UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e97783, p. 1-22, 2026 • https://dx.doi.org/10.5902/2357797597783
Submissão: 18/07/2026 • Aprovação: 14/09/2026 • Publicação: 02/10/2026

Artigos Dossiê

Cabos submarinos em Fortaleza: soberania digital e o papel do Exército Brasileiro

Submarine cables in Fortaleza: digital sovereignty and the role of the Brazilian Army

Cileno Ribeiro[I]
Nícolas de Araújo Moreira[II]

[I]Exército Brasileiro, Brasília, DF, Brasil
[II]Universidade Federal do Ceará, Fortaleza, CE, Brasil

Resumo

Fortaleza concentra 17 cabos submarinos de fibra óptica, posicionando-se como o segundo maior hub de conectividade de dados do mundo e respondendo por mais de 90% do fluxo internacional de dados do Brasil. Essa concentração estratégica representa simultaneamente uma vantagem geopolítica e uma vulnerabilidade crítica para a soberania informacional do país. O presente artigo analisa a relevância estratégica dos cabos submarinos que chegam a Fortaleza, identifica lacunas normativas e operacionais na sua proteção, e propõe o emprego de um centro de telemática do Exército Brasileiro sediado na cidade como ator central de resiliência cibernética nesse ecossistema. A pesquisa adota análise documental, revisão bibliográfica e relato de exercício operacional, tendo como marcos normativos o PPSI 2.0 (Portaria SGD/MGI nº 9.511/2025), as recomendações da ICPC e as diretrizes da ITU. Os resultados evidenciam que a proteção efetiva dessas infraestruturas requer abordagem interinstitucional integrada e que a criação de um laboratório de resiliência cibernética constituiria avanço significativo para a resiliência digital nacional.

Palavras-chave: Cabos submarinos; Soberania digital; Resiliência cibernética; Infraestruturas críticas; Fortaleza

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

Fortaleza hosts 17 submarine fiber-optic cables, ranking as the world's second-largest data connectivity hub and accounting for over 90% of Brazil's international data traffic. This strategic concentration represents both a geopolitical advantage and a critical vulnerability to the country's informational sovereignty. This article analyzes the strategic relevance of the submarine cables landing in Fortaleza, identifies normative and operational gaps in their protection, and proposes the deployment of a Brazilian Army telematics center based in the city as a central actor in cyber resilience within this ecosystem. Document analysis, bibliographic review, and operational exercise reporting are used as methodological approaches, grounded in the PPSI 2.0, the ICPC recommendations, and ITU guidelines. Results indicate that effective protection requires an integrated inter-agency approach and that establishing a cyber resilience laboratory would represent a significant advancement in national digital resilience.

Keywords: Submarine cables; Digital sovereignty; Cyber resilience; Critical infrastructure; Fortaleza

1 INTRODUÇÃO

A crescente dependência da economia global em relação às infraestruturas digitais elevou os cabos submarinos de fibra óptica à condição de ativos estratégicos de soberania nacional. Responsáveis por mais de 95% do tráfego internacional de dados em todo o mundo, esses sistemas interligam continentes e sustentam operações financeiras, diplomáticas, governamentais e militares em escala planetária. Apesar dessa relevância, parcela significativa da população desconhece a existência e o funcionamento dos backbones e do tráfego de dados que circulam pelo mundo por meio de cabos de fibra óptica e linhas de alta capacidade que interligam a internet mundial à rede urbana brasileira (POLESI, 2020, p. 17).

No Brasil, essa realidade adquire contornos singulares em Fortaleza, capital do Estado do Ceará. A cidade abriga 17 cabos submarinos e concentra mais de 90% do fluxo internacional de dados do país, segundo a Agência Nacional de Telecomunicações (ANATEL) (ANATEL, 2024). Sua posição geográfica privilegiada — a capital brasileira mais próxima da Europa, da América do Norte e Central, e do norte da África — transformou-a no segundo maior hub de conectividade de dados do mundo, superada apenas pela cidade japonesa de Shima (SUBMARINE CABLE MAP, 2025).

Esse protagonismo, no entanto, cria uma assimetria crítica: a concentração de infraestrutura estratégica em um único ponto amplia exponencialmente os impactos de qualquer incidente físico, lógico ou ambiental. A crescente atenção de atores estatais e não estatais a essa tipologia de infraestrutura — evidenciada por sabotagens documentadas no Mar Báltico e no Mar Vermelho (OTAN, 2024; LILLY, 2022) — confere urgência à discussão sobre os mecanismos de proteção disponíveis no Brasil.

É nesse contexto que se insere o papel de um centro de telemática do Exército Brasileiro sediado em Fortaleza. Subordinado à cadeia de comando de telemática da Força, esse centro reúne capacidade técnica, localização estratégica e alinhamento institucional para contribuir com a resiliência cibernética das infraestruturas de conectividade ali concentradas.

O presente artigo tem como objetivo analisar a relevância estratégica dos cabos submarinos em Fortaleza para a Segurança Nacional, mapear as lacunas normativas e operacionais existentes, e propor linhas de emprego institucional para a resiliência cibernética dessas infraestruturas. A pesquisa fundamenta-se em análise documental, revisão bibliográfica e relato da Operação Tridente — exercício interagências realizado em novembro de 2025 —, tendo como marco normativo o PPSI 2.0, as recomendações da ICPC e as diretrizes da ITU.

2 METODOLOGIA

Este estudo adota abordagem qualitativa com delineamento exploratório e descritivo. O corpus de análise é composto por: (a) documentos normativos nacionais e internacionais relativos à segurança de infraestruturas críticas e cabos submarinos; (b) literatura científica especializada sobre vulnerabilidades de cabos submarinos e resiliência cibernética; e (c) documentação institucional e relatos da Operação Tridente, exercício interagências realizado no litoral cearense em novembro de 2025.

A análise documental seguiu protocolo sistemático de leitura, categorização e síntese, orientado pelas dimensões: (i) contexto estratégico de Fortaleza para a Segurança Nacional; (ii) marco normativo aplicável; (iii) lacunas identificadas; e (iv) propostas de emprego institucional. O referencial teórico articula conceitos de soberania digital, resiliência de infraestruturas críticas e Poder Nacional.

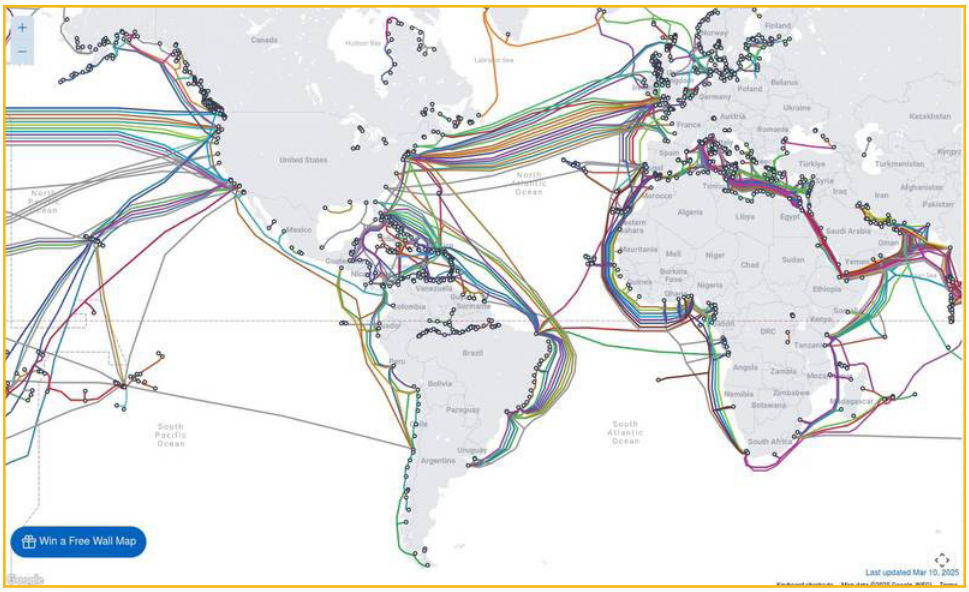
3 CONTEXTUALIZAÇÃO ESTRATÉGICA DOS CABOS SUBMARINOS EM FORTALEZA

Esta seção contextualiza a posição estratégica de Fortaleza no ecossistema global de conectividade submarina. São apresentados o estado atual dos cabos que chegam à cidade, sua qualificação como infraestrutura crítica de interesse da Segurança Nacional e o relato da Operação Tridente, exercício interagências de novembro de 2025 que evidenciou as capacidades e lacunas na proteção dessas infraestruturas.

3.1 Situação atual dos cabos submarinos

Fortaleza é atualmente o segundo maior hub de conectividade de dados do mundo, contando com 17 cabos submarinos de fibra óptica (Figura 1) (ANATEL, 2024). Segundo a ANATEL (2024), mais de 90% dos dados de comunicação internacional do Brasil passam pela capital cearense antes de serem distribuídos para outras regiões. A conectividade submarina de Fortaleza remonta ao ano 2000, com expansão significativa a partir de 2014, quando os primeiros nove cabos instalados na Praia do Futuro foram complementados por outros oito sistemas.

Figura 1 – Ligações de cabos submarinos partindo de Fortaleza



Fonte: Adaptado de Submarine Cable Map. Disponível em: https://www.submarinecablemap.com. Acesso em: 9 dez. 2025.

Entre as empresas proprietárias de cabos que chegam a Fortaleza destacam-se Angola Cables, V.Tal, AT&T, Altice Portugal, CANTV, Embratel, Liberty Latin America (LLA), Lumen, Orange, Sparkle, T-Mobile, Tata Communications, Verizon, Cirion Technologies, Telxius, America Móvil (Claro), EllaLink, Algar Telecom, Antel Uruguay, Google e China Unicom/Camtel. A Angola Cables tem em andamento a construção de um novo data center na Praia do Futuro (Figura 2 e Figura 3), com conclusão prevista para o primeiro semestre de 2026.

Figura 2 – Lançamento de cabo submarino na Praia do Futuro, em Fortaleza



Fonte: Diário do Nordeste. Disponível em: https://diariodonordeste.verdesmares.com.br. Acesso em: 9 dez. 2025.

Figura 3 – Novo Data Center da empresa Angola Cables, na Praia do Futuro



Fonte: Techcom News. Disponível em: https://www.techcomnews.net.br. Acesso em: 9 dez. 2025.

3.2 Cabos submarinos como infraestruturas críticas de interesse da Segurança Nacional

A ANATEL (2020) define Infraestrutura Crítica como as instalações, serviços e bens que, se interrompidos ou destruídos, provocariam sério impacto social, econômico, político, internacional ou à segurança nacional. Os cabos submarinos (Figura 4) enquadram-se diretamente nessa definição e integram o conjunto de ativos estratégicos do Poder Nacional. A regulação específica é estabelecida pelo Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução ANATEL nº 740/2020, que criou o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber).

Figura 4 – Exemplo de cabo submarino no fundo do oceano



Fonte: ANATEL. Disponível em: https://www.gov.br/anatel. Acesso em: 9 dez. 2025.

O lançamento de cabos em Águas Jurisdicionais Brasileiras submete-se à NORMAM-11/DPC, enquanto o licenciamento ambiental compete ao IBAMA e a regularização fundiária à Secretaria do Patrimônio da União (SPU). Essa multiplicidade de instâncias regulatórias representa um dos principais desafios para a governança integrada dessas infraestruturas.

3.3 Operação Tridente (novembro de 2025)

Em novembro de 2025, foi realizada a Operação Tridente, exercício interagências que simulou cenários de ameaça e resposta a incidentes envolvendo cabos submarinos no litoral cearense. A iniciativa teve origem no Workshop sobre Proteção de Cabos Submarinos de 2024, que evidenciou a necessidade urgente de capacidades operacionais específicas para a proteção dessas infraestruturas.

O exercício, realizado entre os dias 10 e 14 de novembro de 2025 (Figura 5), mobilizou 385 militares e 23 meios navais, incluindo o Navio de Socorro Submarino Guillobel (K120), o Submarino Humaitá (S41) (Figura 6) e o helicóptero SH-16 Seahawk. Participaram o GSI/PR, a ABIN, a Polícia Federal, a ANATEL e empresas privadas do setor. O Exército Brasileiro esteve presente no briefing inicial, por meio de representante de comando regional e de comitiva técnica de telemática.

Figura 5 – Briefing da Operação Tridente, Fortaleza, novembro de 2025



Fonte: Marinha do Brasil (2025)

Figura 6 – Navio de Socorro Submarino Guillobel (K120) e Submarino Humaitá (S41)



Fonte: Marinha do Brasil (2025)

O exercício consolidou um modelo interagências de segurança e resiliência tecnológica. O comandante do Terceiro Distrito Naval sintetizou o propósito ao declarar que o compartilhamento de dados entre instituições e empresas é essencial, pois o objetivo final é proteger os cabos submarinos e contribuir para a soberania do país (MARINHA DO BRASIL, 2025).

4 POTENCIALIDADES ESTRATÉGICAS DO ECOSSISTEMA DE FORTALEZA

Além do hub óptico, Fortaleza e o Estado do Ceará concentram ativos estratégicos que ampliam sua relevância para a Segurança Nacional. No campo educacional e científico, destaca-se a construção do novo campus do Instituto Tecnológico de Aeronáutica (ITA) na Base Aérea de Fortaleza (BAFZ) (Figura 7), inaugurado em maio de 2026 — primeira expansão do ITA fora de São José dos Campos.

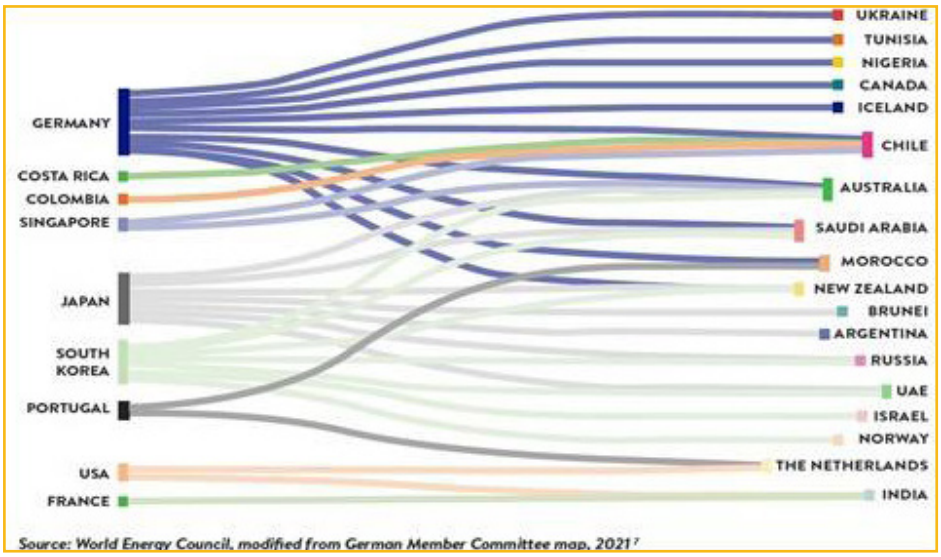
Figura 7 – Obras do novo campus do ITA em Fortaleza



Fonte: Força Aérea Brasileira (2025)

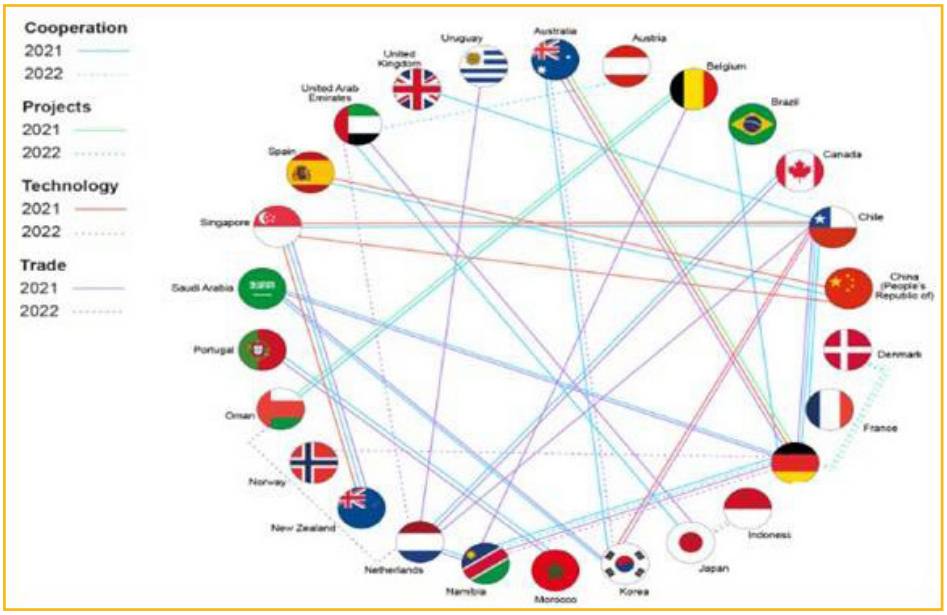
No campo energético, o Ceará desponta como polo de hidrogênio verde (H2V), com acordos firmados com parceiros europeus — especialmente Alemanha e Países Baixos (Figura 8 e Figura 9) — no âmbito do Corredor de Hidrogênio Verde Pecém-Roterdã. Em 2025, novo acordo com o porto de Rostock ampliou o acesso aos mercados do Mar Báltico. Além do polo de hidrogênio verde, o Complexo do Pecém já abriga a Companhia Siderúrgica do Pecém (CSP), controlada pelo grupo sul-coreano POSCO, consolidando a Zona de Processamento de Exportação (ZPE) do Ceará como um dos mais relevantes polos industriais da América do Sul, com sinergias estratégicas diretas para a Segurança Nacional.

Figura 8 – Cooperação internacional no mercado do hidrogênio



Fonte: World Energy Council (2021)

Figura 9 – Acordos de cooperação em economias para o H2



Fonte: Agência Internacional de Energia (2022)

No campo da infraestrutura de dados, o Complexo do Pecém está sendo estruturado para abrigar um mega data center com investimento inicial de R$ 50 bilhões (Figura 11), operando 100% em energia renovável (Figura 10), voltado a atrair empresas como Amazon, Google, Meta, Microsoft e TikTok (MOVIMENTO ECONÔMICO, 2025). O projeto inclui duas novas rotas de fibra óptica conectando o Porto do Pecém às estações de aterragem de cabos submarinos em Fortaleza.

Figura 10 – Cápsula de armazenamento de hidrogênio no Complexo do Pecém



Fonte: Complexo do Pecém(2024)

Figura 11 – Projeto do mega data center no complexo do Pecém



Fonte: Infomoney (2024)

Esse conjunto de ativos configura um ambiente de alta densidade estratégica, que amplia tanto as oportunidades quanto as responsabilidades de proteção por parte das instituições presentes, em especial no que se refere à Segurança Nacional e ao Poder Nacional.

5 LACUNAS NORMATIVAS E RECOMENDAÇÕES TÉCNICAS

Esta seção analisa o marco normativo nacional e internacional aplicável à proteção de cabos submarinos, identifica as principais lacunas operacionais existentes e apresenta recomendações técnicas para sua superação.

5.1 Marco normativo de referência

O Programa de Privacidade e Segurança da Informação 2.0 (PPSI 2.0), instituído pela Portaria SGD/MGI nº 9.511/2025, estabelece controles detalhados para governança, gestão de ativos, continuidade e resposta a incidentes no âmbito da Administração Pública Federal. Os controles diretamente aplicáveis ao domínio de cabos submarinos incluem inventário de ativos, gestão de infraestrutura de rede, monitoramento e resiliência de rede, gestão de fornecedores e resposta a incidentes.

No plano internacional, destacam-se as recomendações da ITU sobre sistemas de fibras submarinas e cabos SMART, as orientações da International Cable Protection Committee (ICPC) e o Action Plan da União Europeia sobre segurança de cabos. Esses documentos tratam de aspectos físicos e operacionais como mapeamento de traçado, zonas de proteção, procedimentos de notificação a navegantes e gestão de reparos.

5.2 Lacunas identificadas e recomendações

A análise dos marcos normativos existentes revela cinco lacunas prioritárias para a proteção dos cabos submarinos em Fortaleza, com implicações diretas para a Segurança Nacional.

A primeira lacuna refere-se à ausência de um inventário geográfico integrado.

Recomenda-se a criação de inventário com coordenadas de lançamento, profundidade, pontos de aterragem e metadados de propriedade, em formato compatível com os padrões IHO/ICPC.

A segunda lacuna diz respeito à limitação dos mecanismos de monitoramento físico. Propõe-se a integração de telemetria de integridade com sensores SMART — capazes de detectar pressão, ruptura e anomalias de atenuação ótica — conectados a um centro de operações de segurança e de rede dedicado.

A terceira lacuna concerne à ausência de cláusulas contratuais específicas nos acordos com operadoras privadas. Recomenda-se a inserção de requisitos de SLA de reparo, obrigação de notificação imediata e planos de contingência, em alinhamento com o PPSI 2.0.

A quarta lacuna é a inexistência de governança interinstitucional formalizada. Propõe-se a celebração de Acordos de Cooperação (MoUs) entre as instituições responsáveis pela defesa cibernética, a ANATEL, a Polícia Federal, a ABIN e as operadoras, com a criação de um playbook nacional para incidentes envolvendo cabos submarinos.

A quinta lacuna envolve a ausência de exercícios conjuntos periódicos. Recomenda-se a realização sistemática de exercícios de mesa e simulações de desconexão e restauração, com resultados incorporados aos planos de continuidade exigidos pelo PPSI 2.0.

6 PROPOSTA DE EMPREGO INSTITUCIONAL E DO LABORATÓRIO DE RESILIÊNCIA CIBERNÉTICA

Esta seção apresenta as propostas de emprego institucional de um centro de telemática do Exército Brasileiro como ator de resiliência cibernética em Fortaleza. São descritas a inserção do Exército Brasileiro no ecossistema estratégico local, a proposta de um laboratório de resiliência cibernética e o papel de governança exercido pela cadeia hierárquica que sustenta essas iniciativas.

6.1 Inserção do Exército Brasileiro no ecossistema estratégico de Fortaleza

A Operação Tridente de 2025 demonstrou que a proteção dos cabos submarinos demanda a atuação coordenada de múltiplos atores — Forças Armadas, órgãos reguladores, agências de inteligência e empresas privadas. A Força Aérea Brasileira contribui com o apoio à instalação do novo campus do ITA. O questionamento que se impõe é como o Exército Brasileiro pode ampliar sua contribuição nesse ecossistema estratégico, especialmente no campo da resiliência cibernética.

A resposta emerge das atribuições constitucionais do Exército e das competências específicas de seus centros de telemática regionais. Em complemento às ações já desenvolvidas por outras instituições, o Exército Brasileiro pode assumir papel relevante: monitoramento contínuo, análise de vulnerabilidades, resposta a incidentes e continuidade de serviços essenciais para o Poder Nacional.

Essa atuação fortalece a interoperabilidade entre as Forças Armadas e demais instituições, permitindo o alinhamento de protocolos e a consolidação de uma abordagem integrada de resiliência e resposta a incidentes, em linha com as melhores práticas do NATO CCDCOE e com a Doutrina Militar de Defesa Cibernética do Ministério da Defesa. O contexto internacional reforça a urgência dessa atuação: em maio de 2023, o Secretário-Geral da OTAN destacou que os cabos submarinos transportam cerca de US$ 10 trilhões em transferências diariamente e que aproximadamente 95% do fluxo global de dados trafega por esses sistemas, alertando para a necessidade de cooperação entre governos e setor privado para sua proteção (OTAN, 2023). Em fevereiro de 2024, os Ministros da Defesa da OTAN decidiram criar a Critical Undersea Infrastructure Network, cuja primeira reunião ocorreu em maio de 2024, reunindo especialistas para discutir compartilhamento de informações, consciência situacional e uso de tecnologias inovadoras — como drones submarinos, novos sensores e inteligência artificial — para detecção de atividades suspeitas (OTAN, 2024). A Aliança estabeleceu ainda um Maritime Centre for the Security of Critical Undersea Infrastructure, sediado no Comando Marítimo da OTAN (MARCOM) em Northwood, Reino Unido. Esse modelo de governança multinível — com célula de coordenação, rede especializada e centro marítimo dedicado — oferece referencial concreto para a estruturação do papel do Exército Brasileiro no ecossistema nacional de proteção de infraestruturas submarinas.

6.2 Proposta de Laboratório de Resiliência Cibernética

Um centro de telemática do Exército Brasileiro sediado em Fortaleza apresentou, em nível hierárquico superior, proposta de construção de um Laboratório de Resiliência Cibernética em suas instalações (Figura 12). A estrutura seria empregada em missões que envolvam militares especializados em resiliência cibernética, voltados ao monitoramento, à continuidade operacional e à proteção de infraestruturas críticas, incluindo o fluxo informacional dos cabos submarinos.

Figura 12 – Sugestão de construção de um Laboratório de Resiliência Cibernética junto a um centro de telemática do Exército Brasileiro



Fonte: Autores (2025)

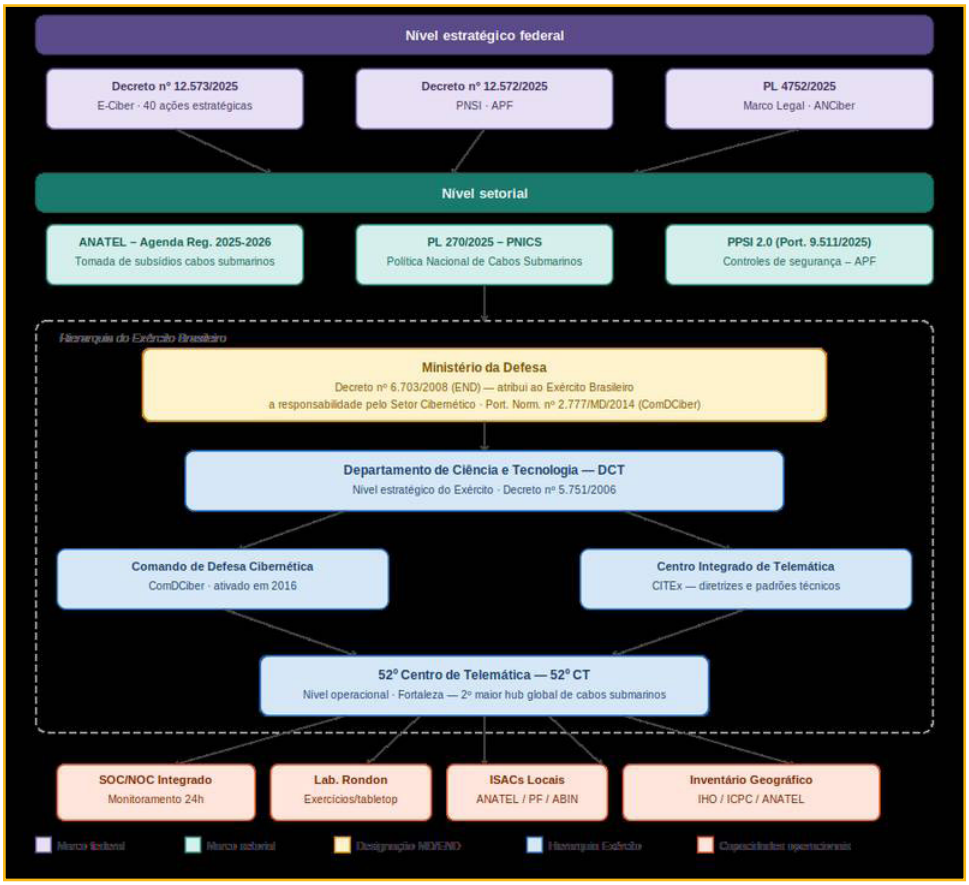
A proposição está fundamentada nas diretrizes do Comando de Defesa Cibernética (ComDCiber) e alinhada ao PPSI 2.0. O laboratório viabilizaria exercícios de integração com o ComDCiber, cenários tabletop com degradação de backbone internacional e simulações envolvendo a Polícia Federal, a ANATEL, a ABIN e os operadores das estações de aterragem (“landing stations”).

6.3 Governança vertical na cadeia de telemática do Exército

O órgão central do Sistema de Telemática do Exército exerce função essencial na governança técnica dos centros regionais, definindo diretrizes, padrões e critérios de interoperabilidade. Viabiliza a integração vertical entre o nível estratégico (ComDCiber), o nível gerencial técnico e o nível operacional, promovendo continuidade institucional e otimização dos fluxos informacionais de resiliência cibernética de interesse da Segurança Nacional.

A Figura 13 sintetiza o posicionamento institucional desse centro de telemática no ecossistema normativo e hierárquico da defesa cibernética brasileira, evidenciando os instrumentos legislativos que fundamentam sua atuação e a cadeia de comando que vai do Ministério da Defesa ao nível operacional em Fortaleza.

Figura 13 – Posicionamento institucional de um centro de telemática do Exército Brasileiro no ecossistema normativo e hierárquico da defesa cibernética brasileira



Fonte: Autores (2025)

7 CONSIDERAÇÕES FINAIS

Os cabos submarinos que chegam a Fortaleza constituem uma das mais relevantes infraestruturas críticas de comunicação do Brasil e um ativo estratégico de primeira grandeza para o Poder Nacional. Sua concentração em um único município — responsável por mais de 90% do fluxo internacional de dados do país — cria uma assimetria estratégica que exige resposta institucional coordenada, permanente e tecnicamente qualificada. Essa realidade se insere em um contexto normativo em plena maturação: a Estratégia Nacional de Defesa (END), instituída pelo Decreto nº 6.703/2008 e reafirmada em suas edições subsequentes, reconheceu o setor cibernético como um dos três setores estratégicos da Defesa Nacional e atribuiu ao Exército Brasileiro a responsabilidade por sua condução, sob coordenação do Ministério da Defesa.

Este artigo demonstrou que as lacunas existentes na proteção dessas infraestruturas são de natureza tanto normativa quanto operacional, e que sua superação requer a articulação entre Forças Armadas, órgãos reguladores, agências de inteligência e operadoras privadas. A Operação Tridente de 2025 representou avanço significativo nessa direção, mas evidenciou também a necessidade de protocolos permanentes, exercícios periódicos e estruturas dedicadas. Esse cenário é reforçado pelo novo arcabouço normativo federal: os Decretos nº 12.572 e 12.573/2025 instituíram, respectivamente, a Política Nacional de Segurança da Informação (PNSI) e a nova Estratégia Nacional de Cibersegurança (E-Ciber), com cerca de quarenta ações estratégicas voltadas à proteção de infraestruturas críticas, certificação de operadores e criação de mecanismos de compartilhamento de incidentes. No plano legislativo, o PL 4752/2025 — aprovado pela CCJ do Senado em dezembro de 2025 — avança na criação da Autoridade Nacional de Cibersegurança (ANCiber), enquanto o PL 270/2025 institui a Política Nacional de Infraestruturas de Cabos Submarinos (PNICS), em tramitação na Comissão de Relações Exteriores e Defesa Nacional da Câmara. Paralelamente, a ANATEL abriu, em 2026, tomada de subsídios para atualização do marco regulatório específico sobre cabos submarinos, no âmbito de sua Agenda Regulatória 2025-2026.

Um centro de telemática do Exército Brasileiro sediado em Fortaleza, por sua localização privilegiada e sua missão institucional em telemática e resiliência cibernética, apresenta-se como ator relevante nesse ecossistema. Sua atuação se insere na cadeia hierárquica do Exército Brasileiro, em alinhamento com as diretrizes do Comando de Defesa Cibernética (ComDCiber) — ativado em 2016 pela Portaria Normativa nº 2.777/MD e responsável pela coordenação das atividades de defesa cibernética no âmbito do Ministério da Defesa. A proposta de um Laboratório de Resiliência Cibernética representa passo concreto para dotar o Exército Brasileiro de capacidade operacional compatível com a relevância estratégica de Fortaleza no cenário global de conectividade e Segurança Nacional.

Como agenda de pesquisa futura, identificam-se quatro frentes prioritárias: (a) o acompanhamento e contribuição ao processo de elaboração do marco jurídico específico para cabos submarinos, com ênfase na participação do Exército Brasileiro na tomada de subsídios da ANATEL e nas discussões do PL 270/2025 na Comissão de Relações Exteriores e Defesa Nacional; (b) a avaliação técnica dos requisitos de um centro integrado de monitoramento em tempo real para as estações de aterragem de Fortaleza, em consonância com os controles do PPSI 2.0 e com as futuras exigências da ANCiber; (c) a investigação comparada de modelos internacionais de governança interinstitucional — em especial os adotados pelo NATO CCDCOE e pela União Europeia no âmbito de seu Action Plan sobre cabos submarinos —, com vistas à identificação de boas práticas adaptáveis ao contexto brasileiro; e (d) a análise do posicionamento institucional do Exército Brasileiro no Sistema Nacional de Cibersegurança a ser estruturado pela ANCiber, avaliando as condições para que o laboratório proposto seja reconhecido como referência para infraestruturas críticas de telecomunicações no âmbito do Setor Cibernético da Defesa Nacional.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Desafios da Inteligência 2026**. Brasília: ABIN, 2026. Disponível em: https://www.gov.br/abin/pt-br/sem-logo-de-gov_abin_desafios_2026.pdf. Acesso em: 10 maio 2026.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Resolução nº 740, de 21 de dezembro de 2020**. Brasília: ANATEL, 2020.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Cabos submarinos. Brasília**: ANATEL, 2024. Disponível em: https://www.gov.br/anatel/pt-br/dados/infraestrutura/cabos-submarinos. Acesso em: 9 dez. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001:2023** — Tecnologia da Informação — Segurança da Informação — Sistemas de Gestão. Rio de Janeiro: ABNT, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002:2023** — Tecnologia da Informação — Segurança da Informação — Controles de Segurança. Rio de Janeiro: ABNT, 2023.

BRASIL. **Comando de Defesa Cibernética (ComDCiber)**. Diretrizes Operacionais para a Defesa Cibernética. Brasília, 2023.

BRASIL. **Decreto nº 5.751, de 12 de abril de 2006**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Ministério do Exército. Diário Oficial da União: Brasília, DF, 2006.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa. Diário Oficial da União: Brasília, DF, 2008.

BRASIL. **Decreto nº 12.572, de 4 de agosto de 2025**. Institui a Política Nacional de Segurança da Informação (PNSI). Diário Oficial da União: Brasília, DF, 2025.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. **Institui a Estratégia Nacional de Cibersegurança (E-Ciber)**. Diário Oficial da União: Brasília, DF, 2025.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, 2022.

BRASIL. Ministério da Defesa. **Portaria Normativa nº 2.777/MD, de 26 de novembro de 2014**. Cria o Comando de Defesa Cibernética (ComDCiber) e estabelece suas competências no âmbito do Setor Cibernético da Defesa Nacional. Brasília: MD, 2014.

BRASIL. Ministério da Gestão e da Inovação. **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025**. Institui o Programa de Privacidade e Segurança da Informação 2.0. Diário Oficial da União: seção 1, Brasília, DF, 28 out. 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-9.511-de-28-de-outubro-de-2025-665815455. Acesso em: 30 nov. 2025.

BRASIL. Secretaria de Governo Digital. **PPSI 2.0 — Guia do Framework**. Versão 1.0. Brasília: MGI, 2025. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-0-22nov2025.pdf. Acesso em: 30 nov. 2025.

CÂMARA DOS DEPUTADOS. **Proposta de Política Nacional de Infraestruturas de Cabos Submarinos (PL nº 270/2025)**. Brasília, 2025.

CARTER, L. et al. Submarine cables and marine cyber-risk: a critical infrastructure threat. **Journal of Cyber Policy**, London, 2021.

INTERNATIONAL CABLE PROTECTION COMMITTEE (ICPC). **Best Practices for the Protection of Submarine Cable Systems**. ICPC, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27005:2018** — Information Security Risk Management. Geneva: ISO, 2018.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Recommendations on Submarine Cable Systems**. Geneva: ITU, 2023.

LILLY, J. **Russia's sovereign internet tests**: implications for global internet fragmentation. Washington, DC: Center for Strategic and International Studies, 2022.

MARINHA DO BRASIL. Exer**cício inédito da Marinha garante manutenção de cabos submarinos**. Agência Marinha de Notícias, nov. 2025. Disponível em: https://www.agencia.marinha.mil.br/defesa-naval/exercicio-inedito-da-marinha-garante-manutencao-de-cabos-submarinos. Acesso em: 20 nov. 2025.

MARINHA DO BRASIL. **Fundamentos Doutrinários da Marinha**. 1. ed. Brasília: Estado-Maior da Armada, 2023.

MARINHA DO BRASIL. **Operação Tridente**: Brasil reforça proteção de cabos submarinos em exercício inédito em Fortaleza (CE). Agência Marinha de Notícias, nov. 2025. Disponível em: https://www.agencia.marinha.mil.br/defesa-naval/brasil-reforca-protecao-de-cabos-submarinos-em-exercicio-inedito-em-fortaleza-ce. Acesso em: 20 nov. 2025.

MARINHA DO BRASIL. **Plano Estratégico da Marinha 2040**. Brasília: MB, 2020.

MARINHA DO BRASIL. **Política Naval**. Brasília: MB, [s.d.].

MOVIMENTO ECONÔMICO. **E se Fortaleza falhar?** Governo quer espalhar os cabos submarinos do Brasil. 2025. Disponível em: https://movimentoeconomico.com.br/tecnologia/2025/05/14/e-se-fortaleza-falhar-governo-quer-espalhar-os-cabos-submarinos-do-brasil. Acesso em: 20 maio 2025.

NEVES, Tiago Duarte. **Infraestruturas críticas e ameaças cibernéticas: uma análise da cibersegurança dos cabos submarinos brasileiros**. 2024. Disponível em: https://repositorio.esg.br/handle/123456789/1979. Acesso em: 20 maio 2026.

NIC.br. **Indicadores de conectividade internacional do Brasil**. São Paulo: NIC.br, 2024.

NORTH ATLANTIC TREATY ORGANIZATION (OTAN). **NATO holds first meeting of Critical Undersea Infrastructure Network**. NATO News, 23 maio 2024. Disponível em: https://www.nato.int/en/news-and-events/articles/news/2024/05/23/nato-holds-first-meeting-of-critical-undersea-infrastructure-network. Acesso em: 20 maio 2026.

NORTH ATLANTIC TREATY ORGANIZATION (OTAN). **NATO Maritime Activities**. Disponível em: https://www.nato.int/en/what-we-do/operations-and-missions/natos-maritime-activities. Acesso em: 20 maio 2026.

NORTH ATLANTIC TREATY ORGANIZATION (OTAN). **NATO Secretary General engages industry on critical undersea infrastructure**. NATO News, 5 maio 2023. Disponível em: https://www.nato.int/en/news-and-events/articles/news/2023/05/05/nato-secretary-general-engages-industry-on-critical-undersea-infrastructure. Acesso em: 20 maio 2026.

POLESI, Felipe Hansen. **A existência das fronteiras cibernéticas e sua segurança no âmbito nacional**. Trabalho de Conclusão de Curso (Graduação) — Academia Militar das Agulhas Negras, Resende, 2020.

RODRIGUEZ FILHO, Ernesto Serrano; PORCHÉRA, Pablo Moreira. **Infraestruturas críticas de comunicaçõe**s: uma análise sobre cabos submarinos no Brasil. 2023. Disponível em: https://repositorio.esg.br/handle/123456789/1763. Acesso em: 20 maio 2026.

RYAN, J. **A critical analysis of global undersea cable vulnerabilities**. Naval War College Review, Rhode Island, 2020.

SOUTER, G. **Submarine cables and the oceans — connecting the world**. Cambridge: UNEP-WCMC, 2009.

SUBMARINE CABLE MAP. **Mapa global de cabos submarinos**. Disponível em: https://www.submarinecablemap.com. Acesso em: 9 dez. 2025.

TELESÍNTESE. **No Brasil, maior risco aos cabos submarinos está em terra**. 2025. Disponível em: https://telesintese.com.br/no-brasil-maior-risco-aos-cabos-submarinos-esta-em-terra. Acesso em: 10 maio 2025.

THE ECONOMIST. **Undersea cables**: the weak link of the internet. 2024. Disponível em: https://www.economist.com. Acesso em: 15 jan. 2025.

ZÚÑIGA, Luis Olavo Athayde; FONSECA, Ricardo Magno Teixeira. **Cabos submarinos de comunicação à luz da governança de Segurança, Desenvolvimento e Defesa Nacional**. 2024. Disponível em: https://repositorio.esg.br/handle/123456789/2086. Acesso em: 20 maio 2026.

Autoria

1 Cileno Ribeiro

Formação militar na área de Comunicações pela Academia Militar das Agulhas Negras; Especialista em Telecomunicações e Guerra Eletrônica; Mestre em Operações Militares pela Escola de Aperfeiçoamento de Oficiais; Mestre em Engenharia Elétrica com concentração em Segurança Cibernética pela Universidade de Brasília; Oficial
https://orcid.org/0000-0002-9329-1243 • cilenomag@gmail.com

2 Nícolas de Araújo Moreira

Graduado em Engenharia Elétrica pela Universidade Federal do Ceará; Mestre em Engenharia de Teleinformática pela Universidade Federal do Ceará; Doutor em Eletrônica, Microeletrônica, Óptica e Lasers, Optoeletrônica, Microondas e Robótica pela Université de Lille; Professor
https://orcid.org/0000-0001-8340-4382 • nicolas@ufc.br

Como citar este artigo

RIBEIRO, C.; MOREIRA, N. A. Cabos submarinos em Fortaleza: soberania digital e o papel do Exército Brasileiro. **InterAção**, Santa Maria, v. 17, n. 3, e97783, p. 1-22, 2026. DOI 10.5902/2357797597783. Disponível em: https://dx.doi.org/10.5902/2357797597783. Acesso em: dia mês abreviado. ano.