proporcionais em áreas sensíveis, com vistas à proteção de interesses vitais, preenchendo o vácuo de proteção sem ruptura explícita com o texto convencional (Lott, 2025).

A viabilidade operacional dessa reinterpretação encontra seu vetor de *enforcement* mais robusto na tutela ambiental. No caso de dutos de energia, o nexo é direto, uma vez que o artigo 79, § 2º, autoriza o Estado costeiro a adotar medidas razoáveis destinadas à prevenção, redução e controle da poluição decorrente de dutos submarinos, enquanto o artigo 221 legitima a adoção de providências além do mar territorial diante de ameaças graves de poluição resultantes de acidentes marítimos, categoria na qual a sabotagem mecânica deliberada pode ser enquadrada por analogia (Lott, 2025). A reorientação hermenêutica consiste, nesse contexto, em reconhecer que danos intencionais ou manobras deliberadamente arriscadas dirigidas a essas infraestruturas configuram não apenas um ilícito potencial, mas um perigo ambiental iminente, apto a acionar poderes de interdição e perseguição com fundamento na proteção do meio marinho. Ainda que tal lógica encontre maior resistência no caso dos cabos de fibra óptica, cujo corte raramente produz poluição marinha convencional, a doutrina tem identificado uma convergência funcional entre a proteção da infraestrutura e a conservação ambiental. Em especial, as CPZs, ao restringirem práticas como a pesca de

arrasto e a ancoragem em corredores estratégicos, operam simultaneamente como mecanismos de salvaguarda da conectividade e como instrumentos de preservação de ecossistemas bentônicos sensíveis (Carter *et al*., 2009). Essa dualidade permite ao Estado costeiro fundamentar restrições sob o amparo das obrigações gerais de proteção ambiental previstas nos artigos 56, 192 e 194 da CNUDM, transformando a tutela ecológica, não em um argumento acessório, mas em um fundamento jurídico integrado à defesa da infraestrutura crítica, capaz de reduzir o vácuo de *enforcement* sem subverter a arquitetura normativa da Convenção (Azaria, 2025).

Para além do vetor ambiental, emerge na literatura uma proposta de construção dogmática não convencional: a aplicação do instituto da pirataria, previsto no artigo 101 da CNUDM, aos atos de sabotagem dirigidos contra cabos submarinos em áreas além da jurisdição nacional. Embora o instituto seja tradicionalmente associado a atos de roubo ou violência cometidos no alto-mar por um navio contra outro, exigindo a presença de duas embarcações distintas (o navio agressor e o navio vítima), uma interpretação funcional do Art. 101, alínea *a*, inciso ii, revela uma via interpretativa plausível para superar esse requisito. Enquanto o inciso I condiciona a tipificação do ato à violência dirigida contra outro navio, o inciso II admite, de forma disjuntiva, que a conduta de depredação recaia contra navio, pessoas ou bens situados em lugar fora da jurisdição de qualquer Estado (BRASIL, 1990). A partir dessa distinção textual, sustenta-se que, quando o alvo do ataque é um bem localizado fora de qualquer jurisdição nacional, a exigência da presença de uma segunda embarcação não se impõe de maneira necessária (Hartmann, 2025). Nessa perspectiva, cabos e dutos submarinos instalados no leito do alto-mar podem ser qualificados como bens (*property*) para os fins do artigo 101, preenchendo os requisitos normativos da figura da pirataria, ainda que essa interpretação desafie o conservadorismo da prática estatal histórica (Azaria, 2025; Hartmann, 2025). O fundamento dessa posição reside no princípio da efetividade (*effet utile*), inerente à regra geral de interpretação, segundo o qual as normas de um tratado devem ser interpretadas de modo a conferir efeito pleno aos seus termos e utilidade real ao seu propósito protetivo, evitando-se o esvaziamento da tutela jurídica de bens comuns em alto-mar (CORTE INTERNACIONAL DE JUSTIÇA, 1994; Trindade, 2013).

O segundo entrave normativo à aplicação do instituto reside na exigência dos fins privados (*private ends*), critério que tradicionalmente excluiria ações politicamente motivadas ou atribuíveis a Estados. Contudo, conforme analisado na seção precedente, a própria arquitetura das ameaças híbridas, operada sob a cobertura da negação plausível e por meio de intermediários civis, oferece o vetor argumentativo para superar essa restrição. Nesse

contexto, a incerteza atributiva assume uma função jurídica paradoxal: ao repudiar formalmente o vínculo com a operação para evitar a responsabilização internacional, o Estado patrocinador despoja a conduta de sua imunidade soberana. Dessa forma, o ato passa a ser juridicamente privatizado pela própria estratégia de ocultação, para fins de repressão internacional (Lott, 2025). Ademais, a doutrina contemporânea ressalta que a remuneração direta da tripulação ou dos executores materiais configura, por si só, elemento de ganho pessoal suficiente para satisfazer o requisito dos *private ends*, independentemente da origem última do financiamento (Lott, 2025). Essa construção viabiliza a subsunção do comportamento ao regime jurídico da pirataria e, por conseguinte, a ativação dos mecanismos de repressão de caráter universal.

A consequência normativa dessa requalificação jurídica é a incidência do artigo 105 da CNUDM, dispositivo que confere a todo e qualquer Estado a competência para apresar a embarcação pirata, deter sua tripulação e adjudicar as penas cabíveis, sem a necessidade de consentimento prévio do Estado de bandeira (artigo 92), prerrogativa que, na prática, frequentemente atua como um escudo de impunidade em cenários de guerra híbrida (Hartmann, 2025). Ao elevar a proteção dos cabos ao estatuto de interesse universal, o instituto da pirataria transforma o sabotador em *hostis humani generis* (inimigo de toda a humanidade), autorizando navios de guerra de terceiros Estados a intervir coercitivamente para cessar a ameaça. Essa possibilidade impõe um cálculo de risco dissuasório inédito aos atores estatais que operam na zona cinzenta, pois retira a garantia de inviolabilidade operacional que atualmente incentiva essas incursões (Lott, 2025).

Contudo, a transposição dessa arquitetura teórica enfrenta obstáculos dogmáticos intransponíveis. A doutrina majoritária aponta a incompatibilidade ontológica entre a guerra híbrida e o requisito dos fins privados, alertando para a incongruência de se classificar uma estratégia estatal como pirataria. Nesse sentido, Sari é taxativo ao apontar a exclusão mútua entre essas categorias: "não se pode dizer ao mesmo tempo que [a sabotagem] é potencialmente atribuível a um Estado e também que é pirataria, pois são categorias mutuamente exclusivas"[36] (UNITED KINGDOM, 2025, Q25). Essa natureza estatal do ato esvazia o requisito normativo da pirataria e cria uma contradição insanável: classificar a conduta sob esse tipo penal exigiria negar seu vínculo com o Estado patrocinador, reforçando a impunidade do mandante ao focar apenas no executor material (Lott, 2025). Ademais, inexiste prática estatal ou *opinio juris* que corrobore a equiparação de cabos a bens para fins

[36] No original: "You cannot say in the same breath that this [sabotage] is potentially attributable to a state and also to piracy, because they are mutually exclusive categories."

do artigo 101 da CNUDM (Azaria, 2025; Hartmann, 2025), entendimento chancelado pela interpretação restritiva dos elementos do tipo penal estabelecida no caso *Arctic Sunrise* (CORTE PERMANENTE DE ARBITRAGEM, 2015, para. 238). Por fim, a expansão conceitual acarreta riscos pragmáticos de *over-inclusion*, podendo criminalizar acidentes de pesca e ser instrumentalizada por Estados para justificar interdições abusivas em alto-mar sob pretexto de segurança, desestabilizando o delicado equilíbrio da ordem pública dos oceanos (Lott, 2025).

Diante da fragilidade dogmática que cerca a tese da pirataria, parte da doutrina busca em institutos de natureza subsidiária uma fundamentação alternativa para a intervenção estatal. Nesse cenário, emerge o estado de necessidade, codificado no artigo 25 do Projeto de Artigos sobre Responsabilidade dos Estados da Comissão de Direito Internacional (CDI), como base autônoma para intervenções excepcionais. Tal preceito opera como uma excludente de ilicitude, legitimando condutas estatais que, embora *a priori* irregulares, constituam o único meio de salvaguardar um interesse essencial contra um perigo grave e iminente. A reorientação conceitual reside, nesse cenário, na redefinição do que compõe o interesse essencial na era da informação. Sob essa ótica, o reconhecimento pela Assembleia Geral da ONU da criticidade dos cabos submarinos para a segurança nacional e a estabilidade econômica global (ILA, 2024) permite a qualificação da integridade dessas redes como um bem jurídico vital. Essa subsunção é particularmente incontornável em contextos de dependência estrutural acentuada, como no caso de Estados insulares ou nações energeticamente vulneráveis, em que o colapso da conectividade digital equivaleria a uma ameaça existencial à soberania (Azaria, 2025).

Nessa conjuntura, a presença de embarcações exibindo padrões de navegação anômalos sobre leitos de cabos críticos transcende a mera violação do dever de devida consideração, configurando a materialização de um perigo grave e iminente, apto a justificar medidas preventivas de interdição. A invocação do estado de necessidade, contudo, não constitui prerrogativa ilimitada; sua legitimidade submete-se a escrutínio estrito, notadamente ao teste do "único meio" (*only way*), que impõe o ônus de demonstrar a absoluta ineficácia de alternativas menos gravosas, como a comunicação via rádio ou a via diplomática (ILA, 2024). Entretanto, diante da opacidade das ameaças híbridas, da incomunicabilidade deliberada de "frotas fantasmas" (*shadow fleet*) e de navios sob bandeiras de conveniência[37], a interdição

[37] O conceito clássico de bandeiras de conveniência (*flags of convenience* - FOC) designa a prática comercial de registrar uma embarcação mercante em um Estado soberano distinto daquele de nacionalidade de seus proprietários efetivos. Essa estratégia de registro aberto visa, sobretudo, à redução de custos operacionais e à elisão fiscal e regulatória, permitindo aos armadores evitar normas trabalhistas, de segurança e ambientais mais

física pode se tornar a *ultima ratio* para evitar o colapso dos eixos estruturantes da economia digital, sem comprometer desproporcionalmente interesses da comunidade internacional, em especial a liberdade de navegação (Lott, 2025). Assim compreendido, o estado de necessidade não opera como uma autorização geral de *enforcement*, mas como uma ferramenta residual e altamente controlada, destinada a preencher o vácuo de segurança em situações-limite. Essa natureza excepcional e essencialmente reativa, todavia, é incapaz de oferecer a previsibilidade requerida para uma governança preventiva das infraestruturas submarinas, expondo, em última análise, a exaustão dos remédios hermenêuticos diante do anacronismo do regime internacional vigente.

Em conjunto, as construções hermenêuticas examinadas revelam que a CNUDM, embora demande reformas estruturais de longo prazo, ainda dispõe de margens interpretativas capazes de oferecer respostas juridicamente defensáveis às ameaças contemporâneas dirigidas às infraestruturas submarinas. Todavia, tais respostas emergem menos como soluções automáticas e mais como produtos de um exercício interpretativo complexo, que exige constante calibragem entre a proteção de interesses vitais e a preservação das liberdades marítimas. Esse equilíbrio é particularmente precário diante do risco de reciprocidade indesejada, em que a elasticidade interpretativa mobilizada para a proteção dos cabos pode ser instrumentalizada por potências rivais para restringir a navegação sob pretexto de segurança. A tutela das redes submarinas deixa, assim, de ser um problema meramente técnico ou setorial para expor tensões estruturais do Direito Internacional na era digital. Torna-se oportuno, portanto, confrontar essa arquitetura hermenêutica com a realidade operacional de espaços marítimos saturados e contestados, nos quais a teoria jurídica é testada pelo pragmatismo das relações de poder. É sob essa lente de fricção que se analisa, a seguir, o Mar Báltico na condição de laboratório para a observação dos incidentes associados às ameaças híbridas e das reações estatais observadas entre 2023 e 2024.

rigorosas vigentes em seus países de origem (Tan, 2024). A problemática central deste regime reside na inexistência de um vínculo genuíno (*genuine link*) entre o navio e o Estado de registro, exigido pelo Art. 91 da CNUDM (BRASIL, 1990). Contudo, a literatura jurídica mais recente, incorporando a terminologia cunhada pela *Lloyd's List* (2024) ao investigar as frotas fantasmas, identifica a evolução desse instituto para as chamadas bandeiras de engano (*flags of deceit* - FOD) (Mello Filho, 2025). Diferentemente das FOCs, cuja motivação é econômica, as FODs caracterizam-se pela falta de vontade política deliberada do Estado de registro em exercer o controle efetivo exigido pelo Art. 94 da CNUDM (Mello Filho, 2025). Esses registros atuam como refúgios intencionais, servindo como instrumento geopolítico ao oferecer anonimato corporativo e impunidade para evadir sanções internacionais e dificultar a atribuição de responsabilidade por atos de sabotagem em zonas cinzentas (Mello Filho, 2025; Finelli, 2026).

4 O MAR BÁLTICO COMO LABORATÓRIO DAS AMEAÇAS HÍBRIDAS: UMA ANÁLISE DOS INCIDENTES DE 2023–2024 NA PERSPECTIVA DAS LACUNAS DA CNUDM

A ordem marítima contemporânea atravessa uma transformação silenciosa, na qual o oceano deixa de constituir apenas o espaço de circulação da navegação para converter-se no suporte material das arquiteturas energéticas e informacionais que sustentam a economia global. Ao concentrar no leito marinho infraestruturas críticas responsáveis pela transmissão de dados, eletricidade e fluxos estratégicos de comunicação, o domínio oceânico passa a operar simultaneamente como meio de conectividade sistêmica e como superfície de vulnerabilidade geopolítica, dissolvendo a separação clássica entre espaço de interdependência funcional e espaço de competição estratégica que orientou historicamente a construção do Direito do Mar.

Essa mutação altera não apenas o significado estratégico do oceano, mas a própria essência dos dilemas jurídicos que nele emergem. As dificuldades contemporâneas relacionadas à proteção de infraestruturas submarinas não decorrem exclusivamente da insuficiência de normas existentes, mas da fricção crescente entre uma arquitetura jurídica concebida para regular a mobilidade da navegação e uma realidade estratégica na qual o principal objeto de disputa reside na materialidade imóvel das redes que, invisíveis, atravessam o fundo marinho. Nesse contexto, o problema da responsabilização internacional deixa de ser apenas uma questão de aplicação normativa e passa a refletir um desalinhamento estrutural mais profundo entre a racionalidade do regime jurídico vigente e as novas formas de coerção que se desenvolvem no domínio oceânico.

A partir dessa moldura analítica, o presente capítulo examina o Mar Báltico como laboratório empírico das ameaças híbridas dirigidas contra infraestruturas submarinas críticas. Inicialmente, procede-se à contextualização estratégica e geopolítica do espaço regional, identificando os determinantes geofísicos, oceanográficos e operacionais que o converteram em um ambiente particularmente suscetível à atuação em zonas cinzentas. Em seguida, analisa-se a fenomenologia dos incidentes ocorridos no biênio 2023–2024, evidenciando o padrão operacional de sabotagem e suas implicações para a continuidade da conectividade energética e informacional regional. Por fim, investiga-se o impasse jurídico da responsabilização internacional desses eventos, explorando a tensão entre as potencialidades interpretativas da CNUDM e a autocontenção estatal na mobilização de respostas coercitivas,

bem como suas repercussões para a efetividade do regime internacional de proteção das infraestruturas submarinas.

A análise dos eventos ocorridos no biênio 2023–2024 revela um padrão tático específico: a inexistência de registros públicos de ciberataques estritamente lógicos responsáveis por interrupções sistêmicas na região. Essa constatação, contudo, não reduz a centralidade da dimensão cibernética, mas impõe seu exame a partir da materialidade infraestrutural da conectividade digital. Nesse contexto, a ruptura física dos cabos configura um ataque direto à Camada 1 (*Physical Layer*) do Modelo OSI, produzindo efeitos funcionalmente equivalentes a uma negação de serviço (DoS) por meios cinéticos.

A preferência pelo método físico expressa a racionalidade própria da zona cinzenta, na medida em que a sabotagem material tende a ser absorvida pela lógica dos acidentes de navegação prevista na CNUDM, ampliando o espaço de negação plausível. Paralelamente, a dimensão lógica manifestou-se de forma instrumental mediante a manipulação do espectro eletromagnético, com o desligamento seletivo de sistemas AIS e episódios de *spoofing* de GPS, o que reforça a natureza integrada das operações analisadas.

4.1 CONTEXTUALIZAÇÃO ESTRATÉGICA E GEOPOLÍTICA DO MAR BÁLTICO: DE “LAGO DA OTAN” A ZONA DE ATRITO HÍBRIDO

A reconfiguração da arquitetura de segurança europeia e euro-atlântica no século XXI encontra no Mar Báltico um laboratório empírico das transformações contemporâneas do poder marítimo e das dinâmicas de segurança regional. Historicamente, esse corpo hídrico semifechado constituiu uma *pivot area* entre o poder continental euroasiático e as talassocracias ocidentais, desempenhando simultaneamente as funções de corredor comercial estratégico e de zona tampão defensiva. No período pós-Guerra Fria, o Báltico passou a ser percebido como uma região de relativa previsibilidade, percepção reforçada pelos sucessivos alargamentos da OTAN, que levaram analistas e meios de comunicação ocidentais a consagrá-lo discursivamente como o “Lago da OTAN”, em alusão à predominância de Estados-membros em seu entorno imediato, com exceção dos enclaves russos de São Petersburgo e Kaliningrado (Livermore, 2024). Essa designação, contudo, projeta uma imagem de hegemonia incontestada e de estabilidade assegurada pela segurança coletiva da Aliança, o que não corresponde à realidade operacional emergente (Savitz; Winston, 2024).

A invasão em larga escala da Ucrânia pela Federação Russa, em 2022, somada à subsequente adesão da Finlândia e da Suécia à OTAN, promoveu uma reordenação profunda

da geografia política do Mar Báltico, resultando no progressivo cerco estratégico dos acessos russos ao Atlântico e no isolamento relativo de Kaliningrado. A partir desse momento, com o colapso das expectativas remanescentes de uma ordem de segurança cooperativa na Europa, o espaço báltico passou a ser reinterpretado não apenas como área de projeção de poder naval, mas como um domínio estratégico no qual infraestruturas críticas, fundos marinhos e rotas marítimas integram de forma indissociável o cálculo de segurança estatal. Incapaz de desafiar a OTAN em um confronto naval convencional simétrico, a Rússia passou a operar nesse ambiente adotando a lógica operacional da zona cinzenta (Lokker *et al.*, 2023) como vetor alternativo de projeção de poder. Nesse novo enquadramento, a ambiguidade deixa de ser uma abstração teórica para se converter em instrumento tático: a própria liberdade de navegação é instrumentalizada para mascarar ações hostis, explorando as fissuras normativas e operacionais do regime marítimo vigente. Assim, o Mar Báltico mantém suas dinâmicas de cooperação regional, coexistindo, contudo, com um padrão crescente de competição encoberta que testa, no limite, os limiares de reação da Aliança.

A centralidade do Mar Báltico como laboratório das dinâmicas contemporâneas de segurança marítima não pode ser plenamente compreendida sem a consideração de seus determinantes geofísicos e oceanográficos, que moldam de maneira decisiva tanto as possibilidades de vigilância, controle e proteção de infraestruturas críticas quanto às condicionantes práticas enfrentadas pelos Estados costeiros e pela própria OTAN na fiscalização e na dissuasão de atividades hostis encobertas. Diferentemente dos oceanos abertos, o Mar Báltico configura-se como um mar epicontinental raso, com profundidade média aproximada de 55 metros, característica que reduz significativamente as barreiras técnicas para a realização de operações no leito marinho (Höller, 2024). Essa superficialidade amplia o espectro de atores capazes de acessar fisicamente cabos submarinos e gasodutos, permitindo que não apenas submarinos militares avançados, mas também veículos submersíveis não tripulados de uso comercial, mergulhadores especializados ou equipamentos adaptados realizem intervenções diretas sobre infraestruturas críticas (Monaghan *et al*., 2023; Martinage, 2015). Em termos estratégicos, isso implica numa diminuição substancial dos custos operacionais e dos riscos associados a ações de sabotagem, tornando o ambiente particularmente atrativo para operações indiretas e de baixa visibilidade (Sunak, 2017).

A complexidade do ambiente hidroacústico do Mar Báltico aprofunda ainda mais esse quadro de vulnerabilidade. A hidrografia regional é marcada por uma estratificação persistente da coluna d’água, decorrente da combinação entre o aporte contínuo de água doce proveniente dos grandes rios do norte e do leste europeu e a entrada periódica de águas salinas

mais densas pelos Estreitos dinamarqueses (Lehmann *et al*., 2022). Esse arranjo físico dá origem a camadas estáveis de diferenciação de salinidade que interferem na propagação das ondas sonoras, comprometendo a eficácia dos sistemas de detecção acústica e operando, na prática, como zonas de refração e sombra acústica, o que dificulta a vigilância por sonar e cria condições favoráveis para a movimentação furtiva de meios submersíveis de pequeno porte (Höller, 2024). Além disso, a reduzida profundidade intensifica esse quadro ao gerar elevada reverberação acústica e múltiplos ecos, degradando a clareza dos sinais captados por sensores ativos e passivos, efeito que é potencializado tanto pelo intenso tráfego comercial na região, responsável por um ruído de fundo constante capaz de mascarar assinaturas acústicas sutis (Hunt, 1998), quanto pela própria topografia do fundo marinho, marcada por naufrágios históricos, detritos e irregularidades naturais. Em conjunto, esses elementos produzem um cenário de *clutter*[38] visual e acústico que pode ser explorado para a ocultação de dispositivos de escuta, sensores ou cargas explosivas posicionadas nas proximidades de cabos submarinos e gasodutos, dificultando a identificação de anomalias e reduzindo a capacidade de monitoramento contínuo (Hunt, 1998; Strachan, 2022).

Do ponto de vista geográfico, essas vulnerabilidades são reforçadas pela presença de pontos de estrangulamento estratégicos que condicionam a circulação marítima regional. O acesso ao Oceano Atlântico é controlado pelos Estreitos dinamarqueses, enquanto o Golfo da Finlândia e as aproximações a São Petersburgo são delimitados por costas densamente monitoradas, o que concentra o tráfego marítimo em corredores previsíveis (Savitz; Winston, 2024). Paradoxalmente, esses mesmos corredores tendem a abrigar elevada densidade de infraestruturas submarinas, formando verdadeiros nós de vulnerabilidade nos quais cabos de telecomunicações, gasodutos e rotas comerciais coexistem em estreita proximidade. Nesse contexto, torna-se particularmente difícil distinguir atividades legítimas de operações maliciosas, circunstância que favorece estratégias assimétricas baseadas na exploração deliberada das condicionantes físicas e geográficas para minimizar a probabilidade de detecção e maximizar a ambiguidade operacional (Sunak, 2017; Monaghan *et al*., 2023). Essa saturação do espaço marítimo converte-se, em última análise, em um fator de proteção operacional e jurídico para atores hostis, aprofundando os obstáculos à atribuição de responsabilidade internacional (Kaushal, 2023; Sari, 2025) e desafiando a aplicação das

[38] No contexto da acústica subaquática e tecnologia de sonar, o termo clutter refere-se a "características de falsa reflexão" ou ecos indesejados gerados pelo ambiente que se sobrepõem ao sinal de interesse. Estes sinais surgem da interação da energia acústica com irregularidades do fundo marinho ou devido à reverberação de múltiplos caminhos, comum em águas rasas. O *clutter* cria um cenário de ruído visual e acústico que degrada a resolução da imagem, dificultando a distinção entre objetos reais (como anomalias ou ameaças) e o fundo marinho (Grządziel, 2023; Hunt, 1998).

ferramentas de *enforcement* examinadas no capítulo anterior, circunstância que evidencia a distância entre as potencialidades interpretativas do regime jurídico do mar e a forma limitada como os mecanismos existentes têm sido efetivamente mobilizados na prática estatal contemporânea.

4.2 A FENOMENOLOGIA DA SABOTAGEM EM ZONA CINZENTA NO MAR BALTICO: OS INCIDENTES DE 2023–2024

É precisamente nesse contexto estrutural de vulnerabilidade geofísica e ambiguidade estratégica que, em outubro de 2023, o Mar Báltico ingressou em uma fase de crise operacional aberta, marcada por uma sucessão de incidentes que testaram de forma inédita os limites da vigilância marítima e dos mecanismos tradicionais de atribuição jurídica. Longe de representarem meras falhas contingenciais de segurança, os eventos observados ao longo do biênio 2023–2024 revelam a exploração deliberada de um descompasso normativo estrutural na arquitetura da CNUDM. Essa inflexão manifestou-se por meio de operações que prescindiram do emprego de meios cinéticos convencionais, como explosivos ou torpedos, em favor de métodos mecânicos deliberadamente ambíguos, passíveis de serem mimetizados como acidentes de navegação. O episódio inaugural dessa cronologia foi a súbita queda de pressão detectada pelos sensores da operadora finlandesa *Gasgrid* e da estoniana *Elering* no gasoduto *Balticconnector*[39], que interliga as redes energéticas da Finlândia e da Estônia, na madrugada de 8 de outubro de 2023 (Lindholm, 2025). A análise sistêmica do ocorrido indica, contudo, que o dano ao gasoduto não constituiu um evento isolado, mas integrou uma sequência de rupturas quase simultâneas que atingiram o cabo de fibra óptica que liga Finlândia a Estônia e, em período temporal próximo, o cabo EE-S1 (Estônia–Suécia) (Chiappa; Ngendakumana, 2023), evidenciando um padrão de interrupção coordenada de fluxos estratégicos de energia e dados.

A materialidade empírica desses incidentes demonstra que a sabotagem em ambiente de zona cinzenta no Mar Báltico não se caracteriza pela espetacularidade do dano físico, mas pela seletividade estratégica dos alvos e pela temporariedade calculada da interrupção dos fluxos. Diferentemente de ataques destinados à destruição permanente da infraestrutura, os

[39] Segundo a Yle (2023), este gasoduto apresenta características técnicas semelhantes às do sistema de gasodutos de gás natural que ligava a Rússia à Alemanha (Nord Stream 1 e 2), danificado pelas explosões ocorridas em setembro de 2022. Trata-se de um gasoduto marítimo típico, constituído por um tubo de aço com revestimento externo de concreto, solução empregada para assegurar estabilidade estrutural, proteção mecânica e adequada ancoragem ao leito marinho.

eventos registrados em 2023 indicam uma lógica operacional voltada à geração de incerteza, à sinalização estratégica e à testagem das capacidades de resposta dos Estados costeiros e das organizações regionais. No caso do *Balticconnector*, que constitui o marco inaugural dessa sequência de eventos, o episódio foi inicialmente tratado com cautela pelas autoridades da Finlândia e da Estônia, que evitaram descartar prematuramente a hipótese de falha técnica. Contudo, investigações técnicas subsequentes conduzidas pelo Departamento Nacional de Investigação da Finlândia (NBI – *National Bureau of Investigation*) apontaram para a existência de danos mecânicos consistentes com o arrasto deliberado de uma âncora de grandes proporções sobre o leito marinho, hipótese corroborada pela identificação de sulcos profundos no solo e pela recuperação da própria âncora desprendida, associada a um navio mercante operado por empresa privada e registrado sob bandeira estrangeira (POLIISI, 2023). Nesse contexto, o foco investigativo concentrou-se no navio porta-contêineres chinês *NewNew Polar Bear*, de bandeira de Hong Kong, cuja trajetória apresentava coincidência espacial e temporal com as rupturas e que foi posteriormente fotografado em um porto russo exibindo sinais visíveis da ausência da âncora de bombordo (Benner, 2025). Dinâmica semelhante foi observada no cabo de fibra óptica *EE-S1*, cuja interrupção não resultou em colapso prolongado dos sistemas de comunicação, mas produziu impactos imediatos sobre a redundância das redes e sobre a percepção de segurança das infraestruturas digitais regionais (Praks, 2024).

Este quadro evidencia como o sistema concebido em 1982 pressupõe um grau de boa-fé internacional que se mostra cada vez mais raro entre competidores geopolíticos: ao exigir padrões probatórios típicos do direito civil, pautados na difícil demonstração do dolo ou da negligência, para atos que produzem efeitos sistêmicos comparáveis aos de agressões estatais, a CNUDM acaba por favorecer a impunidade operacional do mentor da operação (Hartmann; Lott, 2025). Na ausência de acesso aos registros de bordo ou à cooperação do Estado da bandeira, o agressor encontra espaço para sustentar narrativas de erro humano ou contingência técnica, convertendo a incerteza causal deliberadamente produzida em vantagem estratégica.

A hipótese de que os eventos de 2023 constituíssem incidentes acidentais foi definitivamente fragilizada pela ocorrência de uma nova sequência de rupturas em novembro de 2024, que evidenciou a reiteração do *modus operandi* de sabotagem mecânica por meios civis, sugerindo a progressiva normalização da sabotagem em zona cinzenta no Mar Báltico (Tammikko, 2025). Em um intervalo inferior a 24 horas, entre os dias 17 e 18 de novembro de 2024, dois cabos submarinos cruciais para a conectividade europeia foram rompidos: o cabo

BCS East-West Interlink, que conecta a Lituânia à Suécia, e o *C-Lion1*, única conexão direta de fibra óptica entre a Finlândia e a Alemanha (Astier; Kirby, 2024). Assim como no caso do *Balticconnector*, a fenomenologia desses incidentes apontou para a intervenção externa de um navio mercante estrangeiro, desta vez o graneleiro chinês *Yi Peng 3*, que havia partido de um porto russo e realizou manobras atípicas sobre áreas sensíveis do leito marinho, cujos movimentos coincidiram precisamente com as coordenadas das rupturas (REUTERS, 2024).

Embora o navio tenha sido monitorado por meios navais da Dinamarca e da OTAN (Lott, 2024), a aplicação do Direito de Visita, previsto no artigo 110 da CNUDM, revelou-se juridicamente inviável. A norma restringe a abordagem coercitiva em alto-mar a um rol taxativo de crimes, a exemplo de pirataria, tráfico de escravos e transmissões não autorizadas, no qual a sabotagem de infraestruturas submarinas não foi incluída. Na prática, isso significa que, na ausência de flagrante delito e mantida a aparência formal de embarcação mercante regular, o Estado costeiro encontra-se, sobretudo na ZEE, juridicamente limitado em suas possibilidades imediatas de intervenção[40], permitindo que o vetor de sabotagem se evada para a proteção das águas internacionais antes que qualquer perícia física ou oitiva da tripulação possa ser realizada.

Se os incidentes de novembro sinalizaram a reiteração do método, a escalada observada em 25 de dezembro de 2024 elevou o patamar de hostilidade ao atingir, simultaneamente, vetores de dados e eletricidade no Golfo da Finlândia. Nesse evento, o navio petroleiro *Eagle S*, operando sob bandeira das Ilhas Cook, foi associado ao rompimento do interconector elétrico *Estlink 2*, responsável pela transmissão de energia entre a Finlândia e a Estônia, bem como aos danos simultâneos nos cabos de fibra óptica FEC 1 e FEC 2, pertencentes à operadora Elisa Corporation (REUTERS, 2026; Lott, 2024). Registros de tráfego marítimo e dados de monitoramento do leito marinho indicaram que a embarcação realizou manobras de baixa velocidade e mudanças reiteradas de curso precisamente sobre as áreas em que essas infraestruturas coexistem em estreita proximidade, o que reforçou a hipótese de sabotagem mecânica por arrasto deliberado de âncora ao longo de extensa faixa da ZEE finlandesa (Ruys; Bamnios, 2025), consolidando a leitura regional de um padrão mais amplo de pressão estratégica indireta.

[40] Cumpre observar que, nos termos do artigo 111 da CNUDM, o Estado costeiro pode exercer o direito de perseguição (*right of hot pursuit*) quando a infração ocorre no mar territorial, na zona contígua ou, ainda, na zona econômica exclusiva, desde que envolva violação de leis e regulamentos cuja aplicação nessas zonas lhe seja juridicamente atribuída. Todavia, a sabotagem de cabos submarinos situados na ZEE ou na Plataforma Continental, onde se localiza a maior parte da malha global, não configura, em regra, afronta direta aos direitos soberanos taxativamente previstos no artigo 56 da Convenção. Nessas circunstâncias, a ativação do *hot pursuit* torna-se inaplicável, persistindo o déficit de *enforcement* apontado.

A resposta ao incidente evidenciou, ademais, a complexidade operacional dessas ações híbridas no domínio marítimo, uma vez que a tripulação teria informado falsamente às autoridades que as âncoras se encontravam devidamente recolhidas, permitindo a continuidade da navegação e a ampliação progressiva dos danos (Ruys; Bamnios, 2025). Após o evento, as autoridades finlandesas interceptaram e detiveram a embarcação sob suspeita de "dano criminal agravado" e interferência nas comunicações, nos termos do Código Penal finlandês, descobrindo a bordo equipamentos atípicos para um navio mercante, como dispositivos de escuta e gravação, sensores e laptops configurados com teclados em russo e turco (Rintakumpu *et al*., 2025; Bockmann, 2024). A apreensão do *Eagle S* estabeleceu um precedente importante para a adoção de medidas de execução jurisdicional por Estados-membros da União Europeia (PARLIAMENT OF THE REPUBLIC OF POLAND, 2025), ao buscar superar as restrições de jurisdição executiva mediante o teste dos limites do artigo 97 da CNUDM diante da necessidade de proteção de infraestrutura crítica (Ruys; Bamnios, 2025). Este movimento sinaliza uma tentativa de ruptura estratégica com a interpretação ortodoxa da Convenção, na medida em que desafia o dogma da exclusividade jurisdicional do Estado da bandeira (artigo 92) e expõe a falência prática do conceito de vínculo substancial (*genuine link*) em contextos marcados pela opacidade deliberada associada às chamadas frotas fantasmas.

Nesse sentido, os indícios de espionagem e a ausência de transparência operacional observados no caso do *Eagle S* não constituem uma anomalia isolada, mas refletem uma tendência estrutural amplamente documentada na literatura: a expansão dessas "frotas fantasmas". Compostas por embarcações registradas sob bandeiras de conveniência, frequentemente vinculadas a países com regimes regulatórios permissivos, operadas por estruturas societárias opacas e inseridas em circuitos logísticos paralelos (PARLIAMENT OF THE REPUBLIC OF POLAND, 2025), essas frotas funcionam como mecanismo estratégico de saturação e mascaramento do tráfego marítimo, situando operações potencialmente ilícitas no limiar entre a atividade comercial formalmente lícita e a instrumentalização de meios civis para fins de pressão geopolítica. No contexto do Mar Báltico, o *Eagle S* representa uma manifestação concreta dessa dinâmica, evidenciando os desafios centrais da responsabilização internacional frente a atos híbridos em zonas de alta densidade de infraestrutura crítica.

A recorrência desses métodos, observada de forma persistente desde os danos ao cabo EE-S1 em 2023 até a escalada contra os interconectores Estlink em 2024, revela uma combinação deliberada entre a seletividade técnica dos alvos e a exploração da ambiguidade causal. Este delineamento sugere que o objetivo primordial dessas operações não reside na

destruição ou paralisação definitiva dos serviços, mas na ocupação sistemática de zonas de incerteza situadas entre o acidente náutico, o ato ilícito internacional e o uso da força, espaço no qual a resposta jurídica e política dos Estados afetados tende a revelar-se retardada, fragmentada ou ineficaz (Monaghan *et al*., 2023; Sari, 2025). A instrumentalização de vetores civis e de frotas opacas para a produção de danos estratégicos insere esses episódios no que a literatura especializada qualifica como formas de sabotagem por procuração (*proxy sabotage*), nas quais a cadeia de execução é propositalmente dissociada do eventual mentor estatal da operação (Monaghan *et al*., 2023). Essa estratégia não apenas amplia as camadas de negação plausível, como transfere o ônus da prova para as nações atingidas, que se veem compelidas a demonstrar, sob rigorosos critérios de atribuição, o nexo causal entre a conduta de entes privados e a eventual responsabilidade internacional de um Estado soberano (Sari, 2025), expondo a zona de fricção na qual a interpretação jurídica colide com a opacidade operacional.

Todavia, a eficácia dessas operações não depende apenas da manipulação física das infraestruturas, mas também da capacidade de degradar os sistemas de detecção e rastreamento responsáveis por identificar anomalias no domínio marítimo. É nesse ponto que a fenomenologia das ameaças no Báltico expande-se para o domínio imaterial da guerra eletrônica. Ao longo de 2024, diversos Estados da região, incluindo Polônia, Suécia e Estônia, relataram episódios recorrentes de interferência e *spoofing* em sistemas de posicionamento global (GPS), afetando a navegação de milhares de aeronaves e embarcações civis (PARLIAMENT OF THE REPUBLIC OF POLAND, 2025). Essas interferências eletromagnéticas, amplamente associadas a sistemas de guerra eletrônica e de negação de área (*Anti-Access/Area Denial – A2/AD*) posicionados nos enclaves de Kaliningrado e na região de São Petersburgo, produziram efeitos que transcendem a mera perturbação da navegação civil, contribuindo para a degradação sistemática da consciência situacional marítima no Mar Báltico (Livermore, 2024; Swistek; Paul, 2023). Ao gerar uma "neblina digital", tais práticas mascaram a posição real de embarcações, dificultam o rastreamento preciso de atividades ilícitas por meio do Sistema de Identificação Automática (AIS) e facilitam a movimentação encoberta de meios submersíveis, ampliando de forma significativa as vulnerabilidades associadas à proteção de infraestruturas submarinas críticas e operando como um multiplicador de força para a sabotagem física. Nesse cenário, a dificuldade de qualificação jurídica desses eventos transcende a complexidade técnica das operações, revelando um impasse fundamental: a relutância dos Estados em recorrer às interpretações expansivas

disponíveis no Direito do Mar acaba por converter a ambiguidade operacional em paralisia jurídica.

Em última análise, o Mar Báltico consolidou-se como o laboratório definitivo para a observação das novas formas de agressão infraestrutural, no qual a "cegueira marítima" clássica foi substituída por uma "neblina digital" intencional. A experiência do biênio 2023–2024 demonstra que a arquitetura da conectividade digital global não pode mais ser protegida exclusivamente por uma "Constituição dos Oceanos" que ignora a desmaterialização da agressão e a instrumentalização de meios civis. O esgotamento da racionalidade jurídica da CNUDM frente aos incidentes do *NewNew Polar Bear*, *Yi Peng 3* e *Eagle S* demonstra que a segurança das redes submarinas deslocou-se do plano estritamente normativo para o domínio da vigilância ativa e da resiliência tecnológica. Esse cenário de paralisia jurídica e impunidade sistêmica tem forçado os Estados costeiros a buscar alternativas que transcendem o Direito Internacional clássico, inaugurando uma nova fase da governança oceânica baseada na dissuasão por negação e na proteção proativa de ativos vitais.

4.3 O IMPASSE DA RESPONSABILIZAÇÃO INTERNACIONAL NO MAR BÁLTICO: ENTRE AS POTENCIALIDADES INTERPRETATIVAS DA CNUDM E A AUTOCONTENÇÃO ESTATAL

A transição da descrição empírica dos incidentes para a análise de sua repercussão jurídica revela que os eventos ocorridos no Mar Báltico não constituem meras falhas contingenciais de segurança, mas a exploração deliberada de um descompasso normativo estrutural. Tais episódios evidenciam como o emprego de meios civis e a produção intencional de incerteza causal permitem navegar na zona cinzenta da legalidade, na qual as ferramentas tradicionais de atribuição e resposta da CNUDM mostram-se ineficazes. Nesse sentido, o desafio da proteção das infraestruturas submarinas críticas desloca-se da simples vigilância física para a necessidade de uma nova arquitetura de governança que considere a natureza híbrida e a opacidade das frotas que exploram as lacunas de vigilância e resposta do Direito Internacional.

A sucessão de incidentes ocorridos no Mar Báltico entre 2023 e 2024 demonstra que o obstáculo à responsabilização internacional não decorre da carência de ferramentas hermenêuticas, mas do descompasso entre as potencialidades interpretativas da CNUDM e a prudência geopolítica com que os Estados têm optado por mobilizá-las no plano operacional, em uma conjuntura de elevada tensão estratégica. Nesse contexto, a paralisia jurídica

observada diante de episódios como os envolvendo os navios *NewNew Polar Bear* e *Yi Peng 3* reflete o temor de cair em uma armadilha reflexiva: a percepção de que a elasticidade interpretativa necessária para punir o sabotador na ZEE poderia gerar precedentes sensíveis, passíveis de instrumentalização por potências rivais para cercear liberdades de navegação em outros teatros globais (Tammikko, 2025). A prática estatal no Mar Báltico demonstrou, assim, uma notável autocontenção (*self-restraint*) no emprego desses instrumentos, caracterizada pela adesão estrita e cautelosa aos protocolos tradicionais de investigação criminal e diplomática. Tal postura indica que, para as democracias liberais da região, o custo político de tensionar a Convenção e precipitar crises diplomáticas com potências nucleares ou parceiros comerciais sistêmicos supera, no cálculo estratégico imediato, os benefícios de uma ação coercitiva unilateral. Consolida-se, desse modo, um impasse normativo-operacional, no qual a ambiguidade deliberadamente explorada por atores estatais e paraestatais encontra correspondência em uma prudência interpretativa que, embora politicamente compreensível, reduz a efetividade prática dos mecanismos jurídicos existentes e amplia a vulnerabilidade das infraestruturas submarinas estratégicas.

A prudência interpretativa demonstrada pelos Estados costeiros é potencializada pela própria arquitetura operacional das ações de sabotagem em zona cinzenta, estruturadas de modo a maximizar a negação plausível e a elevar substancialmente o ônus probatório necessário à atribuição de responsabilidade internacional. Ao recorrer ao emprego de embarcações civis e bandeiras de conveniência, os perpetradores deslocam o centro de gravidade do conflito para o plano probatório, no qual a comprovação do elemento subjetivo e do vínculo estrutural com um Estado soberano colide com os elevados padrões de prova exigidos pelo Direito Internacional. A estratégia de sabotagem revela, portanto, uma racionalidade jurídica calculada: não se trata apenas de causar dano físico à infraestrutura crítica, mas de estruturar a operação de forma a manter o evento permanentemente situado na zona cinzenta entre o acidente náutico e o ato ilícito internacional, espaço no qual a resposta jurídica tende a ser retardada, fragmentada ou politicamente inviabilizada, convertendo a ambiguidade operacional em vantagem estratégica para o agressor.

Diante desse dilema, a resposta dos Estados bálticos e nórdicos tem progressivamente se deslocado do plano estritamente normativo para o domínio da resiliência operacional e da dissuasão por negação (Monaghan *et al*., 2023). Esse movimento indica que, diante da dificuldade de mobilizar de forma efetiva os instrumentos clássicos de responsabilização internacional, os Estados têm buscado compensar as fragilidades do regime jurídico por meio de um paradigma de dissuasão baseado na resiliência. Em vez de concentrar esforços

exclusivamente na punição *ex post* dos responsáveis, frequentemente inviabilizada pela ambiguidade causal e pelas restrições interpretativas autoimpostas, as estratégias adotadas passaram a priorizar mecanismos preventivos destinados a mitigar a utilidade coercitiva das operações de sabotagem (Tammikko, 2025). Essa lógica pragmática reconhece que, se o Direito Internacional carece de meios de execução imediatos para punir agressores operando sob o manto da negação plausível, a segurança das redes deve emanar da capacidade de tornar o ataque ineficaz, seja pela complexidade de sua consecução, seja pela garantia de que o serviço será mantido apesar do dano físico.

A materialização dessa virada operacional ocorre por meio da institucionalização da vigilância estratégica e do aumento da consciência situacional marítima. A resposta institucional ao vácuo jurídico traduziu-se na ativação de missões de monitoramento ostensivo, como a operação "Baltic Sentry", lançada pela OTAN, e a iniciativa "Nordic Warden", capitaneada pela Força Expedicionária Conjunta (JEF – *Joint Expeditionary Force*)[41], ambas voltadas para coordenar a detecção de ameaças (Tammikko, 2025; JOINT EXPEDITIONARY FORCE, 2024). Esses esforços marcam a transição de patrulhas navais genéricas para um modelo de saturação sensorial do ambiente marítimo, operacionalizado por uma rede integrada de vigilância automatizada que alia ativos convencionais a sistemas não tripulados, tais como veículos aéreos (UAVs) e de superfície (USVs), o que evidencia uma reconfiguração funcional da governança dessas redes estratégicas, deslocando o foco da regulação passiva para a proteção ativa. O objetivo central é consolidar um efeito panóptico no leito marinho: ao reduzir o anonimato essencial à atuação das frotas fantasmas, a governança regional eleva o risco político do sabotador, convertendo a detecção imediata de anomalias em um fator de dissuasão que antecede e independe da morosidade dos processos judiciais. Essa arquitetura de vigilância, coordenada por centros especializados como o

[41] A JEF (2026), estabelecida formalmente em 2014 sob a liderança do Reino Unido (*framework nation*), constitui uma coalizão de defesa congregada por dez nações do norte europeu com interesses estratégicos convergentes: Dinamarca, Estônia, Finlândia, Islândia, Letônia, Lituânia, Países Baixos, Noruega, Suécia e o próprio Reino Unido, com foco geográfico no Alto Norte, Atlântico Norte e Mar Báltico (JEF, 2024). Diferentemente da OTAN, a JEF não é uma força permanente, mas um conjunto de forças de alta prontidão que opera sob um modelo flexível de *opt-in* (adesão voluntária por missão), o que elimina a necessidade de consenso unânime para o destacamento de tropas (FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS, 2024). Essa característica confere à JEF a agilidade necessária para atuar como vetor de primeira resposta em crises que ocorrem abaixo do limiar de guerra convencional (zona cinzenta) e antes da invocação do artigo 5º da OTAN, preenchendo lacunas operacionais em zonas de tensão híbrida (JEF, 2024). Em resposta à sabotagem do gasoduto Nord Stream e à invasão da Ucrânia em 2022, a JEF reorientou significativamente sua postura estratégica para a proteção de Infraestruturas Submarinas Críticas (Arnold, 2024; JEF, 2024). Nesse contexto, a iniciativa "Nordic Warden" foi executada em junho de 2024 como uma Opção de Resposta da JEF (*JEF Response Option - JRO*), coordenando aproximadamente 28 navios e 6 aeronaves para monitorar o tráfego marítimo suspeito e proteger rotas vitais de energia e comunicação (JEF, 2024), operacionalizando a vigilância integrada e assegurando a resiliência das conexões vitais para a segurança europeia.

NMCSCUI (*NATO Maritime Centre for Security of Critical Undersea Infrastructure*)[42], atua diretamente na tomada de decisões e na coordenação de ações relacionadas à proteção desses ativos vitais (NATO, 2025), buscando reduzir drasticamente a janela de oportunidade para ações hostis, sinalizando que a impunidade operacional não é mais uma garantia para o agressor.

No plano tecnológico e infraestrutural, essa mutação funcional é consolidada pela conversão da infraestrutura passiva em sensores ativos e pela busca por uma redundância automática. A implementação da tecnologia DAS (*Distributed Acoustic Sensing*)[43], que utiliza a própria fibra óptica para detectar vibrações e interferências físicas em tempo real (Jüris, 2020), permite que o sistema identifique manipulações no leito marinho antes mesmo da consolidação do dano, mitigando a histórica "cegueira" do domínio subaquático. Paralelamente, iniciativas de vanguarda como o projeto HEIST (*Hybrid Space and Submarine Architecture to Ensure Information Security of Telecommunications*)[44] buscam neutralizar a

[42] Instituído politicamente na Cúpula de Vilnius (2023), na qual o domínio submarino foi reconhecido como teatro prioritário de defesa contra a guerra híbrida, e tendo atingido sua Capacidade Operacional Inicial (IOC - *Initial Operational Capability*) em maio de 2024, o *NATO Maritime Centre for Security of Critical Undersea Infrastructure* (NMCSCUI) opera junto ao Comando Marítimo Aliado (MARCOM) em Northwood, Reino Unido (NATO, 2023, para. 65; NATO, 2024). Sua missão central consiste em identificar vulnerabilidades sistêmicas nas redes de energia e dados, fornecendo consciência situacional em tempo real para preparar, dissuadir e defender o espaço euro-atlântico contra táticas híbridas e o uso coercitivo de infraestruturas por atores estatais e não estatais (Monaghan *et al*., 2023). Na prática, o Centro funciona como um *hub* tático de fusão de dados e inteligência, cuja função é assistir o Comandante do MARCOM na tomada de decisões, no destacamento de forças e na coordenação de ações, atuando como a estrutura de comando responsável por sustentar operações de vigilância ativa (NATO, 2024). A arquitetura de governança da OTAN para a proteção dessas infraestruturas é dual: enquanto o NMCSCUI foca na vigilância operacional, ele atua em complementaridade com a Célula de Coordenação de Infraestrutura Crítica Submarina (*Critical Undersea Infrastructure Coordination Cell*), localizada no Quartel-General da OTAN em Bruxelas, que detém o mandato de articulação político-estratégica e de ligação com a indústria privada, estabelecendo uma comunidade de confiança para o compartilhamento de melhores práticas entre autoridades civis e militares, visando integrar as capacidades civis de monitoramento à rede de vigilância aliada (Bueger, 2024).

[43] O DAS opera transformando um cabo de fibra óptica padrão em uma matriz contínua de milhares de sensores acústicos e sísmicos virtuais. O princípio físico baseia-se no monitoramento do retroespalhamento Rayleigh (*Rayleigh backscattering*): uma Unidade de Interrogação (*Interrogator Unit* - IU) instalada na estação de aterragem do cabo envia pulsos de laser de alta coerência através de uma fibra (geralmente uma fibra escura/não utilizada) (Cox *et al*., 2012); qualquer perturbação acústica ou vibratória externa, como a aproximação de um submarino, o arrasto de uma âncora, a movimentação de um veículo subaquático autônomo (UUV) ou atividades sísmicas (Drapp; Mildner, 2025), induz microdeformações na fibra que alteram a fase da luz refletida. O interrogador óptico processa essas variações de fase para determinar a localização e a intensidade do evento, convertendo efetivamente dezenas de quilômetros de cabos de telecomunicações passivos em uma densa matriz linear de microfones virtuais com resolução espacial métrica (Drapp; Mildner, 2025). No ambiente marítimo, o DAS supera as limitações de sensores pontuais discretos, oferecendo uma vigilância contínua que minimiza as lacunas de cobertura, com reduzido custo logístico ao instrumentalizar a infraestrutura pré-existente (Wei *et al.*, 2024).

[44] O projeto HEIST, lançado oficialmente em julho de 2024 com o co-financiamento do programa *Science for Peace and Security* (SPS) da OTAN e liderado pela Universidade de Cornell em um consórcio internacional (incluindo a *Swedish Defence University*, *Bifröst University* e ETH Zürich) (NATO, 2024), representa uma mudança de paradigma na segurança de infraestruturas críticas, movendo-se da proteção passiva para a resiliência ativa automatizada. Tecnicamente, o HEIST opera como uma arquitetura de "sistema de sistemas" composta por três segmentos integrados: (1) um *Hub* de Consciência Situacional, que funde dados de sensores submarinos (como a tecnologia DAS e C-OTDR) e vigilância espacial para detectar ameaças em tempo real; (2)

eficácia política da sabotagem ao estabelecer uma redundância híbrida, integrando o tráfego de dados a constelações de satélites em caso de ruptura física (Boschetti *et al.*, 2025). Essa lógica de fusão de dados é institucionalizada pela OTAN através do conceito de "Oceano Digital" (*Digital Ocean Vision*), endossado em 2023 para criar uma rede de sensores em escala global, do leito marinho ao espaço, que utiliza inteligência artificial (IA) e sistemas autônomos para prever, identificar e combater ameaças (Monaghan *et al.*, 2023). Ao garantir que o corte de um componente material não resulte no isolamento digital do Estado-alvo, a governança operacional esvazia o valor coercitivo das ameaças híbridas. Conclui-se, portanto, que a estabilidade das comunicações globais no século XXI depende de uma arquitetura de segurança transversal: enquanto a CNUDM permanece como o marco de referência para a ordem normativa, a proteção fática das redes passa a repousar na superioridade informacional e na capacidade de resiliência tecnológica, sinalizando que o domínio marítimo tornou-se um ambiente cuja segurança demanda a integração funcional multidomínio, materializada no conceito de Consciência Situacional do Leito Marinho ao Espaço (S3A)[45] (Braca, 2023).

Nesse contexto, a experiência báltica não deve ser compreendida como uma anomalia regional, mas como o sinal precursor de uma transformação mais ampla da governança oceânica, na qual a segurança das infraestruturas submarinas passou a depender menos da vigência de normas jurídicas e mais do emprego ostensivo de meios navais capazes de constranger, pela projeção dissuasória de capacidades, a atuação de atores hostis. No entanto, essa securitização pela presença constitui uma solução insustentável a longo prazo, dado que

uma Camada de Contratação Inteligente (*Smart Contracting Layer* - SCL), baseada em *blockchain* e *Distributed Ledger Technology* (DLT); e (3) um ecossistema satelital heterogêneo multi-órbita (LEO/MEO). A inovação central do projeto reside na utilização de contratos inteligentes (algoritmos autônomos) que, ao receberem o alerta de ruptura do cabo via *Hub* de monitoramento, negociam e ativam instantaneamente a alocação de largura de banda ociosa de operadoras comerciais de satélite (como *Starlink* ou *Eutelsat/OneWeb*) (Boschetti *et al.*, 2025), reduzindo o tempo de interrupção de dias (tempo de reparo físico) para minutos ou segundos (tempo de comutação lógica). Dado o descompasso de capacidade entre a fibra óptica (escala de Terabits) e os satélites (Gigabits), o sistema utiliza protocolos de priorização de tráfego, assegurando que dados governamentais, militares e financeiros críticos sejam redirecionados automaticamente, mitigando o isolamento estratégico do Estado-alvo enquanto os reparos físicos são organizados, garantindo assim a continuidade de serviços essenciais mesmo em cenários de guerra híbrida (Boschetti *et al.*, 2025).

[45] O conceito de *Seabed-to-Space Situational Awareness* (S3A) representa a evolução da tradicional Consciência Situacional Marítima (MSA) para uma arquitetura holística de vigilância voltada para Operações Multidomínio (MDO) (NATO, 2023), que integra dados de sensores heterogêneos distribuídos verticalmente desde o leito marinho até os ativos espaciais. Operacionalmente, a S3A trata a segurança marítima como um problema de *Maritime Big Data*, fundamentando-se na fusão de informações e na IA (*Maritime AI and Information Fusion*) para processar volumes massivos de dados provenientes de fontes acima da água (como satélites de Radar de Abertura Sintética - SAR, sensores óticos e AIS) e abaixo da água (como Veículos Submarinos Autônomos - AUVs, planadores submarinos e sensores acústicos passivos/ativos) (Soldi *et al.*, 2023). O diferencial tecnológico reside na aplicação de algoritmos de aprendizado de máquina (*machine learning*) sobre essa base de dados *Multi-INT* (*Multi-Intelligence*), utilizando o conhecimento adquirido para antecipar comportamentos futuros e identificar anomalias (Soldi *et al.*, 2023), permitindo que o sistema mantenha a custódia virtual de um alvo mesmo quando este transita entre domínios ou explora as lacunas de cobertura entre o fundo do mar e a superfície.

exige recursos navais desproporcionais para monitorar extensas redes de infraestrutura estruturalmente indefesas (Van Soest *et al.*, 2025). O caso do Báltico confirma, portanto, a constatação de que o regime jurídico atual, concebido para um contexto de cooperação e estabilidade, tornou-se disfuncional diante da instrumentalização hostil da conectividade global. A paralisia observada, materializada pelo fato de que as construções hermenêuticas examinadas, embora defensáveis em plano abstrato, não foram mobilizadas pelos Estados afetados, revela que tais saídas carecem da robustez necessária para conferir segurança jurídica à ação estatal em cenários de alta tensão. Nesse sentido, a preferência pela autocontenção demonstra que os remédios interpretativos são insuficientes para mitigar o risco político e a ambiguidade normativa que cercam os ativos submarinos.

Por conseguinte, a crise de responsabilização afirma-se não como um acidente de percurso, mas como o resultado estrutural de uma ordem jurídica que, embora tenha logrado êxito em proteger a circulação marítima, permanece insuficientemente equipada para assegurar a proteção dos fluxos informacionais e energéticos que sustentam a economia digital contemporânea. A crescente dissociação entre a arquitetura normativa da CNUDM e as exigências estratégicas da era das infraestruturas críticas deve, assim, impelir a UE, enquanto organismo intrinsecamente orientado à resiliência dos regimes internacionais, a protagonizar o fomento de atualizações normativas condizentes com a complexidade da conjuntura geopolítica atual (Besch; Brown, 2024). Em última análise, a inércia forçada observada no Báltico desvela a exaustão funcional do modelo vigente, conferindo caráter de imperatividade à proposição de um novo marco regulatório capaz de substituir a precariedade da adaptação interpretativa pela clareza de um comando normativo explícito.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa dedicou-se a analisar a adequação do regime normativo da CNUDM frente às ameaças híbridas e cibernéticas dirigidas aos cabos submarinos de comunicação. O percurso investigativo permitiu o cumprimento dos objetivos propostos, validando a premissa de que o arcabouço jurídico vigente, concebido em uma era analógica e estatal-cêntrica, revela-se estruturalmente inadequado diante da complexidade das novas táticas de guerra na zona cinzenta. Forjada sob os imperativos de estabilidade estratégica e de distribuição de recursos característicos da Guerra Fria, a CNUDM excluiu deliberadamente diversas dimensões relativas à paz e à segurança, produzindo orientações estruturalmente ambíguas para a proteção de infraestruturas críticas que sequer figuravam como preocupação estratégica à época de sua negociação. Nesse contexto, demonstrou-se que a denominada "Constituição dos Oceanos", ao condicionar a tutela jurídica à materialidade do dano físico e à identificação inequívoca do Estado de bandeira, acabou por instituir, paradoxalmente, um ambiente de permissividade operacional sistêmica explorado por atores que instrumentalizam a conectividade global como vetor de coerção estratégica.

Inicialmente, constatou-se que, a despeito de os cabos submarinos terem transcendido sua natureza técnica para se consolidarem como o sistema nervoso central da segurança e da economia global, a resposta jurídica internacional não acompanhou essa evolução estratégica. O exame dogmático revelou um descompasso estrutural: a proteção conferida pelos artigos 113 a 115 da CNUDM permanece essencialmente limitada aos casos de ruptura culposa ou negligente, típicos de acidentes de pesca, deixando um vácuo normativo absoluto para atos de sabotagem estatal deliberada e operações cibernéticas contra infraestruturas submarinas. Essa lacuna não pode ser legitimamente suprida por hermenêutica extensiva, uma vez que a tentativa de enquadrar tais condutas no instituto da pirataria carece de amparo consistente na prática estatal e colide com o princípio da legalidade estrita (Azaria, 2025), consolidando a percepção de que o Direito do Mar dispõe de ferramentas para punir o ator negligente, mas permanece inerte diante do sabotador estratégico.

Essa fragilidade normativa não permaneceu circunscrita ao plano das abstrações teóricas; materializou-se, com vigor incontestável, nas águas do Mar Báltico. Os incidentes recentes demonstraram que a arquitetura jurídica vigente, concebida sob a premissa da cooperação e da visibilidade, converteu-se, involuntariamente, em um mecanismo de blindagem para a agressão híbrida. Ao exigir padrões de atribuição de responsabilidade incompatíveis com a opacidade deliberada das operações contemporâneas, o sistema atual

institucionalizou uma zona de impunidade, na qual a negação plausível e o emprego instrumental de frotas civis esvaziam, na prática, a efetividade da norma internacional. Diante desse silêncio do Direito, a comunidade internacional viu-se compelida a substituir a segurança jurídica por arranjos de segurança baseados na força. A militarização da vigilância e a aposta na resiliência física surgem, assim, não como estratégias complementares de governança, mas como indícios da falência funcional do regime de proteção, representando um retrocesso institucional que fragmenta a ordem marítima e amplia o risco de escaladas indesejadas.

Nesse cenário, a experiência empírica demonstrou que a distinção acadêmica entre ameaça física e ameaça cibernética tende a se dissolver na prática da guerra híbrida. Ao atacar a Camada Física da rede mediante o emprego de frotas mercantes, os atores estatais alcançam efeitos cibernéticos paralisantes, como a interrupção de dados e a violação da soberania digital, sem incorrer nos riscos de atribuição de uma ciberguerra declarada. A CNUDM, ao focar estritamente na ruptura material e ignorar a intencionalidade estratégica de negar o serviço digital, falha em proteger a espinha dorsal da conectividade, independentemente de o ataque ser perpetrado por um *malware* ou por uma âncora.

Conclui-se, assim, que, diante da inviabilidade política de emendas diretas ao texto de 1982 (Besch; Brown, 2024), a superação da obsolescência normativa não reside em remendos hermenêuticos, mas demanda a negociação de um tratado multilateral temático ou a adoção de um Protocolo Adicional à CNUDM, especificamente orientado à segurança de infraestruturas submarinas críticas (Beckman, 2014). Essa agenda normativa deve transcender a lógica restrita da responsabilidade civil para promover uma modernização estrutural da governança dos oceanos, espelhando-se na arquitetura jurídica do Acordo BBNJ, também conhecido como Tratado de Alto Mar (Besch; Brown, 2024). A consecução desse arranjo pressupõe, por sua vez, a superação da visão da "Constituição dos Oceanos" como estrutura monolítica e autossuficiente, reconhecendo que o regime de 1982, embora fundamental, não oferece respostas exaustivas aos dilemas de segurança característicos da era digital.

Diante dessa insuficiência, a institucionalização de um regime complementar torna-se a via necessária para conferir densidade jurídica à proteção das infraestruturas críticas submarinas. O novo instrumento deverá, portanto, contemplar: (i) a tipificação internacional do crime de dano intencional a infraestruturas críticas, superando a atual ambiguidade associada aos acidentes de navegação (Beckman, 2014; Davenport, 2015); (ii) a instituição de mecanismos de jurisdição universal ou concorrente, autorizando Estados costeiros e Estados diretamente afetados pela interrupção dos serviços a proceder à interdição e inspeção de

embarcações suspeitas em águas internacionais, mediante salvaguardas jurídicas estritas e independentemente do Estado de bandeira (Davenport, 2015); e (iii) o estabelecimento de obrigações reforçadas de cooperação em investigação forense, mitigando o ônus probatório que atualmente paralisa a capacidade de resposta estatal (Davenport, 2015). Sem essa atualização estrutural, a governança dos oceanos permanecerá assimétrica: densamente regulamentada no tocante à proteção ambiental e à exploração de recursos minerais, mas perigosamente anárquica quanto à proteção das infraestruturas de dados que sustentam o funcionamento sistêmico das sociedades contemporâneas.

As implicações sistêmicas dessa evolução normativa seriam profundas. Tal transformação fortaleceria a responsabilização internacional, elevando a proteção dos cabos ao status de interesse comum da humanidade, análogo ao tratamento conferido à pirataria, e encerrando o ciclo de impunidade explorado por frotas fantasmas e por atores estatais que operam na zona cinzenta. Potencializaria, ainda, os mecanismos de cooperação interestatal, ao fornecer o lastro jurídico necessário para operações conjuntas de vigilância e *enforcement*, legitimando iniciativas como as já incipientes ações da OTAN e da JEF no Báltico e no Atlântico Norte (Monaghan *et al*., 2023). Sobretudo, ampliaria a capacidade preventiva dos Estados costeiros, conferindo-lhes prerrogativas de fiscalização mais assertivas sobre embarcações que demonstrem comportamento anômalo em suas ZEEs. Dessa forma, a atual postura de passividade compulsória seria substituída por um modelo de dissuasão jurídica e operacional credível, no qual o custo político e legal da sabotagem tende a superar seus benefícios táticos.

Em última análise, a "Constituição dos Oceanos" precisa adaptar-se às exigências da era digital, sob pena de a proteção da espinha dorsal da internet permanecer refém da *realpolitik* e as profundezas oceânicas converterem-se, na prática, em uma *terra nullius* digital. Para preservar sua relevância como instrumento de ordem e estabilidade, o Direito Internacional do Mar deve reconhecer que, no século XXI, a segurança das nações depende não apenas da inviolabilidade de suas fronteiras territoriais, mas também da resiliência de suas conexões digitais. A proteção do leito marinho deixa, assim, de constituir uma preocupação periférica associada à mera manutenção de cabos para afirmar-se como um dos eixos estruturantes da soberania, da defesa coletiva e da governança internacional na era da hiperconectividade global.

REFERÊNCIAS

ABC NEWS. Internet outage hits businesses from Cairo to Colombo. New York, 1 fev. 2008. Disponível em: https://www.abc.net.au/news/2008-02-01/internet-outage-hits-businesses-from-cairo-to/1029498?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web. Acesso em: 20 nov. 2025.

AGNEW, John. The territorial trap: the geographical assumptions of international relations theory. *Review of International Political Economy*, v. 1, n. 1, p. 53-80, 1994. Disponível em: https://polgeog.jp/wp-content/uploads/2019/12/TerritorialTrap.pdf. Acesso em: 11 fev. 2026.

AGNORELLI, Erik. *Under the sea and above the law: Analyzing States' possibilities to respond to episodes of sabotage to submarine infrastructure*. 2025. Dissertação (Mestrado em Direito) — Faculdade de Direito, Lund University, Lund, 2025.

ANDERSSON, Patrik; JERDÉN, Björn; VON SYDOW, Alexis. *What the Yi Peng 3 cable-cutting incident reveals about China-Russia relations.* Stockholm: Swedish National China Centre, 5 mar. 2025. Disponível em: https://kinacentrum.se/publikationer/what-the-yi-peng-3-cable-cutting-incident-reveals-about-china-russia-relations/. Acesso em: 13 fev. 2026.

ARNOLD, Ed. *The Joint Expeditionary Force and its contribution to European security.* London: Royal United Services Institute for Defence and Security Studies (RUSI), 9 dez. 2024. Disponível em: https://static.rusi.org/the-joint-expeditionary-force-and-its-contribution-to-european-security.pdf. Acesso em: 12 fev. 2026.

ARQUILLA, John; RONFELDT, David (orgs.). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation, 2001.

ASTIER, H.; KIRBY, P. Germany suspects sabotage behind severed undersea cables in the Baltic. *BBC News*, 2024. Disponível em: https://www.bbc.com/news/articles/c9dl4vxw501o. Acesso em: 5 jan. 2026.

AVEN, Terje. *Risk analysis*. 2. ed. Hoboken: John Wiley & Sons, 2015.

AZARIA, Danae. *Expert report: Security of submarine cables and pipelines under public international law: use of force and the law of the sea*. [S.l.]: CAHDI, 2025.

BECKMAN, Robert. Protecting submarine cables from intentional damage—The security Gap. In: BURNETT, Douglas R.; BECKMAN, Robert; DAVENPORT, Tara (org.). Submarine cables: The handbook of law and policy. Leiden: Martinus Nijhoff Publishers, 2014. cap. 12, p. 281–297.

BELLI, Luca; FRANQUEIRA, Bruna; *et al*. *Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano*. Rio de Janeiro: FGV Direito Rio, 14 jun. 2023. (CyberBRICS). Disponível em: https://cyberbrics.info/wp-content/uploads/2023/10/Ciberseguranca-uma-visao-sistemica-rum

o-a-uma-proposta-de-Marco-Regulatorio-para-um-Brasil-digitalmente-soberano-1.pdf. Acesso em: 14 ago. 2025.

BENNER, T. The Underwater Battlefield: Protecting Submarine Critical Infrastructure. *Internationale Politik Quarterly*, 2025. Disponível em: https://ip-quarterly.com/en/underwater-battlefield-protecting-submarine-critical-infrastructure. Acesso em: 5 jan. 2026.

BESCH, Sophia; BROWN, Erik. *A Chinese-flagged ship cut Baltic Sea internet cables: this time, Europe was more prepared.* Carnegie Endowment for International Peace, 3 dez. 2024. Disponível em: https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security. Acesso em: 5 fev. 2026.

BESCH, Sophia; BROWN, Erik. *Securing Europe's subsea data cables.* Washington, D.C.: *Carnegie Endowment for International Peace*, dez. 2024. Disponível em: https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables. Acesso em: 10 fev. 2026.

BLANCATO, Filippo G.; CARR, Madeline. *The trust deficit: EU bargaining for access and control over cloud infrastructures*. Journal of European Public Policy, v. 1–32, 2024.

BOCKMANN, Michelle W.. *Russia-linked cable-cutting tanker seized by Finland 'was loaded with spying equipment'. Lloyd's List*, 27 dez. 2024. Disponível em: https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment. Acesso em: 7 jan. 2026.

BOSCHETTI, Nicolò *et al*. *Hybrid Space and Submarine Architecture to Ensure Information Security of Telecommunications (HEIST)*. IEEE Access, v. 11, 2023.

BRACA, Paolo. *Multi-Domain Situational Awareness: Seabed-to-Space Situational Awareness (S3A)*. La Spezia: NATO Science and Technology Organization – Centre for Maritime Research and Experimentation (STO-CMRE), 2023. Disponível em: https://ieee-aess.org/files/ieeeaess/slides/Braca_Multi_Domain%20SA%202023_compress.pdf. Acesso em: 3 fev. 2026.

BRASIL. Carta das Nações Unidas (promulgada pelo Decreto nº 19.841, de 22 out. 1945). Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm. Acesso em: 24 dez. 2025.

BRASIL. Decreto nº 99.165, de 12 de março de 1990. Promulga a Convenção das Nações Unidas sobre o Direito do Mar. *Diário Oficial da União*, Brasília, 1990. Disponível em: https://www2.camara.leg.br/legin/fed/decret/1990/decreto-99165-12-marco-1990-328535-publicacaooriginal-1-pe.html. Acesso em: 12 nov. 2025.

BRASIL. Ministério da Defesa. *Glossário das Forças Armadas – MD35-G-01*. 5. ed. Brasília: Ministério da Defesa, 2015.

BUEGER, Christian. *NATO's contribution to critical maritime infrastructure protection. Center for Maritime Strategy*, 19 jan. 2024. Disponível em:

https://centerformaritimestrategy.org/publications/natos-contribution-to-critical-maritime-infrastructure-protection/. Acesso em: 13 fev. 2026.

BUEGER, Christian; EDMUNDS, *Timothy. Beyond seablindness: A new agenda for maritime security studies. International Affairs*, v. 93, n. 6, p. 1293-1311, 2017. DOI: https://doi.org/10.1093/ia/iix174.

BUEGER, Christian; LIEBETRAU, Tobias. Protecting hidden infrastructure: the security politics of the global submarine data cable network. *Contemporary Security Policy*, v. 42, n. 3, p. 391-413, mar. 2021. DOI: https://doi.org/10.1080/13523260.2021.1907129.

BURNETT, D. Out-of-Service Submarine Cables. In: BURNETT, Douglas R.; BECKMAN, Robert; DAVENPORT, Tara (org.). Submarine cables: The handbook of law and policy. Leiden: Martinus Nijhoff Publishers, 2014. cap. 8, p. 213–222.

BURNETT, D.; CARTER, Lionel; DAVENPORT, Tara (org.). *Submarine cables: the handbook of law and policy*. Leiden: Martinus Nijhoff Publishers, 2014.

BURNETT, D.; FREESTONE, D.; DAVENPORT, T. *Submarine cables in the Sargasso Sea: Legal and environmental issues in areas beyond national jurisdiction*. Relatório de workshop realizado em 23 de outubro de 2014, publicado em 16 de janeiro de 2015. Disponível em: https://www.sargassoseacommission.org/storage/documents/Submarine_Cables_in_the_Sargasso_Sea_Final_Workshop_Report_dated_16_January_2015.pdf. Acesso em: 10 ago. 2025.

CARTER, Lionel; BURNETT, D. Subsea telecommunications. In: SMITH, Hance D.; SUÁREZ DE VIVERO, Juan Luis; AGARDY, Tundi S. (org.). *Routledge handbook of ocean resources and management*. New York: Taylor & Francis, 2015. p. 349–365.

CARTER, Lionel; *et al*. *Submarine cables and the oceans: connecting the world*. Cambridge: UNEP-WCMC; ICPC, 2009. (UNEP-WCMC Biodiversity Series, n. 31). Disponivel em: https://www.iscpc.org/documents/?id=132. Acesso em: 17 jul. 2025.

CAVELTY, Myriam Dunn. *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge, 2007.

CAVELTY, Myriam Dunn. *Cyberwar: concept, status quo, and limitations*. CSS Analyses in Security Policy, n. 71, Zurich: Center for Security Studies (CSS), ETH Zurich, abr. 2010. Disponível em: https://www.files.ethz.ch/isn/114442/CSS_Analysis_71.pdf. Acesso em: 5 jan. 2026.

CEPIK, Marco; CANABARRO, Diego R.; BORNE, Thiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: SOUZA, André de M.; NASSER, Reginaldo M.; MORAES, Rodrigo F. (org.). *Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI*. Brasília: IPEA, 2014. p. 161–186.

CHANG, Cheng-Chi Kirin. *Wires of War: Legal Reforms for Submarine Cable Security*. *University of Pennsylvania Journal of International Law*, Philadelphia, v. 46, p. 1-23, 2025. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2112&context=jil. Acesso em: 27 jan. 2026.

CHIAPPA, Claudia; NGENDAKUMANA, Pierre Emmanuel. ‘*Everything indicates’* Chinese ship damaged Baltic pipeline on purpose, Finland says. *Politico*, 1 dez. 2023. Disponível em: https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/. Acesso em: 6 jan. 2026.

CISCO SYSTEMS. *What is network management?* San Jose: Cisco, s.d. Disponível em: https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-management.html. Acesso em: 17 nov. 2025.

CLARE, Mike. *Submarine Cable Protection and the Environment*. Issue 11, Nov. 2025. London: International Cable Protection Committee (ICPC), 07 nov. 2025. Disponível em: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/. Acesso em: 5 jan. 2026.

COLLIER, Stephen J.; LAKOFF, Andrew. The vulnerability of vital systems: how “critical infrastructure” became a security problem. In: DUNN CAVELTY, Myriam; KRISTENSEN, Kristian Søby (eds.). *Securing “the homeland”: critical infrastructure, risk and (in)security*. Londres: Routledge, 2008. p. 17-39.

CONVENTION FOR THE PROTECTION OF SUBMARINE TELEGRAPH CABLES (1884). Convention for the Protection of Submarine Telegraph Cables, Paris, 14 mar. 1884. Canberra: Department of Foreign Affairs and Trade, 1999. (Australian Treaty Series, 1901 No. 1). Disponível em: https://www.gc.noaa.gov/documents/seabed-icpc_1884.pdf. Acesso em: 29 jan. 2026.

CORTE INTERNACIONAL DE JUSTIÇA. *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Sentença de 27 de junho de 1986. Disponível em: https://www.acerislaw.com/wp-content/uploads/2022/06/ICJ-Nicaragua.pdf. Acesso em: 3 jan. 2026.

CORTE INTERNACIONAL DE JUSTIÇA. *Corfu Channel Case (United Kingdom v. Albania)*. Sentença de 9 de abril de 1949. Disponível em: https://www.acerislaw.com/wp-content/uploads/2023/12/Corfu-Channel-case.pdf. Acesso em: 4 jan. 2026.

CORTE INTERNACIONAL DE JUSTIÇA. *Territorial Dispute (Libyan Arab Jamahiriya/Chad)*. Sentença de 3 de fevereiro de 1994. Disponível em: https://www.icj-cij.org/sites/default/files/case-related/83/083-19940203-JUD-01-00-EN.pdf. Acesso em: 29 jan. 2026.

CORTE INTERNACIONAL DE JUSTIÇA. *Whaling in the Antarctic (Australia v. Japan): Separate Opinion of Judge Cançado Trindade*, Order of 6 February 2013. Disponível em: https://www.icj-cij.org/sites/default/files/case-related/148/148-20130206-ORD-01-02-EN.pdf. Acesso em: 30 jan. 2026.

CORTE PERMANENTE DE ARBITRAGEM. *In the matter of the Duzgit Integrity Arbitration (The Republic of Malta v. The Democratic Republic of São Tomé and Príncipe):*

Award. PCA Case No. 2014-07. Haia: Permanent Court of Arbitration, 5 set. 2016. Disponível em: https://pcacases.com/web/sendAttach/1915. Acesso em: 27 jan. 2026.

CORTE PERMANENTE DE ARBITRAGEM. *The Arctic Sunrise Arbitration (Kingdom of the Netherlands v. The Russian Federation): Award on the Merits*. PCA Case No. 2014-02. The Hague: Permanent Court of Arbitration, 14 ago. 2015. Disponível em: https://pcacases.com/web/sendAttach/1438. Acesso em: 7 fev. 2026.

COX, Barbara *et al. Distributed Acoustic Sensing for Geophysical Measurement, Monitoring and Verification*. *CSEG Recorder*, Calgary: Canadian Society of Exploration Geophysicists, fev. 2012. Disponível em: https://cseg.ca/wp-content/uploads/2012-02-RECORDER-Distributed_Acoustic_Sensing.pdf. Acesso em: 13 fev. 2026.

CRAWFORD, James. *State responsibility: the general part*. Cambridge: Cambridge University Press, 2013.

CRAWFORD, James. *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge: Cambridge University Press, 2002.

DAVENPORT, Tara. *Intentional Damage to Submarine Cable Systems by States*. Stanford: Hoover Institution, Stanford University, 2023. (Aegis Series Paper, n. 2305).

DAVENPORT, Tara. Submarine cables, cybersecurity and international law: an intersectional analysis. *Catholic University Journal of Law and Technology*, v. 24, n. 1, p. 57-109, dez. 2015.

DE BRUIJNE, Mark; VAN EETEN, Michel. Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*, [s. l.], v. 15, n. 1, p. 18–29, mar. 2007.

DRAPP, Bernd; MILDNER, Matthias. *Enhancing coastal critical infrastructure protection with distributed acoustic sensing (DAS)*. Böblingen: AP Sensing GmbH, 2025.

EDWARDS, Paul N. Infrastructure and modernity: force, time, and social organization in the history of sociotechnical systems. In: BREY, Philip; RIP, Arie; FEENBERG, Andrew (org.). *Technology and modernity: the empirical turn*. Cambridge: The MIT Press, 2003. p. 185-226.

ENISA. *Subsea Cables: What is at Stake?* Athens: European Union Agency for Cybersecurity, 2023. Disponível em: https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf. Acesso em: 18 nov. 2025.

EUROPEAN UNION. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance). *Official Journal of the European Union*, L 321, 15 Dec. 2022.

FEDERAL COMMUNICATIONS COMMISSION. *Protecting the Nation's Communications Systems from Cybersecurity Threats: Order on Reconsideration*, PS Docket No. 22-329; FCC

25-81. Washington, D.C.: Federal Communications Commission, 20 nov. 2025. Disponível em: https://docs.fcc.gov/public/attachments/FCC-25-81A1.pdf. Acesso em: 18 dez. 2025.

FINELLI, Francesca. *The European Union against Russia's shadow fleet: sanctions, circumvention and hybrid threats. DPCE Online*, v. 72, n. 4, p. 2601-2610, 2026.

FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS (FIIA). *Joint Expeditionary Force in Northern Europe.* Briefing Paper 389, May 2024. Disponível em: https://www.fiia.fi/wp-content/uploads/2024/05/bp389_joint-expeditionary-force-in-northern-europe.pdf. Acesso em: 13 fev. 2026.

FORD-RAMSDEN, Keith; DAVENPORT, Tara. The Manufacture and Laying of Submarine Cables. In: BURNETT, Douglas R.; BECKMAN, Robert; DAVENPORT, Tara (org.). Submarine cables: The handbook of law and policy. Leiden: Martinus Nijhoff Publishers, 2014. cap. 5, p. 123-154.

GRZĄDZIEL, A. *The Impact of Side-Scan Sonar Resolution and Acoustic Shadow Phenomenon on the Quality of Sonar Imagery and Data Interpretation Capabilities.* Remote Sensing, v. 15, n. 23, 5599, dez. 2023. Disponível em: https://doi.org/10.3390/rs15235599. Acesso em: 3 jan. 2026.

HARTMANN, Jacques. *Piracy and Undersea Cables: An Overlooked Interpretation of UNCLOS?* EJIL: Talk! – Blog of the *European Journal of International Law*, 6 mar. 2025. Disponível em: https://www.ejiltalk.org/piracy-and-undersea-cables-an-overlooked-interpretation-of-unclos/. Acesso em: 29 jan. 2026.

HARTMANN, Jacques; LOTT, Alexander. *The prosecution 'gap' for attacks on subsea cables and pipelines.* EJIL: Talk! – Blog of the *European Journal of International Law*, 13 nov. 2025. Disponível em: https://www.ejiltalk.org/the-prosecution-gap-for-attacks-on-subsea-cables-and-pipelines/. Acesso em: 29 jan. 2026.

HÖLLER, Linus. *The shallow Baltic Sea holds deep secrets about a hybrid war on NATO.* Defense News, [S. l.], 9 dez. 2024. Disponível em: https://www.defensenews.com/special-reports/2024/12/09/the-shallow-baltic-sea-holds-deep-secrets-about-a-hybrid-war-on-nato/. Acesso em: 3 jan. 2026.

HUNT, C. J. *Low Frequency Active Sonar (Generic UK) Performance Assessment in the Operationally Significant Area of the Northwest Approaches to the United Kingdom*. Naval Postgraduate School, Monterey, CA, 1998.

Impact of fiber optics on submarine cables: revolutionizing global connectivity. *MarketsandMarkets*, [s.l.], [s.d.]. Disponível em: https://www.marketsandmarkets.com/ResearchInsight/industry-reports-impact-of-fiber-optics-on-submarine-cables.asp. Acesso em: 11 ago. 2025.

INTERNATIONAL CABLE PROTECTION COMMITTEE. *Subsea landslide is likely cause of SE Asian communications failure*. Press release, 21 mar. 2007. Disponível em: https://www.iscpc.org/documents/?id=9. Acesso em: 18 nov. 2025.

INTERNATIONAL LAW ASSOCIATION. Committee on Submarine Cables and Pipelines under International Law. *Submarine Cables and Pipelines under International Law: Third Interim Report 2024*. [S.l.]: International Law Association, 2024.

INTERNATIONAL TELECOMMUNICATION UNION. *ITU-T Recommendation X.200 (07/94): Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.* Geneva: ITU, 1994.

INTERNATIONAL TELECOMMUNICATION UNION. *Recommendation ITU-T X.1205: Overview of cybersecurity*. [S.l.]: ITU-T, abr. 2008. Disponível em: https://www.itu.int/rec/T-REC-X.1205-200804-I. Acesso em: 10 ago. 2025.

INTERNATIONAL TELECOMMUNICATION UNION. *Submarine cable resilience*. [S.l.]: ITU, nov. 2024. Disponível em: https://www.itu.int/digital-resilience/submarine-cables/. Acesso em: 17 jul. 2025.

JOHNSON, Tim. Undersea cables: too valuable to leave vulnerable? *GovTech*, 12 dez. 2017. Disponível em: https://www.govtech.com/network/Undersea-Cables-Too-Valuable-to-Leave-Vulnerable.html. Acesso em: 17 jul. 2025.

JOINT CHIEFS OF STAFF. *Joint Publication 3-12: Cyberspace Operations*. [S. l.]: Joint Chiefs of Staff, 8 jun. 2018. Disponível em: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2018-JP-3-12-Cyberspace-Operations.pdf. Acesso em: 13 jan. 2026.

JOINT EXPEDITIONARY FORCE. *About the JEF.* Disponível em: https://jefnations.org/about-the-jef/. Acesso em: 13 fev. 2026.

JOINT EXPEDITIONARY FORCE. *JEF 2024 information booklet.* [S.l.]: Joint Expeditionary Force, 2024. Disponível em: https://jefnations.org/wp-content/uploads/2024/02/JEF-2024-Info-Booklet.pdf. Acesso em: 13 fev. 2026.

JOINT EXPEDITIONARY FORCE. *JEF Response Option NORDIC WARDEN contributes to the protection of critical underwater infrastructure*. 8 jul. 2024. Disponível em: https://jefnations.org/2024/07/08/jef-response-option-nordicwarden-contributes-to-the-protection-of-criticalunderwater-infrastructure/. Acesso em: 13 fev. 2026.

JOINT EXPEDITIONARY FORCE. *Nordic Warden enhances protection of critical undersea infrastructure*. 10 jun. 2024. Disponível em: https://jefnations.org/2024/06/10/nordic-warden-enhances-protection-of-critical-undersea-infrastructure/. Acesso em: 4 fev. 2026.

JÜRIS, Frank. *Handing over infrastructure for China's strategic objectives: "Arctic Connect" and the Digital Silk Road in the Arctic.* Prague: Sinopsis / Estonian Foreign Policy Institute, 7

mar. 2020. Disponível em: https://sinopsis.cz/wp-content/uploads/2020/03/jyrisarctic.pdf. Acesso em: 5 fev. 2026.

KAUSHAL, Sidharth. Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure. *RUSI Commentary*. Londres: Royal United Services Institute (RUSI), 25 maio 2023. Disponível em: https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure. Acesso em: 16 jan. 2026.

KEATING-BITONTI, Caitlin. *United Nations Convention on the Law of the Sea (UNCLOS): living resources provisions*. CRS Product R 47744. Washington, D.C.: Congressional Research Service, 2023. Disponível em: https://www.congress.gov/crs_external_products/R/PDF/R47744/R47744.5.pdf. Acesso em: 17 jul. 2025.

KEOHANE, Robert; NYE JR., Joseph. *Power and interdependence*. 4. ed. Boston: Pearson Education, 2011.

KUEHL, Daniel T. From cyberspace to cyberpower: defining the problem. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry (ogs.). *Cyberpower and national security*. Washington: National Defense University Press, 2009.

KWAN, Martin. *Gaps in accountability for submarine cable protection: inadequacies in the current legal framework. Ocean and Coastal Law Journal*, Portland, v. 30, n. 1, p. 1-30, 2025. Disponível em: https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1444&context=oclj. Acesso em: 6 jan. 2026.

LEHMANN, Andreas. *et al*. Salinity dynamics of the Baltic Sea. *Earth System Dynamics*, [s. l.], v. 13, p. 373–392, fev. 2022. DOI:10.5194/esd-13-373-2022.

LESSIG, Lawrence. *Code: and other laws of cyberspace, version 2.0*. New York: Basic Books, 2006.

LINDHOLM, Rickard. *Mapping Undersea Infrastructure Attacks in the Baltic Sea*. Washington, D.C.: Wilson Center, 24 mar. 2025. Disponível em: https://www.wilsoncenter.org/article/mapping-undersea-infrastructure-attacks-baltic-sea. Acesso em: 5 jan. 2026.

LIVERMORE, Doug. *NATO's Baltic Build-Up*. Washington, D.C.: Center for European Policy Analysis (CEPA), 4 set. 2024. Disponível em: https://cepa.org/article/natos-baltic-build-up/. Acesso em: 03 jan. 2026.

LLOYD'S LIST. *Flags of deceit could take shipping back to the bad old days.* Opinion, 2 fev. 2024. Disponível em: https://www.lloydslist.com/LL1148156/Flags-of-Deceit-could-take-shipping-back-to-the-bad-old-days. Acesso em: 12 fev. 2026.

LOKKER, N. *et al*. *How Finnish and Swedish NATO Accession Could Shape the Future Russian Threat: A Report of the Transatlantic Forum on Russia*. Washington, D.C.: Center for

a New American Security (CNAS), jan. 2023. Disponivel em: https://www.cnas.org/press/press-release/how-finnish-and-swedish-nato-accession-could-shape-the-future-russian-threat. Acesso em: 3 jan. 2026.

LOTT, Alexander. *Christmas Day Cable Cuts in the Baltic Sea*. EJIL: Talk!, 31 dez. 2024. Disponível em: https://www.ejiltalk.org/christmas-day-cable-cuts-in-the-baltic-sea/. Acesso em: 5 jan. 2026.

LOTT, Alexander. *The Baltic Sea cable-cuts and ship interdiction: the C-Lion1 incident.* Lieber Institute for Law and Warfare (Articles of War), 26 nov. 2024. Disponível em: https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/. Acesso em: 16 jan. 2026.

LOTT, Alexander. *Unconventional legal approaches to protecting underwater infrastructure*. Org. Michel Rademaker. The Hague: The Hague Centre for Strategic Studies, 2025.

MARTINAGE, R. *Under the Sea: The Vulnerability of the Commons*. *Foreign Policy*, v. 94, n. 1, p. 117-126, jan./fev. 2015.

MARTINO, L. International Law, State Sovereignty and Competition in the Digital Age. *Jura Gentium*, v. XXI, n. 2, p. 136-164, 2024.

MELLO FILHO, Eduardo Cavalcanti de. From 'Flags of Convenience' to 'Flags of Deceit': The Future of the Law Governing the Nationality of Ships. *International and Comparative Law Quarterly*, Cambridge, v. 74, supl., p. 121-137, 2025

MELLO FILHO, Eduardo Cavalcanti de. *The normative porosity of the UN Convention on the Law of the Sea: from "human rights at sea" to the "ocean-climate nexus"*. *Minnesota Journal of International Law*, Minneapolis, v. 34, n. 1, p. 87-161, 2025.

METZGER, J. The concept of critical infrastructure protection (CIP). In: BAILES, A. J. K.; FROMMELT, I. (eds.). *Business and Security: Public–Private Sector Relationships in a New Security Environment*. Oxford: Oxford University Press, 2004. p. 197-209.

MONAGHAN, Sean. *Countering Hybrid Warfare: conceptual foundations and implications for Defence Forces*. MCDC Information Note, mar. 2019. Disponível em: https://assets.publishing.service.gov.uk/media/5da9a79ae5274a5ca507c6bb/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf. Acesso em: 10 ago. 2025.

MONAGHAN, Sean. *et al*. *NATO's Role in Protecting Critical Undersea Infrastructure*. CSIS Briefs, 2023.

MONTEVIRGEN, Karl. *The rise of hyperscalers: Reshaping cloud computing and business*. Encyclopedia Britannica, [s.l.], [s.d.]. Disponível em: https://www.britannica.com/money/hyperscaler-data-centers. Acesso em: 13 nov. 2025.

MORCOS, Pierre; WALL, Colin. *Invisible and vital: undersea cables and transatlantic security*. Washington, D.C.: Center for Strategic and International Studies (CSIS), 11 jun. 2021. Disponível em:

https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security. Acesso em: 17 jul. 2025.

MUHAMAD, Zainab Hassan; ABDULMONIM, Dhafer Abdulameer. *Comparative Study Between the OSI Model and the TCP/IP Model: Architecture and Protocols in Computer Networking Systems. International Journal of Engineering and Computer Science*, v. 13, n. 8, p. 26358–26372, ago. 2024.

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION (NOAA). *Submarine cables*. Washington, D.C.: NOAA, 2024. Disponível em: https://www.noaa.gov/submarine-cables. Acesso em: 17 jul. 2025.

NORTH ATLANTIC TREATY ORGANIZATION. *NATO Baltic Sentry steps up patrols in the Baltic Sea to safeguard critical undersea infrastructure*. 2025. Disponível em: https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure. Acesso em: 6 fev. 2026.

NORTH ATLANTIC TREATY ORGANIZATION. *NATO-funded project to reroute internet to space in case of disruption to critical infrastructure*. 6 ago. 2024. Disponível em: https://www.nato.int/en/news-and-events/articles/news/2024/08/06/nato-funded-project-to-reroute-internet-to-space-in-case-of-disruption-to-critical-infrastructure. Acesso em: 13 fev. 2026.

NORTH ATLANTIC TREATY ORGANIZATION. *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure.* 28 maio 2024. Disponível em: https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui. Acesso em: 13 fev. 2026.

NORTH ATLANTIC TREATY ORGANIZATION. *Science and Technology Organization (STO): 2022 Highlights*. Brussels: NATO, 2023. Disponível em: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2023/3/pdf/230327-NATO-STO-Highlights.pdf. Acesso em: 13 fev. 2026.

NYE JR., Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.

OBAID, Hadeel S.; ABEED, Esamaddin H. *DoS and DDoS Attacks at OSI Layers. International Journal of Multidisciplinary Research and Publications (IJMRAP)*, v. 2, n. 8, p. 1–9, 2020.

OXMAN, Bernard H. *The rule of law and the United Nations Convention on the Law of the Sea*. European Journal of International Law, p. 353–371, 1996.

PAPAPAVLOU, Charalampos *et al*. Toward SDM-Based Submarine Optical Networks: A Review of Their Evolution and Upcoming Trends. *Telecom*, v. 3, n. 2, p. 234–280, 2022.

PARLIAMENT OF THE REPUBLIC OF POLAND. *Security in the Baltic Sea Region: Russian hostilities – attempts to change borders and circumvent EU sanctions. Background note – Session IV.* Warsaw: Polish Presidency of the Council of the European Union, 2025. Disponível em:

https://parleu2025.pl/wp-content/uploads/2025/03/EN_19Mar_Background_note_Session_IV.pdf. Acesso em: 5 jan. 2026.

POLIISI. *Investigations into the gas pipeline damage proceed*. Vantaa: Police of Finland, 2023. Disponível em: https://poliisi.fi/en/-/investigations-into-the-gas-pipeline-damage-proceed?languageId=en_US. Acesso em: 5 jan. 2026.

POLIISI. *National Bureau of Investigation launched investigation into the incident in the Gulf of Finland*. Vantaa: Police of Finland, 2023. Disponível em: https://poliisi.fi/en/-/national-bureau-of-investigation-launched-investigation-into-the-incident-in-the-gulf-of-finland?languageId=en_US. Acesso em: 5 jan. 2026.

PRAKS, Henrik. *Russia's hybrid threat tactics against the Baltic Sea region: from disinformation to sabotage*. Hybrid CoE Working Paper, n. 32. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2024.

QIU, Winston. *Statistics on subsea cable fault and repair*. *Submarine Networks*, 28 jun. 2025. Disponível em: https://www.submarinenetworks.com/en/nv/insights/statistics-on-subsea-cable-fault-and-repair. Acesso em: 5 jan. 2026.

RECORDED FUTURE. *Submarine cables face increasing threats amid geopolitical tensions and limited repair capacity*. Insikt Group Research, 28 maio 2025. Disponível em: https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats. Acesso em: 5 jan. 2026.

REUTERS. Chinese ship linked to Baltic Sea cable breach resumes voyage. *Reuters*, 21 dez. 2024. Disponível em: https://www.reuters.com/world/chinese-ship-linked-baltic-sea-cable-breach-resumes-voyage-2024-12-21/. Acesso em: 5 jan. 2026.

REUTERS. *Recent suspected underwater sabotage incidents in the Baltic Sea*. 5 jan. 2026. Disponível em: https://www.reuters.com/world/europe/recent-suspected-underwater-sabotage-incidents-baltic-sea-2024-12-03/. Acesso em: 5 jan. 2026

RIBEIRO, Anna. *FCC proposes new cybersecurity mandates for submarine cable operators in major rule review, seeks public input*. *Industrial Cyber*, 14 mar. 2025. Disponível em: https://industrialcyber.co/regulation-standards-and-compliance/fcc-proposes-new-cybersecurity-mandates-for-submarine-cable-operators-in-major-rule-review-seeks-public-input/. Acesso em: 5 jan. 2026.

RINGBOM, Henrik. New Threats—Old Rules: Law of the Sea Issues Raised by Suspected Attacks on Submarine Infrastructure in the Baltic Sea. *Ocean Development & International Law*, [S.l.], v. 56, n. 3, p. 390-414, 2025.

RINTAKUMPU, Frida; ARTS, Sophie; ONDRASKOVA, Jana. *Tensions Under the Baltic Sea.* German Marshall Fund of the United States, 10 jan. 2025. Disponível em: https://www.gmfus.org/news/tensions-under-baltic-sea. Acesso em: 7 jan. 2026.

ROSENAU, James; CZEMPIEL, Ernst-Otto (org.). *Governance without government: order and change in world politics*. Cambridge: Cambridge University Press, 1992.

RUYS, Tom; BAMNIOS, Yiannis. *Anchoring Criminal Jurisdiction at Sea: The Helsinki District Court's Eagle S Judgement and its impact for the protection of submarine cables and pipelines*. *EJIL: Talk!*, 7 nov. 2025. Disponível em: https://www.ejiltalk.org/anchoring-criminal-jurisdiction-at-sea-the-helsinki-district-courts-eagle-s-judgement-and-its-impact-for-the-protection-of-submarine-cables-and-pipelines/. Acesso em: 5 jan. 2026.

SARI, A. *Protecting maritime infrastructure from hybrid threats: legal options*. Hybrid CoE Research Report, n. 14. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, mar. 2025.

SAVITZ, S.; WINSTON, I. *A Brief Naval Overview of the Baltic Sea Region*. Santa Monica: RAND Corporation, jun. 2024. Disponível em: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA2100/PEA2111-1/RAND_PEA2111-1.pdf. Acesso em: 3 jan. 2026.

SCHMITT, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

SHERMAN, Justin. *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*. Washington, D.C.: Atlantic Council, 2021.

SINGER, P. W.; FRIEDMAN, Allan. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

SOLDI, Giovanni *et al*. *Monitoring of underwater critical infrastructures: the Nord Stream and other recent case studies.* 2023.

SOWDEN-CARVALHO, Bruno; VALENÇA, Marcelo M. *Addressing 'maritime aphasia' in international relations. Contexto Internacional*, Rio de Janeiro, v. 47, n. 2, 2025.

STANDAGE, Tom. *The Victorian Internet: the remarkable story of the telegraph and the nineteenth century's on-line pioneers*. New York: Berkley Books, 1999.

STAROSIELSKI, Nicole. "Warning: do not dig": negotiating the visibility of critical infrastructures. *Journal of Visual Culture*, v. 11, n. 1, p. 38-57, 2012. DOI: https://doi.org/10.1177/1470412911430465.

STEINBERG, Philip E. *The social construction of the ocean*. Cambridge: Cambridge University Press, 2001.

STRACHAN, David R. *Racing to the Bottom: Seabed Warfare Brings Threats, Opportunities*. *Marine Technology Reporter*, [s. l.], v. 65, n. 9, p. 34-37, dez. 2022.

Submarine Cable Map 2024. TeleGeography; Telecom Egypt, [s.l.], 12 abr. 2024. Disponível em: https://submarine-cable-map-2024.telegeography.com. Acesso em: 11 ago. 2025.

Submarine Cable Map 2025. TeleGeography; Telecom Egypt, [s.l.], 20 jan. 2025. Disponível em: https://submarine-cable-map-2025.telegeography.com. Acesso em: 11 ago. 2025.

Submarine cable market outlook 2025 to 2035: advancement. *OpenPR*, 8 maio 2025. Disponível em: https://www.openpr.com/news/4132793/submarine-cable-market-outlook-2025-to-2035-advancement. Acesso em: 11 ago. 2025.

SUBMARINE NETWORKS. *Finnish court dismisses case against Eagle S — Alleged Sabotage of Cables in the Baltic Sea.* Disponível em: https://www.submarinenetworks.com/en/nv/insights/finnish-court-dismisses-case-against-eagle-s. Acesso em: 11 fev. 2026.

SUBMARINE NETWORKS. Submarine cable cuts in Jan–Feb, 2008 in the Persian Gulf and the Mediterranean. 2011. Disponível em: https://www.submarinenetworks.com/en/nv/news/cable-cuts-in-jan-feb-2008. Acesso em: 20 nov. 2025.

Submarine optical fiber cable market research. *Persistence Market Research*, [s.l.], [s.d.]. Disponível em: https://www.persistencemarketresearch.com/market-research/submarine-optical-fiber-cable-market-research.asp. Acesso em: 11 ago. 2025.

SUBTEL FORUM. *Submarine telecoms industry report*. Sterling, VA: Submarine Telecoms Forum, 2023. Disponível em: https://subtelforum.com/submarine-telecoms-industry-report/. Acesso em: 16 jul. 2025.

SUNAK, Rishi. *Undersea cables: indispensable, insecure.* London: Policy Exchange, 2017. Disponivel em: https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf. Acesso em: 28 nov. 2025.

SWISTEK, Göran; PAUL, Michael. *Geopolitics in the Baltic Sea Region*. SWP Comment, n. 2023/C 09, Berlin: Stiftung Wissenschaft und Politik (SWP), fev. 2023. Disponível em: https://www.swp-berlin.org/10.18449/2023C09/. Acesso em: 5 jan. 2026.

TAMMIKKO, Teemu. *The EU and NATO in pursuit of better deterrence: Baltic Sea sabotage prompts rethink of current practices.* Helsinki: Finnish Institute of International Affairs (FIIA), fev. 2025. (Briefing Paper, n. 404). Disponível em: https://fiia.fi/wp-content/uploads/2025/02/BP404_The-EU-and-NATO-in-pursuit-of-better-deterrence.pdf. Acesso em: 1 fev. 2026.

TAN, Pham Van. *The impact of the Flag of Convenience Regime into Shipping Industry. Journal of Maritime Research*, v. 21, n. 3, p. 280-284, 2024.

TRIBUNAL INTERNACIONAL DO DIREITO DO MAR. Advisory Opinion – Request for an Advisory Opinion submitted by the Commission of Small Island States on Climate Change and International Law (Case No. 31), 21 May 2024. *Advisory Opinion*. [S.l.]: ITLOS, 21 May 2024. Disponível em:

https://www.itlos.org/fileadmin/itlos/documents/cases/31/Advisory_Opinion/C31_Adv_Op_21.05.2024_orig.pdf. Acesso em: 29 jan. 2026.

TRIBUNAL INTERNACIONAL DO DIREITO DO MAR. *M/V "Saiga" (No. 2) (Saint Vincent and the Grenadines v. Guinea):* Sentença de 1 julho de 1999. Disponível em: https://www.itlos.org/fileadmin/itlos/documents/cases/case_no_2/published/C2-J-1_Jul_99.pdf. Acesso em: 31 jan. 2026.

UNITED KINGDOM. Parliament. Joint Committee on the National Security Strategy. *Oral evidence: Undersea cables.* Evidence Session No. 3, 19 May 2025. Disponível em: https://committees.parliament.uk/oralevidence/15935/html/. Acesso em: 6 fev. 2026.

UNITED NATIONS GENERAL ASSEMBLY. Oceans and the law of the sea (Resolução 65/37, de 7 dez. 2010). In: *Resoluções da Assembleia Geral adotadas na 65.ª sessão plenária*. Nova Iorque: ONU, 2010. Disponível em: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_65_37.pdf. Acesso em: 17 jul. 2025.

UNITED NATIONS**.** *1958 Geneva Conventions on the Law of the Sea*. Disponível em: https://legal.un.org/avl/pdf/ha/gclos/gclos_e.pdf. Acesso em: 23 dez. 2025.

UNITED NATIONS. *Agreement under the United Nations Convention on the Law of the Sea on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction.* New York: United Nations, 2023.

UNITED NATIONS**.** *UN 'high seas' treaty clears ratification threshold, to enter into force in January*. ONU News, 2025. Disponível em: https://news.un.org/en/story/2025/09/1165901. Acesso em: 2 jan. 2026.

UNITED NATIONS. *United Nations Convention on the Law of the Sea of 10 December 1982: overview and full text*. Disponível em: https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm. Acesso em: 17 jul. 2025.

UNITED STATES. Department of Justice. Office for Victims of Crime. *Responding to terrorism victims: Oklahoma City and beyond*. Washington, DC: Office of Justice Programs, 2000. NCJ 183949.

VAN SOEST, Henri; FINE, Harper; BLACK, James; RETTER, Lucia; WOLFORD, Zsofia. *Undersea cables: evidence submission. Prepared for the Joint Committee on National Security Strategy.* Santa Monica; Cambridge: RAND Corporation, 2025. Disponível em: https://www.rand.org/content/dam/rand/pubs/testimonies/CTA4100/CTA4112-1/RAND_CTA4112-1.pdf. Acesso em: 25 jan. 2026.

WEI, Jiayi; GONG, Wende; XING, Junhui; XU, Haowei. Distributed acoustic sensing technology in marine geosciences. *Intelligent Marine Technology and Systems*, v. 2, art. 26, 2024.

WHITMAN, Michael E.; MATTORD, Herbert J. *Principles of Information Security.* 7. ed. Boston: Cengage Learning, 2021.

YE, Yimin. Global fisheries: current situation and challenges. In: SMITH, Hance D.; SUÁREZ DE VIVERO, Juan Luis; AGARDY, Tundi S. (org.). Routledge Handbook of Ocean Resources and Management. Abingdon: Routledge, 2015. p. 215-231.

Yle. *Suomen ja Viron välisessä kaasuputkessa on reikä – mikään muu syy ei selitä nopeaa paineen laskua*, 2 fev. 2023. Disponível em: https://yle.fi/a/74-20054276. Acesso em: 6 jan. 2026.

YOUDE, Jeremy. High politics, low politics, and global health. *Journal of Global Security Studies*, v. 1, n. 2, p. 157–170, 2016.

ZIOLKOWSKI, K. *Ius ad bellum in cyberspace: some thoughts on the "Schmitt criteria" for use of force*. Tallinn: NATO CCD COE Publications, 2012.

ZÜRN, Michael. *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford: Oxford University Press, 2018.