DOI 10.21544/1809-3191.v26n2.p326-346

# A DEFESA DA INFRAESTRUTURA DE CABOS SUBMARINOS: POR UMA INTERFACE ENTRE A DEFESA CIBERNÉTICA E A SEGURANÇA MARÍTIMA NO BRASIL

Leonardo Perin Vichi[1]
Danielle Jacon Ayres Pinto[2]
André Luiz Nery de Sá[3]

**RESUMO**

O presente trabalho tem por objetivo analisar a importância de se pensar em políticas de segurança para a infraestrutura de cabos submarinos utilizada pelo Brasil, tendo em vista que nessa tecnologia reside grande parte da capacidade de comunicação do país com outros atores globais, formando um extenso hub, cuja relevância se protrai, em especial, para todas as cadeias econômicas, sociais e políticas nacionais. Foram analisados a dimensão do uso dos cabos submarinos no Brasil, o quantitativo de empresas que operam essas infraestruturas no país e os tipos de ameaças capazes de causar danos aos cabos submarinos. Na sequência, foi abordada a necessidade da interação entre as instituições públicas e privadas para o sucesso dos mecanismos da defesa dessa infraestrutura de comunicação. O fato de o fluxo mundial de informações depender dos cabos submarinos, somado à característica multi-domínio do ciberespaço, apontam para a correlação entre defesa cibernética e segurança marítima. A análise indica a necessidade de ampliar os estudos e a discussão sobre o tema no meio acadêmico, nas forças armadas e nas diversas instâncias do governo brasileiro, a fim de assegurar a proteção dessas infraestruturas, garantindo, assim, a integridade, confiabilidade e disponibilidade do fluxo de informação entre o Brasil e o mundo.

**Palavras-chave:** Cabos Submarinos. Infraestruturas Críticas. Defesa Nacional. Segurança Marítima.

[1] Doutor. Universidade Federal de São Carlos (UFScar). São Paulo (SP), Brasil. E-mail: contact@leonardovichi.com / http://orcid.org/0000-0001-7527-8419

[2] Doutora. Universidade Federal de Santa Catarina (UFSC). Santa Catarina (SC), Brasil. Email: djap2222@yahoo.com / http://orcid.org/0000-0001-9539-3844

[3] Mestrando. Escola de Comando e Estado-Maior do Exército (ECEME), Rio de Janeiro (RJ), Brasil. E-mail: andrenery@protonmail.com / http://orcid.org/0000-0001-6265-0103

## INTRODUÇÃO

Em um mundo cada vez mais integrado pela tecnologia, as economias globais dependem das infraestruturas de comunicação para realizar uma parcela substancial da logística necessária à produção de bens de consumo. Um produto comercial contém insumos e peças originárias de dezenas de países, separados em uma cadeia logística de construtores de subcomponentes, montadores de produtos, fornecedores, atacadistas e varejistas. Esses participantes são capazes de se integrar de maneira transparente usando a Internet, permitindo maior especialização e economias de escala em cada etapa do processo de fabricação. Isso propicia o crescimento econômico inclusive para países que não produzem um produto completo por conta própria (CLARK, 2016).

Segundo Farahani (2011), a implementação de sistemas de tecnologias de informação e comunicação pode desempenhar funções na gestão da cadeia de suprimentos e de logística, sendo aplicados à coleta e análise de dados, no apoio à tomada de decisão, no controle e monitoramento das operações da cadeia de suprimentos, e para facilitar a comunicação entre os membros dessa cadeia. Para que haja o correto fluxo de informação entre os diversos atores participantes das cadeias logísticas é necessária uma infraestrutura capaz de atender a toda demanda mundial. Dentre as tecnologias atuais, a única capaz de suportar todo o tráfego de dados é a tecnologia de cabos de fibra ótica submarinos. Como afirma Clark (2016), atualmente, quase todo o tráfego de voz e Internet, incluindo as transmissões militares e financeiras, passa através de cabos submarinos. Desse modo, mesmo danos temporários a essas linhas de comunicação podem ter sérias consequências, razão pela qual sua segurança depende de quão bem as nações resguardam essa tecnologia. O Brasil, como parte das maiores economias mundiais, depende fortemente dessa infraestrutura para manter o fluxo de informação com os demais países, o que significa que as cadeias logísticas das quais o Brasil participa estão diretamente dependentes dos meios físicos de comunicação entre o país e o exterior. Portanto, uma análise sobre o tema se torna de suma importância, em especial no que concerne à defesa nacional, pois, para que a informação seja disseminada de forma íntegra, confiável e com alta disponibilidade, a infraestrutura de comunicação de dados deve estar protegida de ameaças externas. Diante desse panorama, este trabalho analisa a importância de se assegurar a proteção e defesa do fluxo de dados que trafega do Brasil

para o exterior por meio cabos submarinos. Afinal, informação relevante e oportuna é essencial para o desenvolvimento e a operação eficientes de sistemas logísticos (DA SILVA; MUSETTI, 2003).

Considerando a dinâmica variável das novas ameaças que surgem com os avanços tecnológicos, os desafios encontrados pelas instituições responsáveis pela defesa de ativos de informação são cada vez maiores. No que tange aos cabos submarinos, é necessário considerar a questão à luz das limitações impostas pela atual documentação. Enquanto a Estratégia Nacional de Defesa (BRASIL, 2008, p.93) delimita o ciberespaço sob responsabilidade do Exército Brasileiro, é importante considerar a capacidade de esse domínio interpor-se sobre outros domínios e, ao mesmo tempo, ser afetado por eles. Dessa forma, a segurança das comunicações realizadas através das estruturas de cabos submarinos pode ser afetadas tanto por ameaças provindas do ciberespaço, quanto por ameaças vindas do domínio marítimo, já que a interceptação ou a ruptura proposital desses cabos representa uma grande ameaça para as comunicações por esse meio. Esse contexto multi-domínio que caracteriza os cabos submarinos brasileiros dá mostras da importância do desenvolvimento de políticas que visem incrementar a segurança marítima no entorno estratégico do Atlântico, a fim de reduzir a vulnerabilidade das comunicações através dess as infraestruturas.

Outra questão central no debate da defesa dos cabos submarinos é a responsabilidade por sua proteção. Nesse cenário é possível fazer uma leitura dupla, pois, apesar de a defesa das infraestruturas críticas nacionais estar sob a alçada do Estado, a maioria dessas infraestruturas são privadas, sendo que parte do processo de protegê-las está sob responsabilidade de seus detentores. Assim, para determinar o alcance da responsabilidade das Forças Armadas do Brasil na proteção dos cabos submarinos, é essencial determinar qual a diferença entre defesa e segurança cibernética e como isso está diretamente ligado à proteção dessa infraestrutura crítica para a manutenção das comunicações nacionais.

## O FLUXO DA INFORMAÇÃO

Segundo Kress (2002), as redes de informação logística se apresentam como uma grade hierárquica, composta por níveis interconectados de nós de informação. Nos últimos anos, a tendência de uma logística orientada para a velocidade alterou as características da

informação, que deve ser relevante, atualizada e precisa. No que tange à importância para a logística, cabe mencionar Min (2015, p.16, tradução nossa), que afirma: "(...) uma integração bem-sucedida da cadeia de suprimentos depende da capacidade dos parceiros de sincronizar e compartilhar informações em tempo real."[4]

Em complemento, Yoho (2013) expressa a ideia de que os processos de planejamento, programação, controle de estoque, desenho da rede de logística, armazenagem, coordenação, entre outras funções, persistem hoje da mesma forma como eram há 150 anos. O que mudou, contudo, foi a tecnologia, a velocidade e a economia, além de um necessário ajuste na logística, a fim de atender às demandas emergentes, cada vez mais baseada em informações.

A informação pode ser vista como a força vital de um sistema de logística e distribuição. Logo, é importante se desenvolver uma estratégia apropriada para suprir os requisitos de informação (RUSHTON, 2014), uma vez que a informação é considerada como uma peça chave. Em essência, a informação atua como cola nas funções logísticas, mantendo o sistema unido, coordenando todos os componentes das operações logísticas (FARAHANI, 2011). Por outro lado, há de se considerar o relevante fator das comunicações em redes necessitarem de redundância para manutenção de sua estabilidade. A segurança da infraestrutura de comunicação requer que se assegure sua confiabilidade, confidencialidade e disponibilidade. Isso, em tempos de Revolução da Informação, representa um elemento de vantagem, em que a difusão da informação em redes denota que o poder será largamente distribuído de forma rizomática, sem apoiar-se no monopólio das burocracias tradicionais (NYE, 2012). Desse modo, o que caracteriza a revolução tecnológica não é a centralidade do conhecimento e da informação, mas, por outro lado, é a difusão da informação que neutraliza a assimetria do poder, achatando as hierarquias burocráticas e as substituindo por uma rede de organizações (FRANCHI; VICHI, 2019).

A importância da infraestrutura de comunicação como forma de se obter o rápido fluxo da informação pode ser descrita nas palavras do Jomini (2008, p. 219, tradução nossa), ao citar o uso do telégrafo:

> "(...) devo declarar o que deve ser obtido usando um sistema de sinais. Destes, existem vários tipos. Sinais telegráficos podem ser citados como os mais importantes de todos. Napoleão deve o seu espantoso

[4] "(…) successful supply chain integration depends on the supply chain partners' ability to synchronize and share "real-time" information."

> sucesso em Ratisbon, em 1809, pelo fato de ter estabelecido uma comunicação telegráfica entre a sede do exército e a França. Ele ainda estava em Paris quando o exército austríaco atravessou Inn at Braunau com a intenção de invadir a Baviera, e romper sua linha de acantonamentos. Informado em vinte e quatro horas do que se passava a uma distância de setecentas milhas, atirou-se em sua carruagem de viagem e, uma semana depois, obtivera duas vitórias sob as muralhas de Ratisbon. Sem o telégrafo, a campanha teria sido perdida. Este único fato é suficiente para nos impressionar com uma ideia de seu valor. Foi proposto o uso de telégrafos portáteis. Tal arranjo telegráfico, operado por homens a cavalo afixados em terreno elevado, podia comunicar as ordens do centro para as extremidades de uma linha de batalha, bem como os relatórios das asas para a sede."[5]

Como afirma Papilla (2014, p. 136, tradução nossa), "desde que o telégrafo foi introduzido, foi mais fácil obter informações sobre o inimigo. Anteriormente, a inteligência tinha a velocidade de um cavalo correndo, agora ela podia ser enviada por grandes distâncias instantaneamente"[6].

Nesse contexto, o fato de o fluxo de informação ser relevante para o funcionamento das economias globais, fortemente atreladas à capacidade logística de cada país, aponta para a necessidade de se aprofundar em estudos das infraestruturas pelas quais a informação percorre o mundo. As infraestruturas que atualmente exercem o papel preponderante de condutoras do fluxo de informação são os cabos submarinos, constituindo a base da era da informação e da economia moderna Sunak (2017). A partir da percepção de sua importância, podem ser avaliados os riscos

[5] "(…) I must state what is to be gained by using a system of signals. Of these there are several kinds. Telegraphic signals may be mentioned as the most important of all. Napoleon owes his astonishing success at Ratisbon, in 1809, to the fact of his having established a telegraphic communication between the headquarters of the army and France. He was still at Paris when the Austrian army crossed the Inn at Braunau with the intention of invading Bavaria and breaking through his line of cantonments. Informed, in twenty-four hours, of what was passing at a distance of seven hundred miles, he threw himself into his traveling-carriage, and a week later he had gained two victories under the walls of Ratisbon. Without the telegraph, the campaign would have been lost. This single fact is sufficient to impress us with an idea of its value. It has been proposed to use portable telegraphs. Such a telegraphic arrangement, operated by men on horseback posted on high ground, could communicate the orders of the center to the extremities of a line of battle, as well as the reports of the wings to the head-quarters."

[6] "Since the telegraph was introduced it was easier to get information about the enemy. Previously intelligence had a speed of a running horse, now it could be sent over large distances instantly"

que disrupções nessa infraestrutura podem provocar não apenas no setor econômico, mas no âmbito social.

## A INFRAESTRUTURA DE CABOS SUBMARINOS

Na maior parte da história, a informação se restringia a regiões delimitadas. Isso acontecia não pelo fato de faltar ao ser humano o ímpeto de se comunicar com áreas mais distantes, mas pela dificuldade na transmissão da informação por distâncias maiores. Se havia dificuldade na comunicação dentro de uma mesma região, a comunicação imediata entre mares e oceanos, sem depender das lentas navegações, era desejo antigo das nações, mas que residia apenas no campo da imaginação. Um passo decisivo para a quebra dessa dificuldade se deu em 1852, quando o primeiro cabo submarino bem-sucedido entrou em operação, realizando a ligação telegráfica da Inglaterra com França, com a finalidade de conectar as bolsas de valores dos dois países (KOCHER, 2014). O sucesso da empreitada resultou na operação subsequente de diversos outros cabos, inclusive no Brasil, onde em 1854 foi instalada uma linha ligando o Rio de Janeiro a Petrópolis e, em 1873, interligando o país com a Europa. Na década de 1880 já era fato a integração de todas as zonas econômicas do globo por meio de cabos submarinos de telégrafo, ajudando a formar um sistema econômico mundial (KOCHER, 2014).

Desde então, o mundo acompanhou a rápida evolução dessa tecnologia e o crescimento vertiginoso pelo consumo de informação. Carter et al. (2009) afirmam que há um equívoco comum de que maioria das comunicações internacionais são encaminhadas via satélite, enquanto, na verdade, o tráfego é encaminhado por cabos submarinos. A transferência de dados e voz por esses cabos não é apenas mais barata, mas também mais rápida do que via satélite. Segundo Clark (2016), atualmente, pelo menos 95% de todo o tráfego de voz e Internet realiza-se por meio de cabos de fibra ótica ao longo do fundo dos oceanos, incluindo transmissões militares. Como revela Martinage (2015), grande parte da economia global depende dessa infraestrutura. Como exemplo, cita-se a S*ociety for Worldwide Interbank Financial Telecommunication*, responsável por transmitir milhões de transações para mais de oito mil organizações bancárias, instituições de segurança e clientes corporativos em quase duzentos países, conciliando trilhões de dólares em ativos nos mercados financeiros globais. Cadeias globais de fabricação e serviços financeiros somente são possíveis graças

aos cabos submarinos, e mais cabos são instalados a cada ano para atender à crescente demanda (CLARK, 2016).

A quantidade de dados trafegados aumentou de forma significativa. Enquanto em 1993 eram transmitidos pela Internet em torno de 100 terabits de dados ao longo de um ano, em 2015 o valor passou para cerca de 150 terabits por segundo, e o número deverá ultrapassar mil terabits por segundo até 2020 (MARTINAGE, 2015). No início de 2019, 378 cabos submarinos encontravam-se operacionais, interligando os continentes por meio de mais de um milhão de quilômetros, sendo o maior cabo com extensão de vinte mil quilômetros, ligando países asiáticos, e o menor com 131 quilômetros, ligando Irlanda a Grã-Bretanha (TELEGEOGRAPHY, 2019). De acordo com Sunak (2017), os cabos submarinos são responsáveis por garantir, por dia, 15 milhões de transações financeiras, que proporcionam a transferência de 10 trilhões de dólares.

Operadoras de telecomunicações, operadoras móveis, corporações multinacionais, governos, provedores de conteúdo e instituições de pesquisa dependem dos cabos submarinos para enviar dados ao redor do mundo (TELEGEOGRAPHY, 2019). A propriedade de cabos submarinos tradicionalmente sempre foi de empresas privadas de telecomunicações, mas, nos últimos anos, provedores de conteúdo, como Google, Microsoft e Amazon, passaram a investir em novos cabos, de forma a se tornarem independentes das operadoras, diante da perspectiva de crescimento expressivo atual e da necessidade de expansão futura (SEAL, 2019). Sunak (2017) argumenta que, pelo fato de os cabos submarinos pertencerem a empresas privadas, os governos têm papel pouco ativo sobre essa infraestrutura, o que não ocorre em outros setores, como os de energia e transporte. Para o autor, embora os investimentos por parte das empresas privadas desonerem os gastos governamentais, e aumente a resiliência da infraestrutura, as empresas pouco refletem sobre a relevância dos cabos submarinos para a segurança dos países. Além disso, uma vez que a infraestrutura não configura uma propriedade formal dos Estados, não há uma proteção robusta estabelecida no que tange ao direito internacional (SUNAK, 2017). Desse modo, os cabos submarinos atravessam várias jurisdições, sem uma identidade soberana. Eventuais questões derivadas da operação da infraestrutura, como segurança e proteção, ficam sob responsabilidade apenas das empresas privadas (O'MALLEY, 2019).

Além de sua contribuição às economias dos país, Clark (2016) afirma que os países dependem de cabos submarinos para segurança

nacional, como para coordenar operações militares, realizar missões diplomáticas e coletar informações, uma vez que os circuitos de radiofrequência usados pelos satélites de comunicação têm pouca capacidade para atender o volume de dados e para satisfazer as ordens operacionais necessárias para suportar operações militares globais. Desse modo, as comunicações militares compartilham a mesma rede de cabos submarinos, tornando-os suscetíveis à escuta clandestina. De fato, a interceptação de informações é uma preocupação recorrente. Em 2017 a OTAN se tornou apreensiva após perceber um aumento significativo da atividade de submarinos russos em torno dos cabos submarinos no Atlântico Norte (BIRNBAUM, 2017). Embora não esteja claro se a OTAN acredita na capacidade russa de interceptar os dados diretamente dos cabos submarinos, outras preocupações emergem, como a possibilidade de danos intencionais a essa infraestrutura. Uma indisponibilidade da rede de comunicações por conta de sabotagem, por exemplo, poderia dificultar uma resposta militar dos EUA nas primeiras horas de uma guerra (HINCK, 2018), da mesma forma como ocorreu durante a invasão da Criméia em 2014, quando as forças russas tomaram o principal ponto de conexão de Internet da península, isolando a Crimeia da Internet e, consequentemente, do resto do mundo, em um momento chave do conflito (GILES, 2016). Portanto, a capacidade de ameaçar ou proteger cabos submarinos será cada vez mais importante em conflitos futuros (CLARK, 2016), em especial pelo fato de as informações sobre as rotas globais dos cabos estarem disponíveis na Internet, facilitando a identificação dos pontos fracos de um determinado país (MARTINAGE, 2015). Para Sunak (2017) é preocupante o fato de interrupções de cabos submarinos serem possíveis e terem o potencial de gerar consequências negativas para a segurança e prosperidade (SUNAK, 2017).

Segundo Barker (2018), diversas são as formas de ataque a essas infraestruturas. O modo mais básico ocorre com o corte do cabo, uma vez que a estrutura de construção é relativamente simples e o ataque pode ser feito tanto mecanicamente, quanto por meio de pequenas cargas explosivas. Portanto, múltiplos ataques, particularmente em rotas de cabo alternativas, intensificariam rapidamente o problema, causando indisponibilidades de conexão em grandes regiões. A mesma fragilidade acontece nas estações de aterragem, onde os cabos submarinos encontram a terra. Tais locais são amplamente conhecidos e pouco protegidos, o que representa desafios adicionais na defesa da infraestrutura. Kono (2019)

afirma que nesses pontos os cabos são mais acessíveis, sem a exigência de equipamento especializado, com submarinos ou mergulhadores, de modo que podem ser alvo de ações terroristas. Além disso, são possíveis ataques cibernéticos aos elementos que compõe a infraestrutura, composta de equipamentos elétricos e dispositivos de rede (O'MALLEY, 2019).

O fato de existirem milhares de veículos submarinos, operados de forma semiautomática ou remotamente, é um fator preocupante. Um grupo terrorista bem financiado poderia direcionar esforços para sabotar os principais cabos e pontos de junção, criando uma perturbação generalizada nos mercados mundiais e interrompendo os sistemas militares de comando e controle. Do mesmo modo, atores estatais e não-estatais poderiam realizar ataques anônimos, ou agir com falsa bandeira, o que dificultaria a atribuição de responsabilidade, tornando a dissuasão extremamente difícil. Ressalta-se, no entanto, que tais táticas já dominavam as comunicações globais antes das fibras óticas submarinas, e que o corte de cabos era uma parte regular nas guerras (MARTINAGE, 2015).

Além de ataques de forma física, por meio de corte ou explosão da estrutura, existe a possibilidade de ataques de interceptação de dados sem o dano ao cabo submarino, de forma furtiva, sem que os usuários dos cabos percebam a coleta não autorizada do sinal. De acordo com reportagem publicada em 2005 (NEW YORK TIMES, 2005), o submarino norte-americano USS Jimmy Carter, da classe Seawolf, teria a capacidade de obter os sinais que trafegam pelos cabos submarinos. Portanto, Barker (2018) argumenta que os estrategistas militares devem entender que defender a rede de cabos submarinos não significa simplesmente evitar ataques físicos, mas também garantir a integridade dos dados que estão sendo transmitidos. Assim como os EUA, a Rússia tem dedicado recursos para esse fim, com o desenvolvimento de submarinos construídos especificamente para realizar trabalhos técnicos no fundo do oceano. Para imersões mais profundas, o país tem realizado a conversão de submarinos de mísseis balísticos em submarinos especializados (NORDENMAN, 2018). Conforme afirma Clark (2016, p. 237, tradução nossa) "para sustentar sua segurança nacional e preservar a estabilidade, grandes economias e potências nucleares precisarão melhorar sua capacidade de monitorar e controlar as águas de suas costas, assim como fazem com os céus acima de suas terras"[7].

[7] "To sustain their national security and preserve stability, large economies and nuclear powers will need to improve their ability to monitor and control the waters off their shores, just as they do the skies above their lands."

Entretanto, não só danos provocados por ações militares afetam a disponibilidade dos cabos submarinos. Segundo Martinage (2015), estima-se que todos os anos ocorram cerca de cem casos de danos importantes à infraestrutura, sendo 70% resultado de atividades humanas, como pesca e ancoragem. Em 2016, um terremoto submarino perto de Taiwan atingiu nove cabos, sendo necessários onze navios e quarenta e nove dias de trabalho para concluir os reparos. Por razão desse incidente, China, Japão, Filipinas, Cingapura, Taiwan e Vietnã perderam canais de comunicação críticos, comprometendo a atividade bancária e o comércio regional. Em 2018, uma avaria no cabo submarino ACE[8] causou problemas significativos em dez países da costa oeste da África, como Serra Leoa, Libéria, Guiné-Bissau e Gambia. A Mauritânia permaneceu completamente sem acesso à Internet por quarenta e oito horas consecutivas (BELSON, 2018).

Frente a esses possíveis modos de ataque às infraestruturas de cabos, vale entender de forma sucinta a diferença entre defesa e segurança cibernética. A defesa é relacionada à proteção da soberania do Estado e suas regiões, assim, ações de respostas aos cortes de cabos em alto mar, mas do que uma proteção aos cabos, é de fato uma proteção do território marítimo do Estado, considerando-se aqui o Estado como o ator central da proteção. A segurança cibernética tem relação mais direta com os atores privados e os usuários desse sistema de informação. Assim, a proteção dos dados que trafegam pelos cabos e das aterragens dos cabos está mais associada à função do ente privado detentor do cabo do que do Estado. Na proteção das aterragens, a responsabilidade do ente privado é mais clara, visto que por estar tal infraestrutura em território nacional, já goza de proteção efetiva do Estado. Todavia, deve ter o ente privado a preocupação em proteger o bem, garantindo que ele não seja violado dentro da área privada em que se encontra. Já no caso dos dados há uma responsabilidade dupla, Estado e ente privado, sendo que o primeiro deve buscar proteger fisicamente os cabos de forma a evitar que dados sejam roubados, tendo o entre privado a responsabilidade constante de procurar maneiras de criptografar e proteger esses dados, para que, mesmo que sejam roubados, não seja possível obter as informações que estavam sendo enviadas (AYRES PINTO, 2019).

Essa distinção é central para evitar a acumulação de responsabilidade protetivas ao Estado, mais especificamente para as forças armadas, em relação às infraestruturas críticas, retirando do ente privado a

[8] Sigla para African Coast to Europe.

necessidade de seu compromisso constante com essa demanda securitária, que muitas vezes não gera retornos financeiros, mas que é essencial para manutenção da atividade econômica por eles praticada. Assim, a divisão dessa responsabilidade deve ser bem-feita, de forma a evitar que o Estado tenha demasiada carga de responsabilidade por problemas que ele não deu causa e que, muitas vezes, não consegue evitar que ocorram, pois as decisões para evitá-los estão na esfera decisória do ente privado.

Todavia, quando pensamos na relação público e privado na esfera da defesa do Estado, parece existir um limite que efetivamente se assenta na questão estratégica e sigilosa que tal ação contém. Como abrir dinâmicas estratégicas do Estado a entes privados sem que isso seja mais um flanco de ameaça a ser considerado? Como promover a cooperação entre entes tão distintos e com responsabilidades e metas quase opostas?

A resposta para tais questionamentos está ligada à capacidade de atribuir cada vez mais ao ente privado a noção de responsabilidade efetiva por essa seara, principalmente quando falamos da proteção de cabos submarinos de fibra ótica. E a maneira de atribuir mais responsabilidades a esses atores é permitir que eles, ao mesmo tempo, tenham capacidade decisória em todo processo, dando também abertura das ações desses entes para o Estado, tornando, assim, toda a informação entre eles estratégica e efetivamente central, tanto para a ação de defesa do Estado, como para a ação empresarial do privado. Para determinar de maneira prática como isso poderia ser feito, Pagliari, Ayres Pinto e Viggiano (2020, p. 153) descrevem que é preciso que o Estado promova a chamada "tríplice hélice estratégica" para o setor da defesa nacional. As autoras propõem uma cooperação constante do setor público, representado pelas forças armadas, a academia e o setor privado, tanto na execução de ações, mas principalmente no planejamento para pensar e executar meios de proteção das infraestruturas críticas do país. Nesse sentido, essa tríplice hélice seria a forma ideal de garantir transparência e coesão entre as ações de proteção dos cabos em alto-mar, ao mesmo tempo que são protegidos efetivamente quando tocam o solo nacional, e passam a ser exclusivamente propriedade dos entes privados que os financiaram.

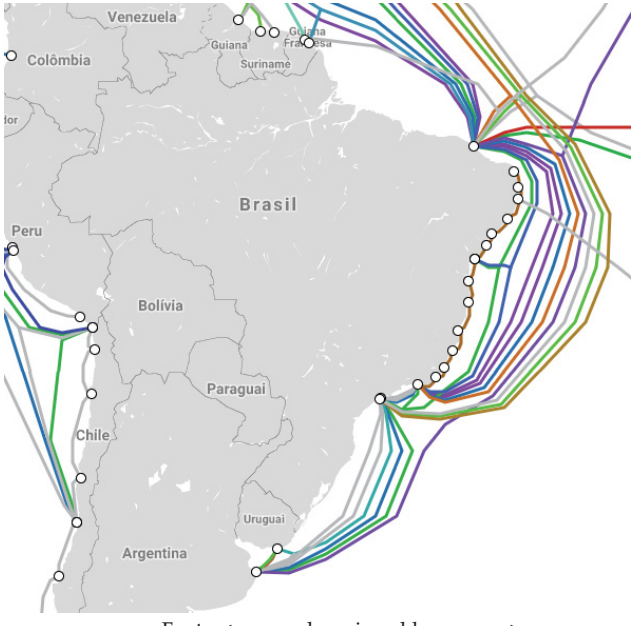
Uma estratégia de proteção para cabos submarinos não pode depender, portanto, somente da ação militar, uma vez que é impossível proteger toda a rede de cabos, dada a sua extensão global (BARKER, 2018). Nesse caso, a solução poderia ser enfatizar a identificação e interceptação de navios capazes de interferir na infraestrutura de cabos. Porém, a

dificuldade aumenta se for considerado o uso de submarinos, que são de difícil rastreamento e interceptação, exigindo o uso de satélites, inteligência e sensores subaquáticos. Para um comandante militar, a tarefa de proteger os cabos submarinos de ataques pode ser difícil e, portanto, as estratégias nacionais talvez precisem se concentrar em métodos alternativos de salvaguardar a troca de informações, como o aumento no nível de redundância dentro das infraestruturas, assim como da efetivação da tríplice hélice estratégia para defesa, com a participação do setor privado que opera nessa seara. Do contrário, uma proteção que não considere a responsabilidade do ente privado nesse processo tenderá a ser falha e a sobrecarregar o Estado no processo securitário e de defesa.

## A INFRAESTRUTURA DE CABOS SUBMARINOS NO BRASIL

O Brasil é o quarto país com maior número absoluto de usuários de Internet, atrás apenas dos Estados Unidos, Índia e China (UNCTAD, 2017). A partir de pesquisa realizada em fontes especializadas, verificou-se que o país possui dezesseis cabos submarinos interligando seu território ao exterior. A figura 1 apresenta a distribuição da infraestrutura pelo litoral nacional.

**Figura 1 – Infraestrutura de Cabos Submarinos no Brasil.**




Fonte: <www.submarinecablemap.com>

Fato relevante a ser observado se refere às estações as quais os cabos submarinos são conectados ao emergirem do oceano. Verifica-se que os pontos de convergência dos cabos se localizam, quase na totalidade, nos estados do Ceará, Rio de Janeiro e São Paulo. Esses cabos são acoplados de um lado em estações em solo brasileiro e, do outro lado, em estações em solo norte-americano. Em se tratando de segurança da informação, essa questão conduz a discussões acerca da proteção da informação trafegada, em especial face à revelação sobre supostos atos de espionagem praticados por Agências de Segurança. Se por um lado é possível proteger as instalações onde os cabos submarinos tocam o solo nacional, o mesmo não ocorre em pontos do exterior onde os cabos alcançam o continente. Desse modo, mesmo que sejam realizados acordos bilaterais no que tange à segurança dessa infraestrutura, o resultado pode não ter o efeito prático desejado, uma vez que, assim como no Brasil, são empresas privadas que operam os cabos submarinos nos EUA.

O quadro 1 apresenta os dezesseis cabos submarinos utilizados no Brasil, assim como as respectivas empresas proprietárias. Observa-se que, majoritariamente, as operadoras dos cabos utilizados pelo país são de capital estrangeiro.

**Quadro 1 – Empresas proprietárias de cabos submarinos no Brasil**

| Cabo Submarino[9] | Empresa Proprietária |
|---|---|
| Americas-II | Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, CNT, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, CenturyLink |
| Atlantis-2 | Embratel, Deutsche Telekom, Telecom Italia Sparkle, Telecom Argentina, Telxius, Portugal Telecom, Orange, Telefónica Larga Distância de Puerto Rico, AT&T, Proximus, KT, SingTel, Sprint, Tata Communications, Verizon, BT, Orange Polska |
| BRUSA | Telxius |
| EllaLink[10] | EllaLink Group |

[9] Os cabos Festoon e Junior não foram contemplados no quadro por não possuírem interligação direta com o exterior.

[10] Início da operação prevista para 2020

| | |
|---|---|
| GlobeNet | BTG Pactual |
| Monet | Angola Cables, Google, Algar Telecom, Antel Uruguay |
| South America-1 (SAm-1) | Telxius |
| South American Crossing (SAC) | Telecom Italia Sparkle, CenturyLink |
| South Atlantic Cable System (SACS) | Angola Cables |
| South Atlantic Inter Link (SAIL) | Camtel, China Unicom |
| Tannat | Google, Antel Uruguay |
| ARBR[11] | Werthein Group, Seaborn Group |
| Malbec[12] | GlobeNet, Facebook |
| South Atlantic Express (SAEx1)[13] | SAEx International Ltd. |
| Seabras-1 | Seaborn Group |
| America Movil Submarine Cable System-1 (AMX-1) | América Móvil |

Fonte: elaborado pelos autores a partir de informações de <www.submarinecablemap.com>.

Algumas iniciativas estão sendo realizadas para contornar as fragilidades de segurança e dependência de conexão com os EUA, como a parceria do Brasil com a *Angola Cables*, multinacional angolana de telecomunicações. Em 2018, a empresa concluiu a instalação do SACS, o primeiro cabo submarino a ser instalado no Atlântico Sul, ligando a África à América do Sul (CAIAFA, 2018). Dessa forma, foi criada uma rota alternativa para o tráfego de dados com o continente africano, a Ásia e a Europa, sem a necessidade de, primeiramente, passar por solo norte-americano. Outra rota alternativa, por meio do cabo submarino EllaLink, está em fase de projeto, cuja perspectiva é ligar a Espanha e Portugal diretamente ao Brasil (BUCCO, 2018).

[11] Início da operação prevista para 2021
[12] Início da operação prevista para 2020
[13] Início da operação prevista para 2021

## SEGURANÇA MARÍTIMA E DEFESA CIBERNÉTICA

Deve-se levar em conta que a garantia da integridade, confidencialidade, privacidade, não-repúdio e disponibilidade das comunicações realizadas via cabos submarinos é importante não apenas ao Brasil. Todos os seus parceiros comerciais, aliados militares e todo uma série de *stakeholders* que utilizam essas vias como hub para comunicar-se com o entorno regional, necessitam ser coparticipes da formação de políticas marítimas que incentivem a criação de uma governança oceânica, tendo em vista a segurança marítima para formar um ambiente seguro para essa modalidade de comunicação; assegurando, assim, a estabilidade das relações comerciais e do tráfego de informações confiáveis entre os segmentos públicos e privados dos países beneficiados por essas infraestruturas. Por isso, a preocupação no desenvolvimento de operações conjuntas entre as forças armadas do país, no caso do Brasil entre Exército Brasileiro, responsável pelo domínio cibernético, e Marinha do Brasil, responsável pelo domínio marítimo, e também por meio da cooperação internacional das marinhas dos diversos países do Atlântico. Essa preocupação de cooperações, seja interagências, dentro do país, seja entre forças de outras nações, é elemento fundamental para compreender os desafios gerados pelas dinâmicas do Poder Marítimo e do Poder Cibernético, quais sejam, aquelas das comunicações no ciberespaço transmitidas por cabos submarinos. Dada a forçosa participação de poderes diferentes na gestão da segurança destes ativos e, necessariamente, de interesses de Estados diversos, esse cenário oferece uma grande questão de geopolítica. Como afirma Germond (2015, p. 141, tradução nossa), "A segurança marítima é intrinsicamente geopolítica, posto que se trata de projetar o poder público além das suas fronteiras externas dentro do domínio global marítimo". Logo, a segurança dos cabos submarinos é, antes de ser um problema nacional, um problema global.

Nesse contexto, existe uma tendência de que os países considerem os cabos submarinos, nas zonas marítimas nacionais, como infraestrutura crítica (CARTER, 2019). Alguns, percebendo a importância dos cabos, adotaram políticas para mitigar incidentes com essas infraestruturas. Como exemplo, cita-se a Nova Zelândia, que criou zonas de proteção especiais, de modo a minimizar danos aos cabos submarinos causados por atividades de transporte e pesca (SUNAK, 2017). Na mesma região, a Austrália elaborou leis para proteção para os cabos, cuja zona de restrição

se estende até 2.000 metros de profundidade. No interior dessa região, a pesca de arrasto e a ancoragem são proibidas, e é realizado monitoramento permanente da guarda costeira australiana (CARTER, 2009).

## CONSIDERAÇÕES FINAIS

Tal qual o telégrafo impressionou Jomini quanto à capacidade de prover agilidade na logística de informação, atualmente os cabos submarinos são os responsáveis por grande parte do fluxo de informação entre o Brasil e os demais países. As cadeias logísticas das quais o Brasil participa são dependentes desse tipo de meios físicos de comunicação. Danos e interrupções nessa infraestrutura têm o potencial de influenciar de forma substancial a presença do país nas cadeias logísticas globais, impactando diretamente na economia nacional e, em última instância, na sua soberania. Observou-se neste trabalho que são poucos os pontos de contato dos cabos submarinos com o território nacional e que, majoritariamente, esses pontos são operados por empresas privadas. Além disso, há pouca diversidade de conexões dos cabos com o exterior, sendo a maioria conectada ao solo norte-americano. Diante desse fato, aliado ao multi-domínio do ciberespaço, a análise aponta para a necessidade de ampliar a discussão sobre o tema, assim como compreender a relação público e privado na esfera da defesa do Estado. Expandir os estudos sobre a relevância dos cabos submarinos, e sua inserção no contexto da defesa cibernética e da segurança marítima, pode colaborar para garantir a integridade, confiabilidade e disponibilidade do fluxo de informação entre o Brasil e o mundo. Considerando a posição solar do Brasil no Atlântico Sul, em especial como a nação de maior extensão costeira da ribeira ocidental atlântica, o desenvolvimento de uma política de defesa dos cabos submarinos é elemento-chave para consolidar a imagem do país frente às nações de seu entorno estratégico, em especial as outras nações componentes da Zona de Paz e Cooperação do Atlântico Sul, haja vista que a defesa da infraestrutura de comunicação por cabos submarinos impacta diretamente na segurança da região e na consciência situacional marítima de todo o Atlântico Sul. Nesse sentido, é importante que a estratégia de defesa dos cabos submarinos privilegie um planejamento de longo prazo, com participação das forças armadas, da academia e do setor privado, de modo a proteger essa infraestrutura no Brasil.

# THE DEFENCE OF SUBMARINE COMMUNICATIONS CABLE INFRASTRUCTURE: A FRAMEWORK BETWEEN CYBER DEFENCE AND MARITIME SECURITY IN BRAZIL

**ABSTRACT**

This current paper aims to analyse the importance of thinking in Public Policies on the Security of the Submarine Communications Cable Infrastructure on use in Brazil, considering that in this kind of technology resides most part of communication capacities the country uses to communicate itself with other global actors, compounding a comprehensive hub, which relevance protrudes, in special, to all nodes in the national supply chain regarding economy, social and national policies. This paper analyses the dimension of the use of submarine communications cables in Brazil, the quantity of companies that operates this kind of infrastructure in the country and the kind of threats that could inflict real damages to this kind of communication. Afterwards, an approach has been made to identify the need of a joint work force between public and private institutions to guarantee that defence measures of this kind of mean of communication be successful. The fact that the information being transmitted but this means worldly relies on the submarine communication cables, added to the multi-domain aspect of the cyberspace, points to the correlation between cyber defence and maritime security. That analysis indicates, then, that research and debates on this subject must be enlarged in the academic, military and governmental fields in Brazil, in order to ensure the protection of this infrastructures, safeguarding, thus, the integrity, reliability and availability of the data flows between Brazil and the World.

**Keywords:** Submarine Communications Cables. Critical Infrastructure. National Defence. Maritime Security.

## REFERÊNCIAS

BARKER, Pete. Undersea Cables and the Challenges of Protecting Seabed Lines of Communication. Center for International Maritime Security, 2018. Available: http://cimsec.org/undersea-cables-challenges-protecting-seabed-lines-communication/35889. Accessed on: 14 jun. 2019.

BELSON, David. ACE Submarine Cable Cut Impacts Ten Countries. Oracle Internet Intelligence, 2018. Avaible: https://blogs.oracle.com/internetintelligence/ace-submarine-cable-cut-impacts-ten-countries. Accessed on: 16 jun. 2019.

BIRNBAUM, Michael. Russian submarines are prowling around vital undersea cables. It's making NATO nervous. The Washington Post, 22 dec. 2017. Available: https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?utm_term=.93ca6dbd1013&noredirect=on. Accessed on: 14 jun 2019.

BUCCO, Rafael. Cabo submarino Brasil-Espanha começa a operar em 2019. TeleSintese, 24 abr. de 2017. Disponível em: http://www.telesintese.com.br/cabo-submarino-brasil-espanha-comeca-operar-em-2019. Acesso em: 2 jul. 2019.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa. Brasília, DF: Ministério da Defesa, 2008.

CAIAFA, Roberto. SACS: O primeiro cabo submarino ligando o Brasil a África chega a Fortaleza (Ceará). Tecnologia & Defesa, 22 fev. 2018. Disponível em: http://tecnodefesa.com.br/sacs-o-primeiro-cabo-submarino-ligando-o-brasil-a-africa-chega-a-fortaleza-ceara. Acesso em: 22 mar. 2019.

CARTER, Lionel et al. Submarine cables and the oceans: connecting the world. Cambridge: UNEP - WCMC; Lymington: ICPC, 2009. (UNEP-WCMC Biodiversity Series No. 31).

CLARK, Bryan. Undersea cables and the future of submarine competition. Bulletin of Atomic Scientists, v. 72, No. 4, p. 234-237, 2016.

FARAHANI, Reza; REZAPOUR, Shabnam. Logistics Operations and Management: concepts and models. London: Elsevier, 2011.

FRANCHI, Tassio; VICHI, Leonardo. The beginning of warfare on the internet: Zapatista Strategic Communications. Defense Strategic Communications, v. 6, p. 123-156, spring, 2019.

GERMOND, Basil. The Geopolitical Dimension of Maritime Security. Marine Policy, v. 54, p. 137-142, 2015.

GILES, Keir. Russia´s 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. London: Chatham House, The Royal Institute of International Affairs, mar. 2016.

HINCK, Garrett. Evaluating the Russian Threat to Undersea Cables. The Lawfare Institute, 5 mar. 2018. Available: https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables. Accessed on: 20 jul. 2019.

JOMINI, Baron Antoine Henri de. The Art of War: Restored Edition. Legacy Books Press, 2008.

KOCHER, José Mauro. Cabos submarinos no século XIX: considerações técnicas e econômicas. In: SEMINÁRIO NACIONAL DE HISTÓRIA DA CIÊNCIA E DA TECNOLOGIA, 14., 2014, Belo Horizonte. Anais [...]. Belo Horizonte: 2014.

KONO, Keiko. Strategic Importance Of, And Dependence On, Undersea Cables. Cooperative Cyber Defence Centre of Excellence. Nov. 2019.

KRESS, Moshe. Operational Logistics: The Art and Science of Sustaining Military Operations. New York: Springer, 2002.

MARTINAGE, Robert. Under the Sea: the vulnerability of the commons. Foreign Affairs, jan./feb. 2015. Available: https://www.foreignaffairs.com/articles/global-commons/under-sea. Accessed on: 10 jun. 2019.

MIN, Hokey. The essentials of supply chain management: new business

concepts and applications. United States of America: FT Press, 2015.

NEW Nuclear Sub Is Said to Have Special Eavesdropping Ability. The New York Times, 20 feb. 2005. Available: https://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html. Accessed on: 14 mar. 2019.

NORDENMAN, Magnus. Russian Subs Are Sniffing Around Transatlantic Cables. Here's What to Do About It. Defense One, 17 jan. 2018. Available: https://www.defenseone.com/ideas/2018/01/russian-subs-are-sniffing-around-transatlantic-cables-heres-what-do-about-it/145241/?oref=d-skybox. Accessed on: 8 abr. 2019.

NYE, Joseph. O Futuro do Poder. São Paulo: Benvirá, 2012.

O'MALLEY, Sean. Assessing Threats to South Korea's Undersea Communications Cable Infrastructure. The Korean Journal of International Studies, v. 17, n. 3, p. 385-414, 2019.

PAGLIARI, Graciela de Conti; PINTO, Danielle Jacon Ayres; VIGGIANO, Juliana. Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: Um estudo prospectivo. In: OLIVEIRA, Marcos Aurélio Guedes de. Defesa cibernética e Mobilização Nacional, Recife: Editora da UFPE, 2020, p. 153-174.

PAPILLA, Ove. The Birth of Operational Art. Baltic Security & Defence Review, v.17, 2014.

PINTO, Danielle Jacon Ayres. Políticas Públicas de Defesa Cibernética em Perspectiva Comparada: uma análise dos casos de EUA, China, Rússia e Israel. In: RAMOS, Carlos Eduardo De Franciscis (org.) et al. XXI Ciclo de Estudos Estratégicos - Ciberespaço: a nova dimensão do campo de batalha. Rio de Janeiro: ECEME, 2019, p.138-146.

PINTO, Danielle Jacon Ayres; FREITAS, Riva Sobrado; PAGLIARI, Graciela de Conti. Fronteiras virtuais: um debate sobre segurança e soberania do Estado In: PINTO, Danielle Jacon Ayres; FREIRE, Maria Raquel; CHAVES, Daniel Santiago. Fronteiras Contemporâneas Comparadas:

desenvolvimento, segurança e cidadania. Macapá: Editora da UNIFAP, 2018, p. 40-53.

RUSHTON, Alan; CROUCHER, Phil; BAKER, Peter. The Handbook of Logistics and Distribution Management. London: Kogan Page, 2010.

SEAL, Thomas. The Undersea Cable Market Is Booming Again, This Time Funded by Big Tech. Bloomberg Businessweek. 18 mar. 2019. Available: https://www.bloomberg.com/news/articles/2019-03-14/undersea-cables-are-no-longer-underwater-as-fiber-booms-again. Accessed on: 27 jul. 2019.

SILVA, Carlos Alberto Vicente da; MUSETTI, Marcel Andreotti. Logísticas militar e empresarial: uma abordagem reflexiva. Revista de Administração da Universidade de São Paulo, São Paulo, v.38, n.4, p.343-354, out./dez. 2003.

SUNAK, Rishi. Undersea Cables: indispensable, insecure. London: Policy Exchange, 2017

SUBMARINE Cable Frequently Asked Questions. Telegeography. Available: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions. Accessed on: 14 jun. 2018.

UNCTAD. Information Economy Report 2017: digitalization, trade and development. United Nations Conference on Trade and Development. 23 Oct. 2017. Availabe: http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf. Accessed on: 14 jun. 2018

YOHO, Keenan D.; RIETJENS, Sebastiaan; TATHAM, Peter. Defence logistics: an important research field in need of researchers. International Journal of Physical Distribution & Logistics Management, v. 43, No 2, p. 80-96, 2013.

Recebido em: 29/01/2020
Aceito em: 04/08/2020