



CF (FN) Fabio Vimenev Simas  
vimenevsimas@gmail.com

## Terminais Portuários: segurança de infraestruturas críticas



O CF (FN) SIMAS serve atualmente no Comando da Força de Fuzileiros da Esquadra, como Chefe da Seção de Comunicações e Guerra Eletrônica. É oriundo da Escola Naval, realizou todos os cursos de carreira, sendo digno de destaque, o Curso de Estado Maior para Oficiais Superiores (C-EMOS) da EGN, em 2018, e o Curso de Estado Maior para Oficiais Intermediários (C-EMOI), em 2010. Foi Imediato do BtlCmndoCt e serviu, por mais de cinco anos, no GptFNRRG; foi Oficial de Operações do GptFNRRJ e participou da Operação Acolhida, em Roraima, em 2020. Também participou do Planejamento do Exercício FELINO 2023, em Bissau – Guiné-Bissau.

### Resumo

A importância da proteção das infraestruturas críticas econômicas, voltadas para o mar, está muito longe de ser mera fantasia militar. Fatos históricos ocorridos no Atlântico Sul, confirmam tal preocupação. O Brasil possui vulnerabilidades litorâneas que precisam ser consideradas e para as quais devemos dar tratamento adequado, sob pena de comprometermos a economia e o desenvolvimento nacional. Analisando as possíveis ameaças que poderiam incidir sobre nossos terminais, podemos classificá-las como ameaças cinéticas, como vetores aéreos capazes de executar reconhecimento e ataques, para os quais a defesa antiaérea tem sido objeto de preocupação. Há, também, ameaças não cinéticas de natureza NBQR, da Guerra Eletrônica e da Cibernética. Tais ameaças têm sido consideradas com de maior probabilidade de ocorrência, particularmente a NBQR que envolvem produtos químicos. É importante que os Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav) de Defesa de Porto contem com equipe especializadas para responder a tais desafios. Deve realizar a segurança de pontos sensíveis utilizando seus militares, comunicações eficientes, câmeras de segurança, sensores de presença, cães, drones, em fim, lançar mão de todo aparato tecnológico disponível, de forma a facilitar a obtenção da Consciência Situacional e garantir o funcionamento ininterrupto do terminal. Bem como, articular, as vezes em espaços restritos, seus componentes de Combate Terrestre, de Combate aéreo e de Apoio Serviço ao Combate.

**Palavras-chave:** infraestruturas críticas; vulnerabilidade litorânea; terminais portuários; ameaças cinéticas; ameaças não-cinéticas; defesa antiaérea; defesa NBQR; guerra eletrônica; cibernética; agente perturbador da ordem pública; APOP; defesa de instalações portuárias.

### Abstract

*The importance of protecting critical economic infrastructure facing the sea is far from being a mere military fantasy. Historical facts that occurred in the South Atlantic confirm this concern. Brazil has coastal vulnerabilities that need to be considered and for which we must provide adequate treatment, otherwise we risk compromising the economy and national development. Analyzing the possible threats that could affect our terminals, we can classify them as kinetic threats, such as aerial vectors capable of carrying out reconnaissance and attacks, for which anti-aircraft defense has been an object of concern. There are also non-kinetic threats of an NBQR, Electronic Warfare and Cybernetics nature. Such threats have been considered to be more likely to occur, particularly NBQR involving chemicals. It is important that the Port Defense Marine Air-ground task Force have specialized teams to respond to such challenges. It must carry out the security of sensitive points using its military, efficient communications, security cameras, presence sensors, dogs, drones, and finally, make use of all available technological devices, in order to facilitate obtaining Situational Awareness and guarantee operation uninterrupted from the terminal. As well as articulating, sometimes in restricted spaces, its Land Combat, Air Combat and Combat Service Support components.*

**Keywords:** critical infrastructures; coastal vulnerability; port terminals; kinetic threats; non-kinetic threats; anti-aircraft defense; CBRN defense; electronic warfare; cybernetics; agent disturbing public order; defense of port facilities.

## Introdução

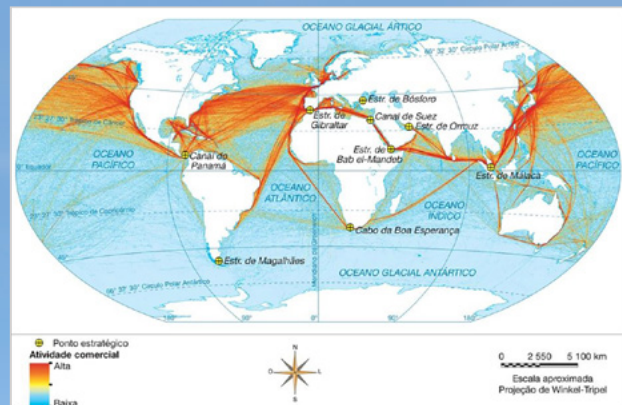
No contexto da importância da proteção das infraestruturas críticas econômicas, voltadas para o mar, a segurança de nossos terminais portuários, que figuram hoje como pontos de importância estratégica, está muito longe de ser mera fantasia militar. Historicamente, pelo Atlântico Sul, fatos ocorridos no século XX, como a II Guerra Mundial (1939-1945), a Guerra da Lagosta (1961-1963), e o conflito das Malvinas (1982) entre o nosso vizinho argentino e o Reino Unido, que ocorreu dentro do nosso entorno estratégico, confirmam tal preocupação (Xavier, 2020).

O Brasil tem se destacado na economia, principalmente no campo do agronegócio, causando preocupação em alguns países concorrentes nesse seguimento. Como já ocorrido entre outros Estados no passado e na atualidade, como ocorre entre a Rússia e a Ucrânia, em casos de tensões e crises entre eles, o Estado com uma Marinha mais forte pode implementar um bloqueio aos portos do país adversário, atingindo-o em sua atividade econômica. Porém, outro ponto de preocupação relevante são nossas riquezas litorâneas, como o petróleo, gás, terras raras, o potencial pesqueiro e outros, que são alvos de cobiça de outros Estados, requerem assim um Poder Naval adequado para lhes proteger. Com isso, os terminais portuários servem como bases de apoio e de escoamento de produção e também integram toda uma cadeia logística, necessitando com isso, da proteção das Forças Navais, com seus componentes terrestres e aéreos.

Nesse sentido, é importante chamar a atenção para a nossa vulnerabilidade litorânea, que é de importância vital para o país. Relembre-se que, no nosso país, cerca de 95% do comércio exterior, 95% do petróleo e 80% do gás advém do mar, além de outras fontes econômicas com grande potencial de exploração, como a mineração em águas profundas (Xavier, 2020).

Nos dias atuais, com a possibilidade de ameaças externas se aproximarem de nossos Terminais Portuários, com chances de causar severos danos econômicos, impedindo ou restringindo o escoamento de nossas produções, torna-se cada vez mais importante que a Marinha do Brasil e as Agências, no âmbito Federal e Estadual, estejam preparadas para o enfrentamento e dissuasão dessas ameaças.

Figura 2: Rotas marítimas comerciais



Fonte: Pontos estratégicos e principais rotas marítimas (2018).

Figura 1: Foto região portuária de Rio Grande (RS)

Fonte: EsqdHU-5.

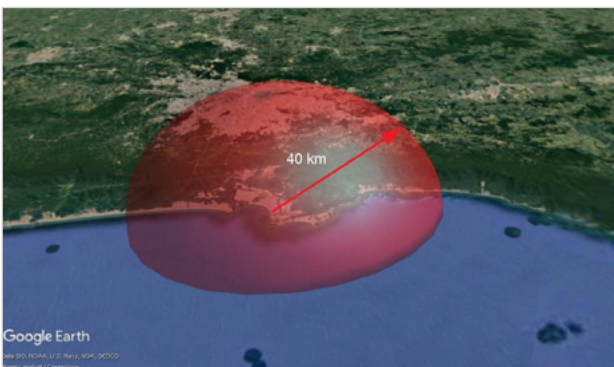


## Possíveis Ameaças

Analisando as possíveis ameaças que poderiam incidir sobre nossos terminais, podemos separá-las em dois grupos: **ameaças cinéticas** e **ameaças não cinéticas**. Observando as possíveis ameaças cinéticas, com a tecnologia presente atualmente em alguns países, observa-se que os vetores aéreos possuem a capacidade de executar reconhecimento e de realizar ataques sobre as instalações de vital importância de um terminal, além da existência da capacidade de observação satelital de outros Estados. Assim, a necessidade de possuir uma capacidade de defesa antiaérea adequada à importância estratégica brasileira se reveste de grande importância nesse cenário, pois havendo na Força um sistema de defesa antiaéreo de média altura, por exemplo, com capacidade de detectar e atingir alvos até 40 km de distância, seria possível neutralizar grande parte dessas ameaças, incluindo os mísseis de cruzeiro e foguetes inimigos.

A defesa antiaérea tem sido objeto de preocupação de nossas Forças, há alguns anos, para diversas situações, ressaltamos a iniciativa do Exército Brasileiro no desenvolvimento de radares antiaéreos nacionais, como o SABER M60 e o SABER M200, que podem detectar alvos até 60 km e 200 km, respectivamente (Xavier, 2021).

Figura 3: Imagem da região de Santos, incluindo a região portuária



Fonte: Google Earth (2015).

No mesmo sentido, recentemente, o Ministério da Defesa deu um passo muito importante na busca da implementação de um Sistema de Defesa Antiaérea que possa atender os requisitos das nossas Forças e mitigar a vulnerabilidade do nosso país contra as ameaças aéreas. A previsão é da aquisição de um sistema de artilharia antiaérea de média altura e médio alcance que poderá engajar alvos aéreos até 40 km de distância (Brasil, 2020b).

Com o apoio da imagem da região portuária e projetando-se em escala o alcance pretendido de 40 km, nota-se que seria possível realizar uma proteção antiaérea de toda a região em tela, sem necessitar que o radar de defesa estivesse posicionado em algum dos terminais portuários, o que seria desejável para a segurança das operações.

Com relação a possíveis ameaças não cinéticas, destacam-se as ameaças de natureza **NBQR**, as ameaças de **Guerra Eletrônica** e as ameaças **Cibernéticas**. Tais ameaças, nos dias atuais, são aquelas com a maior probabilidade de emprego, pois quando um oponente as utiliza, normalmente não há evidência de quem a acionou e seu causador pode permanecer oculto, não assumindo a autoria do dano provocado. Se o agressor não for identificado, não há como protestar, por meio diplomático e nem lançar mão de dispositivos do direito internacional e o agressor poderá sair ileso.

Para as ameaças de natureza NBQR, a de maior probabilidade de ocorrência, nos Terminais brasileiros, são aquelas envolvendo produtos químicos, sendo nosso país grande importador desses produtos, como é o caso dos fertilizantes, por exemplo. Esses produtos, se não manuseados, armazenados e transportados de forma adequada, podem causar incêndios ou até explosões, com consequentes perdas de materiais ou até de vidas humanas. Nesse contexto, as ameaças podem atuar por meio de sabotadores dentro dos próprios Terminais. Assim, é importante que, nos Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav) de Defesa de Porto, haja uma Equipe de ligação com os seus Componentes, com o propósito de contribuir com a prevenção de acidentes e para efetuar um rápido acionamento do BtlDefNBQR, caso necessário.

No que tange às possíveis ameaças com capacidade de Guerra Eletrônica, é importante realizar um cuidadoso estudo de Inteligência Operacional, a fim de verificar as possibilidades do inimigo ou do Agente Perturbador da Ordem Pública (APOP), dependendo da situação enfrentada. Atualmente, as Marinhas bem equipadas no mundo possuem a capacidade realizar ataques eletrônicos, a partir de seus navios, contra radares e algumas possuem ainda a capacidade de realizarem ataques eletrônicos contra as comunicações do seu oponente.

Além disso, dependendo do tipo de ameaça enfrentada, hoje existem equipamentos de baixo custo no mercado, com capacidade de escaneamento de diferentes frequências de comunicações. Com isso, Organizações Criminosas (ORCRIM), dentro do país, podem monitorar comunicações realizadas em claro, realizadas em determinado Terminal portuário, tendo acesso a informações sigilosas sobre as operações portuárias, suas cargas, seu armazenamento e de suas vulnerabilidades de operação.

Em face dessas ameaças eletrônicas, para o caso de navios inimigos de capacidade de realização de Medida de Ataque Eletrônico (MAE), é importante que as Forças de Defesa de Porto e de Defesa de Costa planejem linhas limites de defesa, de forma que o navio inimigo com o alcance do armamento eletrônico não se aproxime do Terminal Portuário defendido.

Para as situações de ameaças eletrônicas internas, com equipamentos de monitoramento de frequências, torna-se importante o emprego de equipamentos de comunicações com recursos de criptografia digital ou de salto de frequências, que praticamente impedem que equipamentos scaneadores de frequências possam monitorar as suas comunicações. Nessas situações, o GptOpFuzNav de Defesa de Porto, Agentes de Segurança e Operadores de Pontos Sensíveis devem evitar a execução de qualquer comunicação em modo claro.

Uma outra possível ameaça não cinética para as operações portuárias é a ameaça Cibernética. Grande parte das operações portuárias, em todo mundo, funcionam por sistemas eletrônicos digitais e com canais de informações de longas distâncias conectadas em redes e com portas de acesso à internet. Assim, a ocorrência de ataque cibernético, nesse contexto, é de grande probabilidade, dado o baixo custo em executá-lo, pois um hacker pode executar esse ataque a partir de qualquer lugar do mundo, de forma inesperada. Destarte, essas redes administrativas, essenciais à operação portuária, tornam-se suscetíveis a ações cibernéticas ofensivas como *ransomware*, *phishing*, *DOS (denied of service)*, capazes de sequestrar dados para posterior cobrança de resgates, comprometer informações restritas, ou até mesmo deixar parte do sistema informatizado inoperante.

Como parte de um processo para aumentar a segurança e permitir a continuidade das operações do sistema portuário, em relação ao ambiente cibernético, pode se pensar em utilizar redes próprias de intranet, com acessos restritos e segurança de criptografia, bem como a utilização de ferramentas de busca de vulnerabilidades e detecção antecipada de ameaças ou intrusões, analisando padrões de comunicação via protocolo de internet TCP/IP e rede virtual VPN, no intuito de detectar anomalias na rede de computadores, inclusive com o auxílio de inteligência artificial. Adicionalmente, em uma situação de crise, elementos especializados em segurança cibernética, civis ou militares, neste caso integrando um Destacamento de Proteção Cibernética, poderão elevar o nível de segurança a patamares adequados, além de adicionarem uma capacidade de efetuar tratamento de incidentes de rede e forense computacional, inclusive como forma de evitar novos incidentes cibernéticos.

## Defesa da Porção Marítima

Conforme previsto em nossa doutrina, para a Defesa de Porto, há a previsão de organização da porção marítima ou fluvial de um porto, para garantir a segurança da entrada e saída de navios autorizados em um determinado porto.

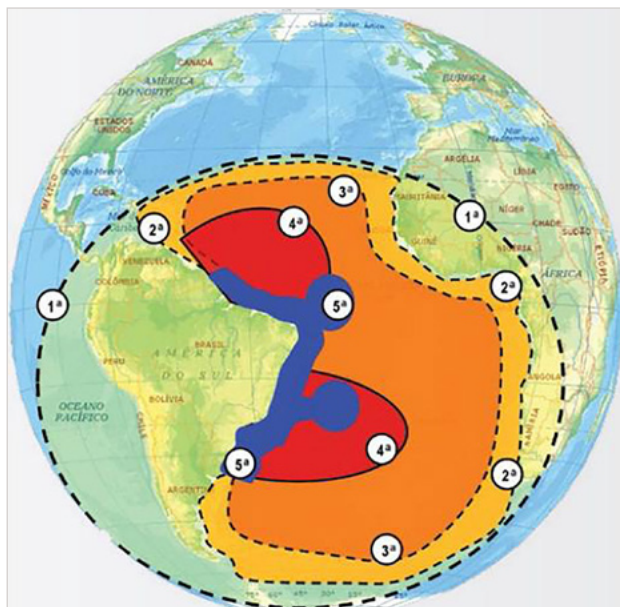
A fim de garantir essa segurança, uma série de operações será prevista, utilizando-se o patrulhamento dos meios navais com a intenção de barrar a aproximação de meios adversários por superfície (embarcações inimigas) e submersos (principalmente por meio de ataques de torpedos e ações especiais por parte de mergulhadores inimigos). Para isso, deve-se prever o emprego de minagem defensiva e redes metálicas anti-torpedos/submersíveis. Será também necessária a instalação de boias que delimitem a aproximação de embarcações, sensores dotados de imagem termal, de movimento e infravermelho, bem como a utilização de Lanchas Rápidas, com fuzileiros navais embarcados ou Grupo de Visita e Inspeção e Grupo de Presa (GVI e GP) com militares devidamente adestrados, que garantirão o patrulhamento e as abordagens a embarcações suspeitas que adentrem os limites estabelecidos pelas boias, bem como para aquelas que se apresentem como ameaças além desses limites.

No mesmo contexto, as Operações de Minagem Defensiva são importantes, na entrada dos portos, com intuito de dificultar ou impedir a entrada de forças inimigas no porto de referência. Assim, serão estabelecidos corredores de tráfego e pontos de controle, a fim de possibilitar o trânsito de navios e embarcações autorizadas.

Radares de Vigilância também devem ser estabelecidos de forma integrada às armas de defesa antiaéreas, conforme já destacado.

Como exemplo de atuais estratégias defensivas pelo mundo, observa-se hoje, no Mar do Sul da China e da China Oriental, China, Japão, Rússia e Taiwan têm desenvolvido sistemas com esse propósito, sendo esses Estados possuidores de Marinhas menos poderosas do que a Marinha americana e a Marinha britânica, por exemplo, e assim, nas áreas descritas, estabeleceram o *Anti-Access and Area Denial* – A2/AD, estratégia própria para se contrapor a um adversário militarmente mais forte. Caso o Brasil venha a adotar, no futuro, uma estratégia defensiva semelhante, isso contribuirá de forma muito positiva para a defesa dos portos brasileiros (Ferreira, 2014).

Figura 4: Esboço das camadas para a defesa da Amazônia Azul



Fonte: Ferreira (2014, p. 78).

## Defesa das Instalações Portuárias

No que tange à defesa das instalações portuárias propriamente ditas, o GptOpFuzNav fará a segurança dos pontos sensíveis, utilizando seus militares, com o devido apoio mútuo entre eles, comunicações eficientes, com auxílio das câmeras

de segurança, sensores de presença, cães e drones. Nesse sentido, é recomendável que o Componente de Comando do GptOpFuzNav esteja posicionado nas instalações de controle do próprio terminal, facilitando ao máximo a obtenção da Consciência Situacional da segurança do porto, com acesso às câmeras de controle e segurança e às comunicações do próprio terminal.

Atualmente, é de grande importância lançar mão de todo aparato tecnológico disponível, a fim de manter ao máximo possível a higidez física dos combatentes anfíbios em operação, procurando manter sempre o seu moral elevado, com capacidade de oferecer uma pronta resposta eficiente, quando for necessária uma reação.

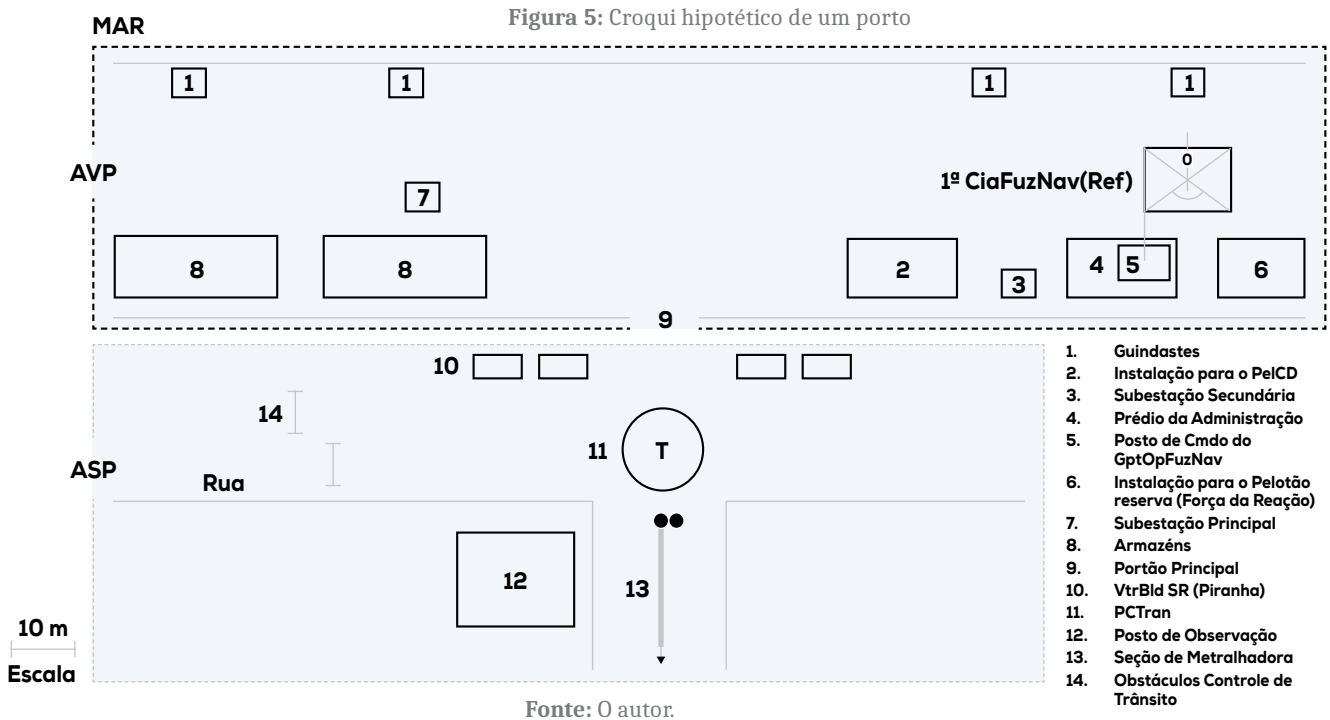
O emprego judicioso dos combatentes nesse tipo de operação é importante, pois a Defesa de Porto, em sendo uma Operação de natureza defensiva, produz a tendência de desgastar o militar com o passar do tempo, com risco de acomodação em tarefas repetitivas. Sendo assim, é recomendável ocorrer o revezamento de tropas, principalmente quando a Operação se perdurar por mais de duas semanas.

Para a Defesa de Porto, de acordo com o Manual de Defesa de Porto, ComOpNav 316, estão previstas ações para a defesa das instalações críticas ao funcionamento de um Terminal portuário, o controle de acesso ao Porto, tanto de pessoas quanto de veículos, assim como das ações marítimas para a proteção de entrada e saída do Porto.

Nesse sentido, um GptOpFuzNav, em nível adequado para o Terminal (Brigada, Unidade ou Subunidade), deverá proteger suas instalações e garantir seu funcionamento ininterrupto, enquanto prosseguirem as Operações de sua defesa, permitindo assim o trabalho de seus operadores, em coordenação com outras Agências de segurança, como Guarda Portuária, Polícia Federal, Receita Federal e com Empresas civis de segurança portuária (Brasil, 2020a).

As seguintes ações são recomendadas para incremento da segurança e para o controle adequado do terminal guarnecido:

- reforçar as cercaduras, lançar concertina, lançar obstáculos contra o acesso de viaturas, fortificar guaritas e postos de sentinelas com saco de aninhagem, melhorar a iluminação externa, verificar a viabilidade de instalar



metralhadoras para bater os setores mais críticos e estabelecer rígido controle de acesso de pessoal;

- realizar patrulhas motorizadas e a pé em itinerários preestabelecidos no interior e exterior das instalações;
- concentrar a tropa de Controle de Distúrbios (CD) em posição central, no interior das instalações, de modo a empregá-la rapidamente nos portões principais e secundários;
- estabelecer postos de sentinelas nos pontos sensíveis vitais e essenciais das instalações; e
- estabelecer as seguintes tarefas, em regime de rodízio, para as frações de tropa envolvidas: Controle de Distúrbios, Segurança de Pontos Sensíveis, Patrulhas e Reação. As tarefas poderão variar de acordo com as características de cada terminal.

Abaixo segue um exemplo hipotético de croqui de como poderia estar guarnecido um Terminal Portuário por um GptOpFuzNav, de nível ElemAnf. Conforme a doutrina em vigor, a Área Terrestre a ser defendida deve ser organizada em **AVP** (Área Vital do Porto) – região portuária propriamente dita, normalmente controlada e cercada com muros e portões, onde estão suas instalações, armazéns, cais, guindastes, casas de força etc., chamados de Pontos Sensíveis (PS) do Terminal e **ASP** (Área de Segurança do Porto) – área externa ao

Porto, onde estão as ruas e áreas das proximidades de acesso ao Porto, onde é importante estabelecer ações preventivas de segurança (Brasil, 2002).

Levando-se ainda em consideração que as Operações de Defesa de Porto podem também compreender situações de distúrbios de operários do porto ou até de forças de segurança, é importante que o GptOpFuzNav tenha o material adequado, como menos letal e assim possa empregar o uso gradual da força, de acordo com as regras de engajamento estabelecidas para a operação, atendendo também, dessa forma, as nossas leis em vigor. Para tanto, os fuzileiros navais, nessas operações, devem estar adestrados para lidar, de forma adequada, não apenas com inimigos externos, mas também com os APOP nacionais.

Com relação aos componentes do GptOpFuzNav, sempre que possível, é preferível que os Componentes de Comando(CCmndo) e de Componente de Combate Terrestre (CCT) se posicionem no interior da AVP, a fim de manter a Consciência Situacional e de obter as vantagens dos consagrados princípios de guerra como os da **Segurança** (mantendo posição em área segura e protegendo os PS do Terminal), da **Oportunidade** (detendo o inimigo ou APOP logo que ele se mostrar vulnerável), da **Iniciativa** (adotando as ações importantes de forma tempestiva) e de **Economia de Meios** (evitando a execução de transportes desnecessários).



Figura 6: Tropa de CD preparada para atuação em porto  
Fonte: 1ºBtlOpRibFuzNav.

“Para os Componentes de Apoio de Serviço ao Combate (CASC) e Componente de Combate Aéreo (CCA), nem sempre haverá instalações ou espaços disponíveis dentro do Terminal e, nesses casos, esses Componentes poderão ser estabelecidos fora do Terminal, mantendo suas atividades, por meio de comunicações seguras.”

Para os Componentes de Apoio de Serviço ao Combate (CASC) e Componente de Combate Aéreo (CCA), nem sempre haverá instalações ou espaços disponíveis dentro do Terminal e, nesses casos, esses Componentes poderão ser estabelecidos fora do Terminal, mantendo suas atividades, por meio de comunicações seguras. O CASC poderá trazer o apoio de rancho de uma Organização Militar (OM) situada próxima e transportar outros itens, quando necessário. O CCA necessitará de espaço e de instalações específicas, para controle aerotático e para defesa antiaérea, que nor-

malmente um porto não possui. É importante que a posição de seus radares e unidades de tiro possibilitem a defesa eficaz do Terminal, mantendo o enlace entre o CCA e o CCmdo (Brasil, 2020a).

## Conclusão

As infraestruturas terrestres, destinadas às atividades marítimas e portuárias, logo de interesse da MB, compreendem uma série de terminais estabelecidos entre Rio Grande-RS e Rio de Janeiro-RJ (Rio Grande-RS, Portonave-SC, Itajaí-SC,

Itapoá-SC, Paranaguá-PR, Santos-SP, *DpWorld* Santos-SP, Rio de Janeiro-RJ, Porto de Suape-PE, Fortaleza-CE, Porto do Pecém-CE, Porto de Itaqui-MA, Porto de Santarém-PA, Porto Chibatião-AM e Porto de Santana-AP). Tais portos brasileiros carregam uma enorme importância, figurando como elos de um grande ciclo de produção que ora exporta e ora importa produtos, gerando substanciais riquezas nacionais.

Os portos, além de operarem a maior parte do comércio nacional, ainda proporcionam apoio logístico para a exploração sustentada de nossa Amazônia Azul, como por exemplo, por meio da pesca ou pela exploração do petróleo. Assim,

percebesse uma íntima ligação entre eles, fazendo com que os portos necessitem da proteção do nosso Poder Naval.

As peculiaridades das ações nos terminais demandam reconhecimento e adestramento específico das tropas que farão a sua proteção, sendo esse fator dificultado por se tratar de um tipo de operação com ações de controle e de defesa, em que o porto precisa ser mantido em funcionamento, com trânsito de civis, não sendo fácil a identificação de um APOP ou inimigo. Por isso, nesses casos é importante o emprego de uma tropa flexível, versátil, bem adestrada e equipada como é a vocação dos nossos Fuzileiros Navais da Marinha do Brasil.



## Referências

BRASIL. Marinha. Comando de Operações Navais. **ComOpNav- 316:** manual de Defesa de Porto. 1. rev. Rio de Janeiro: ComOpNav, 2002.

BRASIL. Marinha. Comando-Geral do Corpo de Fuzileiros Navais. **CGCFN 0-1:** manual básico do Grupamento Operativo de Fuzileiros Navais. Rio de Janeiro: CGCFN, 2020a.

BRASIL. Ministério da Defesa. Gabinete do Ministro. Portaria nº 4.181/GM-MD, de 11 de dezembro de 2020. Aprova os Requisitos Operacionais Conjuntos (ROC) para o Sistema de Artilharia Antiaérea de Média Altura/Médio Alcance das Forças Armadas - ROC no 54/2020. **Diário Oficial da União:** seção 1, Brasília, DF, ano 158, n. 240, p. 21, 16 dez. 2020b.

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

FERREIRA, Renato Rangel. Operações Navais no século XXI: a Amazônia Azul (Parte 2). **Revista Marítima Brasileira**, Rio de Janeiro, RJ, v. 134, n. 04/06, p. 63-89, abr./jun. 2014.

PONTOS estratégicos e principais rotas marítimas. [S. l.], 18 maio 2018. Disponível em: <https://brainly.com.br/tarefa/16025496>. Acesso em: 9 jun. 2022.

XAVIER, Alexandre Tito dos Santos. Série vulnerabilidades do Brasil: efes ntaírea. In: XAVIER, Alexandre Tito dos Santos. **Tito Geopolítica**. [S. l.], 11 jan. 2021. Disponível em: <https://www.atitoxavier.com/post/s%C3%A9rie-vulnerabilidades-do-brasil-defesa-antia%C3%A9rea>. Acesso em: 9 jun. 2022.

XAVIER, Alexandre Tito dos Santos. Sistemas A2/AD: precisamos para a defesa da nossa fronteira oriental (Atlântico Sul)? In: XAVIER, Alexandre Tito dos Santos. **Tito Geopolítica**. [S. l.], 6 maio 2020. Disponível em: <https://www.atitoxavier.com/post/sistemas-a2-ad-precisamos-para-a-defesa-da-nossa-fronteira-oriental-atl%C3%A2ntico-sul>. Acesso em: 9 jun. 2022.

