VITÓRIA nas Sombras

Revista do Comando Naval de Operações Especiais

Nº 01/2024 - ISSN: 2966-084X

AS ATIVIDADES DE OPERAÇÕES ESPECIAIS E DE INFORMAÇÃO NA MARINHA DO BRASIL

VITÓRIA nas Sombras

Editorial

Caros leitores,

É com grande orgulho e entusiasmo que apresentamos a primeira edição da revista *Vitória nas Sombras!*, dedicada a explorar e divulgar os intricados domínios das Operações Especiais e das Operações de Informação e suas capacidades relacionadas.

Em um mundo em constante evolução, no qual a batalha vai além dos campos de combate convencionais, é imperativo que compreendamos e nos adaptemos às nuances da guerra moderna. Acompanhando a dinâmica do ambiente operacional, desde 2019, a Marinha do Brasil conta com o Comando Naval de Operações Especiais para atender às demandas do Poder Naval em relação a: assessoria de Ameaças Híbridas; Operações Especiais e Operações de Informação; ações de Guerra Cibernética, Operações Psicológicas, Assuntos Civis, Guerra Acústica e Guerra Eletrônica; e demais Capacidades Relacionadas à Informação (CRI).

O nome meticulosamente escolhido para a revista – *Vitória nas Sombras!* – também é o lema do Comando Naval de Operações Especiais, pois reflete a essência de nossas operações ao evocar a natureza discreta e muitas vezes não reconhecida das Operações Especiais. Para nós, a vitória não é conquistada apenas nas operações das forças convencionais, conduzidas nos campos de batalha tradicionais, mas também se deve aos esforços conduzidos nas operações especiais veladas nas sombras da noite, escondidas em códigos no ambiente cibernético ou nas profundezas da psique humana, ou até mesmo dissimuladas nas ondas eletromagnéticas e acústicas.

Nesta edição inaugural abordamos, inicialmente, a criação deste Comando Naval, uma Organização Militar focada no emprego coordenado e sinérgico de Operações Especiais e de Informação. O primeiro artigo destaca a necessidade de uma compreensão holística do cenário atual e a importância do uso de capacidades militares para influenciar percepções e sustentar narrativas de maneira a obter a superioridade informacional.

Do segundo ao quinto artigo, são analisadas as Operações Especiais, especialmente o seu emprego no amplo espectro da guerra e a sua eficiência multidimensional em operações de alta complexidade. Os textos também evidenciam como as Operações Especiais têm se mostrado eficientes nas Operações Conjuntas realizadas pelo Ministério da Defesa e avaliam as ações do ponto de vista de um operador especial, salientando a importância de sua liderança e influência em variados aspectos.

Nos artigos seguintes, mergulhamos nas estratégias das Operações de Informação, progredindo para o conceito do Teatro de Operações 5.0, que representa um paradigma fundamental nas operações militares modernas. Os textos apontam a importância da adaptação e da resiliência cibernética, enfatizando como a convergência tecnológica e a tomada de decisão baseada em dados são cruciais para o sucesso nas operações militares

Na sequência, do oitavo ao décimo primeiro artigo, apresentamos a importância das ações realizadas no Quinto Domínio do Combate, evidenciando como os desafios e as oportunidades presentes na era da Guerra Cibernética podem influenciar a guerra no mar. A abordagem do tema prossegue mostrando como a Guerra Cibernética pode apoiar as atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA) e como a integração dos dados cibernéticos com outras informações de Inteligência pode aumentar a consciência situacional e influenciar as decisões no campo de batalha. Busca-se demonstrar, também, como a mentalidade de Segurança Cibernética e Consciência Situacional Cibernética em Operações Militares Marítimas é primordial para a salvaguarda dos ativos navais operacionais e como o uso de *Software* Livre aprimora as Operações Cibernéticas, enfatizando a importância da integração de recursos humanos, *hardware* e *software* na Marinha do Brasil.

A influência e o poder das Operações de Informação continuam sendo tópicos explorados nos artigos seguintes, buscando provocar uma reflexão sobre a estrutura existente e a necessidade de desenvolvimento contínuo para efetivar a coordenação das Capacidades Relacionadas à Informação. No artigo sobre as Operações Psicológicas, discutimos a sua importância tanto em operações de guerra naval e no emprego limitado da força, quanto em situações de resposta a desastres humanitários, salientando não só o seu papel estratégico nas Operações de Paz, na resposta a crises e na construção de relações internacionais sólidas, como também a sua influência nos comportamentos e na facilitação da execução de tarefas militares.

VITÓRIA NAS SOMBRAS!

"Ao lançar esta revista, nos desafiamos a fornecer uma análise aprofundada e perspicaz das Operações Especiais e das Operações de Informação..."

Nos artigos catorze e quinze, destacamos o importante papel das capacidades de Guerra Eletrônica e Acústica nas operações navais, analisando não só a forma como a guerra moderna depende cada vez mais do espectro eletromagnético, como também o papel crítico da Inteligência de Comunicações (COMINT) para obter informações críticas sobre o inimigo e, ainda, o avanço da telemetria acústica terrestre, que oferece novas capacidades em ambientes de conflitos fluidos e acelerados.

O décimo sexto artigo examina o papel vital da capacidade de Assuntos Civis nos conflitos atuais, particularmente no Russo-Ucraniano, demonstrando como a eficácia das relações entre civis e militares é essencial para minimizar danos colaterais e garantir a execução integrada de operações de combate e ações humanitárias.

O artigo seguinte realiza uma análise perspicaz sobre as ameaças híbridas, diferenciando-as das ameaças comuns, além de enfatizar a sua complexidade e a obrigatoriedade de uma resposta apropriada por parte do Estado e de uma abordagem multidisciplinar pela defesa nacional.

Por fim, o último artigo discute as mudanças tecnológicas e destaca a necessidade de adaptação dos serviços de Inteligência à realidade do século XXI, realçando o equilíbrio entre eficiência e privacidade.

Ao lançar esta revista, nos desafiamos a fornecer uma análise aprofundada e perspicaz das Operações Especiais e das Operações de Informação, materializadas em suas Capacidades Relacionadas à Informação, com o intuito de oferecer aos leitores uma compreensão mais clara das táticas e estratégias modernas que moldam a atual conjuntura militar em constante e acelerada mudança.

Comando Naval de Operações Especiais:

VITÓRIA NAS SOMBRAS!

Luís Manuel de **Campos Mello**
Contra-Almirante (FN)

Sumário

Expediente

Distribuição Gratuita

ISSN: 2966-084X, nº 01/2024
Publicação anual do Comando Naval de Operações Especiais com tiragem de 1.000 exemplares.

.....

Comandante de Operações Navais

Almirante de Esquadra
Cláudio Henrique **Mello** de Almeida

Comandante do CoNavOpEsp

Contra-Almirante (FN)
Luís Manuel de **Campos Mello**

Editor-Chefe

CMG (RM1-FN) Leonardo Lago **Deza**
deza@marinha.mil.br

Editora Adjunta

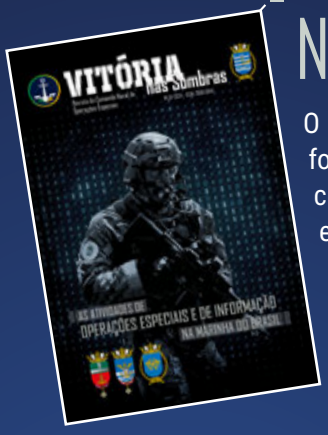
3ºSG-AD **Tamyris Salgueiro** Santana Almeida
tamyris@marinha.mil.br

Projeto Gráfico

Agência 2A Comunicação

Revisão

Marcia Lopes Mensor Lessa



Nossa Capa

O pensamento tradicional de alinhar domínios de forma rígida (terrestre com Exército, marítimo com Marinha, aéreo com Força Aérea) não é mais eficaz. O futuro operacional será desafiador, com adversários que podem comprometer nossa liberdade de manobra e nossa superioridade em todos os domínios: aéreo, terrestre, marítimo, espacial e informacional. A nova linha de contato transcende a visão física, traz o combate para o cotidiano e nos mergulha no reino das sombras cognitivas, digitais, operacionais e estratégicas.

A Marinha do Brasil, por realizar operações terrestres com seus Fuzileiros Navais, aéreas com suas Unidades Aeronavais e marítimas com suas Forças Navais de Superfície e Submarinas, é histórica e particularmente vocacionada para operações em múltiplos ambientes. O Comando Naval de Operações Especiais (CoNavOpEsp) é uma evolução natural dessa postura e renova o compromisso inabalável do Poder Naval de operar com excelência e coordenação em uma ampla gama de ambientes desafiadores.

A capa desta edição da Revista *Vitória nas Sombras* reflete o papel essencial das Operações Especiais e das Operações de Informação (OpInfo) e suas Capacidades Relacionadas à Informação (CRI). A imagem central de um soldado sobre um fundo digital, simbolizando a prontidão e a resiliência, destaca a integração entre a inteligência e as operações especiais e informacionais. Ao abrir esta revista, o leitor é convidado a compreender a complexidade das operações que a Marinha planeja e executa, reafirmando o compromisso com a defesa e a segurança nacional. Estamos diante do advento de operações integradas que moldam o futuro do combate e fortalecem a posição estratégica do Brasil no cenário global.

1. Isenção de Responsabilidade Editorial

- Esta revista é uma publicação informativa e não reflete necessariamente a opinião ou a posição oficial das Forças Armadas, da Marinha do Brasil ou de qualquer outra instituição mencionada.
- As opiniões expressas pelos autores são de sua responsabilidade e não representam necessariamente a visão desta revista.

2. Precisão e Atualização da Informação

- Envidamos esforços para garantir a precisão e a atualização das informações contidas nesta revista. No entanto, não podemos garantir que todas as informações sejam sempre completas, precisas ou atualizadas.
- Os leitores são incentivados a verificar as informações por conta própria, quando necessário.

3. Direitos Autorais

- Todos os direitos autorais do conteúdo publicado nesta revista são reservados.
- A reprodução, a distribuição ou o uso não autorizado do conteúdo sem permissão por escrito é proibida.

4. *Feedback* e Política de Comentários

- Valorizamos o *feedback* dos leitores e incentivamos comentários construtivos que farão parte de nossa edição online e da publicação seguinte.
- No entanto, nos reservamos o direito de moderar e revisar antes da publicação, excluindo quaisquer comentários que considerarmos inapropriados.

Comando Naval de Operações Especiais: integração das atividades de Operações Especiais e Operações de Informação no âmbito da Marinha do Brasil

1

Vice-Almirante (FN) Rogério Ramos **Lage**

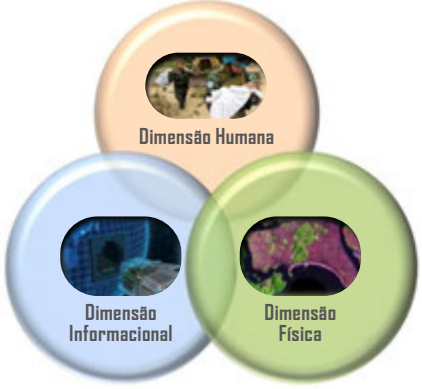
Atual Comandante do Material de Fuzileiros Navais, é graduado pela Escola Naval e realizou diversos cursos, com destaque para: Especial de Comandos Anfíbios, Aperfeiçoamento de Oficiais do Corpo de Fuzileiros Navais (CAOCFN), Paraquedista (Básico, Expedito de Salto Livre, Mestre de Salto e Precursor Paraquedista), Estado-Maior para Oficiais Superiores (C-EMOS) e Política e Estratégia Marítimas (C-PEM). Durante sua carreira, foi Comandante da Companhia de Carros de Combate, Comandante do Batalhão de Operações Especiais de Fuzileiros Navais e Comandante da Divisão Anfíbia; Subchefe de Operações de Paz do Ministério da Defesa e Subchefe de Inteligência Operacional do Comando de Operações Navais; e Adido na Adidância Naval do Paraguai. Foi Comandante Naval de Operações Especiais de setembro de 2019 a abril de 2021.

Introdução

Atualmente, os conflitos armados ocorrem de forma assimétrica, impossibilitando interpretações assentadas nos mesmos preceitos teórico-doutrinários que regeram as guerras do passado e dificultando a percepção dos limites de guerra e paz.

Nesse contexto, o Ambiente Operacional, cuja compreensão é condição fundamental para o êxito nas operações militares, pode ser caracterizado como um conjunto de fatores que interagem, de forma específica em cada situação, a partir de três dimensões: a física, a humana e a informacional. A Dimensão Física está ligada ao terreno e às condições meteorológicas; a Dimensão Humana compreende os elementos relacionados às estruturas sociais e aos comportamentos e interesses, normalmente geradores de conflito; e a Dimensão Informacional abrange os sistemas utilizados para obter, produzir, difundir e atuar sobre a informação.

Figura 1: As Dimensões do Ambiente Operacional.



Fonte: Brasil, 2018.

Vale ressaltar, ainda, a crescente utilização de ações cibernéticas ilícitas, o uso da guerra informacional e o desencadeamento de diversas atividades à margem da lei, como crimes ambientais, terrorismo e pirataria, com a finalidade de provocar desestabilização, medo e incerteza.

Nesse cenário complexo e dinâmico, é crucial o desenvolvimento do poder de combate em três vetores específicos: Operações Especiais (OpEsp), Operações de Informação (OpInfo) e Contraposição às Ameaças Híbridas.

1. Operações Especiais

Conduzidas em ambientes sensíveis, por tropa rigorosamente selecionada, treinada e equipada que emprega métodos, táticas, técnicas, procedimentos e equipamentos não convencionais, as Operações Especiais se apresentam como uma ferramenta extremamente eficiente: com suas tradicionais ações de reconhecimento especial e ações diretas e indiretas, neutralizam ameaças e contribuem para o enfrentamento dos conflitos atuais em operações no amplo espectro dos níveis de condução da guerra.

Operações Especiais podem ser realizadas tanto em tempo de paz quanto em períodos de crise ou conflito armado, em situações de normalidade institucional ou não, de forma ostensiva, sigilosa ou coberta, em áreas negadas, hostis ou politicamente sensíveis, independentemente ou em coordenação com operações realizadas por forças convencionais.

Figura 2: Tropa de Operações Especiais.

Fonte: O autor.

2. Operações de Informação

De acordo com a Doutrina de Operações de Informação (EMA-335), as Operações de Informação, cada vez mais presentes no campo de batalha, atuam:

> (...) influenciando pessoas ou grupos hostis, neutros ou favoráveis, capazes de impactar positivamente ou negativamente o alcance dos objetivos políticos e militares, bem como para comprometer o processo decisório dos oponentes ou potenciais oponentes, enquanto garantindo a integridade do nosso processo (BRASIL, 2018).

Nesse processo, é necessária uma eficiente coordenação do emprego das Capacidades Relacionadas à Informação (CRI), destacando-se as Operações Psicológicas (OpPsico) e as Ações de Guerra Eletrônica (AGE), Guerra Acústica (AGA) e Guerra Cibernética (AGCiber), a fim de atingir o efeito desejado, seja ele militar ou não.

A convergência dessas capacidades permite a manipulação de narrativas, a amplificação de mensagens e a orquestração de efeitos que se estendem além do âmbito cinético.

3. Contraposição às Ameaças Híbridas

Explorando a interconexão de diferentes aspectos do conflito moderno, o Comando de Operações Navais assim define as Ameaças Híbridas (COMOPNAVINST 30-01):

> Emprego sob medida, por ator oponente, de múltiplos instrumentos, militares ou não, como operações psicológicas, ataques cibernéticos, pirataria, ações terroristas, propaganda, contrapropaganda, desinformação, ações econômicas, crimes ambientais, interferências nas comunicações, ações de forças regulares e irregulares contra infraestruturas críticas, ataques nucleares, biológicos, químicos ou radiológicos, bem como outras atividades criminosas ou subversivas de naturezas diversas, combinando ações simétricas e assimétricas com seu efeito sinérgico, podendo atuar em ambientes físicos ou não, particularmente o informacional, direcionados a vulnerabilidades específicas do alvo visando atingir os efeitos desejados pelo agressor e, normalmente, a partir de desestabilização, medo e incerteza gerados na sociedade como um todo ou em parte dela (BRASIL, 2020).

A contraposição a essas ameaças é desafiadora, pois exige respostas coordenadas e abrangentes que levem em consideração inúmeras dimensões e métodos de influência.

Figura 3: Operações de Informação.

Fonte: O autor.

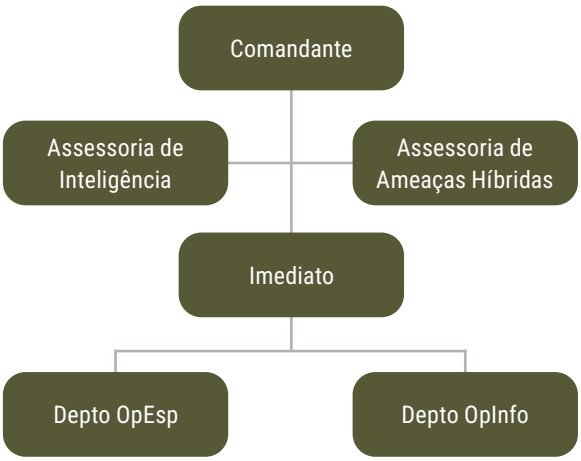
Figura 4: Contraposição às Ameaças Híbridas.

Fonte: European Parliament, 2018.

4. CoNavOpEsp – criação, organização e integração entre os departamentos

A Marinha do Brasil criou o Comando Naval de Operações Especiais (CoNavOpEsp) em 16 de agosto de 2019, centralizando os assuntos relativos a Operações Especiais, Operações de Informação e Ameaças Híbridas. Em sua estrutura organizacional, o CoNavOpEsp está alicerçado em dois departamentos, conforme ilustra a Figura 5.

Figura 5: Organograma do CoNavOpEsp.



Fonte: O autor.

O Departamento de Operações Especiais (OpEsp), além de estudar sobre o tema, tem como finalidades: assessorar o Comandante nos aspectos relativos às Operações Especiais; constituir ou compor o Estado-Maior de uma Força de Operações Especiais conjunta, combinada ou singular; e planejar e coordenar a participação da MB em operações, adestramentos e exercícios conjuntos e combinados de Operações Especiais. Para cumprir essas tarefas, o Departamento possui duas divisões subordinadas: a Divisão de Comandos Anfíbios e a Divisão de Mergulhadores de Combate. Caso necessário, é previsto que a Organização Militar (OM) receba, por destaque, militares de outras OMs, especializadas ou não.

O Departamento de Operações de Informação (OpInfo) foi constituído para tratar das principais Capacidades Relacionadas à Informação (CRI), tendo como atribuições: compor Forças-Tarefas de Guerra Cibernética singulares, combinadas ou conjuntas, quando determinado; assessorar o Comandante nos aspectos relativos às Operações de Informação; planejar e coordenar a participação da MB em operações, adestramentos e exercícios conjuntos que envolvam Operações de Informação, Operações Psicológicas, Ações de Guerra Eletrônica, Ações de Guerra Acústica e Ações de Guerra Cibernética; conduzir Ações de Guerra Cibernética de caráter operativo no âmbito da MB, particularmente as atividades de exploração e ataque; desenvolver armas cibernéticas e procedimentos para a realização de ações cibernéticas; atuar como elemento de ligação do Setor Operativo com o Comando de Defesa Cibernética; e planejar e conduzir os exercícios e adestramentos de Guerra Cibernética no âmbito da MB.

O Departamento de OpInfo possui, em sua estrutura: as Divisões de Operações Psicológicas, Produção de Informação, Relações Civis e Institucionais, e Guerra Acústica e Eletrônica, que foram criadas, principalmente, para realizar estudos e assessorar o Comandante em relação aos respectivos temas; e a Divisão de Guerra Cibernética, que atua não apenas no nível operacional, mas também no nível tático, estando previstos, em sua lotação, militares especializados para a condução de ações cibernéticas de exploração e ataque.

A sinergia entre os departamentos possibilita que ações de OpEsp de efeito cinético sejam potencializadas à medida que são orientadas para a consecução de uma meta psicológica, usada pela propaganda nos níveis político e estratégico, o que faz parte de um contexto informacional mais amplo para influenciar percepções e a opinião pública, podendo ou não ocultar o propósito, o escopo, o momento e a localização da operação.

Nesse enquadramento, as OpInfo também podem ser fortalecidas com ações de OpEsp para degradar as capacidades relacionadas à informação do oponente. Como exemplo, podem ser citadas ações diretas realizadas contra infraestruturas de Comando e Controle.

Conclusão

A criação de uma Organização Militar vocacionada para Operações Especiais e Operações de Informação responde à demanda atual relativa à crescente importância

dessas atividades que, juntas, oferecem uma abordagem estratégica poderosa para influenciar percepções, moldar narrativas e alcançar objetivos militares, além de exercerem efeito multiplicador de forças. Afinal, se o cenário é complexo, sua compreensão deve ser, necessariamente, holística, privilegiando abordagens integradas e soluções multidisciplinares.

Referências Bibliográficas

BRASIL. Marinha do Brasil. Comando de Operações Navais. **COMOPNAVINST 30-01** – Definição da expressão "Ameaças Híbridas". Rio de Janeiro, 2020.

_____._____. Estado-Maior da Armada. **EMA-335 – Doutrina de Operações de Informação**. Brasília-DF, 2018.

EUROPEAN PARLIAMENT. Directorate General for External Policies. Policy Department. **Countering hybrid threats: EU and the Western Balkans case**. Workshop, 26 February 2018. Jean-Jacques Patry and Nicolas Mazzucchi. Brussels, 2018. Disponível em: <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/603851/EXPO_STU%282018%29603851_EN.pdf>. Acesso em: 26 fev. 2024.

Figura 6: Elementos de Operações Especiais/GRUMEC.
Fonte: Acervo MB.

Operações Especiais no amplo espectro da guerra

2

Capitão de Fragata Paulo **Ricardo** Rodrigues dos Santos

É graduado em Ciências Navais pela Escola Naval. Ao longo de sua carreira, realizou diversos cursos, com destaque para: Aperfeiçoamento de Mergulhadores de Combate (MEC) para Oficiais – CAMECO, Básico de Paraquedistas (EB), Salto Livre Operacional (CFN) e Desativação de Artefatos e Explosivos – DAE (CIAMA-MB). Foi instrutor dos cursos de MEC e DAE no CIAMA. Entre as principais comissões, participou de operações internacionais (Espabras 2008, Panamax Tridente 2010, Líbano 7 e Guinex 21) e nacionais, como a Copa do Mundo 2014, os Jogos Olímpicos 2016 e a Intervenção Federal no Rio de Janeiro em 2018.

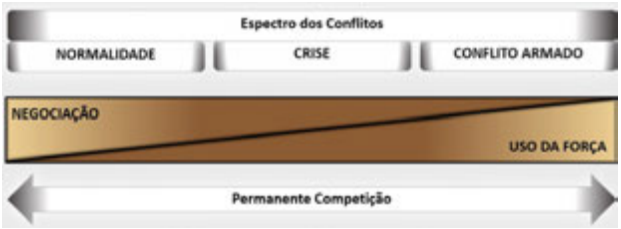
Um elemento de Operações Especiais deve, primeiramente, ter a capacidade de resistir a qualquer vicissitude que aparecer. Ele simplesmente não pode desistir. Teoricamente, a única forma de parar um Comando Anfíbio ou um Mergulhador de Combate é matando-o, porque senão ele vai continuar. Costumo dizer: rastejar é aceitável. Suar é aceitável. Sangrar é aceitável. Desistir não é aceitável. (Mergulhador de Combate da Marinha do Brasil).

Introdução

Hoje, vemos uma desconcertante diversidade de guerras separatistas, violência ética e religiosa, *coups d'État*[1], disputas de fronteiras, levantes civis, ataques terroristas empurrando ondas de imigrantes miseráveis expulsos pela guerra, hordas de traficantes de drogas por fronteiras nacionais e o uso cada vez mais irrestrito de Sistemas Aéreos não Tripulados (SARP) e Sistemas Marítimos não Tripulados (SMNT) no campo de batalha.

Diante desse amplo espectro dos conflitos (Figura 1), a Marinha do Brasil (MB) resolveu criar, em 16 de agosto de 2019, por meio da Portaria nº 232 do Comandante da Marinha, o Comando Naval de Operações Especiais (CoNavOpEsp), cujo propósito é adequar o emprego das Operações Especiais para fazer frente à evolução do ambiente operacional multifacetado com características de um mundo volátil, incerto, complexo e ambíguo (VUCA)[2], no qual há participação crescente de atores estatais e não estatais em atividades irregulares, difusas e com alto grau de letalidade.

Figura 1: Espectro dos Conflitos.



Fonte: Brasil, 2023b.

1. Histórico das Operações Especiais nos últimos 80 anos

No fim da Segunda Guerra Mundial, o primeiro-ministro do Reino Unido à época, Winston Churchill, em uma tentativa de conter o avanço do Terceiro *Reich*[3] alemão no Norte da África e da França, determinou a criação das tropas de Operações Especiais inglesas. Entre outras tarefas, a principal era tentar influenciar, treinar e conduzir a população local para lutar em uma espécie de guerrilha em prol dos aliados, criando o conceito de Ação Indireta, até hoje utilizado pelas Operações Especiais de todo o mundo.

[1] *Coup d'État*, golpe de Estado ou simplesmente golpe é, tipicamente, uma tentativa ilegal e evidente de uma organização militar ou de outras elites do governo para derrubar uma liderança incumbente. Um autogolpe é quando um líder, tendo chegado ao poder através de meios legais, tenta permanecer no poder através de meios ilegais.

[2] VUCA – acrônimo formado pelas palavras em inglês *volatility, uncertainty, complexity e ambiguity*, as quais significam, respectivamente, volatilidade, incerteza, complexidade e ambiguidade.

[3] *Reich* – termo alemão empregado para se referir a um império e/ou reino. A Alemanha nazista, comandada por Hitler, adotou a denominação Terceiro *Reich* em referência aos dois impérios germânicos anteriores: o Sacro Império Romano-germânico na Idade Média (Primeiro *Reich*) e o Império Alemão de 1871 a 1914 (Segundo *Reich*).

No Brasil, o início das Operações Especiais, então únicas na América Latina, teve papel relevante na eliminação da subversão e do terrorismo no final dos anos 1960 e no início dos anos 1970, tendo sido reconhecidas por esse fato. No final do século XX, operadores especiais foram empregados na região da Serra do Traíra, no Amazonas (Figura 2), a fim de esclarecer a conturbada situação naquela fronteira, que sofria com incursões das Forças Armadas Revolucionárias da Colômbia (FARC) e com o garimpo ilegal.

Figura 2: Operadores Especiais empregados na região da Serra do Traíra.

Fonte: Correio – o Portal de Carajás, 2022.

Na Marinha do Brasil, para os Mergulhadores de Combate (Figura 3), pertencentes ao Corpo da Armada, as Operações Especiais nasceram a partir de uma grande influência tanto da marinha americana (*U.S.Navy*) e das antigas equipes de demolição submarina (*Underwater Demolition Team* – UDT), voltadas para operações de pré-desembarque durante a Segunda Guerra Mundial, quanto dos nadadores de combate (*Nageurs de Combat*) franceses, cujas atividades se destinavam a sabotagens e ataques mergulhados a navios e portos.

Figura 3: Mergulhadores de Combate.

Fonte: War News, 2020.

Nos dias atuais, pode-se dizer que o Grupamento de Mergulhadores de Combate (GRUMEC) possui táticas, técnicas, procedimentos (TTP) e equipamentos semelhantes àqueles dos *U.S.Navy SEALS*, permitindo ações tanto no nível operacional quanto no nível tático.

Cabe ressaltar que, durante os conflitos mais recentes, como a Guerra do Iraque e a Guerra do Afeganistão, as ações se concentraram na atuação em terra. A MB, entretanto, apesar dessa influência, manteve sua essência predominantemente no meio aquático, aos moldes do *Nageur de Combat* francês.

As Operações Especiais executadas pelos Comandos Anfíbios do Corpo de Fuzileiros Navais (Figuras 4 e 5) nasceram da grande influência do Exército Brasileiro em operações de reconhecimento e contraguerrilha. Atualmente, pode-se dizer que o Batalhão de Operações Especiais do Corpo de Fuzileiros Navais (Tonelero) possui TTP e equipamentos semelhantes aos do Comando de Operações Especiais da Marinha dos Estados Unidos (U.S.MARSOC – *Marine Corps*). Ao contrário do GRUMEC, sua essência de emprego é principalmente terrestre, característica peculiar da Ação de Comandos do Exército Brasileiro.

Figura 4: Comandos Anfíbios.

Fonte: Wikipédia, 2016.

Figura 5: Operação Ágata Fronteira Norte – prisão de garimpeiros em atividade ilegal.

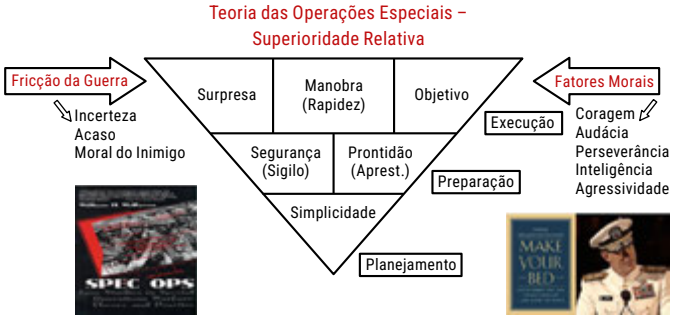
Fonte: Agência Marinha de Notícias, 2023.

2. Amplo espectro da guerra atual

Normalmente, as Operações Especiais exigem abordagens não ortodoxas, sem negar os princípios de guerra tradicionais, que são aplicados com ênfase diferente na sua combinação ou na importância relativa de cada um. Em determinadas missões ou tarefas, a surpresa alcançada por meio de rapidez, ousadia, sigilo e dissimulação, aliada a novas técnicas, táticas e procedimentos, pode ser muito mais efetiva do que as táticas convencionais (conceito de Superioridade Relativa, do Almirante SEAL William Harry McRaven, da Marinha dos Estados Unidos – Figura 6).

Não se discute, neste artigo, o conceito de Superioridade Relativa de McRaven, mas alguns pontos sobre a forma como as características das Operações Especiais (alto risco, baixa visibilidade, elevado grau de precisão, dificuldade de coordenação e apoio) e seus princípios no nível operacional (adaptabilidade, flexibilidade, integração, modularidade, restrição e seletividade) devem ser considerados no cenário atual.

Figura 6: Superioridade Relativa – Almirante SEAL William Harry McRaven.



Fonte: McRaven, 1996.

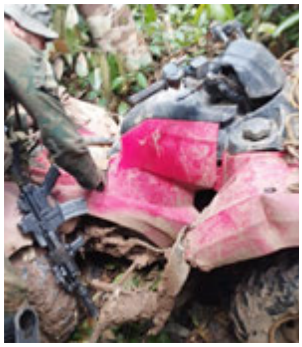
Entre as diversas realidades da MB no combate às ameaças dentro do entorno estratégico brasileiro, com atuação das OpEsp contribuindo para os Objetivos Nacionais de Defesa nesse amplo espectro da guerra atual, podem ser citados dois exemplos:

- a abordagem de navios que praticam pesca ilegal no Arquipélago de São Pedro e São Paulo por Equipes de Abordagem de Mergulhadores de Combate (Figura 7), permitindo a proteção dos recursos marinhos e da Amazônia Azul;
- neutralização, realizada por Comandos Anfíbios, de dragas e pistas de pouso clandestinas utilizadas por garimpeiros na Região Norte.

Figura 7: Abordagem de navio de pesca ilegal por Equipe de Abordagem de Mergulhadores de Combate.

Fonte: Acervo MB.

Figura 8: Neutralização de draga e pista de pouso clandestinas realizada por Comandos Anfíbios.



Fonte: Acervo MB.

3. Preponderância das Operações Especiais da MB no cenário atual

A preponderância das OpEsp reflete, principalmente, a necessidade de adaptabilidade e flexibilidade nesse ambiente difuso. O emprego das Forças de Operações Especiais (FOpEsp) tem se mostrado a forma mais adequada de combate, uma vez que é a força militar interveniente no espectro de atuação das ameaças híbridas atuais.

Como exemplo de sucesso e comprometimento das Forças Armadas Brasileiras com a defesa dos interesses nacionais e a promoção da estabilidade na região fronteiriça do País, vale destacar as Operações Conjuntas Ágata, capitaneadas pelo Ministério da Defesa, em especial a Operação Ágata Comando Conjunto Uiara, realizada de maio a junho de 2023. A participação das FOpEsp como Força Componente Conjunta, estabelecida com um Estado-Maior próprio, possibilitou uma visão completa da Área de Operações (AOp), viabilizando o emprego das tropas com o valor militar requerido, principalmente por meio de ações de Reconhecimento Especial (Rec Esp), e também como vetor essencial de emprego em situações que demandaram elevado risco, discrição e precisão.

Figuras 9 e 10: Participação das Forças de Operações Especiais da MB.

Fonte: Acervo MB.

Conclusão

A Marinha do Brasil enfrenta desafios contemporâneos relacionados a diversos atores não convencionais que se manifestam nas Águas Jurisdicionais Brasileiras. As Operações Especiais, ao integrarem tecnologias avançadas, inteligência e táticas especializadas, capacitam a Marinha a enfrentar esses desafios de maneira eficiente e coordenada.

Portanto, a necessidade de constantes investimentos em treinamento especializado, tecnologias inovadoras e inteligência estratégica são cruciais para manter a preponderância das Operações Especiais, assegurando que a Marinha esteja pronta para enfrentar os desafios presentes e futuros no cenário marítimo.

Referências Bibliográficas

AGÊNCIA MARINHA DE NOTÍCIAS. **Operação Ágata Fronteira Norte: Marinha participa de ação que prendeu 13 garimpeiros em atividade ilegal.** Por Primeiro-Tenente (RM2-T) Vanessa Mendonça Silva. Boa Vista (RR), 21 jul. 2023. Disponível em: <https://www.marinha.mil.br/agenciadenoticias/operacao-agata-fronteira-norte-marinha-participa-de-acao-que-prendeu-13>. Acesso em: 19 abr. 2024.

BRASIL. Marinha do Brasil. **Estratégia de Defesa Marítima (EDM) – EMA 310.** 1. ed. 2023a.

_____. _____. **Fundamentos Doutrinários da Marinha (FDM) – EMA 301.** 1. ed. 2023b.

_____. _____. Comando da Marinha. **Portaria nº 232, de 16 de agosto de 2019**. Cria o Comando Naval de Operações Especiais (CoNavOpEsp) e dá outras providências. Disponível em: <https://www.defesaaereanaval.com.br/naval/marinha-do-brasil-cria-o-comando-naval-de-operacoes-especiais>. Acesso em: 19 abr. 2024.

CORREIO – o Portal de Carajás. **50 anos depois, saiba como Marabá foi envolvida na Guerrilha do Araguaia**. Redação, 9 de abril de 2022. Disponível em: <https://correiodecarajas.com.br/50-anos-depois-saiba-como-maraba-foi-envolvida-na-guerrilha-do-araguaia/>. Acesso em: 19 abr. 2024.

LISBOA, R. **Operações Especiais: abordagens sobre as ações militares não convencionais**. Ed Griffo's, 2022.

MCRAVEN, William H. **Spec Ops – Case Studies in Special Operations Warfare: Theory and Practice**. New York: Presidio Press – Random House, Inc., 1996.

WAR NEWS. Página no Facebook. **Operadores SEAL, COT e GRUMEC em treinamento antiterrorismo.** Imagem publicada em 20 de abril de 2020. Disponível em: <https://www.facebook.com/100050206731857/posts/1358543294356909>. Acesso em: 19 abr. 2024.

WIKIPÉDIA. **Ficheiro: Operação Formosa 2016** (30388031181).jpg. Disponível em: <https://pt.wikipedia.org/wiki/Ficheiro:Opera%C3%A7%C3%A3o_Formosa_2016_(30388031181).jpg>. Acesso em: 19 abr. 2024.

Figura 11: MEC e Embarcação de Desembarque Pneumática (EDPN). **Fonte:** Acervo MB.

O estabelecimento da Força Conjunta de Operações Especiais nas Operações Conjuntas

3

Capitão de Mar e Guerra Marcelo de **Souza Machado**

É graduado em Ciências Navais pela Escola Naval com habilitação em Eletrônica. Realizou o Curso de Estado-Maior e o Mestrado em Ciências Militares na Academia Naval da Marinha da China (PLA Navy). Entre as principais comissões, foi Encarregado da Divisão de Convés do Navio-Patrulha Bracuí, Encarregado da Divisão Charlie de Operações Especiais do Grupamento de Mergulhadores de Combate (GRUMEC), Oficial de Operações da Missão das Nações Unidas no Nepal (UNMIN), Comandante do Rebocador de Alto-Mar Tritão, Imediato do GRUMEC, Oficial da Subchefia de Operações do Comando de Operações Navais (ComOpNav), Chefe do Departamento de Estratégia da Escola de Guerra Naval, Chefe do Departamento de Operações Especiais do Comando Naval de Operações Especiais (CoNavOpEsp) e atualmente é o Comandante do Grupamento de Mergulhadores de Combate.

Introdução

Para entender o universo em que se situam os assuntos atinentes ao instigante tema das Operações Especiais, é necessário, primeiramente, reforçar alguns conceitos importantes que proporcionam consistência para melhor compreender a abordagem proposta neste sucinto artigo, como: o que são as Operações Especiais e quem compõe as Forças de Operações Especiais.

1. As Forças de Operações Especiais

O Ministério da Defesa estabelece que as Operações Especiais sejam conduzidas por forças militares especialmente organizadas, treinadas e equipadas, e executadas em ambientes hostis, negados ou politicamente sensíveis visando atingir objetivos militares, políticos, psicossociais e/ou econômicos por meio do emprego de capacitações militares específicas não encontradas nas forças convencionais. Podem ser conduzidas de forma singular, conjunta ou combinada, normalmente interagências, em qualquer parte do espectro dos conflitos (BRASIL, 2015).

As Operações Especiais (OpEsp), quando empregadas adequadamente e em sincronia com as convencionais, tornam-se um fator multiplicador do poder de combate, oferecendo ao Comandante do Teatro de Operações/Área de Operações (ComTO/AOp) a capacidade de incrementar a iniciativa, aumentar a flexibilidade e ampliar a consciência situacional do campo de batalha, o que facilita o desencadeamento da campanha militar em consonância com a consecução dos objetivos políticos/estratégicos. Por atuarem antes, durante e após as operações convencionais, as OpEsp revestem-se de características de alto nível de risco, ensejando que o Estado-Maior Conjunto compreenda seus fundamentos básicos a fim de assessorar o ComTO/AOp na decisão sobre a melhor maneira de empregá-las na solução de um conflito.

Figura 1: Exercício de *helocasting* (infiltração de tropas especiais na água utilizando helicóptero) em Angra dos Reis/RJ.

Fonte: Acervo MB.

Portanto, em termos gerais, as Forças de Operações Especiais (FOpEsp) podem ser caracterizadas como tropas de altíssimo desempenho que possuem habilitações e especializações para realizarem missões especiais baseadas em suas capacidades específicas.

2. As Operações Especiais nas Operações Conjuntas

Em relação ao comando e à composição das Forças empregadas, as Operações Especiais podem ser classificadas como:

- singulares – desenvolvidas por apenas uma das Forças;
- conjuntas – envolvem o emprego coordenado de elementos de mais de uma Força mediante a constituição de um Comando Conjunto;
- combinadas – empreendidas por elementos ponderáveis de Forças Armadas multinacionais sob a responsabilidade de um comando único;
- interagências – envolvem as Forças Armadas e agências governamentais[1] com a finalidade de conciliar interesses e coordenar esforços para a consecução de objetivos ou propósitos convergentes que atendam ao bem comum com eficiência, eficácia, efetividade e menores custos, evitando a duplicidade de ações, a dispersão de recursos e a divergência de soluções; e
- multinacionais – constituídas pelas Forças Armadas ou por agências de dois ou mais Estados e estruturadas segundo mandato específico (das Nações Unidas, de uma organização de segurança regional ou de uma coalizão de Estados) para uma determinada situação, com missão definida por finalidade, espaço e período de tempo.

Adicionalmente, as Operações Conjuntas (OpCj) são caracterizadas pelo emprego coordenado de elementos de mais de uma Força Singular, com propósitos interdependentes ou complementares visando a um objetivo comum mediante a constituição de um Comando Operacional Conjunto.

3. Aspectos legais que regem as Operações Conjuntas

A Lei Complementar nº 136, de 25 de agosto de 2010, que alterou a Lei Complementar nº 97, de 09 de junho de 1999, entre outras determinações, conferiu às Forças Armadas (FA), como atribuições subsidiárias, preservadas as competências exclusivas das polícias judiciárias, atuar, por meio de ações preventivas e repressivas, na faixa de fronteira terrestre, no mar e nas águas interiores, independentemente de posse, propriedade, finalidade ou qualquer gravame que sobre ela recaia, contra delitos transfronteiriços e ambientais, isoladamente ou em coordenação com outros órgãos do Poder Executivo.

Até o ano de 2010, as FA, os Órgãos de Segurança Pública (OSP) e as agências governamentais realizavam, de maneira isolada e por iniciativa própria, operações na faixa de fronteira contando com os seus próprios recursos humanos e materiais, recebendo, ocasionalmente, apoio de outras instituições em caráter limitado.

Desde junho de 2011, com a criação do Plano Estratégico de Fronteiras (PEF), as FA passaram a coordenar com os entes federativos, os OSP e as agências do Estado brasileiro ações integradas contra ilícitos transfronteiriços e ambientais. Com a finalidade de combater esses ilícitos, foram adotadas as medidas preventivas e repressivas estabelecidas pelo Ministério da Defesa (MD) por meio das Operações Ágata, cuja finalidade é maximizar os efeitos das ações em ambientes distintos, buscando atividades sistematizadas e, principalmente, a evolução da interoperabilidade.

O Programa de Proteção Integrada de Fronteiras (PPIF), instituído por Decreto Federal em novembro de 2016 e alterado pelo Decreto nº 11.273, de 05 de dezembro de 2022, foi estabelecido com vistas à evolução do processo, estendendo o entendimento do conceito de região de fronteiras em relação aos delitos transnacionais e adicionando a essencial área da Plataforma Marítima, por onde escoa, aproximadamente, 95% do comércio brasileiro.

De maneira geral, o PPIF visa restringir a ocorrência de delitos transfronteiriços e ambientais nas regiões de fronteira, incluindo as águas interiores e a costa marítima, e tem como diretriz a atuação integrada e coordenada dos órgãos federais, estaduais e municipais tanto para o fortalecimento da prevenção, do controle, da fiscalização e da repressão às infrações administrativas e penais de caráter fronteiriço como para a cooperação e a integração com os países vizinhos.

4. A evolução do ambiente em que são realizadas as Operações Conjuntas

O crime organizado tem se desenvolvido e se atualizado ao longo dos anos, articulando-se, de forma sistemática,

[1]Agência, de modo geral, é a denominação dada a qualquer organização, instituição ou entidade fundamentada em instrumentos legais e/ou normativos e dotada de competências específicas, podendo ser governamental ou não, militar ou civil, pública ou privada, nacional ou internacional.

Figura 2: Grupo Especial de Retomada e Resgate – adestramento de reconhecimento hidrográfico de praias.

Fonte: Acervo MB.

em vários países da América do Sul e atuando por meio de diversas atividades, tais como produção e comercialização de drogas e tráfico de armas e munições, além de crimes transfronteiriços.

No mesmo contexto espaço-temporal, outros atores, em conjunto ou isoladamente, praticam ilícitos ambientais, como pesca predatória e ilegal, desmatamento não autorizado e garimpo ilegal, entre outros, impactando significativamente no desenvolvimento socioeconômico e provocando reflexos sociais negativos em grande parte dos países deste subcontinente, onde o crescimento da criminalidade e o esgotamento dos sistemas de segurança se tornaram problemas estruturais, desaguando na corrupção em diversos segmentos da sociedade.

Com dimensões continentais, o Brasil faz fronteira com 10 dos 12 países que compõem a América do Sul e possui um litoral de mais de 7.500 km de extensão, o que pode se ampliar ainda mais caso se considerem as baías. Estendendo-se pelos biomas da Amazônia, do Pantanal, da Mata Atlântica e dos pampas, nosso território abriga uma grande diversidade geográfica e antropológica e apresenta uma permeabilidade enorme, o que gera um grande desafio para que se consiga estabelecer um controle efetivo e perene.

Nesse contexto, foram estabelecidos quatro objetivos estratégicos para o PPIF:

I – integrar e articular ações de segurança pública da União, de inteligência, de controle aduaneiro e das Forças Armadas com as ações dos estados e municípios situados na faixa de fronteira, incluídas suas águas interiores, e na costa marítima;

II – integrar e articular com países vizinhos as ações previstas no inciso I;

III – aprimorar a gestão dos recursos humanos e da estrutura destinada à prevenção, ao controle, à fiscalização e à repressão a delitos transfronteiriços; e

IV – buscar a articulação com as ações da Comissão Permanente para o Desenvolvimento e a Integração da Faixa de Fronteira (CDIF).

Assim, as Operações Ágata valorizam o caráter interagências a fim de maximizar seus resultados, tendo se consolidado como uma ação do Ministério da Defesa para potencializar a atuação do Estado brasileiro e fortalecer a prevenção, o controle, a fiscalização e a repressão dos crimes transfronteiriços e ambientais, observando a Constituição Federal e os preceitos do Direito Internacional. Essas operações buscam, principalmente, o incremento do poder dos Órgãos de Segurança Pública nas ações contra o crime organizado e a cooperação com as agências do Estado nas esferas federal, estadual e municipal, tendo como foco o estabelecimento da presença do Estado nas regiões remotas.

5. As Forças Conjuntas de Operações Especiais

Imersas nesse cenário incerto e volátil, onde coexistem diversas ameaças difusas e multifacetadas, estão as Forças de Operações Especiais, sempre prontas e em condições de serem empregadas, de maneira singular ou conjunta, com vistas a contribuir com o estado final desejado tanto em situações de guerra como também de "não guerra", em normalidade institucional. Vale ressaltar que, embora estejamos abordando as Operações Conjuntas como conceito estabelecido, o caráter conjunto é inerente à natureza das Operações Especiais, pois elas quase sempre empregam meios terrestres, aéreos, fluviais e/ou navais, além de FOpEsp das três Forças Singulares.

Nesse sentido, faz-se mister destacar a Operação Ágata Conjunta Oeste 2023, sob o Comando do 6º Distrito Naval que, entre outras operações conjuntas já realizadas, ratificou a importância do emprego de uma Força Conjunta de Operações Especiais. Na ocasião, a Área de Operações (AOp) foi estabelecida na faixa de fronteira dos Estados de Mato Grosso e Mato Grosso do Sul com a Bolívia e com o Paraguai, ficando limitada ao norte pela cidade de Vila Bela da Santíssima Trindade-MT e, ao sul, por Mundo Novo-MS, se estendendo por 150 km para o interior do nosso território.

Essa AOp foi estabelecida devido à intenção de concentrar meios e pessoal adjudicados ao Comando

Conjunto (CCj) Oeste em área sobre a qual havia informações de possíveis ilícitos que foram mapeados durante anos de operações de inteligência, objetivando-se, com isso, aumentar a efetividade no combate a ilícitos transfronteiriços, bem como realizar uma demonstração de força para as organizações criminosas ao utilizar o princípio da massa.

É de conhecimento geral que as organizações criminosas (OrCrim), em suas diversas áreas de atuação (tráfico de drogas, armas, munições e explosivos; roubo de cargas, de veículos e de gado; lavagem de dinheiro; contrabando e descaminho de produtos diversos), utilizam vários modais de transporte para assegurar a continuidade do fluxo de material ilegal e, na região da fronteira brasileira com a Bolívia e o Paraguai, não há exceção a essa regra. Porém, devido ao fato de as Operações Conjuntas ocorrerem em situação de paz, ou seja, não haver guerra ou conflito declarado, existem nuances legais que devem ser rigorosamente observadas, sob pena de se deslegitimar todo o esforço envolvido.

Portanto, além de ser mandatório que todos os envolvidos conheçam e sigam fielmente os dispositivos legais em vigor e as regras de engajamento estabelecidas a fim de que seja assegurada a legalidade das ações durante a execução desse tipo de operação, é imprescindível que haja uma Força Conjunta de Operações Especiais à disposição para realizar ações cirúrgicas, sigilosas e oportunas em ambientes em que as forças convencionais não sejam capazes de atuar.

No caso específico da Operação Ágata Conjunta Oeste 2023, a ativação da FCjOpEsp se deu após a análise dos dados de inteligência disponibilizados pelo Comando do 6º Distrito Naval. Identificou-se a necessidade de atuar em regiões distantes e isoladas nas extremidades da AOp, em locais com fortes indícios de existência de crimes transfronteiriços na faixa sob a responsabilidade do Comando Conjunto, em coordenação com o Núcleo Especial de Polícia Marítima (NEPOM) da Polícia Federal em Guaíra-MS e com o Grupo Especial de Fronteira da Polícia Militar do Estado de Mato Grosso em Comodoro-MT (GEFRON-PMMT).

Figura 3: Operador MEC.

Fonte: Acervo MB.

Naquela oportunidade, o Comando Distrital, em contato com o Comando Naval de Operações Especiais (CoNavOpEsp), solicitou a ativação da FCjOpEsp em virtude da necessidade de coordenação das atividades de tropas de Operações Especiais, o que se materializou na força composta por elementos de Operações Especiais do CoNavOpEsp, do Batalhão de Operações Especiais de Fuzileiros Navais (Batalhão Tonelero), do Grupamento de Mergulhadores de Combate (GRUMEC) e do Esquadrão Aeroterrestre de Salvamento (EAS). Essa composição proporcionou a capacidade de realização de ações de reconhecimento especial, ações diretas, operações psicológicas e ações de guerra cibernética conduzidas pelos destacamentos de guerra cibernética do CoNavOpEsp, sediado na cidade do Rio de Janeiro.

As diversas ações não convencionais levadas a cabo pela FCjOpEsp geraram inúmeros prejuízos ao crime organizado, materializados na degradação da estrutura de apoio logístico, como a inutilização de pistas de pouso, a neutralização e a destruição de balsas e chatas, entre outros meios, além da redução das atividades ilegais em consequência da dissuasão.

Numa visão geral daquela Operação, embora não seja possível precisar os danos causados ao crime organizado pela dissuasão, cujo valor é intangível, observa-se que o saldo é extremamente positivo, uma vez que as apreensões e os prejuízos às atividades ilegais alcançaram o montante aproximado de R$ 46.000.000,00 e o custo da operação, R$ 5.000.000,00, demonstrando um percentual muito favorável quando comparados o investimento e o valor dos resultados tangíveis.

Neste ponto, é importante ressaltar que a interoperabilidade é um ponto crucial a ser alcançado nas operações dessa magnitude. No caso em questão, as operações das aeronaves da Força Aérea Brasileira P-3 Orion, E-99 e A-29, em coordenação com o EAS, foram fundamentais para que a FCjOpEsp realizasse uma operação com o apoio da Força Aérea Componente (FAC) e do GEFRON-PMMT nos arredores da cidade de Comodoro-MT a fim de efetuar ações de repressão contra as OrCrim que fazem uso das diversas pistas de pouso existentes na região. Tamanho foi o nível de coordenação e interação que os oficiais da FAB envolvidos pontuaram que aquele poderia ser um modelo interessante a ser adotado em outras Operações Conjuntas que empregassem meios da FAC, nas quais as unidades de Operações Especiais em terra seriam vetoradas pelas aeronaves de monitoramento em coordenação com as aeronaves de interceptação de modo a direcionar o Tráfego Aéreo Desconhecido (TAD) para pouso e consequente apreensão por elementos de OpEsp no solo.

Conclusão

No atual ambiente informacional em que vivemos, a troca de informações de inteligência entre as Forças, os OSP e as agências são imprescindíveis para que se consiga ampliar conhecimentos essenciais sobre áreas que abrigam ilícitos e para propiciar a produção de novos conhecimentos que permitam ações eficazes.

A confiança mútua necessária ao fluxo de informações geralmente se torna mais forte com o passar do tempo e a execução de tarefas em conjunto. Assim, para que essa relação entre os envolvidos seja mais intensa, é importante que o contato ocorra dentro de uma moldura temporal que permita criar uma atmosfera de confiança em tempo hábil – preferencialmente na fase de preparação – para que haja uma melhor consciência situacional já no início da operação, proporcionando maior efetividade nas ações.

Figura 4: Grupo Especial de Retomada e Resgate – adestramento mergulhado.

Fonte: Acervo MB.

Dessa forma, é necessário que a sociedade possa contar com Forças Armadas capazes de atuar para garantir a manutenção da soberania da pátria, seja em situação de guerra ou de normalidade institucional.

O estabelecimento das Forças Conjuntas de Operações Especiais tem se demonstrado imprescindível nas Operações Conjuntas atuais, possibilitando que ações sensíveis, necessárias ao atingimento do estado final desejado, sejam executadas de maneira adequada e aceitável. As Operações Conjuntas constituem um importante elemento e vetor essencial de emprego em situações de elevado risco, pois atuam com discrição e precisão, o que não seria possível apenas com o emprego das forças convencionais.

Referências Bibliográficas

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Glossário das Forças Armadas** (MD35-G-01). 5. ed. 2015. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf>. Acesso em: 22 abr. 2024.

_____. Presidência da República. **Decreto nº 11.273**, de 05 de dezembro de 2022. Altera o Decreto nº 8.903, de 16 de novembro de 2016, que institui o Programa de Proteção Integrada de Fronteiras e organiza a atuação de unidades da administração pública federal para sua execução. Disponível em: <https://legis.senado.leg.br/norma/36563871/publicacao/36564045>. Acesso em: 08 abr. 2024.

_____._____. **Lei Complementar nº 136**, de 25 de agosto de 2010. Altera a Lei Complementar nº 97, de 9 de junho de 1999, que dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas, para criar o Estado-Maior Conjunto das Forças Armadas e disciplinar as atribuições do Ministro de Estado da Defesa. Disponível em: <https://legis.senado.leg.br/norma/572891/publicacao/15755898>. Acesso em: 08 abr. 2024.

Figura 5: Operação ribeirinha no Pantanal com equipamento de circuito fechado (FROGS).
Fonte: Acervo MB.

A eficiência multidimensional do Grupo de Operações Especiais em operações de alta complexidade

4

Capitão de Fragata (FN) Hugo Marcio Lima **Godinho**

Graduado pela Escola Naval, atualmente é Imediato do Batalhão de Operações Especiais de Fuzileiros Navais. Ao longo de sua carreira, realizou diversos cursos, entre os quais: Aperfeiçoamento de Oficiais do Corpo de Fuzileiros Navais (CAOCFN), Estado-Maior para Oficiais Superiores (CEMOS), Especial de Comandos Anfíbios (C-Esp-ComAnf), Básico Paraquedista (C-Exp-Pqdt), Expedito de Mergulhador Autônomo com Circuito Fechado (C-Exp-MAut-GAS) e Especial de Salto Livre (C-Esp-SaL). Principais comissões: Comandante da Companhia de Reconhecimento do BtlOpEspFuzNav, Encarregado do Curso Especial de Comandos Anfíbios, Oficial de Operações do BtlOpEspFuzNav e Oficial de Logística do BtlOpEspFuzNav.

Introdução

No complexo e dinâmico cenário das operações militares contemporâneas, a necessidade de um comando especializado e adaptável nunca foi tão evidente. É nesse contexto que surge o Grupo de Operações Especiais (GOpEsp), uma organização por tarefas projetada para enfrentar desafios que transcendem a mera aplicação de força, requerendo elevado grau de planejamento, coordenação e execução. A criação do GOpEsp responde a uma série de critérios essenciais que denotam a singularidade de sua missão e o valor inestimável que traz para o teatro operacional, impactando, inclusive, no nível político.

As operações realizadas pelo GOpEsp, como a Ágata Fronteira Norte e a Ágata Oeste, exemplificam sua capacidade multifacetada de enfrentar desafios imensos com agilidade e proficiência. Nessas operações, a combinação de inteligência, reconhecimento, vigilância e ação direta demonstrou a habilidade do GOpEsp de se integrar e coordenar com outras agências governamentais, maximizando o impacto de suas ações enquanto assegurava uma operação legal e efetiva.

Este artigo busca explorar a estrutura, a finalidade, as vantagens e o emprego do GOpEsp em situações reais, destacando como essa organização por tarefas não apenas responde às exigências operacionais complexas dos dias atuais, mas também prepara o caminho para as soluções futuras.

1. Estrutura e finalidade do Grupo de Operações Especiais

O GOpEsp é composto por um ou mais Destacamentos de Operações Especiais (DstOpEsp) que proporcionam uma ampliação significativa nas capacidades de planejamento, comando e controle. Representa a quintessência da estrutura de emprego de elementos de Operações Especiais, configurando-se como uma organização por tarefas. Essa configuração engloba elementos de comando, execução e apoio, delineando-se como a estrutura ideal para enfrentar desafios operacionais de alta complexidade.

A operacionalização do GOpEsp pressupõe uma elevação na capacidade de planejamento, coordenação, controle e execução, tanto operativa quanto logisticamente, por meio de uma estrutura que inclui os seguintes elementos: de Estado-Maior (EM) especializados em Operações Especiais (OpEsp), de Comando e Controle (C2) e de Tecnologia e Informação (TI).

Com um Estado-Maior composto por militares especializados em OpEsp, o grupo possui uma capacidade inigualável de planejamento conforme o Processo de Planejamento Militar (PPM).

2. Critérios para o emprego do GOpEsp

A necessidade do emprego de um GOpEsp pode ser determinada por uma série de critérios, refletindo a complexidade e os desafios das missões enfrentadas. Um indicativo chave é a grande probabilidade de que seja necessário empregar simultaneamente mais de um Destacamento de Operações Especiais visando maximizar a eficácia operacional por meio de uma abordagem coordenada. Ademais, operações que se estendem por períodos médios a longos, caracterizadas por alto risco e complexidade, também sinalizam a necessidade de habilidades especiais em planejamento e execução, exigindo um comando especializado.

Além disso, a grande probabilidade de que as operações especiais futuras sejam planejadas, preparando o terreno para ações subsequentes com antecedência, reforça a importância de uma organização especializada. A disponibilidade de pessoal habilitado em Operações Especiais é essencial para enfrentar missões de alta complexidade, assim como uma razoável necessidade de apoio logístico às Operações Especiais é crucial para garantir a sustentação das missões em termos de recursos e suprimentos. Juntos, esses fatores evidenciam a importância estratégica do emprego de Grupos de Operações Especiais em contextos operacionais desafiadores.

3. Vantagens operacionais do GOpEsp

A implementação de um Grupo de Operações Especiais introduz uma série de vantagens operacionais que complementam os critérios previamente destacados para sua necessidade. Essas vantagens englobam desde o aprimoramento no planejamento até a agilização de respostas em situações críticas, ilustrando o papel vital do GOpEsp na eficácia e na eficiência das operações militares especializadas.

Primeiramente, o aprimoramento no planejamento de Operações Especiais é notável, resultando em uma melhoria significativa na qualidade dos planos. Isso é possível graças à expertise do Estado-Maior dedicado exclusivamente às Operações Especiais, cujo nível de especialização e foco eleva a qualidade do planejamento e da execução das missões. A implementação do GOpEsp também amplia a capacidade de comando e controle e a consciência situacional por meio do Centro de Comando de Operações Especiais, potencializando o entendimento das circunstâncias operacionais e a capacidade de resposta das tropas de Operações Especiais.

A desoneração do Estado-Maior do Comando Apoiado, ao transferir diversas tarefas operacionais para o GOpEsp, permite que o Comando Apoiado se concentre em funções mais críticas, otimizando a distribuição de responsabilidades e melhorando a eficiência geral das operações. Essa realocação de tarefas acelera o Ciclo de Observação, Orientação, Decisão e Ação (OODA), o que propicia uma resposta estratégica mais rápida e efetiva, essencial em ambientes operacionais dinâmicos e desafiadores.

Adicionalmente, o GOpEsp aprimora a capacidade de resposta em situações de emergência, permitindo uma solução coordenada e controlada de crises que envolvam tropas de Operações Especiais. Com a autorização do Comando Apoiado, o GOpEsp assume um papel central na gestão de situações emergenciais, demonstrando sua importância na manutenção da ordem e na resposta efetiva a incidentes críticos. Por fim, a melhoria no fluxo de informações, que facilita a comunicação eficiente entre as tropas de Operações Especiais e o Estado-Maior do Comando Apoiado, otimiza a operacionalização das missões, assegurando que as informações críticas sejam compartilhadas de forma ágil e precisa, o que potencializa o sucesso das operações.

Essas vantagens operacionais reforçam o valor do GOpEsp não apenas em termos de capacidades táticas dos DstOpEsp, mas também na promoção de uma gestão e uma execução mais eficientes das operações complexas e de alto risco, estabelecendo o GOpEsp como um componente que potencializa o sucesso das missões de Operações Especiais.

4. Emprego do GOpEsp em situações reais

4.1. Operações Ágata Fronteira Norte

No mês de maio de 2023, os conflitos entre os garimpeiros e os indígenas passaram a ser evidentes, ocasionando mortes e violência dos dois lados. Com a escalada da crise, uma nova ação de governo instituiu o Decreto nº 11.575, de 21 de junho de 2023, que amplia o escopo da atuação do Ministério da Defesa, torna as ações mais repressivas e concede novos poderes aos militares no combate às ações ilegais.

Nesse cenário, foi estabelecido um Comando Conjunto sob a chefia do Comandante Militar da Amazônia, que estabeleceu suas Forças Componentes com o GOpEsp subordinado à Força Naval Componente.

Figuras 1 e 2: Destruição de equipamentos e infraestruturas de garimpo ilegal dentro da terra indígena ianomâmi.

Fonte: Acervo do BtlOpEspFuzNav.

A missão do GOpEsp era multifacetada: desde realizar ações de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA) e atacar diretamente as estruturas e o pessoal envolvido com garimpo ilegal, até apoiar as agências governamentais com logística, inteligência, comunicações e instrução. O GOpEsp foi encarregado, ainda, de formar uma Força de Reação para enfrentar a emergência em saúde pública e combater o garimpo ilegal na terra indígena ianomâmi, tornando-se um dos pilares das operações do Comando Conjunto.

Para cumprir essas missões, o GOpEsp organizou seu Estado-Maior com quatro militares, que ficaram responsáveis por: Pessoal/Logística, Comunicações/Inteligência, Operações e Comando do Grupo. Para complementar essa equipe, quatro auxiliares supervisionavam as redes de comunicação durante a operação, acompanhados por um gerente-geral de material e um ajudante. No campo, o GOpEsp contava com dois Grupos de Comandos Anfíbios (GruCAnf), cada um com 12 militares, e um Destacamento de Mergulhadores de Combate (DstMeC) com oito militares.

Desenvolvida no coração da selva amazônica, no estado de Roraima, dentro da Reserva Indígena Ianomâmi, a operação enfrentou desafios imensos. A densa vegetação, as condições meteorológicas adversas com chuvas frequentes, as dificuldades de apoio e resgate, as doenças tropicais e a dependência de meios aéreos devido às vastas distâncias já tornavam a operação extraordinariamente complexa. A tarefa de desmantelar os garimpos ilegais, com o apoio de várias agências governamentais em uma terra indígena, intensificou ainda mais a necessidade de mobiliar a estrutura do GOpEsp.

Figura 3: DstOpEsp se preparando para infiltração aérea na Operação Ágata Fronteira Norte.

Fonte: Acervo do BtlOpEspFuzNav.

A coordenação com a Polícia Federal, a Fundação Nacional dos Povos Indígenas (Funai), a Secretaria de Saúde Indígena (Sesai) e o Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama) não apenas ampliou a consciência situacional, mas também conferiu legalidade às operações. Em cada incursão, equipes do Ibama e da Polícia Federal acompanhavam os DstOpEsp a fim de identificar crimes ambientais ou federais *in loco*, proceder com as ações legais necessárias e contribuir para a desarticulação dos garimpos.

Durante essa operação, o GOpEsp assegurou uma supervisão contínua das equipes no terreno por meio de uma vasta rede de comunicações – incluindo *SpotX*[1], comunicação HF (voz e dados), mensagens instantâneas do tipo *flash*, comunicação satelital (voz e dados) e *StarLink*[2] – que possibilitou o envio de fotos e vídeos. Essa capacidade multifacetada permitiu ao Comandante da Força-Tarefa e ao seu Estado-Maior monitorar constantemente as equipes e suas atividades. A célula de operações se dedicou ao planejamento das fases seguintes e à coordenação de múltiplas operações simultâneas, incluindo Ações Cívico-Sociais (ACISO) ao longo da região do Baixo Catrimani e as operações do Grupo de Trabalho (GT) Ribeirinho.

Desde o início das operações, o Estado-Maior do GOpEsp garantiu um acompanhamento contínuo dos destacamentos no terreno, mantendo um estado de prontidão constante que incluiu a ativação de uma cadeia de evacuação e um grupo de reação em alerta prontos para responder a qualquer emergência. A flexibilidade e a agilidade no planejamento foram essenciais, especialmente diante de variáveis imprevisíveis, como condições meteorológicas adversas, necessidade de apreensão de material ou urgência de ajustes táticos devido à permanência prolongada ou à retirada antecipada do terreno. Essa capacidade de adaptação rápida, crucial em ambientes operacionais dinâmicos, foi significativamente aprimorada pela estrutura organizacional do GOpEsp. A tomada de decisões rápidas e eficientes, frequente em situações novas e desafiadoras, destacou a importância da existência do GOpEsp, tornando o processo decisório mais eficaz e contribuindo para o sucesso das missões.

O aprimoramento no planejamento e a eficiência no fluxo de informações com o Estado-Maior da Força-Tarefa e com as agências envolvidas destacaram-se como vantagens críticas do emprego do GOpEsp. Tais aspectos contribuíram para uma execução mais segura das missões por estarem sempre cerrados com o Estado-Maior do escalão superior, otimizando a mobilidade dos grupos de reação e evacuação.

[1] *SpotX* é um comunicador satelital bidirecional que permite a comunicação de texto em locais remotos ou áreas sem cobertura de rede celular. O dispositivo, projetado para oferecer segurança e conectividade em aventuras ao ar livre, operações em áreas isoladas e situações de emergência, tem funcionalidades como envio e recebimento de mensagens de texto, SOS de emergência com rastreamento de localização em tempo real e compartilhamento de coordenadas, garantindo uma linha de comunicação vital com equipes de apoio, agências de resgate e outros elementos da equipe em qualquer lugar do mundo, independentemente da disponibilidade de sinal de celular.

[2] *Starlink* é um serviço de internet via satélite cujo objetivo é fornecer conexão com alta velocidade, baixa latência e cobertura global, especialmente em áreas rurais e remotas onde o acesso convencional à internet é limitado ou inexistente. Utilizando uma constelação de satélites em órbita baixa da Terra (LEO), o *Starlink* busca revolucionar a conectividade ao redor do mundo ao permitir comunicações eficientes e rápidas para usuários individuais, empresas e operações estratégicas em locais isolados.

Nos destacamentos de Operações Especiais, os resultados foram notavelmente expressivos. A profundidade dos levantamentos de inteligência, a precisão na execução dos planos e a rapidez nas tomadas de decisão levaram a conquistas excepcionais, elevando a estima da Marinha do Brasil perante o Exército, a Força Aérea, o Ministério da Defesa e outras agências governamentais.

No total, o GOpEsp realizou 12 operações significativas na área de operação, abrangendo resgates e segurança, coleta de inteligência e, em sua maioria, combate ao garimpo ilegal. Os resultados demonstraram uma marcante redução das atividades ilegais, atestando a eficácia da operação.

Um momento particularmente impactante foi a operação de resgate em Parima[3], na noite de 03 de julho de 2023. Após um confronto que resultou em cinco feridos por armas de fogo, incluindo um homem, uma mulher e três crianças, além de uma equipe de saúde local em situação de risco e isolamento, a missão foi acionada para assegurar a área, dar segurança à equipe isolada e prestar socorro aos feridos. Graças à sua robusta capacidade de combate e à habilidade para operações noturnas, um Grupo de Comandos Anfíbios da Marinha do Brasil, que nucleava um dos DstOpEsp, garantiu a segurança dos feridos e da equipe médica em uma circunstância de elevado perigo. Vale destacar a qualidade dos especialistas em saúde que estavam tecnicamente prontos e com seu material no estado da arte para atender aos vitimados.

Figura 4: Operação de resgate de indígenas feridos na região do Parima.

Fonte: Acervo do BtlOpEspFuzNav.

Após o acionamento para a operação de resgate em Parima, o GOpEsp rapidamente mobilizou sua estrutura de Comando e Controle, compilou e forneceu todas as informações necessárias para a ação iminente. O Destacamento de Operações Especiais designado para executar a tarefa foi ágil: estava pronto para se infiltrar de helicóptero – posicionado na porta da aeronave em menos de 20 minutos –, equipado com todos os dados relevantes e plenamente capaz de cumprir a missão. Essa prontidão exemplar foi possível graças à constante manutenção de alerta das equipes do GOpEsp, que prosseguiam com ensaios e preparações intensivas mesmo na ausência de operações programadas. Esse estado de prontificação assegurou que, no momento crucial, o destacamento estivesse não apenas preparado taticamente, mas também integralmente informado e equipado para realizar o resgate com sucesso, evidenciando a eficiência e a eficácia do GOpEsp em emergências.

Figura 5: Resgate da equipe de saúde em situação de risco e isolamento após estabelecimento da segurança no Parima.

Fonte: Acervo do BtlOpEspFuzNav.

Essa operação não apenas salvou vidas, mas também foi reconhecida em nível nacional, resultando em homenagens aos militares envolvidos pelo Ministério da Defesa. Isso reforça o compromisso do GOpEsp com a excelência operacional e a prontidão inabalável, além de comprovar o impacto positivo no nível político das ações e decisões oportunas do GOpEsp.

4.2. Operação Ágata Oeste

Essa operação, realizada entre 17 e 28 de setembro de 2023, diferiu significativamente da anterior em duração e na abordagem tática empregada. Devido ao ambiente vigiado por olheiros, não foi possível utilizar efetivos completos ou manter os DstOpEsp na mesma cidade onde as ações seriam executadas. Assim, tornou-se essencial adotar técnicas variadas de despistamento e divisão do destacamento em pequenas equipes para preservar o elemento surpresa das operações.

A descentralização imposta pelo ambiente operacional elevou os desafios de comando e controle, tornando indispensáveis as interações com outras agências, especialmente para a obtenção de dados de inteligência que se provaram fundamentais para o sucesso das operações. Diferentemente da Operação Ágata Fronteira Norte, o Grupo de Operações Especiais (GOpEsp) estabeleceu sua base em Iguatemi, no Mato Grosso do Sul, enquanto as ações se desdobravam nas cidades próximas à fronteira com o Paraguai, como Mundo Novo, Guaíra, Terra Roxa e Mercedes, onde foram empregadas táticas de infiltração terrestre, aquática ou uma combinação das duas.

[3]A região do Parima fica dentro da terra indígena ianomâmi, na área do Alto Catrimani, extremo norte do Brasil. É uma vasta extensão territorial que abrange partes dos estados de Roraima e Amazonas, representando uma das maiores reservas indígenas do País. O território é caracterizado por biodiversidade rica e ecossistemas sensíveis, incluindo florestas tropicais, rios e montanhas. É uma região de grande importância cultural e ambiental para o povo ianomâmi, uma das maiores comunidades indígenas relativamente isoladas da América do Sul, conhecida por seu modo de vida tradicional e profunda conexão com a terra.

A colaboração com agentes do Núcleo Especial de Polícia Marítima[4] (NEPOM), atuantes na região, foi essencial para o delineamento das tarefas. O GOpEsp, após processar as informações recebidas e conduzir análises, solicitava a aprovação do Comando da Força-Tarefa para prosseguir com as operações, uma dinâmica que exigia tomadas de decisão e aprovações em tempo recorde, dada a imediata execução das ações propostas.

Figura 6: Militares do DstOpEsp e agente do NEPOM prontos para iniciar infiltração aquática.

Fonte: Acervo do BtlOpEspFuzNav.

A necessidade de decisões ágeis, capazes de surpreender o crime organizado e transfronteiriço, evidenciou a complexidade da operação. A região, com seu vasto número de colaboradores do crime organizado prontos para denunciar movimentações, impôs um desafio constante. A estrutura operacional do GOpEsp provou sua eficácia ao estreitar a cooperação com agências governamentais, otimizar a logística de transporte, acelerar o fluxo de informações e aprovações e manter um controle rigoroso das diversas ações ocorrendo simultaneamente na região.

O impacto da operação foi notável. Ao longo de aproximadamente uma semana, o GOpEsp realizou várias apreensões significativas, incluindo embarcações, motores, cargas de cigarros e um caminhão baú, demonstrando a eficácia e a importância do emprego das Operações Especiais no combate ao crime organizado na região fronteiriça com o Paraguai.

Figuras 7 e 8: Apreensão realizada por DstOpEsp e NEPOM durante a Operação Ágata Oeste.

Fonte: Acervo do BtlOpEspFuzNav.

Conclusão

A análise detalhada da estrutura, da finalidade, das vantagens e do emprego em situações reais do GOpEsp destaca sua importância indiscutível no aprimoramento das Operações Especiais da Marinha do Brasil. O GOpEsp, com sua capacidade de planejamento detalhado, execução eficiente e coordenação ágil, tem se mostrado vital para enfrentar desafios operacionais complexos com precisão e profissionalismo.

As operações Ágata Fronteira Norte e Ágata Oeste, entre outras, não apenas demonstraram a versatilidade e a eficácia do GOpEsp, mas também reafirmaram a importância de uma abordagem dinâmica e adaptável diante das ameaças e dos desafios contemporâneos. O sucesso do GOpEsp nas operações discutidas ilustra claramente o valor de um comando especializado e de um Estado-Maior altamente capacitado, enfatizando a necessidade de contínua evolução e adaptação às novas tecnologias, às doutrinas operacionais e aos cenários de ameaças.

Olhando para o futuro, é imprescindível que o GOpEsp continue a inovar e a incorporar novas capacidades, como as tecnologias emergentes em comunicações, inteligência e reconhecimento, garantindo, assim, a manutenção de sua superioridade tática.

Além disso, a experiência acumulada nas operações reais deve ser sistematicamente analisada para extrair lições aprendidas, promovendo uma cultura de melhoria contínua. Isso inclui aperfeiçoar a cooperação interagências e a integração com outras forças e organizações, o que é essencial para o sucesso em operações multifacetadas e em ambientes operacionais cada vez mais complexos.

Em suma, o Grupo de Operações Especiais se torna uma peça-chave para o emprego em situações mais complexas, garantindo que nossas unidades de Operações Especiais continuem prontas para enfrentar os desafios do presente e do futuro com a máxima efetividade.

[4] O NEPOM é uma unidade da Polícia Federal do Brasil especializada em operações de segurança e vigilância nas áreas marítimas e fluviais do País. Desempenha um papel crucial no combate a crimes transfronteiriços e atividades ilegais, como contrabando, tráfico de drogas, imigração ilegal e pesca irregular, operando em estreita colaboração com outras agências de segurança nacionais e internacionais.

Referências Bibliográficas

BRASIL. Marinha do Brasil. Agência Marinha de Notícias. **Marinha participa de resgate em região isolada de Roraima durante Operação Ágata**. Disponível em: <https://www.marinha.mil.br/agenciadenoticias/marinha-participa-de-resgate-em- regiao-isolada-de-roraima-durante-operacao-agata>. Acesso em: 20 mar. 2024

_____._____. Comando do Desenvolvimento Doutrinário do CFN. **Nota Doutrinária n° 10**: Emprego de Destacamentos de Operações Especiais nos Grupamentos Operativos de Fuzileiros Navais. 2022.

_____._____. Corpo de Fuzileiros Navais. Batalhão de Operações Especiais de Fuzileiros Navais. **Relatório da Operação Ágata Fronteira Norte**. 2023.

_____. Ministério da Defesa. **Glossário das Forças Armadas**. 4. ed. Brasília-DF, 2007.

_____. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. **Decreto nº 11.575**, de 21 de junho de 2023. Altera o Decreto nº 11.405, de 30 de janeiro de 2023, para dispor sobre a atuação do Ministério da Defesa no enfrentamento da Emergência em Saúde Pública de Importância Nacional e no combate ao garimpo ilegal no território Yanomami. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11575.htm>. Acesso em: 13 abr. 2024.

Figura 9: ComAnf Adestramento.
Fonte: Acervo MB.

O Suboficial na Força Conjunta de Operações Especiais

5

Suboficial Fuzileiro Naval (IF) Jamilson **Coimbra** Cunha

Ingressou na MB em 1994 por meio do Curso de Formação de Soldado Fuzileiro Naval no Centro de Instrução de Brasília. Atualmente, exerce a função de SOMor do Comando Naval de Operações Especiais. Entre os cursos realizados, destacam-se: Curso Especial de Comandos Anfíbios; Estágio de Qualificação de Segurança Pessoal no GSI (Brasília-DF), onde foi Instrutor de Armas e Tiro; Curso Especial de Preparação para Suboficial-Mor (CIAA); e Curso de Assessoria em Estado-Maior para Suboficiais Fuzileiros Navais (CIASC). Realizou, ainda, o *Basic Instructor Course* no WHINSEC (Georgia, EUA), onde foi instrutor durante dois anos do Curso de Analista de Inteligência contra Ameaças Transnacionais (*Transnational Threats Network Intelligence Analysis* – T2NIA); e concluiu com aproveitamento os Cursos *Civil-Military Coordination in Peace Operations e Humanitarian Relief Operations no Peace Operations Training Institute* (POTI).

Introdução

À medida que a cultura militar continua a evoluir, Sargentos e Suboficiais enfrentam diversos desafios que, se não forem abordados adequadamente, podem prejudicar o futuro desenvolvimento dos graduados nas Forças Armadas (FFAA), em particular nas Forças de Operações Especiais (ForOpEsp).

Figura 1: Força Conjunta de Operações Especiais na Operação Ágata Amazônia.

Fonte: O autor.

Esses desafios surgem na forma de perguntas fundamentais: Como melhorar a comunicação? Como aproveitar a tecnologia de forma eficaz? De que forma podemos aumentar nossa resiliência? Como manter nossa proficiência tática e técnica e, ao mesmo tempo, instilar em nós mesmos e em nossos soldados os valores éticos essenciais para manter a coesão em diversos ambientes? Superar esses desafios requer o reconhecimento de áreas de melhoria e a adaptação a elas.

O objetivo deste artigo é esclarecer o papel do Suboficial na Força Conjunta de Operações Especiais e destacar as tendências contemporâneas identificadas em nosso contexto estratégico. A discussão também se concentra na utilização de Praças em funções de grande relevância com base nas melhores práticas das doutrinas aplicadas aos graduados pela Organização das Nações Unidas (ONU) e pela Organização do Tratado do Atlântico Norte (OTAN), tendo como referência a publicação *Non-Commissioned Officer – Professional Military Education: Reference Curriculum* (NATO, 2014), e por países com reconhecida excelência militar que se destacam em cenários de treinamento conjunto específico, exercícios combinados ou operações conjuntas, como os Estados Unidos e a Inglaterra.

Além disso, este artigo apresenta um curso de ação recomendado para preparar o Suboficial para uma função-chave – Auxiliar de Operações – de forma que ele se torne um multiplicador de força e conhecimento valioso para a sua unidade. São utilizados como referências os documentos: *Battle Staff NCO Review: NCO Tactical Command Post SOP* (CASTIN, 2003), *FM 6-0: Commander and Staff Organization and Operations* (U.S. ARMY, 2014) e The Staff Noncommissioned Officer's Handbook (TAFT, 2016).

Historicamente, na cultura das Forças Armadas Brasileiras, Praças em funções de liderança não ultrapassaram o nível tático, seja comandando Grupos de Combate, Equipes de Reconhecimento ou Equipes de Ação de Comandos. Ao progredir em suas carreiras e alcançar as graduações de 1º Sargento e Suboficial, Praças

frequentemente assumem funções de adjuntos e auxiliares no Estado-Maior da unidade ou em exercícios. No entanto, com a introdução da função de Suboficial-Mor na Marinha do Brasil em 2015 (BRASIL, 2015; 2019a) e da função de Adjunto de Comando no Exército Brasileiro em 2016 (BRASIL, 2019b), uma nova abordagem para o uso da liderança dos graduados foi implementada.

Todavia, essa iniciativa ainda não está completamente consolidada na cultura militar do nosso País. É essencial identificar áreas nas quais esse tipo de liderança pode ser aplicado para aumentar a eficiência de nossos militares em exercícios e operações. Isso deve ser considerado um aspecto relevante a ser seguido em nosso contexto estratégico e um desafio que requer estudo e aprimoramento contínuos, tendo em vista, especialmente, a importância do Brasil na América Latina e em associações e acordos internacionais com outros países.

1. O Suboficial de Operações da Força Conjunta de Operações Especiais

As normas que tratam dos Comandos Conjuntos, disponibilizadas pelo Ministério da Defesa (MD), não definem explicitamente os papéis individuais de Suboficiais (SO) e Sargentos (SG) no Estado-Maior, geralmente deixando essa responsabilidade a cargo do Comando da Célula (D-10, D-20, D-30, etc.) e das publicações correspondentes.

As funções das Praças no processo de planejamento militar de cada Força são definidas de forma genérica com a incumbência de auxiliar os Oficiais em suas atribuições. Segundo a Organização Geral para o Serviço da Armada (OGSA), "os Suboficiais serão auxiliares diretos dos Oficiais em todos os atos de serviço e na execução das tarefas que aqueles dirigirem" (BRASIL, 2009).

Em contraste, a função de liderança de Suboficiais e Sargentos, exemplificada pelas normas do Exército dos Estados Unidos (U.S. ARMY, 2017; 2020), define o SO de Operações como um líder sênior que supervisiona as Praças e assessora o Oficial de Operações, além de ter a responsabilidade de liderar, orientar, treinar, desenvolver procedimentos operacionais padrão da unidade e garantir o cumprimento dos padrões e da disciplina (U.S. ARMY, 2017). Nesse contexto, cabe ao Suboficial de Operações supervisionar as ações do Estado-Maior depois de receber a orientação do Oficial de Operações, fornecendo conselhos para conduzir as operações do Estado-Maior em direção ao objetivo da missão.

No Brasil, tanto na Marinha quanto no Exército, o papel do Auxiliar de Operações, desempenhado por um Sargento ou um Suboficial, é reportar-se ao Oficial de Operações e auxiliá-lo em suas tarefas. Não havia contemplação das Forças de Operações Especiais atuando em nível tático-operacional ou em um comando de Força, a não ser por meio da participação do Oficial de Ligação de Operações Especiais (OLigOpEsp). No entanto, a introdução de uma Força Conjunta de Operações Especiais nas normas MD30-M-01 (BRASIL, 2020) trouxe responsabilidades condizentes com o emprego dessas forças em outros países.

Portanto, as áreas de conhecimento precisam ser aprimoradas para atender a essas novas demandas. Tanto Praças quanto Oficiais de Operações Especiais devem ser preparados em conhecimento técnico assim como em posições de liderança, de modo que possam ser disseminadores da doutrina, da mentalidade e da missão, independentemente das tarefas que lhes sejam atribuídas em todos os níveis. As Operações Especiais servem como laboratório para a experimentação doutrinária de técnicas, táticas, procedimentos e equipamentos, e seus exemplos de sucesso são frequentemente adotados pelas tropas convencionais.

O entendimento comum é que o Suboficial de Operações, independentemente de ser Comando Anfíbio, Mergulhador de Combate, Forças Especiais ou Paraquedista, devido à sua vasta experiência operacional e ao seu profundo conhecimento técnico, desempenha um papel crucial auxiliando todos os elementos do Estado-Maior. Ele deve se reportar ao Oficial de Operações e prestar assistência em todos os assuntos relacionados ao Estado-Maior. O Chefe do Estado-Maior, por sua vez, lidera todos os elementos do Estado-Maior, e uma extensão de sua influência poderia ser o Suboficial de Operações auxiliando na condução das atividades, esclarecendo dúvidas e apoiando Praças e Oficiais no entendimento de suas responsabilidades à luz das doutrinas vigentes. Isso é particularmente importante, uma vez que nem todos os membros podem realizar os cursos de formação desejados para o exercício de suas funções, tornando o ritmo das operações mais eficaz.

Para que essa posição seja bem-sucedida, o Suboficial de Operações deve ter um conhecimento sólido dos seguintes princípios: competências básicas comuns ao Sargento, liderança, formação de equipe e comando de missão. Ao combinar e aplicar esses conceitos, o Suboficial de Operações é capaz de compreender as capacidades do Estado-Maior, gerenciar eficazmente o pessoal e alinhar os Sargentos do Estado-Maior sob a coordenação do Oficial da célula.

O Ministério da Defesa (MD) adota a definição de capacidade como a aptidão resultante da sinergia de diversos fatores, abrangendo Doutrina, Organização, Pessoal, Educação, Material, Adestramento e Infraestrutura (DOPEMAI). Esse conhecimento é essencial para fornecer assessoramento oportuno.

O papel do Suboficial de Operações visa fazer com que os nós de comando, ou vazios de informação, atuem e funcionem como um grupo dinâmico, disciplinado e profissional dentro e ao redor do comando. Além disso, ele colabora com outros Suboficiais para gerenciar requisitos logísticos, emprego tático e procedimentos de segurança, aplicando a filosofia do comando e mantendo as características da força de origem, além de também compreender os deveres e as responsabilidades das Praças durante os processos de tomada de decisão.

Figura 2: SOMor do CoNavOpEsp e SOMor do BtlOpEspFuzNav na F Cj OpEsp.

Fonte: O autor.

2. Comando da Missão

Durante a apresentação dos militares ao Estado-Maior ao longo da missão, é comum que alguns deles necessitem de reforço ou orientação quanto à intenção do comandante, à iniciativa disciplinada e ao entendimento compartilhado. Muitas vezes, isso é resultado de uma falta de clareza com os militares que normalmente não fazem parte do planejamento ou não têm acesso aos documentos operativos, como a Ordem de Operação, o Plano Logístico e o Plano de Comunicações do Estado-Maior. Consequentemente, pode não haver um entendimento comum das operações em curso ou dos objetivos da missão.

Os Suboficiais e Sargentos mais experientes geralmente demonstram competência em vários princípios do Comando da Missão – incluindo o estabelecimento de confiança mútua com os Oficiais e Sargentos do Estado-Maior de sua unidade –, além de compreensão das ordens da missão e capacidade para mitigar riscos.

3. As responsabilidades e a sinergia da equipe

Frequentemente, os militares são empregados no Estado-Maior de acordo com seus pontos fortes; invariavelmente, essas posições são nichos de especialidades conforme a célula em que estão trabalhando. Com isso, o fluxo de informações, por vezes, não segue um caminho fluido para que o assessoramento seja feito em tempo hábil de compilação das várias informações disponíveis no Estado-Maior como um todo.

Considerando os motivos citados anteriormente (não participar do planejamento ou não ter acesso aos documentos operativos), muitas vezes os sargentos não compreendem totalmente suas responsabilidades e deveres quando estão integrando o Estado-Maior. Esses fatores, juntamente com os pontos de atrito já mencionados, geralmente causam atrasos no gerenciamento de processos ou no ritmo de batalha.

4. Recomendações

Visando à preparação do Suboficial para ser um multiplicador de força e conhecimento como Auxiliar de Operações, a primeira recomendação proposta neste artigo consiste em estabelecer um manual específico para Forças Conjuntas ou Comandos Conjuntos de Operações Especiais detalhando as funções desempenhadas por Praças (adjuntos e auxiliares). Isso deve ser alinhado com as responsabilidades dos Oficiais nas células, seguindo os princípios já estabelecidos nos manuais existentes. Dessa forma, é importante definir e expandir as responsabilidades da função de Suboficial de Operações ou criar a posição de Suboficial-Mor da Força Conjunta de Operações Especiais, semelhante ao que já existe nas unidades de Operações Especiais do Exército e da Marinha. A doutrina deve especificar quem esse Suboficial irá assessorar, garantindo que ele se torne um orientador/assessor no Estado-Maior e amplie sua influência em todos os ambientes operacionais, não se limitando apenas à Seção de Operações. Além disso, a doutrina deve estabelecer que o Suboficial de Operações (ou o Suboficial-Mor da Força Conjunta de Operações Especiais) forneça aconselhamento e gerencie todos os processos dos elementos do Estado-Maior, não apenas as operações.

A segunda recomendação sugere aproveitar o Curso de Assessoria em Estado-Maior para Sargentos (C-ASEMSO). Embora as escolas se concentrem em formar graduados ágeis e adaptáveis, elas não preparam completamente os Sargentos para compreender a abordagem operacional de uma organização do nível tático ao operacional, o que limita o impacto geral que o Suboficial de Operações pode ter na organização para alcançar o estado final desejado pelo comandante nas operações. Portanto, é importante expandir o conhecimento institucional obtido no C-ASEMSO, proporcionando aos Sargentos de nível tático uma base sólida para o sucesso organizacional. Isso pode ser feito por

meio da inclusão do Estágio de Preparação para Futuros Comandantes de Organizações Militares (OM) do Corpo de Fuzileiros Navais (EPrepFutComFN) e do Curso de Preparação para Suboficial-Mor (C-Esp-SOMor) como requisitos antes de assumir a função de Suboficial de Operações.

Essa preparação deve abranger tópicos como formação de equipes, sincronização do trabalho do Estado-Maior, aplicação de meticulosidade, clareza, bom senso, lógica e conhecimento profissional para entender situações, desenvolver opções para resolver problemas e tomar decisões, além das atividades relacionadas ao Posto de Comando (PC), como segurança, comunicações e acompanhamento dos grupos tarefas subordinados, além de organização do poder de combate. Também é importante abordar temas como logística aplicada às Forças de Operações Especiais, suporte da cadeia logística às ações das Forças de Operações Especiais, suporte operacional de controle de alcance, linhas de controle e consciência situacional das outras tropas presentes na Área de Responsabilidade de Operações Especiais durante exercícios de treinamento situacional ou operações reais. Essa preparação é essencial para garantir que as Forças de Operações Especiais sejam capazes de atuar de forma eficaz e eficiente, sem improvisações diante de emergências, e que os elementos que compõem o Estado-Maior estejam devidamente preparados e comprometidos com o sucesso das Operações Especiais.

Conclusão

A definição adequada da posição do Suboficial na Força Conjunta de Operações Especiais é de extrema importância para o sucesso dessa função e para a promoção da participação ativa de Praças em todos os níveis, sempre respeitando a disciplina e a hierarquia. Essa definição deve permitir que Praças assessorem tanto outras Praças quanto os Oficiais no desempenho de suas tarefas, alinhando-se com a intenção do Comando na condução das missões, integrando informações e promovendo o profissionalismo por meio da sinergia da equipe.

Ao proporcionar aos graduados não só essa posição de liderança, por meio da qual eles podem influenciar positivamente, mas também uma educação completa e contínua sobre suas responsabilidades e expectativas, as Forças de Operações Especiais podem formar graduados bem-sucedidos que têm um impacto positivo em suas organizações. Isso resultará em unidades de combate fortes e coesas, preparadas para enfrentar os desafios futuros. Aumentar o nível de influência em múltiplos domínios é crucial para um país de dimensões continentais como o Brasil, tendo em vista a qualidade do capital humano disponível.

Portanto, a definição adequada do papel do Suboficial nas Forças de Operações Especiais é fundamental para alcançar esses objetivos e promover maior eficácia nas operações militares.

Figura 3: ComAnf Adestramento.
Fonte: Acervo MB.

Referências Bibliográficas

BRASIL. Marinha do Brasil. **Portaria 470/MB** de 22 out. 2015. Implantou o Programa Suboficial-Mor na Marinha do Brasil. (2015a). Disponível em: <https://www.gov.br/mme/pt-br/arquivos/do-23-10-2015-s2.pdf>. Acesso em: 02 fev. 2024.

_____._____. Centro de Análises de Sistemas Navais. **Comando e Controle: O Desafio da Interoperabilidade** – Sistema de Planejamento Operacional Militar (SIPLOM). [s.d.]. Disponível em: <https://www.marinha.mil.br/casnav/?q=node/118>. Acesso em: 02 fev. 2024.

_____._____. Diretoria do Patrimônio Histórico e Documentação da Marinha. **Ordenança Geral para o Serviço da Armada (OGSA)**. Ed. revisada. Rio de Janeiro, 2009.

_____._____. Diretoria-Geral do Pessoal da Marinha. **DGPM-307: Normas sobre seleção e indicação para cursos**. Capítulo 11. Rio de Janeiro, 2019a.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Doutrina de Operações Conjuntas – MD30-M-01**. 2. ed., vol. 1 e 2, 2020.

_____._____._____. **Glossário das Forças Armadas**. 5. ed. Brasília-DF: EMCFA, 2015b.

_____._____._____. Assessoria Especial de Planejamento Baseado em Capacidades. **Planejamento baseado em capacidades: sumário executivo**. Minuta de 08 jun. 2018. Brasília-DF: EMCFA, 2018.

_____._____. Exército Brasileiro. **Guia do Adjunto de Comando**. 1. ed. Cruz Alta: EASA, 2019b.

CASTIN, P. **Battle Staff NCO Review: NCO Tactical Command Post SOP**. (2003). Disponível em: <http://asktop.net/wp/download/16/NCO%20Tactical%20Command%20Post%20SOP.pdf/>. Acesso em: 08 mar. 2024.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). **The Non-Comissioned Officer Professional Military Education** (2014). Disponível em: <https://www.nato.int/cps/en/natohq/topics_118000.htm>. Acesso em: 08 mar. 2024.

TRAINING ANALYSIS FEEDBACK TEAM (TAFT). Fort Leavenworth, Kansas. **The Staff Noncommissioned Officer's Handbook**. (2016). Disponível em: <https://bootcampmilitaryfitnessinstitute.files.wordpress.com/2015/07/02-staff-ncos-handbook-the-2015-10.pdf>. Acesso em: 08 mar. 2024.

UNITED STATES DEPARTMENT OF THE ARMY (U.S. ARMY). **ADP 5-0: The Operations Process**. (2019). Disponível em: <https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18126-ADP_5-0-000-WEB-3.pdf>. Acesso em: 08 mar. 2024.

_____. **ATP 6-0.5: Command Post Organization and Operations**. (2017). Disponível em: <https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ATP%206-0_5%20(final).pdf>. Acesso em: 04 fev. 2024.

_____. **FM 6-0: Commander and Staff Organization and Operations**. (2014). Disponível em: <https://armypubs.army.mil/epubs/DR_pubs/DR_a/NOCASE-FM_6-0-002-WEB-6.pdf>. Acesso em: 08 mar. 2024.

_____. **TC 7-22.7 The Noncommissioned Officer Guide**. (2020). Disponível em: <https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN20340-TC_7-22.7-000-WEB-1.pdf>. Acesso em: 04 fev. 2024.

.....

Figura 4: MEC.
Fonte: Acervo MB.

Teatro de Operações 5.0: uma análise do Ambiente Operacional Multidomínio

6

Capitão de Mar e Guerra (FN) **Salvador** Mota Junior

Oficial de Comunicações e Guerra Eletrônica no Comando da Força de Fuzileiros da Esquadra. Ao longo de sua carreira, realizou diversos cursos, entre os quais se destacam: Estágio em Operações de Informação, Operações Psicológicas, Análise de Dados, Inteligência de Negócios, *Ethical Hacker,* Cibersegurança e Gestão de Crises no Ciberespaço, Análise de Mídias e Redes Sociais, Engenharia Social e *Pentest* Profissional. Entre os principais cargos administrativos e operacionais que ocupou, estão os seguintes: Comandante do Batalhão de Comando e Controle, Imediato do Batalhão de Artilharia de Fuzileiros Navais, Oficial de Logística do Comando da Divisão Anfíbia. Também foi Encarregado do Departamento de Operações de Informação, da Divisão de Guerra Cibernética e da Divisão de Operações Psicológicas (CoNavOpEsp) e da Divisão de Inteligência Cibernética (CON-20).

Introdução

O Teatro de Operações é uma parcela do espaço geográfico necessário à condução de Operações Militares, que necessitam de planejamento detalhado, preparo adequado, emprego preciso e acompanhamento constante a fim de que os objetivos propostos sejam atingidos.

Executar um estudo prévio do Teatro é fundamental. Em geral, realiza-se uma análise em dois blocos, conjugando as informações produzidas para assessorar o decisor:

- avaliação de qual domínio do espaço geográfico (terra, mar, ar ou espaço) exerce maior influência na condução da Operação Militar;
- estudo das interações entre as dimensões física, humana e informacional do Ambiente Operacional, nessa ordem de prioridade, observando como o resultado dessas interações afeta a forma de atuar das Forças Militares.

Com a chegada da Era da Informação, combinada com as mudanças sociais experimentadas em escala global, os blocos que serviam de alicerce para o processo analítico do Teatro de Operações experimentaram alterações significativas em sua composição e na escala de prioridade dos estudos de interação:

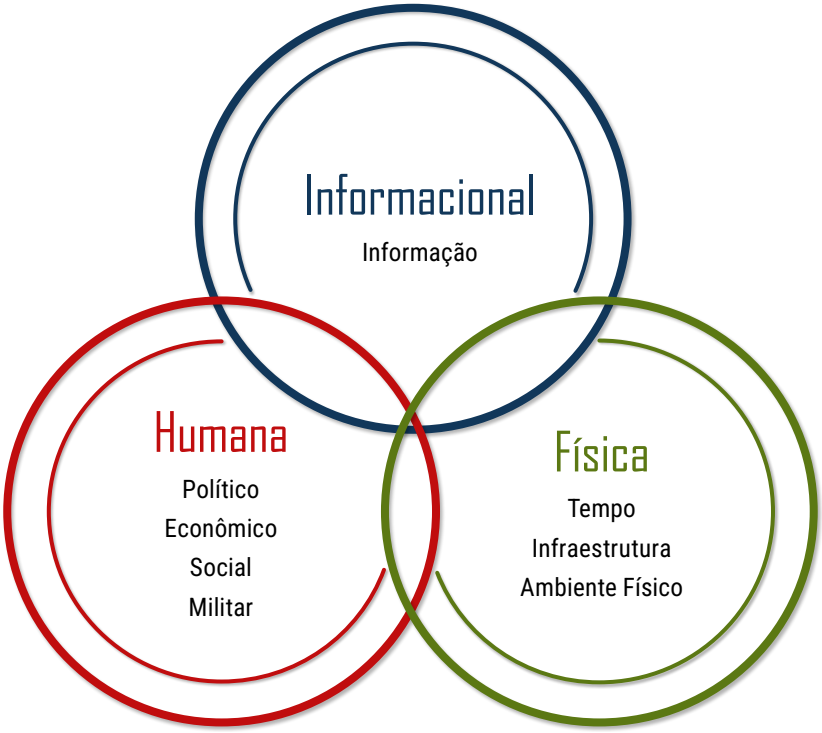
- o surgimento do Domínio Cibernético no rol dos elementos nos quais as Operações Militares poderiam ser conduzidas – um domínio virtual, dinâmico, artificial e transversal capaz de interligar os demais domínios, permitindo o exercício do Comando e Controle sem precedentes; e
- a Dimensão Informacional passa a exercer o protagonismo no processo de avaliação do Ambiente Operacional, influenciando as condições e as circunstâncias responsáveis pela forma de atuar das Forças Militares, sendo seguida pela Dimensão Humana.

Tendo em vista o ingresso do Domínio Cibernético e do incremento da influência exercida pela Dimensão Informacional sobre COMO e POR QUE as Forças Militares serão utilizadas, este artigo propõe uma análise do Ambiente Operacional Multidomínio, elevando, assim, o estudo do Teatro de Operações para a versão 5.0.

Essa expansão transformou o Teatro de Operações em um espaço híbrido no qual se misturam componentes reais e virtuais, permitindo atingir efeitos cinéticos e não cinéticos. A convergência de ações em diferentes níveis de decisão produz efeitos sinérgicos e complexos.

Portanto, este artigo busca fornecer uma compreensão inicial do Teatro de Operações 5.0, enfatizando a importância de uma abordagem multidisciplinar para enfrentar os desafios e explorar as oportunidades presentes no Ambiente Operacional Multidominio. Nas seções seguintes, serão explorados os domínios que compõem o Ambiente Operacional, com destaque para os desafios e as vantagens do Domínio Cibernético, apontando as características do Teatro de Operações 5.0 e suas implicações.

Figura 1: Dimensões do Ambiente Operacional.



Fonte: O autor.

1. O ambiente operacional multidomínio

O Teatro de Operações 5.0 representa uma alteração de paradigma, muito por conta da constante e acelerada evolução do Domínio Cibernético e da Dimensão Informacional. A integração dos cinco domínios (terrestre, marítimo, aéreo, espacial e cibernético) somada à ubiquidade com a qual as diversas camadas da informação interagem com a sociedade presente no Teatro de Operações representam as principais características do multidomínio.

Serão apresentados, a seguir, os domínios que compõem o Ambiente Operacional 5.0, evidenciando suas principais características – com destaque para a chegada do quinto domínio – e o significativo impacto na condução das Operações Militares.

1.1. Domínio Terrestre

É considerado o primeiro espaço a ser disputado pelo homem, permanecendo como elemento essencial do Teatro de Operações 5.0. Esse ambiente inclui o solo, a topografia, as cidades, as vilas e todas as áreas onde as Forças podem realizar suas Operações Militares. Isso pode variar de áreas urbanas densamente povoadas a terrenos rurais e florestais quase desertos.

Por ser a base da civilização, pode-se afirmar que esse domínio foi o primeiro a ser estudado estrategicamente em operações de combate. Combinando, ainda, necessidades territoriais com limitações tecnológicas e aspectos logísticos, o Domínio Terrestre já figurou como o único elemento de estudo na avaliação do Teatro de Operações.

No entanto, ao longo da história, o avanço tecnológico permitiu ao homem lançar-se sobre um segundo domínio – o mar –, capaz de rivalizar em importância com o primeiro e dar início a uma nova era no planejamento e na execução das operações militares.

1.2. Domínio Marítimo

Compreende oceanos, mares, rios e outras massas de água navegáveis. As operações marítimas envolvem a Marinha, podendo incluir patrulha, transporte de tropas e operações de guerra naval, entre outras atividades.

O Domínio Marítimo proporcionou mudanças profundas na Estratégia e nas Operações Militares, permitindo que as nações expandissem seu poder e influência por todo o globo, além de desempenhar um papel vital no comércio internacional e na segurança nacional.

Isso fez da Força Naval uma componente crítica no desenvolvimento das estratégias militares modernas, com destaque para: a construção de uma Estratégia Naval, que influenciou questões militares, comerciais e logísticas como um todo; o incremento da capacidade de projeção de poder a partir do mar; e o desenvolvimento de tecnologias principais e secundárias.

1.3. Domínio Aéreo

O Domínio Aéreo consolidado trouxe uma ampla gama de capacidades estratégicas que afetaram profundamente a forma como as nações passaram a planejar e conduzir as Operações Militares. As possibilidades estratégicas se tornaram tão significativas que transformaram profundamente a natureza dos estudos do Teatro de Operações.

As principais possibilidades que surgiram foram: mobilidade e ataques estratégicos de forma rápida e precisa; ampliação das atividades de reconhecimento e vigilância; supremacia/superioridade aérea oferecendo suporte e proteção aérea; e disponibilidade de uma plataforma avançada para a condução das ações de Guerra Eletrônica e das funções logísticas.

1.4. Domínio Espacial

A consolidação do Domínio Espacial trouxe uma série de vantagens estratégicas significativas para as nações que investiram nas capacidades espaciais avançadas, com destaque para: comunicações globais seguras, permitindo coordenação eficaz a longas distâncias, o que engloba o exercício de Comando e Controle sobre mais de um Teatro de Operações; posicionamento e navegação utilizando sistemas de posicionamento global, como o GPS; e reconhecimento, inteligência e vigilância mais eficientes, permitindo explorar o alerta antecipado e acelerar o processo de tomada de decisão.

1.5. Domínio Cibernético

É o mais recente, mas tem um impacto crescente. Integra os demais domínios e cria um espaço próprio, virtual e dinâmico conhecido como Espaço Cibernético. Ele otimiza o fluxo de informações e permite ações cibernéticas com alto nível de anonimização. No entanto, introduz desafios complexos, como a crescente dependência de infraestruturas críticas e a exposição às ameaças cibernéticas em constante evolução.

O Domínio Cibernético desempenha um papel central, garantindo velocidade e resiliência nas atividades de Comando e Controle, sendo fundamental para uma tomada de decisão baseada em dados.

Em conjunto, esses cinco domínios formam o Teatro de Operações 5.0, representando um Ambiente Operacional Multidomínio volátil, incerto, complexo e ambíguo. A integração desses domínios redefine a estratégia militar, exigindo cooperação interinstitucional em todos os níveis.

Um dos desafios é encontrar o equilíbrio entre a exploração das vantagens oferecidas por esses domínios e a gestão dos desafios que surgem com a crescente conexão e dependência entre os domínios e as dimensões. A capacidade de analisar o Ambiente Operacional Multidomínio considerando seus componentes torna-se crucial para o sucesso das Operações Militares no século XXI.

2. Vantagens e desafios impostos pelo domínio cibernético ao ambiente operacional

O impacto do Domínio Cibernético se estende a todos os domínios do Ambiente Operacional Multidomínio. A ubiquidade das Operações Cibernéticas é responsável pela reconfiguração da dinâmica das Operações Militares conduzidas no Teatro de Operações 5.0.

Serão apresentadas, a seguir, algumas vantagens e alguns desafios que o Domínio Cibernético impôs a cada domínio, considerando os níveis estratégico, operacional e tático.

2.1. Domínio Terrestre

- Nível Estratégico: a Guerra Cibernética tornou-se uma ferramenta de dissuasão, permitindo que as nações protejam seus interesses sem recorrer a conflitos convencionais.
- Nível Operacional: a coordenação das peças de manobra se torna mais eficaz com o uso de sistemas de apoio à decisão cibernética.
- Nível Tático: ataques cibernéticos locais podem ser usados para minar as operações inimigas, mas a vulnerabilidade dos sistemas de Comando e Controle constitui um desafio.

2.2. Domínio Marítimo

- Nível Estratégico: a vantagem está na utilização de sistemas de navegação apoiados em recursos computacionais, próprios ou de terceiros, enquanto o monitoramento e a espionagem cibernética representam um desafio.
- Nível Operacional: o controle de sensores e radares é aprimorado, representando vantagem operacional; contudo, sistemas de comunicação marítima podem ser vulneráveis a ataques cibernéticos.
- Nível Tático: a supressão de comunicações inimigas pode ser realizada, mas proteger os sistemas de armas é um desafio.

2.3. Domínio Aéreo

- Nível Estratégico: a interferência no espaço eletromagnético é uma vantagem, mas sistemas de controle de tráfego aéreo podem ser alvos de ataques cibernéticos.

- Nível Operacional: ataques aéreos coordenados são facilitados com o apoio de operações cibernéticas, enquanto sistemas de navegação aérea são suscetíveis a interferências.
- Nível Tático: o uso de drones em ataques é uma vantagem, mas a defesa antiaérea deve se adaptar para lidar com essa ameaça.

2.4. Domínio Espacial

- Nível Estratégico: a capacidade de negar o acesso ao espaço é uma vantagem estratégica; contudo, a vulnerabilidade dos satélites estratégicos é um desafio.
- Nível Operacional: a utilização de comunicações cibernéticas seguras é benéfica, mas o sensoriamento remoto pode ser comprometido.
- Nível Tático: a desativação de satélites é uma tática disponível; a supressão de comunicações cibernéticas no espaço, porém, é complexa.

O advento do Domínio Cibernético traz a necessidade de adaptação contínua em todos os níveis decisórios. O conceito de Multidomínio ganha relevância à medida que ocorre a integração eficaz de todas as capacidades em resposta a ameaças reais e virtuais. Além disso, a proteção de infraestruturas críticas e sistemas de comunicação é prioridade em todos os domínios. Isso exige Forças Militares ágeis, tecnologicamente avançadas e com profundo conhecimento do Domínio Cibernético.

3. Características inerentes ao Teatro de Operações 5.0

3.1. Convergência tecnológica

A convergência entre os domínios é uma qualidade fundamental no Teatro de Operações 5.0. A sinergia entre os diferentes domínios tira proveito das tecnologias avançadas, como inteligência artificial e computação na nuvem, resultando em uma abordagem inovadora. Essa sinergia promove a interconexão e a interdependência dos domínios, ressaltando a necessidade de coordenação entre as Forças Militares no Teatro de Operações 5.0. Isso não apenas otimiza a eficiência, mas também melhora a eficácia das Operações Militares.

3.2. Tomada de decisão baseada em dados

A ênfase no emprego de dados como subsídios para alimentar o processo decisório é uma característica crítica do Teatro de Operações 5.0. As atividades de coleta contínua, análise cíclica e disseminação oportuna das informações produzidas proporcionam uma visão abrangente quase em tempo real do Ambiente Operacional Multidomínio, permitindo decisões rápidas e bem-sucedidas. A integração de informações de diferentes domínios, que deu origem ao termo Comando e Controle Conjunto, desempenha um papel vital na minimização do risco de erros e fratricídios.

3.3. Resiliência cibernética

Refere-se à capacidade que o Domínio Cibernético empresta ao fluxo informacional entre os demais domínios, permitindo que um sistema, rede ou organização possa se adaptar e se recuperar de forma eficaz após um ataque cibernético, uma falha de segurança ou outra ameaça digital. Isso envolve a capacidade de detectar, responder e se recuperar de eventos adversos de forma a minimizar os danos e manter a operação contínua dos domínios envolvidos, garantindo a disponibilidade e a integridade dos sistemas de informação em um Ambiente Operacional Multidomínio.

A resiliência cibernética inclui a preparação, a resposta e a recuperação após incidentes cibernéticos, bem como a capacidade de resistir a ameaças persistentes e emergentes. O reconhecimento da vulnerabilidade do Espaço Cibernético e a necessidade de resistir às ameaças cibernéticas e se recuperar rapidamente são fundamentais para a continuidade das Operações Militares.

Em síntese, o Teatro de Operações 5.0 representa uma mudança significativa na forma como as Operações Militares são concebidas e conduzidas. A convergência tecnológica, a tomada de decisão baseada em dados e a resiliência cibernética são características centrais que definem esse novo Ambiente Operacional. Compreender e adotar essas características é essencial para garantir a superioridade e a liberdade de ação em futuros conflitos, marcando uma evolução crucial na estratégia militar diante de um cenário em constante transformação.

4. As implicações no Teatro de Operações 5.0

Nesta seção, serão abordadas as mudanças significativas nas Operações Militares geradas pela chegada do Domínio Cibernético. As implicações abrangem áreas como doutrina de emprego, organização para o combate, pessoal especializado e ensino.

Essas implicações serão abordadas a seguir, mantendo o viés Multidomínio do Ambiente Operacional.

4.1. Doutrina de emprego

O primeiro ponto de destaque é a necessidade de integração das operações cibernéticas com as operações convencionais. A doutrina deve estabelecer como essas duas esferas se relacionam, definindo protocolos para a execução das ações de Guerra Cibernética, como proteção, exploração e ataque. Isso requer um alinhamento preciso com estratégias tradicionais, buscando estabelecer os princípios que nortearão a condução da Guerra Cibernética.

Além disso, a doutrina deve esclarecer os objetivos e métodos para operações cibernéticas em tempos de conflito, bem como incorporar avaliações de impacto cibernético. Compreender como as ações de guerra cibernética podem afetar a consecução da missão e a tomada de decisão é fundamental, o que também implica considerar como as operações cibernéticas se encaixam nas doutrinas de outros participantes do Teatro de Operações, exigindo coordenação eficaz e compartilhamento preciso das informações em cada domínio.

4.2. Organização para o combate

A organização das Forças para o combate deve incluir unidades especializadas em Guerra Cibernética e Segurança Cibernética, as quais desempenham um papel crucial na condução de operações cibernéticas e na defesa dos recursos computacionais críticos. Para garantir a resiliência no espaço cibernético de interesse, é imperativo que essas unidades contem com equipes dedicadas de resposta a incidentes.

Além disso, a organização deve estabelecer uma cadeia de comando cibernética clara. Isso é essencial para garantir um fluxo ótimo de tomada de decisões relacionadas às operações cibernéticas, assim como para realizar a coordenação eficiente com outras unidades e domínios operacionais.

4.3. Pessoal especializado

O treinamento do pessoal militar em Operações Cibernéticas é uma prioridade incontestável que engloba não apenas a segurança e a defesa cibernética, mas também a conscientização sobre as ameaças cibernéticas e a responsabilidade de todos na execução das boas práticas no Espaço Cibernético. Os militares precisam ser treinados em detecção de *malware*, análise de ameaças e resposta a incidentes.

Além do treinamento, é crucial o recrutamento e a retenção de especialistas em segurança cibernética, *hackers* éticos e analistas de ameaças cibernéticas em diversos níveis. Esses especialistas desempenham um papel vital na manutenção da vantagem estratégica na condução das ações de Guerra Cibernética.

4.4. Diretrizes de ensino

As implicações do Teatro de Operações 5.0 também alcançam as diretrizes de ensino responsáveis pela disseminação do conhecimento necessário. O ensino sobre Operações Cibernéticas deve ser ministrado de forma abrangente, abordando desde os fundamentos da Segurança Cibernética até táticas avançadas. Além disso, a escolha e a preparação de material adequado são cruciais, o que inclui a implementação de infraestrutura sólida e robusta para simulações e o treinamento prático em ambientes cibernéticos simulados.

A combinação desses elementos permite a execução de adestramentos em diversos níveis de dificuldade, preparando as Forças de maneira eficaz para enfrentar desafios no Ambiente Operacional Multidomínio do Teatro de Operações 5.0. As diretrizes de ensino também devem ser flexíveis o suficiente para se adaptarem às mudanças constantes no ciberespaço, garantindo que o pessoal militar esteja sempre atualizado sobre as ameaças e as tecnologias emergentes.

Em resumo, as implicações do Teatro de Operações 5.0 são amplas e profundas, abrangendo doutrina de emprego, organização para o combate, pessoal especializado e diretrizes de ensino. A integração das operações cibernéticas com as operações convencionais é fundamental, assim como a criação de unidades especializadas em Guerra Cibernética e a formação de pessoal altamente qualificado. Tudo isso é complementado pela importância de diretrizes de ensino sólidas e adaptáveis.

O Ambiente Operacional Multidomínio do Teatro de Operações 5.0 representa um desafio sem precedentes. No entanto, com a adoção de uma abordagem estratégica e de investimentos nas áreas mencionadas, as Forças estarão bem preparadas para enfrentar os desafios cibernéticos e garantir a segurança e a eficácia em um mundo cada vez mais conectado digitalmente.

Conclusão

Na era da evolução tecnológica e estratégica, o Teatro de Operações 5.0 aparece como um paradigma fundamental para as operações militares. A análise do Ambiente Operacional Multidomínio e a compreensão das vantagens e dos desafios trazidos pelo Domínio Cibernético são essenciais para a adaptação bem-sucedida das Forças Militares.

A convergência tecnológica, a tomada de decisão baseada em dados e a resiliência cibernética são as características definidoras desse novo Ambiente Operacional, com destaque para a necessidade de integração

e cooperação entre os domínios. Essas características impulsionam a doutrina de emprego, a organização para o combate e a formação do pessoal militar, promovendo uma abordagem multidisciplinar para enfrentar os desafios do Teatro de Operações 5.0.

Com o crescente foco no Espaço Cibernético, as Operações Militares avançam em direção a uma nova fronteira, onde a superioridade não é mais definida apenas pela capacidade de projetar força, mas também pela capacidade de controlar informações e sistemas críticos. O sucesso nas operações militares dependerá cada vez mais da agilidade, da colaboração e do entendimento profundo do ciberespaço.

Nesse cenário de transformação constante, o Teatro de Operações 5.0 é um chamado para a inovação e a preparação contínua, e as Forças Militares devem se adaptar rapidamente para garantir a segurança e a eficácia no Ambiente Operacional Multidomínio do século XXI. A compreensão dessas dinâmicas e a adoção de abordagens multidisciplinares são cruciais para enfrentar os desafios e explorar as oportunidades apresentadas por esse novo campo de batalha.

Referências Bibliográficas

BRASIL. Marinha do Brasil. **EMA 419 – Doutrina Cibernética da Marinha.** 1. ed. 2021.

_____._____. **EMA 335 – Doutrina de Operações de Informação.** 1. ed. 2018.

_____._____. **EMA 305 – Doutrina Militar Naval.** 1. ed. 2017.

_____. Ministério da Defesa. **MD35-G-01 – Glossário das Forças Armadas.** 5. ed. 2015.

Influência e poder nas Operações de Informação: um novo paradigma de Defesa

7

Capitão de Fragata **Vinícius** Mendonça dos **Santos**

Formado em Ciências Navais com habilitação em Eletrônica na Escola Naval, realizou diversos cursos nas áreas de Comunicação Social, Eletrônica, Segurança de Aviação e Gestão de Manutenção de Aeronaves, entre os quais se destacam: *Airframe, Powerplant, Eletrical* e *Avionics* das Aeronaves AF1B/1C (Embraer); Introdução à Gestão de Projetos, Orçamento Público, Gestão e Fiscalização de Contratos Administrativos e Legislação Aplicada à Logística de Suprimentos (ENAP). Desempenhou funções administrativas e operacionais, entre as quais se destacam: Encarregado da Seção Aviônica do Grupo de Recebimento e Modernização das Aeronaves AF-1/1A, Encarregado da Divisão de Operações no Navio-Tanque Marajó e 1º Ajudante da Divisão O-2 da Corveta Jaceguai.

Introdução

O notório fortalecimento da opinião pública, a onipresença dos órgãos de imprensa, a redução do controle estatal sobre as agências de notícias, o acesso mais facilitado aos meios de comunicação de massa e o protagonismo de cada cidadão por meio das mídias sociais vêm aumentando a relevância das Operações de Informação (OpInfo).

Um olhar mais atento sobre as origens históricas dos grandes conflitos permite-nos inferir que a aquiescência da opinião pública para levar adiante as políticas de Estado, principalmente aquelas relacionadas com o custo para o emprego das Forças Armadas, torna-se cada vez mais importante. O conflito, mais do que um fenômeno político, é oriundo de um dilema social.

Sobre esse aspecto, intensas campanhas de Operações de Informação com propaganda e preparação psicológica destinada a proteger e, até mesmo, inflamar paixões populares passam a preceder o início de certas ações militares, inclusive no período de paz. Não obstante, a própria população civil do Estado antagônico poderia ser vista como um alvo legítimo no ambiente informacional por representar o esteio do poder político do oponente.

Dessa forma, faz-se necessário propor uma reflexão sobre as observações colhidas durante a participação da Marinha do Brasil nas Operações Conjuntas do Ministério da Defesa (MD). Os principais pontos interessantes são: a influência da Revolução da Informação nos ambientes marítimo e fluvial; a atividade de criminosos; e, por fim, a atuação mitigadora das Operações de Informação nas fases do planejamento e da execução, encerrando com as respectivas lições aprendidas.

1. Aspectos do ambiente informacional nos meios marítimo e fluvial

É importante observar a colocação do Almirante Castex sobre a presença humana no ambiente marítimo suportada pela evolução tecnológica que estimula a infraestruturação do mar, sua territorialização e a redução da liberdade estatal. Nesse sentido, destaca-se o relato do Almirante Ilques Barbosa no livro *Oceanopolítica*: ele afirma que a ocupação humana dos espaços oceânicos respalda a ampliação de direitos dos Estados numa espécie de conceito reeditado do *Uti Possidetis*, segundo o qual uma determinada área pertence a quem a ocupa.

Assim, o ambiente informacional vem sofrendo influência do cotidiano marítimo num patamar nunca visto antes, levando à necessidade de uma ação prudente também nesse espectro. O desafio brasileiro é agravado devido à sua extensa rede hidrográfica, que atravessa uma das áreas naturais mais cobiçadas do mundo: a população da região se encontra distante do aparato estatal e pode estar sujeita à manipulação de diversos protagonistas, como organizações criminosas e ONGs.

2. Campo fértil para a atuação de criminosos

A expansão das atividades criminosas no Brasil vem ganhando destaque nos meios de comunicação. A interconectividade global e a facilidade tecnológica acabam por viabilizar a ramificação de redes de comércio ilegal especializadas em drogas, armas, explosivos, descaminho, etc.

Nesse contexto, cumpre analisar o que assegurou Woloszyn (2013) no livro *Guerra nas Sombras*: "O crime organizado, a migração e o extremismo violento estão em alta e possivelmente serão os mais importantes

fatores de desestabilização dos Estados nacionais". Dessa forma, os atores não estatais acirram concorrência com Estados nacionais pela influência sobre a população. No caso brasileiro, organizações criminosas buscam manipular e cooptar jovens, tanto nos aglomerados urbanos quanto nas áreas fronteiriças.

Nesse aspecto, a soberania permanecerá um conceito válido para a integridade territorial, mas a soberania econômica, a soberania da informação e a soberania cultural ficarão cada vez mais difíceis de proteger em razão do efeito imprevisível da Revolução da Informação e de métodos assimétricos de guerra com sua espantosa velocidade de mutação.

3. Planejamento das Operações de Informação nas Missões Conjuntas do MD

O planejamento conjunto da execução das OpInfo dentro da Área de Operações (AOp) pode ficar a cargo da Força Conjunta de Operações Especiais (FCjOpEsp), que se pauta na busca do Estado Final Desejado (EFD) indicado pelo Comandante no mais alto nível do Estado-Maior do Comando Conjunto (EMCCj), com foco restrito ao público-alvo da AOp.

Nesse intento, almeja-se atuação na população local e em lideranças locais, *influencers* e integrantes do crime organizado, Órgãos de Segurança Pública (OSP), mídia local, autoridades da faixa de fronteira e até mesmo os próprios integrantes das Forças Armadas Brasileiras. Dessa forma, a Capacidade Relacionada à Informação (CRI), conhecida como Assunto Civil-Militar, busca conciliar as atividades de autoridades governamentais, ONGs, militares e população local assistida, propiciando sua continuidade mesmo num ambiente conflituoso.

Outro ponto importante sobre o planejamento da campanha informacional e sua respectiva aprovação pelo Comandante do EMCCj é a sua definição anterior à chegada das forças beligerantes na AOp. Ou seja, a modelagem do ambiente informacional demanda tempo prolongado e deve viabilizar apoio a fim de facilitar as ações a serem executadas, como algumas sintetizadas no quadro a seguir.

Quadro 1: Tarefas executadas no planejamento da OpInfo.

Tarefas normalmente executadas no planejamento da campanha de OpInfo
Identificação de narrativas desfavoráveis às Forças Armadas na AOp antes do emprego da tropa.
Identificação de vetores de influência amigos, neutros e hostis na AOp.
Integração das CRIs disponíveis.
Emissão de diretrizes para a confecção de produtos a serem disseminados.

Fonte: O autor.

4. A execução das Operações de Informação nas Missões Conjuntas

O emprego coordenado da CRI potencializa as ações cinéticas por meio do domínio do ambiente informacional – como a CRI focada em Operações Psicológicas, cuja característica peculiar é poder empregar seus destacamentos no terreno antes mesmo do deflagrar da Operação.

A CRI interage com setores de comunicação, assessoria de imprensa, OSP e agências externas às Forças Armadas presentes na AOp, quando observam fielmente o alinhamento do discurso da narrativa em vigor aprovada.

Quadro 2: Tarefas desenvolvidas na execução da OpInfo.

Tarefas normalmente desenvolvidas na execução da campanha de OpInfo
Acompanhamento dos noticiários locais e nacionais veiculados pelas mídias.
Compilação das informações recebidas da CRI relacionadas à identificação de vetores de influência.
Coordenação das ações de apoio aos integrantes das Seções de Comunicação Social e de Assunto Civil-Militar dentro da AOp.
Coordenação da defesa cognitiva dos integrantes que estiveram em contato direto com a população.
Participação no processo decisório em conjunto com as demais seções do Estado-Maior.
Contribuição para a consciência situacional e o estabelecimento da narrativa dominante.

Fonte: O autor.

5. Lições aprendidas nas OpInfo durante as Missões Conjuntas do MD

No intuito de melhor abordar as experiências colhidas durante a realização das OpInfo nas Missões Conjuntas, o tema foi subdividido em: fatos observados, avaliação dos indicadores da campanha e manutenção do domínio do ambiente informacional.

5.1. Fatos observados nas Missões Conjuntas das Forças Armadas

A Inteligência vem se mostrando vital para as Operações de Informação, sendo desejável a sua participação em todo o ciclo do conhecimento necessário ao planejamento, à condução e à avaliação das atividades das Capacidades Relacionadas à Informação.

Doutrinariamente, as ações de OpInfo e Comunicação Social (ComSoc) são controladas no mais alto nível hierárquico, uma vez que o ambiente informacional é único por não haver separação entre os níveis, que variam do político ao tático. Com isso, as apreciações dos produtos, o tipo de propaganda (branca, cinza e negra)[1] e a forma de disseminação são prerrogativas do comandante no mais alto nível hierárquico.

Um desafio à parte é a busca por velocidade no processo decisório e consciência situacional diante da evolução dos acontecimentos previstos pelo conceito conhecido como Ciclo OODA (Observar, Orientar, Decidir, Agir). O desafio é vencido com liberdade de ação e simplificação do canal de comunicação entre o Comandante do EMCCj e os integrantes na cena de ação, que poderão atuar em áreas de difícil acesso e comunicação.

O caso particular das Operações na Amazônia e a extensa fronteira pluvial requer um olhar atento nos comunicadores-chave e/ou nas lideranças locais, que podem incitar a população local contra as operações de combate aos crimes transfronteiriços e ao garimpo ilegal. Quanto ao garimpo ilegal, a população local carece de assistência e emprego, e parte dela depende dessa atividade para o sustento familiar.

Nesse sentido, são fundamentais ações de contrapropaganda mitigatória para expor a manipulação e a falta de credibilidade das lideranças negativas, além de fomentar o sentimento de patriotismo, tão degradado nessas localidades em razão da notória falta de infraestrutura do aparato estatal.

Figura 1: Operação Ágata Fronteira Norte, 28 jul. 2023.

Fonte: Flickr, 2023.

Quanto às atribuições subsidiárias, como Garantia da Lei e da Ordem (GLO) e Ajuda Humanitária, é importante destacar a relevância das OpInfo no que tange ao incentivo às autoridades e à população assistida para se engajarem nas diversas tarefas que seriam executadas apenas pelas Forças Armadas e pelos OSP. Embora seja difícil mensurar em números, uma vez que depende de cada situação, pode-se vislumbrar grande redução do quantitativo de militares envolvidos, recursos despendidos e esforço logístico com transporte, material, alimentação e acomodação.

5.2. Avaliação dos indicadores da campanha de OpInfo

Embora haja previsão de destacamentos na cena de ação para a realização de pesquisa de campo visando à mensuração da campanha com base nos efeitos desejados da Operação, o esforço empregado na avaliação da OpInfo no que se refere às medidas de desempenho e eficácia apresentam resultado abstrato.

As métricas para mensuração apresentam certa dificuldade, pois, além da maioria dos produtos ser disseminada por colaboradores, os destacamentos não possuem controle nem do alcance da influência da disseminação dos produtos, e nem da distância ou da quantidade de pessoas atingidas. Esse controle fica com os vetores de propagação dos produtos realizado por colaboradores por meio de suas rádios, empresas de ônibus, *sites* de universidades, prefeitura, Câmara de Vereadores, entre outros.

Dessa forma, o sucesso do principal ponto decisivo informacional (apoio da população local às ações das Forças Armadas) não pode ser plenamente mensurado, uma vez que o controle está fora da gerência da seção de OpInfo. A título de exemplo, podem ser citados o número de denúncias computado pelo Disque Denúncia, que fica a cargo dos OSP, ou o recebimento de *feedback* das postagens de uma determinada rádio local no seu *site*.

A avaliação da internalização das ideias-força propagadas nos produtos por parte do público-alvo naturalmente é carregada de subjetividade, o que demanda a continuidade dessas ações por um longo período de tempo para que haja assertividade. Não obstante, o emprego de TI, *software* e inteligência artificial para o assessoramento é bem-vindo. Ressalta-se que uma AOp não muito extensa aumenta a possibilidade de sucesso nas medidas de desempenho e alcance eficaz dos produtos da campanha de OpInfo atinente ao público-alvo.

[1]Propaganda Branca é aquela assinada, que identifica claramente a sua origem e é disseminada e endossada pela fonte. Propaganda cinza é aquela em que os produtos ocultam ou não identificam a sua origem sem, no entanto, pretender atribuí-la a outra origem diferente da verdadeira. A propaganda negra é produzida de forma que a sua origem seja atribuída a outra fonte diferente da real.

Figura 2: Dados mensurados na Operação Ágata Sul 2023.

Fonte: Jornal Noroeste, 2023.

Figura 3: Dados mensurados na Operação Ágata Oeste 2023.

Fonte: Destacamento de Operações Psicológicas.

5.3. Manutenção do domínio do ambiente informacional

A pesquisa sobre os habitantes e as forças oponentes na AOp deve ser um processo cotidiano e contínuo, realizado diariamente por Organização Militar sediada no local, podendo contar com a participação de instituições diversas nesse processo, como, por exemplo, escolas e universidades locais. O detalhamento e a análise sistemática do público-alvo e das circunstâncias reinantes no meio ambiente atual geram um banco de dados extremamente importante para o início dos trabalhos dos operadores do ambiente informacional, conhecido como Levantamento de Área para Operações de Informação (LAOI) e Levantamento de Área para Operações Psicológicas (LAOP).

Figura 4: Operação Ágata Oeste 2023.

Fonte: Assessoria de Comunicação Social do Ministério da Defesa.

Por outro lado, é comum, após o deflagrar de uma OpInfo, a atualização mediante contato estreito com a população para a entrega de um banco de dados mais robusto como legado útil à Estratégia Militar de Defesa. Esse documento constitui um valioso subsídio para o Estudo de Situação que, constantemente atualizado, fornece informações relevantes sobre os fatores fisiográficos, políticos, econômicos, psicossociais, militares e de opinião pública da área onde se pretende atuar.

Assim sendo, ao iniciar um planejamento, o ideal é apenas fazer uma breve atualização dos estudos já prontificados por especialistas locais em razão da premência do tempo alocado. Nessa ocasião, conta-se com a participação das seções de Planejamento, Inteligência e Operações, que, juntamente com especialistas em OpPsc, coordenam estreitamente suas atividades com foco nas análises do público-alvo local, nas propagandas adversas e na produção de conhecimentos correntes.

Nas operações ofensivas, o elemento surpresa é sempre um fator chave; as OpInfo, especialmente, ampliam as opções de linhas de ação cinéticas no sentido de manipular a consciência situacional de integrantes adversos, por exemplo, quanto ao verdadeiro local onde será desencadeada a ação, à data da operação e à magnitude da força aplicada.

No entanto, uma breve avaliação do ganho operacional com a coordenação das CRIs frente a um possível

risco de dano colateral político recomenda cautela e liberdade das ações ilusionistas. Ataques eletrônicos e cibernéticos, assim como as propagandas cinza e negra não costumam ser autorizados no Brasil, o que limita tanto a capacidade de obtenção de dados negados das organizações criminosas (OrCrim) quanto a interrupção do seu fluxo de comunicação e a indução a equívocos.

Conclusão

Após analisar as especificidades das Operações de Informação, levando em consideração as experiências constatadas nas Operações Conjuntas, pode-se inferir que a estrutura existente dedicada às OpInfo ainda se encontra em consolidação, carecendo de recursos humanos habilitados nas tarefas de Estado-Maior.

O paulatino desenvolvimento da atividade é uma realidade, uma vez que as OpInfo propiciam não só a prática da coordenação das CRIs, normalmente adjudicadas à FCjOpEsp na AOp, mas também o aprendizado com a sinergia entre OSP, prefeitura, Câmara Municipal, instituições de ensino, organizações governamentais, ONGs, vetores de influência e a população civil local, entre outros segmentos da sociedade.

Por fim, como legado das OpInfo executadas nas missões conjuntas, é desejável que seja mantida de forma perene, por organização militar local, a modelagem da percepção e da aceitação da população do seu entorno às ideias-força da missão, além da continuidade da criação dos laços de amizade e cooperação, tão necessários para a execução das diversas missões diretamente relacionadas ao público, como ajuda humanitária, GLO e combate aos crimes nos ambientes marítimo, ribeirinho e terrestre.

Referências Bibliográficas

BRASIL. Estado-Maior da Armada. **Doutrina de Operações de Informação**. 62 páginas. Brasília: EMA, 2018.

FLICKR. Página Oficial da Marinha do Brasil. Imagens oficiais da atuação da Marinha do Brasil. **Operação Ágata Fronteira Norte – 2023**. Disponível em: <https://www.flickr.com/photos/mboficial/53119136240/in/album-72177720310501706/>. Acesso em: 28 fev. 2024.

JORNAL NOROESTE. **Exército realiza Operação Ágata na região**. Publicação: 06 jul. 2023. Disponível em: <https://jornalnoroeste.com.br/noticia/geral/exercito-realiza-operacao-agata-na-regiao>. Acesso em: 28 fev. 2024.

MCNEILLY, Mark. **Sun Tzu e a arte da guerra moderna**. Rio de Janeiro: Record, 2003.

VISACRO, Alessandro. **A guerra na Era da Informação**. São Paulo: Ed. Contexto, 2018.

_____. **Guerra Irregular: terrorismo, guerrilha e movimentos de resistência ao longo da história**. São Paulo: Ed. Contexto, 2009.

WOLOSZYN, André Luís. **Guerra nas Sombras**: os bastidores dos serviços secretos internacionais. São Paulo: Ed. Contexto, 2013.

Guerra Cibernética nas atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos

8

Capitão de Corveta (AFN) **Vanderlan** Silva da Costa

É graduado pelo Curso de Formação de Oficiais do Centro de Instrução Almirante Wandenkolk. Ao longo de sua carreira, realizou diversos cursos, com destaque para o Curso de Aperfeiçoamento de Oficiais do Corpo de Fuzileiros Navais (CAOCFN), o Curso de Guerra Cibernética para Oficiais e o Curso Superior (C-Sup). Entre as principais comissões, foi Comandante de Pelotão no 1º Batalhão de Infantaria de Fuzileiros Navais (Batalhão Riachuelo) e Encarregado da Seção de Ações Cibernéticas da extinta Subchefia de Inteligência no Comando de Operações Navais.

Introdução

Ao longo da história, tem-se observado que os contendores nos conflitos bélicos que prontamente se adaptam e integram novas tecnologias aos seus arsenais e estratégias obtêm vantagens decisivas sobre seus adversários. Esse fenômeno foi evidenciado pela introdução de elementos como a cavalaria e pelo uso de bigas, arcos, balestras e armas de fogo, entre outros inventos. Atualmente, as inovações tecnológicas continuam a remodelar os campos de batalha, fornecendo meios inovadores para alcançar a vitória (BRASIL, 2022a).

Figura 1: As inovações no campo de batalha.

Fonte: O autor.

Outro aspecto crucial é a aquisição de informações detalhadas sobre as forças oponentes, o que se mostra fundamental para o planejamento e a execução de operações militares exitosas. Nesse panorama, é comum a utilização de tropas especializadas em Operações Especiais e Inteligência, que desempenham atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA). No entanto, o emprego desses operadores implica desafios significativos em termos de Comando e Controle (C2), logística e manutenção do sigilo operacional.

Para mitigar esses desafios, buscando antecipar a coleta de informações e minimizar a exposição dos operadores em territórios hostis, várias nações têm desenvolvido e implementado ferramentas, técnicas e métodos de sensoriamento remoto. Entre eles, destaca-se o uso de plataformas satelitais, drones e sistemas de Guerra Eletrônica. Uma abordagem crescentemente relevante na aquisição de conhecimento é a Guerra Cibernética (GCiber), sobretudo através das ações de Exploração Cibernética (ExplCiber) e Ataque Cibernético (AtqCiber). Essas estratégias são empregadas para exfiltração de dados, estabelecimento e manutenção de vigilância e localização de tropas.

Embora a Guerra Cibernética exija recursos humanos e equipamentos altamente especializados, seus desafios em termos de Comando e Controle, Logística e manutenção do sigilo são consideravelmente menos complexos que aqueles associados ao emprego de operadores especiais, Inteligência ou plataformas de sensoriamento remoto.

Portanto, este artigo busca demonstrar como as ações de Guerra Cibernética podem ser decisivas nas atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos em Operações Navais.

1. Guerra Cibernética

Conforme apontam Singer e Friedman (2017), a Guerra Cibernética se estabelece como uma realidade

crescente nas esferas das operações militares e da segurança nacional, diferenciando-se dos conflitos tradicionais por ocorrer no ciberespaço – um domínio virtual que transcende fronteiras geográficas, propicia ações anônimas e tem rastreamento complexo.

Paralelamente, a Doutrina Militar de Defesa Cibernética do Brasil (BRASIL, 2014) conceitua a Guerra Cibernética como um tipo de conflito operado no ciberespaço, caracterizado por operações ofensivas e defensivas que envolvem sistemas computacionais, redes e ativos de informação. Essa dimensão do campo de batalha moderno foca no uso de tecnologias digitais para obter vantagem estratégica e infligir danos ao oponente. Nesse cenário, o emprego da Guerra Cibernética abrange ataques cibernéticos, espionagem digital e sabotagem de infraestruturas vitais.

Figura 2: Representação dos guerreiros cibernéticos.

Fonte: O autor.

Em consonância, a Doutrina Militar Naval (BRASIL, 2017) descreve a Guerra Cibernética como uma ação de guerra naval aplicável nos níveis operacional e tático visando objetivos ofensivos e defensivos e operando em contextos diversos, como operações de Inteligência e de Informação. As ações cibernéticas são classificadas em três categorias principais: Ataque Cibernético, Exploração Cibernética e Proteção Cibernética.

Dias (2022) enfatiza que as Operações Cibernéticas, sejam ofensivas ou defensivas, podem visar alvos que estejam no espaço cibernético ou que sejam acessíveis por ele. Assim, é importante reconhecer que, em operações militares ofensivas, as ações cibernéticas não se limitam a estratégias ofensivas, e vice-versa. A exploração, o ataque e a proteção cibernética desempenham papéis fundamentais em ambos os contextos, pois, mesmo em operações militares ofensivas, a proteção das próprias forças é essencial, assim como a capacidade de realizar contraofensivas em operações defensivas, alterando o curso do conflito e estabelecendo a iniciativa das ações, inclusive no espaço cibernético.

Um exemplo histórico significativo do uso da Guerra Cibernética é o ataque ao programa nuclear do Irã através do *malware* Stuxnet, descrito por Singer e Friedman (2017) como uma ferramenta avançada projetada para sabotar as centrífugas nucleares iranianas e comprometer a capacidade de enriquecimento de urânio do país. Esse ataque exemplifica o potencial das operações cibernéticas para causar danos significativos às infraestruturas críticas de uma nação.

Figura 3: Ataque cibernético Stuxnet EUA-Israel ao Irã.

Fonte: Yahoo! News, 2019.

Um caso contemporâneo envolve o conflito entre a Federação Russa e a Ucrânia, iniciado na crise da Crimeia em 2014. Nesse contexto, o ciberespaço tem sido um campo de batalha para os dois lados e também para coletivos de *hackers*. A Rússia, em particular, tem realizado ataques cibernéticos para apoiar suas ações militares cinéticas, causar impacto no campo informacional e obter dados estratégicos (CAMPANY, 2022; KILIAN, 2022).

No contexto das Operações de Inteligência, a Guerra Cibernética possibilita a obtenção de informações estratégicas, conforme delineado no Manual de Inteligência de Fuzileiros Navais (BRASIL, 2021a). Isso inclui a determinação e o dimensionamento da presença inimiga, viabilizados por ações de exploração e ataque cibernético que monitoram comunicações de dados e rastreiam dispositivos computacionais.

Por fim, duas características da Guerra Cibernética de especial relevância para as Operações Anfíbias são seu alcance global e a vulnerabilidade das fronteiras geográficas. Essas características simplificam significativamente as demandas logísticas e de comando e controle em comparação com as exigências para a atuação de Operadores Especiais ou de Inteligência infiltrados em território inimigo, permitindo operações efetivas no território adversário sem presença física.

2. Ações de Exploração e Ataque Cibernético

Embora a Doutrina Militar Naval (BRASIL, 2017) estabeleça a distinção entre Exploração e Ataque Cibernético como categorias diferentes, na prática esses dois aspectos se entrelaçam e dependem mutuamente um do outro

a tal ponto que, para os propósitos deste estudo, serão considerados como uma única entidade integrada.

A Doutrina Militar Naval (BRASIL, 2017) atribui à Exploração Cibernética o papel de fornecer consciência situacional do ambiente cibernético e apoiar as ações de Ataque Cibernético. Essa relação evidencia que um ataque eficaz requer uma ação prévia de esclarecimento ou reconhecimento fornecida pela Exploração Cibernética. Além disso, a contribuição da Exploração Cibernética para a geração de conhecimento de Inteligência está intrinsecamente ligada à manipulação de informações em ativos de interesse, uma função que a Doutrina Militar Naval (DMN) associa ao Ataque Cibernético (BRASIL, 2017). A DMN categoriza tanto a exploração quanto o ataque como geradores de efeitos ofensivos desejados, sublinhando ainda mais sua conexão inerente.

Conforme o Manual de Guerra Cibernética dos Grupamentos Operativos de Fuzileiros Navais (BRASIL, 2022a), a Exploração Cibernética é vista como uma fase preparatória essencial para a realização do Ataque Cibernético, podendo ser abrangida por ele.

Portanto, este artigo, ao abordar as Ações de Exploração e Ataque Cibernético (ExpAtqCiber), salienta as ações ofensivas de Guerra Cibernética visando aos seguintes objetivos:

- reconhecimento de espaços cibernéticos de interesse;
- obtenção de acesso a dados, redes, serviços ou sistemas dentro de um espaço cibernético de interesse;
- exfiltração de dados de dispositivos, serviços ou sistemas em um espaço cibernético de interesse;
- neutralização, degradação, corrupção ou destruição de um serviço ou sistema em um espaço cibernético de interesse.

Conforme será discutido mais adiante, ao tratar das atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos, os três primeiros objetivos listados estão diretamente relacionados a essas atividades. Quanto aos dados mencionados, eles podem incluir imagens, áudios e arquivos, enquanto os serviços e os sistemas abrangem as ferramentas de comando e controle, que podem fornecer informações cruciais para estabelecer a ordem de batalha do inimigo [1].

3. Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA)

As atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA) são fundamentais para a coleta coordenada de informações sobre o ambiente operacional, permitindo tanto a identificação e o monitoramento de alvos como o acompanhamento e a avaliação das ações conduzidas por tropas ou plataformas de armas. Essas atividades são cruciais na obtenção de conhecimentos precisos, relevantes e tempestivos que capacitem os comandantes a tomarem decisões com adequada consciência situacional e conduzirem operações eficazes (CANADA, 1999).

Segundo o *Congressional Research Service* (2022), as atividades de Inteligência, Vigilância e Reconhecimento (ISR) englobam a coleta, a análise e a disseminação de informações essenciais para o suporte à tomada de decisões. A Inteligência é adquirida através de múltiplas fontes, incluindo sensores eletrônicos, vigilância visual, interceptação de comunicações e fontes humanas. Esses dados são processados e avaliados para se transformarem em conhecimento de Inteligência, que é posteriormente distribuído aos comandantes e às unidades em campo.

Com o avanço tecnológico, as atividades de IRVA evoluem, incorporando inteligência artificial, análise de *big data* e sistemas de sensoriamento avançados, que aumentam a precisão da coleta de informações, agilizando a análise e aprimorando a eficiência na disseminação da Inteligência aos decisores. A força aérea americana considera o domínio cibernético como um dos campos para obtenção e integração de conhecimentos através das atividades de IRVA em apoio a operações letais e não letais (CONGRESSIONAL RESEARCH SERVICE, 2022).

A doutrina militar canadense aponta que a IRVA "interconecta vigilância, aquisição de alvos e reconhecimento para expandir a consciência situacional do comandante e orientar a manobra e os meios de ataque ofensivos" (CANADA, 1999). Os dados coletados por diversos sensores são tratados em centros de coleta e análise de inteligência, com agências e fontes atuando como sensores, incluindo equipes de reconhecimento especializadas e sistemas de informação.

[1] Ordem de batalha – "Informações sobre pessoal, unidades e equipamentos de uma força, amiga ou inimiga, incluindo, se possível, efetivo, identificação, localização, estrutura de comando, históricos e outros dados relativos a unidades e personalidades militares" (BRASIL, 2015).

O Manual de Inteligência de Fuzileiros Navais do Brasil (BRASIL, 2021a) não menciona diretamente a integração das atividades de IRVA, mas as considera parte da Inteligência Operacional com o objetivo de reduzir a incerteza e aumentar a capacidade decisória do comandante, permitindo o planejamento, a condução e a sustentação das operações militares. Os conceitos de IRVA, seu processamento e difusão pelo Centro de Análise de Inteligência são correlacionados às diversas Operações Navais.

Kilian (2022) descreve a névoa da guerra como um desafio superado pela Inteligência, que utiliza, entre outras ferramentas, a exploração cibernética. No Manual de Inteligência de Fuzileiros Navais (BRASIL, 2021a), a Inteligência é definida como Pesquisa de Inteligência, que se destina à obtenção de dados negados relevantes para o planejamento e a condução de operações militares empregando pessoal qualificado e meios especializados, inclusive tecnológicos.

O Reconhecimento foca na obtenção de dados sobre o inimigo, o terreno e as condições meteorológicas na Área de Operações (BRASIL, 2008), enquanto a Vigilância se concentra no acompanhamento de forças inimigas já identificadas, mantendo um fluxo contínuo de informações sobre sua localização, composição e movimentos (BRASIL, 2021a) e utilizando meios variados para observar o campo de batalha (BRASIL, 2008).

Por fim, as atividades de Aquisição de Alvos visam identificar, localizar e acompanhar alvos designados ou de oportunidade, aconselhando sobre o momento ideal para engajamento e avaliando os danos resultantes do emprego de fogos, sejam cinéticos ou não cinéticos (BRASIL, 2021a).

Assim, apesar de diferenças terminológicas na literatura, as atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos são identificadas como componentes vitais para o processo decisório do comandante, pois utilizam diversas fontes e agências para obtenção, processamento, integração e disseminação de informações cruciais e tempestivas, fundamentais para o planejamento, a execução, o controle e a sustentação das operações militares.

4. A Guerra Cibernética empregada em atividades de IRVA

Como observado anteriormente, as Operações Navais demandam um fluxo constante, coerente e tempestivo de dados em todas as suas fases. A integração das atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos com as ações de Guerra Cibernética amplia significativamente as possibilidades na construção de conhecimentos essenciais, atuando estas últimas como sensores fundamentais nesse processo.

Do ponto de vista organizacional, para a efetivação dessa tarefa podem ocorrer pelo menos duas configurações distintas: a estrutura de Guerra Cibernética (GCiber) pode integrar a Organização por Tarefas (OrgTar) de uma Força-Tarefa (FT), uma Força Componente (FCte) ou um Grupamento Operativo de Fuzileiros Navais (GptOpFuzNav); ou, alternativamente, a estrutura de GCiber pode estar subordinada a uma FT ou uma FCte de Guerra Cibernética, atuando em benefício dos demais (FT/FCte/GptOpFuzNav).

No primeiro cenário, é aconselhável que a estrutura de GCiber esteja diretamente subordinada ao Comandante da Força-Tarefa (CFT) ou do GptOpFuzNav, facilitando a continuidade e a eficiência no Comando e Controle (C2).

No segundo cenário – a formação de uma Força-Tarefa de Guerra Cibernética dentro da estrutura da Força Naval Componente (FNC) –, uma Força Conjunta de Guerra Cibernética (FCjGCiber) ou um Comando Conjunto de Guerra Cibernética (CCjGCiber) podem ser opções mais adequadas, pois são diretamente subordinadas ao Comandante do Teatro de Operações (ComTO) ou aos níveis político e estratégico (BRASIL, 2014). Essa configuração, embora implique uma coordenação adicional, alivia o CFT, ou o CmtGptOpFuzNav, das responsabilidades adicionais de C2. Contudo, é necessário avaliar as vantagens e as desvantagens de operar com tais Forças ou Comandos em detrimento de uma estrutura própria de GCiber, especialmente considerando a agilidade necessária nas Operações Navais em andamento.

4.1. Guerra Cibernética na fase do planejamento

Durante o planejamento das Operações Navais, uma dificuldade primária é a escassez de conhecimentos atuais sobre a Área de Operações (AOp) e os desafios associados ao estabelecimento de equipes de reconhecimento e vigilância no terreno, o que limita os dados aos já existentes em bases de dados ou bibliotecas (BRASIL, 2021b).

Após a definição da AOp, ações de Guerra Cibernética podem ser planejadas para adquirir conhecimentos tanto sobre a área e os objetivos potenciais como sobre a presença e os movimentos de tropas ou meios inimigos. Essas operações podem ser classificadas como Operações de Apoio a cargo de Força Amiga ou Operações Componentes.

Para realizar essas ações iniciais, a Força responsável deverá buscar obter e manter o acesso a sistemas de monitoramento, vigilância eletrônica e circuitos

fechados de TV nos objetivos e vias de transporte relevantes, bem como acessar sistemas de comando e controle dos objetivos e das forças inimigas presentes na AOp ou capazes de reforço.

Todos os conhecimentos adquiridos devem ser transmitidos prontamente ao Centro de Análise de Inteligência, que integrará essas informações com as obtidas por outras fontes.

Uma característica distintiva da Guerra Cibernética é a capacidade de gerar efeitos em locais específicos sem necessidade de proximidade física (BRASIL, 2022a). Portanto, a unidade responsável pelas ações ofensivas na AOp não precisa estar fisicamente presente, operando idealmente a partir da retaguarda. Isso permite manter operações contínuas e aproveitar melhores condições de conectividade para comunicação com o Comando da FT/GptOpFuzNav e para a execução de suas ações.

Se forem identificados objetivos que exigem proximidade física, como redes sem fio, Bluetooth ou dispositivos físicos segregados, uma parcela da Força ou Grupo-Tarefa poderá ser alocada especificamente para essas tarefas mais especializadas.

4.2. Guerra Cibernética durante a execução da Operação

Durante essa fase, a investigação de dados via espaço cibernético deve se concentrar nas variações das condições da Área de Operações. Em relação à Inteligência, o foco deve ser a obtenção de dados que revelem o grau de consciência situacional do inimigo acerca da presença e da localização da Força-Tarefa Anfíbia. Isso inclui informações sobre movimentações de tropas, meios navais e aéreos inimigos, comunicações e transmissão de dados sobre contraofensivas inimigas e os efeitos das ações da Força-Tarefa.

Nas atividades de Reconhecimento e Vigilância, a ênfase deve ser dada à observação de alterações no dispositivo inimigo na Área de Operações. Essa vigilância deve incluir também as tropas inimigas em condições de reforço, monitorando deslocamentos de tropas e meios navais inimigos na AOp com o objetivo de fornecer alertas antecipados e detectar movimentações por direções inesperadas.

Quanto à Aquisição de Alvos, é essencial buscar dados na Lista Integrada e Priorizada de Alvos, além de monitorar os efeitos dos fogos cinéticos e não cinéticos, mantendo atualizações sobre possíveis mudanças de posição.

As ações de Exploração e Ataque Cibernético devem estar em andamento nessa fase com o objetivo de exfiltrar informações de bases de dados e sistemas de Comando e Controle inimigos para atualizar a ordem de batalha do inimigo o mais próximo possível do tempo real.

O Comando e Controle nessa fase se torna mais complexo, visto que a comunicação com o Comando da Força-Tarefa ocorrerá exclusivamente através dos canais disponíveis nos meios navais onde esses Comandos estejam embarcados.

A Área de Operações da Força ou Grupo-Tarefa de Guerra Cibernética pode ser ampliada para incluir locais de onde possam ser mobilizadas tropas inimigas capazes de alterar o equilíbrio de forças na AOp.

Finalmente, a Força ou Grupo-Tarefa de Guerra Cibernética pode permanecer ativa após a conclusão da Operação para apoiar futuras ações de outras FTs na AOp.

Conclusão

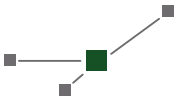
Ao longo deste artigo, foram exploradas as possibilidades de emprego da Guerra Cibernética em atividades de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA) para aprimorar a coleta de informações que auxiliem no planejamento e na execução de Operações Navais.

Buscou-se apontar que as ações de Guerra Cibernética podem ser integradas eficazmente em todas as fases de uma Operação Naval, atuando como sensores cruciais para as atividades de IRVA. Essas ações demandam menos esforço logístico e de Comando e Controle, além de potencialmente envolverem um risco menor de comprometimento do sigilo em comparação com a infiltração e o emprego de Operadores Especiais ou de Inteligência.

Observou-se que tais ações podem ser iniciadas já na fase de planejamento, contribuindo para mitigar as incertezas e as complexidades inerentes ao planejamento, à execução e ao controle das operações militares. Essas ações se mantêm ativas nas fases subsequentes e, se necessário, podem continuar apoiando operações futuras.

Conclui-se, sem pretender esgotar o tema, que a integração dos dados coletados por meio das ações de Guerra Cibernética com aqueles obtidos por outros sensores — como equipes de reconhecimento, operadores de Inteligência em território inimigo e plataformas de sensoriamento remoto — enriquece o fluxo de dados para o Centro de Análise de Inteligência (CAI). Com uma quantidade maior de dados, o CAI pode disseminar informações mais detalhadas e tempestivas, aumentando a consciência situacional dos Comandantes de Forças-Tarefa ou de Grupamentos Operativos de Fuzileiros Navais.

Este artigo buscou destacar, ainda, a importância deste tema para a Marinha do Brasil. O avanço tecnológico, ao oferecer novas ferramentas para as Operações Navais, também aumenta a complexidade do campo de batalha, introduzindo o espaço cibernético como um novo domínio operacional. Assim como ocorreu no passado, quanto maior a consciência situacional do comandante, maiores as chances de tomar decisões acertadas e de superar a capacidade de resposta da força oponente. Dessa forma, ressalta-se a necessidade de obter informações operacionais com volume, qualidade e tempestividade adequados.



Referências Bibliográficas

BRASIL. Marinha do Brasil. Comando-Geral do Corpo de Fuzileiros Navais. **Manual de Ações de Guerra Cibernética dos Grupamentos Operativos de Fuzileiros Navais – CGCFN-60.2.** 1. ed. Rio de Janeiro, 2022a.

_____._____._____. **Manual de Inteligência de Fuzileiros Navais – CGCFN-20.** 1. rev. Rio de Janeiro, 2021a.

_____._____._____. **Manual de Operações de Esclarecimento de Fuzileiros Navais – CGCFN-1-4.** 1. rev. Rio de Janeiro, 2008.

_____._____._____. **Manual de Operações de Força de Desembarque – CGCFN-1-1.** 1. rev. Rio de Janeiro, 2021b.

_____._____._____. **Manual de Planejamento dos Grupamentos Operativos de Fuzileiros Navais – CGCFN-60.4.** 1. ed. Rio de Janeiro, 2022b.

_____._____. Estado-Maior da Armada. **Doutrina Militar Naval (DMN) – EMA-305.** 1. ed. Brasília, 2017.

_____._____._____. **Manual de Planejamento Operativo da Marinha – EMA-331, Vol I** – Processo de Planejamento Militar. 1. ed. Brasília, 2006a.

_____._____._____. **Manual de Planejamento Operativo da Marinha – EMA-331, Vol II** – Diretivas. 1. ed. Brasília, 2006b.

_____._____._____. **Manual de Planejamento Operativo da Marinha – EMA-331, Vol III** – O Trabalho das seções de Estado-Maior. 1. ed. Brasília, 2006c.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética.** 1. ed. Brasília, 2014.

_____._____. **Glossário das Forças Armadas.** 5. ed. Brasília, 2015.

_____. Presidência da República. **Decreto nº 95.480**, de 13 de dezembro de 1987. Dá nova redação para a Ordenança Geral para o Serviço da Armada. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1980-1987/decreto-95480-13-dezembro-1987-446244-publicacaooriginal-1-pe.html>. Acesso em: 26 jul.2023.

CAMPANY, Luiggi. Ameaças Híbridas e Guerras Híbridas – uma breve análise aplicada aos conflitos russo-ucranianos de 2014 e 2022. **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

CANADA. Chief of the Defence Staff. **Information Operations – B-GL-300-005/FP-001**. Kingston, 1999.

CONGRESSIONAL RESEARCH SERVICE (CRS). **Intelligence, Surveillance and Reconnaissance Design for Great Power Competition**. CRS Reports Book 12. Coord. Hoehn, John R.; Smagh, Nishawn S. Kindle edition. Washington: Nimble Books LLC, 2022.

DIAS, Claudio Eduardo Silva. As Operações de Informação e os Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav). **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

KILIAN, Rudibert. Análise do Conflito entre Rússia e Ucrânia. **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

SINGER, P. W.; FRIEDMAN, A. **Segurança e Guerra Cibernéticas:** o que todos precisam saber. Traduzido por Geraldo Alves Portilho Junior. Rio de Janeiro: Biblioteca do Exército, 2017.

VALENTINI, Luis Felippe. Forças Anfíbias Combinadas: o Grupamento Operativo de Fuzileiros Navais em operações multinacionais. **Revista Âncoras e Fuzis**, ano XXIV, nº 53. Rio de Janeiro: Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais, 2022.

YAHOO! NEWS. **Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran**. By Kim Zetter and Huib Modderkolk. September 02, 2019. Disponível em: <https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html?guccounter=1>. Acesso em: 29 fev. 2024.

Cibersegurança Naval: navegando em águas turbulentas na era da Guerra Cibernética

9

Capitão-Tenente Warlley **Paulo Freire**

É formado em Ciências Navais pela Escola Naval, com Habilitação em Eletrônica. Em sua trajetória profissional, realizou diversos cursos, com destaque para: Pós-graduação em Segurança das Informações e Comunicações (CIAW/PUC-RIO) e em Guerra Cibernética (CIGE), *Continuous Monitoring and Security Operations* (BASE4 Security) e Inteligência Cibernética (EsIMar). Entre as principais comissões, foi Ajudante do Encarregado da Divisão O-1 na Corveta Júlio de Noronha, Chefe do Departamento de Operações do Navio-Patrulha Fluvial Pedro Teixeira e Encarregado da Divisão O-2 na Fragata Liberal; atualmente, também é Orientador Pedagógico do CAp-A (CIAA).

Introdução

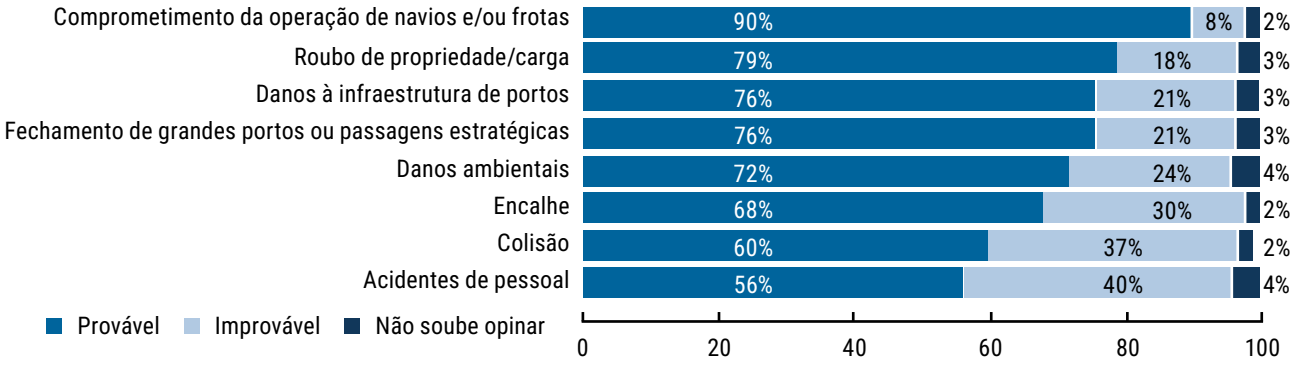
A vertente marítima dos domínios comerciais e militares tem sido a espinha dorsal do comércio internacional e das principais forças de defesa. Segundo o último relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, 2022), em 2022 o setor marítimo movimentou onze bilhões de toneladas em bens, o que representa 80% de todo o volume global de comércio. A evolução do setor marítimo, cada vez mais conectado e digitalizado, tem transformado as operações comerciais e militares no mar, aprimorando a eficiência e a efetividade dos meios navais. Todavia, essa evolução também expõe o setor às crescentes ameaças cibernéticas: dados de 2018 a 2021 mostram um crescimento de 900% nos registros de ataques cibernéticos ao setor marítimo (FREIRE et al., 2021).

Nessa conjuntura, os navios vêm se tornando complexos sistemas ciber-físicos que integram sensores, sistemas de informação e sistemas de controle e automação (FREIRE et al., 2022). Muitos dos sistemas a bordo, como navegação, propulsão e comunicação, são integrados por redes digitais, da mesma forma que os portos dependem de complexos sistemas digitais para logística e segurança. No âmbito militar, navios de guerra operam cada vez mais sob a égide da guerra centrada em redes, com sistemas de comunicação satelitais integrando seus diversos sistemas operativos e de comando e controle.

Doravante, nesses complexos sistemas heterogêneos, cada elemento representa uma potencial vulnerabilidade que pode ser explorada em um ataque cibernético, um potencial elo mais fraco nessa extensa cadeia que pode permitir o comprometimento de outros sistemas do setor marítimo (KESSLER; SHEPARD, 2022).

De forma a dimensionar esse risco, a norueguesa DNV, uma das três maiores sociedades classificadoras de navios do mundo, publicou em seu relatório de Prioridades Cibernéticas para o Setor Marítimo em 2023 uma pesquisa envolvendo 801 profissionais do setor distribuídos em 72 países. Entre as estatísticas apresentadas no documento, uma delas chama a atenção pelo elevado sentimento desses profissionais em relação à ameaça cibernética, como pode ser observado no gráfico da Figura 1.

Figura 1: Expectativa de profissionais do setor marítimo em relação às consequências cibernéticas no futuro próximo.



Fonte: DNV, 2023.

Essa percepção de muitos profissionais reflete o sentimento gerado pelos ataques cibernéticos ao setor marítimo ocorridos no passado que já deixaram grandes cicatrizes. Buscando planejar uma navegação adequada aos desafios vindouros, alguns desses eventos que causaram grande repercussão no setor serão analisados a seguir.

1. Tormentas passadas

Um sábio marinheiro observa o retrospecto dos mares que vai navegar em busca de conhecimentos que o ajudarão em sua rota. Da mesma forma, observar as características dos ataques cibernéticos já ocorridos contra o meio naval propicia um vislumbre do risco adiante. Nesse contexto, um dos eventos de ataques cibernéticos ao setor marítimo de maior notoriedade é, certamente, o de *ransomware*[1] ocorrido em 2017, que afligiu a gigante dinamarquesa Maersk, responsável por operar mais de 70 portos e cerca de 800 navios pelo globo.

É importante ressaltar que a Maersk não era um alvo principal, mas simplesmente se encontrava vulnerável ao *malware* utilizado nessa campanha de *ransomware*. A gênesis desse evento remonta a abril de 2017, quando um grupo *hacker* conhecido como *The Shadow Brokers* vazou um grande número de ferramentas cibernéticas provenientes da CIA e da NSA ao *site WikiLeaks* (KESSLER; SHEPARD, 2022). A mais proeminente dessas ferramentas, conhecida como *EternalBlue*, explorava uma vulnerabilidade em sistemas Windows e, embora a Microsoft tenha publicado uma correção para essa vulnerabilidade em março de 2017, grande parte dos usuários de seu sistema operacional ainda não havia aplicado essa correção quando a primeira onda de ataques ocorreu.

Em maio daquele ano, a primeira onda de ataques começou empregando o *malware* autorreplicante *WannaCry*, uma adaptação da ferramenta publicada no WikiLeaks. Em 48 horas, mais de 230.000 computadores espalhados por 150 países foram infectados, afetando diversos setores, como, por exemplo, o Sistema Nacional de Saúde da Inglaterra, que possuía, em 80% de seus computadores, o sistema operacional Windows XP, vulnerável ao *malware* (KESSLER; SHEPARD, 2022). A Microsoft, então, liberou uma correção de emergência contra o *malware* e o ataque perdeu força em alguns dias.

Um mês depois dos ataques pelo *WannaCry*, um novo *malware* entrou em circulação empregando as mesmas ferramentas. Conhecido como *NotPetya* e com autoria ligada ao grupo *hacker* russo *Cozy Bear*, esse *malware* parecia ter como alvos sites na Ucrânia, mas, devido à sua característica autorreplicante, se espalhou rapidamente pela internet e atingiu a grande rede da Maersk. O ataque obrigou a empresa a paralisar suas operações por vários dias: estima-se que tenha causado um prejuízo entre 200 e 300 milhões de dólares (FORBES, 2017).

Já no âmbito militar, quatro colisões ocorridas em 2017 – envolvendo dois *destroyers* da classe *Arleigh Burke* e dois cruzeiros de mísseis da classe *Ticonderoga* – podem fornecer *insights* das possíveis consequências de um ataque cibernético sofisticado aos meios navais. Apesar de a marinha americana negar que a causa das colisões tenha sido um ataque cibernético, o que é comum em grandes organizações que sofreram esse tipo de ataque por temerem o impacto em suas reputações, dados disponíveis em fontes abertas corroboram um diferente cenário.

Figura 2: Colisões envolvendo meios da marinha americana (*US Navy*) no Pacífico.

Fonte: USNI News, 2017.

Os quatro eventos, todos ocorridos no primeiro semestre de 2017 na região do Pacífico entre a Ásia e a Oceania, evidenciam um mesmo *modus operandi*: os quatro navios navegavam no período noturno em regiões de intenso tráfego quando, subitamente e sem nenhum comando pela equipe do passadiço, tiveram seus lemes completamente travados para um dos bordos. Como consequência dessa situação de "fora de leme" repentina, dois deles – o *USS John McCain* e o *USS Fitzgerald* – colidiram com navios mercantes. O primeiro sofreu um prejuízo material de cerca de 325 milhões de dólares, além da morte de dez de seus marinheiros. O segundo alcançou um prejuízo de 368 milhões de dólares e perdeu sete dos seus militares a bordo. Quanto aos outros dois navios, o *USS Antietam*

[1] *Ransomware*: ataque cibernético no qual um *malware* age de forma a criptografar os dados de seu hospedeiro a fim de cobrar um resgate, geralmente em criptomoedas, em troca da liberação desses dados.

colidiu com a praia sem gerar maiores danos e o *USS Lake Champlain* colidiu com um pequeno pesqueiro, sem causar perda de vidas humanas.

A Figura 2 apresenta uma visão geográfica dos quatro eventos.

No início das investigações, a marinha americana chegou a imputar acusações criminais contra os comandantes dos dois *destroyers* da classe *Arleigh Burke* por conta das vidas perdidas nas duas colisões. Contudo, com o avançar das investigações, as acusações criminais contra os comandantes foram retiradas (FOX NEWS, 2019) e o relatórios finais apontaram despreparo e erros de procedimento como as principais causas das colisões.

Contudo, outras possíveis causas sobre os quatro eventos foram debatidas, e entre elas figura a possibilidade de um ataque de cadeia de suprimentos. Quatro anos antes das colisões, em 2013, acredita-se ter sido iniciado um dos ataques cibernéticos responsáveis por um dos maiores vazamentos de dados de entidades governamentais americanas, o ataque conhecido como *The Big Hack*. Nesse ataque, *microchips* do tamanho da ponta de uma caneta foram implantados em placas de circuito integrado que eram produzidas em Taiwan e enviadas para a Califórnia, onde a empresa *SuperMicro* as empregava na construção de servidores de alta capacidade. Documentos públicos mostraram que esses servidores tiveram como clientes finais várias entidades governamentais americanas, que possivelmente receberam as placas adulteradas. Entre as organizações que receberam esses servidores estão as duas casas do congresso, a NASA e o Departamento de Defesa, inclusive com navios de guerra empregando tais servidores (BLOOMBERG, 2018).

Figura 3: Capa da Bloomberg Businessweek, 2018.

Fonte: Bloomberg, 2018.

Esses *microchips* eram capazes de receber comandos e exfiltrar dados, propiciando aos idealizadores do ataque acesso a dados sensíveis sobre os sistemas usados a bordo dos navios e, consequentemente, como explorá-los. Somente em 2015, a empresa americana *Amazon*, que também estava entre os clientes que adquiriram servidores da *SuperMicro*, percebeu um fluxo anormal de dados saindo de suas redes e, após extensa investigação interna, decidiu por desmontar seus servidores. Finalmente, os *microchips* implantados foram identificados e a empresa tornou público o ataque.

A partir das informações adquiridas por esses *microchips* e considerando que, em 2017, os quatro navios possuíam sistemas ECDIS dotados de posicionamento dinâmico que integravam o sistema de navegação e o sistema de governo, o agente por trás dos ataques reuniu as peças necessárias para findar a cadeia de ataque cibernético (*Cyber Kill Chain*). Teorias sobre o possível gatilho que acionou essa arma cibernética incluem uma junção com Guerra Eletrônica, na qual pulsos radares poderiam ser especialmente preparados para ativar um *malware* sem causar nenhuma mudança de funcionamento perceptível nos radares de navegação, de acordo com Junior e De Sá (2020). Segundo essa abordagem, o efeito dessa arma cibernética seria ativado no momento de maior vulnerabilidade dos navios, como, por exemplo, quando estivessem navegando próximo a grandes navios mercantes, mesmo que totalmente desconectados da internet ou de qualquer conexão externa no momento do ataque.

A análise em conjunto de todos esses eventos isolados, apesar de baseada em suposições, permite um vislumbre de como a capacidade cibernética pode ser empregada contra meios navais. Por meio de uma *Cyber Kill Chain* que se desenvolveu em uma janela temporal de quatro anos, o agente por trás desses ataques empregou técnicas extremamente sofisticadas, como *hardware hacking* e ataques de cadeia de suprimento, para alcançar um objetivo final.

2. Preparar para mau tempo

À medida que a evolução informacional avança, a superfície de ataque dos meios navais continuará aumentando. Destarte, é crucial que entes governamentais e privados entendam o risco atrelado e seus impactos, buscando investir no aprimoramento da cibersegurança dos sistemas navais, que geralmente são pouco maduros no que tange a essa área. Através do levantamento dos riscos e do entendimento da profundidade dessas ameaças, *stakeholders* do setor marítimo podem empregar ações práticas para robustecer suas defesas.

Após o incidente envolvendo a Maersk, a Organização Marítima Internacional (*International Maritime Organization* – IMO) tem enfatizado a importância da implementação de ações efetivas para a segurança dos sistemas a bordo dos meios navais. Em junho de

CIBERSEGURANÇA NAVAL

"O futuro do setor marítimo não mais estará apenas em mares, oceanos e águas interiores, mas também no campo de batalha invisível e transversal do quinto domínio."

2017, o Comitê de Segurança Marítima da IMO adotou a resolução MSC.428 sobre Gerenciamento do Risco Cibernético no setor. O documento tem sua gênese postulando que o Comitê reconhece a urgência de elevar a consciência situacional sobre risco cibernético e vulnerabilidades afetas a fim de fortalecer a segurança do setor (IMO, 2017). A IMO tem amplamente estimulado a adoção de estruturas (*frameworks*) de cibersegurança adequadas para o setor, como o *Guidelines on Cyber Security onboard Ships* (BIMCO, 2016) desenvolvido pelo Conselho Marítimo Internacional, em conjunto com o Conselho Mundial de Navegação e outras organizações correlatas.

Navegar por mares revoltos requer aprestamento adequado, assim como preparar esse gigante setor tão diverso para gerenciar o risco crescente e mitigar as possibilidades de um incidente cibernético a bordo ou no porto. O crescente número de vítimas de ações cibernéticas no meio naval e os eventos significativos já ocorridos têm propiciado uma mudança de postura, com uma tendência positiva de desenvolvimento da Cibersegurança Naval. As ações nesse sentido têm se concentrado em quatro pilares:

- treinamento e conscientização: uma das defesas primárias contra a ameaça cibernética é a conscientização da força de trabalho a fim de elevar sua consciência situacional cibernética. Tanto o setor privado como o militar têm buscado empreender programas de modo a garantir que seu pessoal possa reconhecer e responder perante essa ameaça;
- protocolos de segurança adequados: o emprego de ferramentas de segurança adequadas e bem configuradas é essencial. O uso de *firewall* e sistemas de detecção de intrusão, assim como a realização de auditorias regularmente estão entre as práticas mais bem difundidas;
- colaboração: o compartilhamento de Inteligência sobre as ameaças potenciais e a colaboração internacional para identificar possíveis autores têm produzido ganhos significativos. Projetos como o *Malware Information Sharing Platform* (MISP) têm contribuído para o compartilhamento de Inteligência sobre técnicas, táticas e procedimentos usados pelos *hackers*, propiciando uma consciência compartilhada das possíveis ameaças;
- desenvolvimento seguro: a construção naval e portuária precisa fomentar a ampla adoção do conceito de *Secure by Design*. É essencial que a Cibersegurança seja uma prioridade desde a concepção, com uma abordagem mais proativa a fim de implementar protocolos e sistemas com maturidade de segurança adequada a infraestruturas críticas.

A integração paulatina do setor marítimo aos sistemas digitais apresenta um paradoxo, oferecendo evolução e exposição como dois gumes de uma mesma lâmina. Conforme as ameaças cibernéticas se tornam mais sofisticadas, *stakeholders* privados e militares devem navegar nesses revoltos mares digitais com cautela e tirocínio. O futuro do setor marítimo não mais estará apenas em mares, oceanos e águas interiores, mas também no campo de batalha invisível e transversal do quinto domínio.

Referências Bibliográficas

BIMCO. **The Guidelines on Cyber Security onboard Ships**. p. 36, 2016. Disponível em: <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>. Acesso em: 28 jan. 2024.

BLOOMBERG. **The Big Hack: how China used a tiny chip to infiltrate U.S. companies**. By Jordan Robertson and Michael Riley. Oct. 4, 2018. Disponível em: <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>. Acesso em: 4 mar. 2021.

DNV. **Maritime Cyber Priority 2023: Staying secure in an era of connectivity**. Disponível em: <https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html>. Acesso em: 28 jan. 2024.

FORBES. **NotPetya Ransomware attack cost shipping giant Maersk over $200 million**. By Lee Mathews. Aug. 16, 2017. Disponível em: <https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=6209da744f9a>. Acesso em: 25 ago. 2023.

FOX NEWS. **Navy drops charges against officers involved in fatal USS Fitzgerald collision**. By Bradford Betz. April 11, 2019. Disponível em: <https://www.foxnews.com/us/navy-drops-charges-against-officers-involved-in-fatal-uss-fitzgerald-collision-report>. Acesso em: 14 ago. 2023.

FREIRE, W. P.; et al. Blockchain-based Maritime Monitoring System. 2021 IEEE International Workshop on Metrology for the Sea: Learning to Measure Sea Health Parameters. **MetroSea 2021 – Proceedings**, p. 394-399, 2021. Disponível em: <https://ieeexplore.ieee.org/document/9611587>. Acesso em: 28 jan. 2024.

_____.Towards a Secure and Scalable Maritime Monitoring System using Blockchain and Low-Cost IoT Technology. **Sensors**, v. 22, n. 13, p. 4895, 29 jun. 2022. Disponível em: <https://www.mdpi.com/1424-8220/22/13/4895>. Acesso em: 28 jan. 2024.

INTERNATIONAL MARITIME ORGANIZATION (IMO). Resolution MSC.428(98): **Maritime Cyber Risk Management in Safety Management Systems**. v. 428, June 2017. Disponível em: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf>. Acesso em: 28 jan. 2024.

JUNIOR, W. C. L.; DE SÁ, A. O. Triggering Cyber-electronic Attacks in Naval Radar Systems. **MetroSea 2020** – TC19 International Workshop on Metrology for the Sea, p. 12-16, 2020. Disponível em: <https://www.imeko.org/publications/tc19-Metrosea-2020/IMEKO-TC19-MetroSea-2020-03.pdf>. Acesso em: 28 jan. 2024.

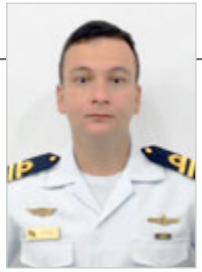
KESSLER, G.; SHEPARD, S. **Maritime Cybersecurity: a Guide for Leaders and Managers**. 2nd edition. [s.l: s.n.]. 2022.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). **Review of Maritime Transport 2022**. Chapter 1: International maritime trade and port traffic. p. 28, 2022. Disponível em: <https://unctad.org/system/files/official-document/rmt2022_en.pdf>. Acesso em: 25 ago. 2023.

U. S. NAVAL INSTITUTE NEWS (USNI NEWS). **Admiral, Captain Removed in ongoing investigations into USS John S. McCain, USS Fitzgerald Collisions; Head of Surface Forces puts in early retirement request**. By Sam Lagrone. Sep. 18, 2017. Disponível em: <https://news.usni.org/2017/09/18/admiral-captain-removed-part-investigation-uss-john-s-mccain-uss-fitzgerald-collisions-head-surface-forces-puts-early-retirement-request>. Acesso em: 14 ago. 2023.

Consciência Situacional Cibernética em Operações Militares Marítimas

10



Capitão-Tenente Françoa **Taffarel** Rosário Corrêa

Graduado em Ciências Navais pela Escola Naval, com especialização em Máquinas e em Tecnologia Nuclear. Foi Oficial de Máquinas na Fragata Rademaker e Encarregado das Equipes de Proteção Cibernética e Exploração da Divisão de Guerra Cibernética do Comando Naval de Operações Especiais. É Tecnólogo em Sistemas de Computação (Universidade Federal Fluminense) e Especialista em Segurança da Informação (UNESA) e em Guerra Cibernética (Exército Brasileiro). Atualmente, é Oficial-Aluno no Centro de Coordenação de Estudos da Marinha em São Paulo (CCEMSP) e candidato a Mestre em Computação com ênfase em Guerra Cibernética (ITA – 2024). É certificado como *Professional and Experienced Penetration Tester* e coautor de três vulnerabilidades críticas em *firmwares* de dispositivos de infraestruturas críticas.

Introdução

A indústria naval, por meio de uma vasta rede composta por navios e portos, além de infraestrutura logística e administrativa, desempenha um papel crucial na dinâmica da economia global. A cada ano, aproximadamente 90% da carga mundial é transportada por essa complexa malha, que, assim como diversas outras indústrias, tem adotado níveis gradativos de automação, interconexão e monitoramento remoto. Contudo, a automação no comércio marítimo não apenas reflete a evolução tecnológica, mas também traz consigo uma vulnerabilidade cada vez maior, destacando-se como alvo primário de ataques cibernéticos. Tal vulnerabilidade é inerente à dependência de tecnologias cruciais para navegação, comunicação e logística.

Nesse cenário, a crescente utilização de operações cibernéticas em ações militares atingiu um ponto crítico de dependência, aumentando a probabilidade de interrupção ou degradação nos sistemas operacionais de um ambiente naval (KUEHL, 2009). As operações cibernéticas, ao criarem um espaço operacional para a ação militar, manifestam-se nas marinhas de maneiras diversas: desde o impacto na superioridade marítima até a perda de domínio em regiões específicas, a negação de informações sobre a posição de navios e a degradação das cadeias de suprimentos.

A progressiva dependência das informações via satélite por parte dos ativos navais ressalta a vitalidade dessas tecnologias para as redes de comunicação, garantindo uma conectividade constante aos Comandos de Força (US DOD, 2018). A capacidade de comunicar e trocar informações torna-se, assim, crucial para o sucesso operacional, proporcionando consciência situacional compartilhada e decisões de comando mais ágeis.

Durante as operações no ambiente marítimo, a comunicação via satélite em cada ativo naval requer monitoramento constante por ativos computacionais dotados da capacidade de detecção e gestão de ameaças. Esses ativos visam fornecer aos operadores a habilidade necessária para garantir que o Comandante da Força-Tarefa Marítima (FTM) tenha a Consciência Situacional Cibernética (CSC) de seus ativos navais, facilitando, assim, o processo de tomada de decisão.

Este artigo é dividido em quatro seções. Inicialmente, é efetuada uma análise de trabalhos correlatos a fim de delinear o conceito de CSC. A segunda seção destaca as características essenciais que um ativo computacional, operando no nível tático, deve possuir para contribuir efetivamente na construção da CSC. Por fim, apresenta-se um modelo de Exercício Cibernético em Operações no Mar focado no processo de tomada de decisão. A Conclusão busca integrar os pontos discutidos, ressaltando a importância da CSC no atual cenário global.

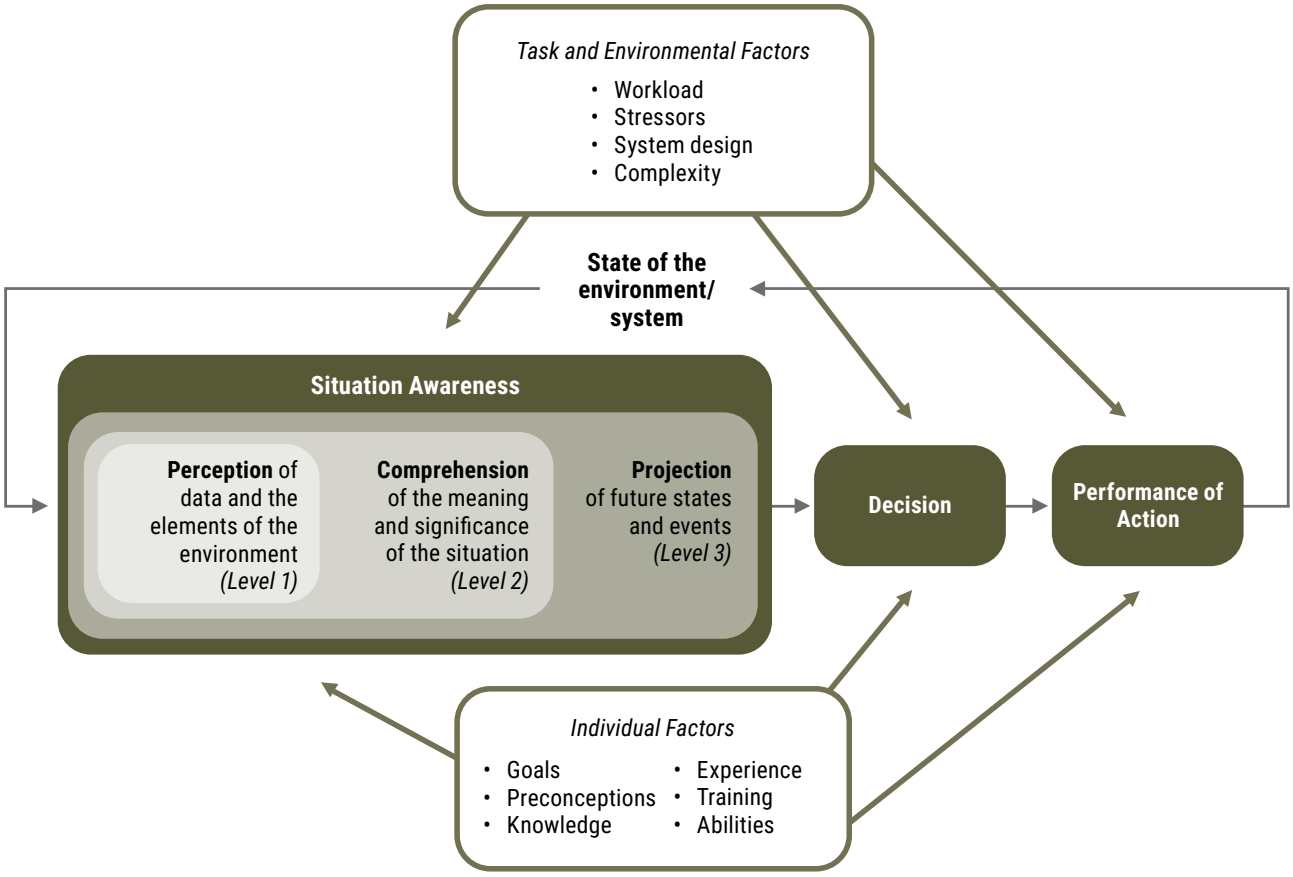
1. Definição de Consciência Situacional Cibernética

De acordo com o Glossário de Termos e Definições da OTAN, a Consciência Situacional (CS) é definida como: "O conhecimento necessário dos elementos no espaço de batalha para tomar decisões bem-informadas" (NATO, 2020b). A Consciência Situacional, integrante do processo da tomada de decisão em ambientes dinâmicos, considera objetivos, expectativas e fatores inerentes à tarefa e ao sistema utilizado.

Ao examinar a literatura existente que aborda a CS, observa-se que a maioria dos autores prefere citar ou adaptar a definição de Endsley (1995): segundo o autor, é possível construir uma CS que permita a tomada de decisões e a subsequente execução de ações, conforme o modelo delineado no Fluxograma 1, que mostra um processo de três etapas baseado em percepção dos elementos no ambiente, compreensão da situação presente e projeção sobre como o ambiente pode se apresentar em breve.

Assim, inferimos que a CSC respalda os tomadores de decisão militares ao fornecer conhecimento sobre o estado de um ambiente operacional e dos meios operacionais relevantes nele inseridos. A Doutrina Conjunta da OTAN para Operações no Ciberespaço define ciberespaço como "o domínio global que consiste em toda comunicação interconectada, tecnologia da informação e outros sistemas eletrônicos, redes e seus dados, incluindo aqueles separados ou independentes que processam, armazenam ou transmitem dados" (NATO, 2020a).

Fluxograma 1: Modelo de Consciência Situacional de Endsley.



Fonte: Endsley (1995).

Stone (2015) define a CSC como o conjunto de todos os dados sobre o estado dos sistemas operacionais que compõem o ciberespaço para uma determinada operação. Para Tyworth et al. (2012), em operações militares compostas por um ou mais meios, a CSC é o entendimento efetivo de tudo o que está associado ao domínio do ciberespaço com potencial de impactar a segurança do pessoal e do material envolvidos nas missões.

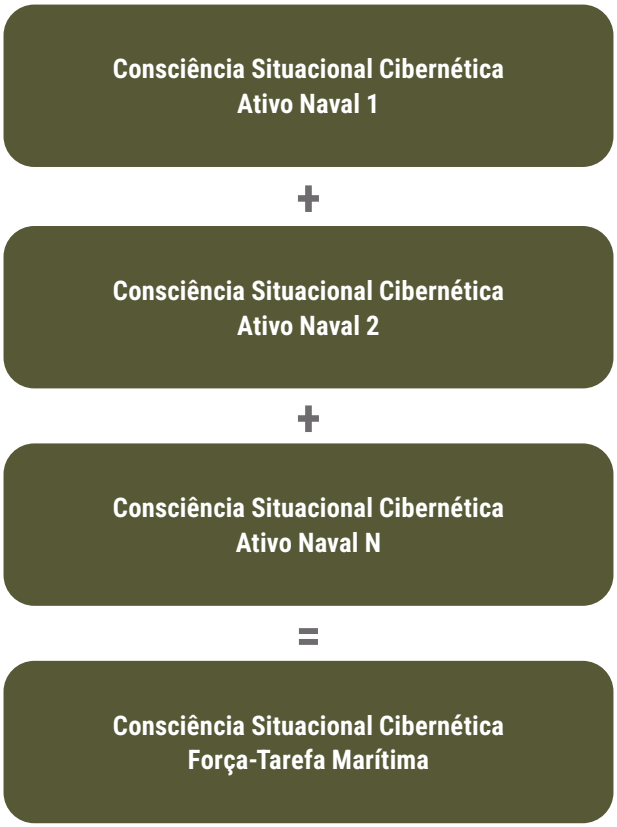
De acordo com Conti et al. (2013), uma definição de CSC em um ambiente militar é "o conhecimento atual e preditivo necessário do ambiente do qual as operações dependem — incluindo os domínios físico, virtual e humano —, bem como todos os fatores, atividades e eventos das forças amigas e adversárias em todo o espectro de conflito".

O ambiente operacional, conforme o conceito de ciberespaço da OTAN, é permeado pela comunicação de redes de computadores. A concepção adotada neste artigo, por sua vez, segue a definição de Levin et al. (2001), segundo a qual CSC é "a percepção de eventos e dados de rede, a compreensão de seu significado em termos de missão, recursos, conectividade, ameaças e vulnerabilidades, e a projeção de seu status em breve".

Assim, combinando o modelo de Endsley com a definição de Levin et al. (2001), conclui-se que a CSC é o subconjunto de toda a consciência situacional necessária para operar no e através do ciberespaço em todos os ativos navais, conforme ilustrado na Figura 1. A CSC não é um fim em si mesma, mas, fundamentada na análise constante da situação da rede de computadores,

é um meio utilizado para apoiar a tomada de decisão, permitindo que a Força-Tarefa Marítima alcance seus objetivos no domínio marítimo.

Figura 1: Consciência Situacional Cibernética da Força-Tarefa Marítima.



Fonte: O autor.

2. Um ativo digital para apoiar como construtor de Consciência Situacional Cibernética

De acordo com Kościelski et al. (2007), a Consciência Situacional Marítima (CSM) é caracterizada como o reconhecimento de eventos, atividades e circunstâncias de natureza militar e civil que ocorrem no ambiente marítimo ou a ele estão associadas. Esses elementos desempenham um papel crucial em operações e exercícios atuais e futuros da OTAN. O Ambiente Marítimo, por sua vez, abrange oceanos, mares, baías, estuários, vias navegáveis, regiões costeiras e portos.

É imperativo compilar um conjunto abrangente de informações que servirão como base para a tomada de decisões estratégicas das Forças-Tarefa Marítimas (FTM). Essa compilação envolve a coleta e a análise contínua de dados provenientes de todos os sensores e ativos computacionais disponíveis. Esse processo meticuloso requer que os dados sejam devidamente encapsulados e transmitidos de forma segura dentro dos meios navais, utilizando a rede de computadores via satélite.

Nesse contexto, com a finalidade de identificar o ativo computacional que facilita a criação da CSC, é necessário realizar ações específicas nos níveis tático e operacional. Essas atividades devem ser conduzidas pelas equipes defensivas e pelos comandantes da FTM, respectivamente. Já no nível tático, a CSC se concentra nas ameaças que exploram vulnerabilidades presentes em redes e sistemas específicos, bem como nas consequências resultantes de tais comprometimentos. As ações defensivas táticas no ciberespaço, ou através dele, visam preservar a liberdade de ação amigável no domínio cibernético, conforme indicado em NATO (2020a).

Essas ações estão em conformidade com três documentos-chave relacionados às operações defensivas no ciberespaço: a Doutrina Conjunta Aliada para Operações no Ciberespaço – AJP-3.20 (NATO, 2020a), o *Framework* de Cibersegurança do Instituto Nacional de Padrões e Tecnologia (NIST, 2018) e as Diretrizes sobre Cibersegurança a Bordo de Navios (BIMCO, 2021). As ações e estratégias defensivas incluem: identificação de ameaças cibernéticas, detecção de vulnerabilidades, avaliação de riscos, desenvolvimento de medidas de proteção e detecção, estabelecimento de planos de contingência e resposta a incidentes de segurança cibernética.

De acordo com a Doutrina Conjunta Aliada para Operações no Ciberespaço (NATO, 2020a), no plano operacional, o comandante da FTM deve levar em consideração os seguintes fatores:

- efeitos no ciberespaço: cruciais para gerar impactos táticos, operacionais e estratégicos que conduzem ao cumprimento dos objetivos militares. Esses efeitos estão intrinsecamente ligados a *softwares*, dados e protocolos, podendo também emanar de níveis cinéticos em outros domínios;
- funções conjuntas: oferecem um arcabouço que auxilia na integração e na sincronização de capacidades e atividades durante operações conjuntas;
- princípios de operação: os princípios que norteiam operações conjuntas são igualmente aplicáveis ao ciberespaço. Contudo, a interpretação desses princípios pode variar devido às características únicas desse domínio. Os princípios incluem segurança, surpresa, concentração de força, manutenção do moral e liberdade de ação.

Para otimizar os processos decisórios no nível operacional, é imperativo monitorar de forma contínua segmentos do ciberespaço a fim de identificar ameaças cibernéticas emergentes de maneira ágil e precisa. Nesse sentido, faz-se necessária a implementação de uma ferramenta eficaz que não apenas operacionalize todas as informações pertinentes, mas também ofereça uma

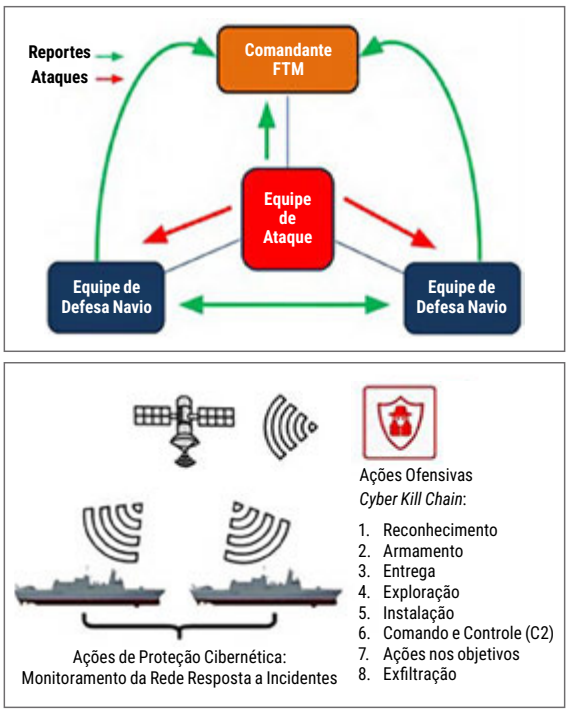
análise profunda das condições presentes e futuras no ciberespaço. Essa ferramenta, idealmente instalada em cada ativo naval pertencente à FTM, deve possuir as seguintes capacidades:

- visibilidade em tempo real: proporcionar uma visão clara e atualizada das ameaças existentes em todo o domínio do ciberespaço;
- identificação rápida de ameaças: reconhecer ameaças de forma rápida e eficiente;
- análise de registros: possuir funcionalidades que permitam a pesquisa e a análise de registros, facilitando a investigação de incidentes potenciais;
- redução do tempo de resposta: minimizar o tempo necessário para responder a incidentes e ameaças, aumentando a eficácia das medidas de proteção implementadas.

3. Conduzindo um exercício cibernético em operações reais no mar

Este artigo propõe a realização de um Exercício Cibernético em Operações Reais no Mar com o propósito de avaliar a eficácia do aumento da Consciência Situacional Cibernética (CSC) no aprimoramento do processo decisório. O exercício sugerido envolve duas equipes operando em posições opostas no ciberespaço da Força-Tarefa Marítima (FTM): uma equipe encarregada da defesa do ciberespaço, e a outra responsável pelo papel de atacante.

Figura 2: Exercícios Cibernéticos via Comunicações por Satélite.



Fonte: O autor.

Conforme ilustrado na Figura 2, ambas as equipes devem reportar ao comandante da FTM os efeitos resultantes de suas ações no ciberespaço da entidade. Essa avaliação contínua (*feedback*) visa fornecer conhecimentos (*insights*) valiosos sobre o impacto das operações cibernéticas no ambiente marítimo.

Segundo Domingo et al. (2021), para aprimorar o processo de tomada de decisão por meio da CSC, o comandante da FTM deve ser capaz de responder a algumas perguntas essenciais, como:

- que operações estão sendo conduzidas no ciberespaço;
- qual o impacto dos efeitos do ciberespaço na missão em curso;
- quantas tecnologias operacionais foram incapacitadas em decorrência do incidente cibernético;
- após o incidente cibernético, qual o nível de comprometimento da infraestrutura de informação dos ativos navais envolvidos na missão.

Essas perguntas são cruciais para avaliar a extensão do dano causado por incidentes cibernéticos e para compreender como tais incidentes podem afetar as operações em curso. Responder a essas perguntas de maneira precisa e tempestiva é fundamental para a implementação de estratégias de resposta eficazes e para a manutenção da integridade das operações marítimas. As ações propostas devem ser executadas na mesma banda de comunicação via satélite utilizada para navegação. Cada equipe de defesa a bordo dos navios tem a responsabilidade de coletar, analisar e identificar dados de rede, além de monitorar ativamente a presença de incidentes cibernéticos críticos que possam afetar a Força-Tarefa Marítima (FTM).

Esse processo contínuo de vigilância e análise fornece ao comandante uma Consciência Situacional Cibernética robusta e atualizada que é fundamental para a tomada de decisões abrangentes, confiáveis e tempestivas visando ao cumprimento bem-sucedido da missão designada.

Na outra vertente, a equipe encarregada das ações ofensivas deve adotar estratégias proativas, valendo-se, por exemplo, da metodologia *Cyber Kill Chain*, desenvolvida por especialistas da Lockheed Martin. De acordo com Hutchins et al. (2011), esse modelo proporciona um *framework* estruturado para a compreensão e a prevenção de ciberataques, como pode ser visualizado na Figura 2. A aplicação da *Cyber Kill Chain* capacita a equipe ofensiva a executar ações coordenadas e estratégicas em todo o ciberespaço da Força-Tarefa Marítima, identificando e explorando vulnerabilidades de maneira eficaz e sistemática.

Uma vez que os exercícios propostos serão realizados em operações reais no mar, direcionadas ao ciberespaço da Força-Tarefa Marítima, é imperativo estabelecer métricas claras e verificáveis para avaliar o desempenho de cada equipe envolvida. Essas métricas servirão como indicadores-chave de desempenho para as ações executadas pelas equipes, fornecendo uma base objetiva para análise e avaliação.

Para a equipe de defesa dos navios, a avaliação pode fundamentar-se no número de incidentes cibernéticos identificados, quantificando a capacidade da equipe de detectar ameaças ativas no ciberespaço. Além disso, o número de incidentes cibernéticos bloqueados mensura a eficácia das estratégias de defesa implementadas para neutralizar ou mitigar ameaças. A comunicação eficiente e tempestiva de eventos críticos ao comando superior também é vital; assim, o número de incidentes reportados ao Comandante da FTM se configura como um indicador relevante para a tomada de decisões informadas e rápidas.

A equipe de ataque, por outro lado, pode ser avaliada por sua proficiência em identificar pontos fracos ou falhas nos sistemas de Tecnologia da Informação (TI) e Tecnologia Operacional (TO) embarcados nos ativos navais, sendo o resultado indicado pelo número de vulnerabilidades descobertas. O impacto efetivo das ações ofensivas também constitui um critério crucial de avaliação, sendo quantificado pelo grau de interrupção ou comprometimento das funções e sistemas críticos a bordo dos navios, ou seja, pelo número de degradações de TI/TO.

Essas métricas proporcionam uma visão clara e quantitativa do desempenho de cada equipe, facilitando a avaliação objetiva de suas competências e sua eficácia durante os exercícios. Além disso, oferecem *insights* valiosos para o aprimoramento contínuo das estratégias de defesa e ataque no ciberespaço marítimo.

Conclusão

Os ataques cibernéticos têm se intensificado no Domínio Marítimo, elevando a segurança cibernética a uma preocupação global crescente. No cenário marítimo militar, no qual as operações podem ser alvos desses ataques, é crucial que os comandantes das Forças-Tarefa Marítimas estejam aptos a integrar a Consciência Situacional Cibernética em suas estratégias e processos decisórios.

O desfecho de conflitos militares futuros será fortemente influenciado pela capacidade de cada lado para coletar, processar e disseminar informações de maneira eficaz e ágil, possibilitando decisões mais acertadas e rápidas do que as do adversário. Nesse contexto, a CSC emerge como ferramenta vital para os Comandantes da FTM, auxiliando-os a navegar com segurança e eficácia diante dos desafios impostos pelos ataques cibernéticos.

Portanto, a segurança de rede não é apenas um desafio, mas também uma responsabilidade compartilhada globalmente. Nenhuma nação pode se dar ao luxo de permanecer alheia, focando exclusivamente em sua própria segurança cibernética. A responsabilidade de garantir uma rede segura e resiliente deve ser compartilhada por toda a comunidade internacional.

Tendo em vista a realização de trabalhos futuros, pretende-se conduzir o Exercício Cibernético e quantificar os riscos e os impactos gerados pelas equipes ofensivas ao Domínio Marítimo durante as operações militares, o que fornecerá *insights* valiosos para fortalecer as estratégias de defesa e resposta a incidentes cibernéticos no ambiente marítimo.

Referências Bibliográficas

BALTIC AND INTERNATIONAL MARITIME COUNCIL (BIMCO). **The Guidelines on Cyber Security Onboard Ships**. Version 4.0, 2021.

CONTI, G.; NELSON, J.; RAYMOND, D. Towards a cyber common operating picture. In: PODINS, K.; STINISSEN, J.; MAYBAUM, M. (Eds.). **International Conference on Cyber Conflict**. Tallinn: NATO CCD COE Publications, 2013. p. 1-17.

DOMINGO, Alberto; et al. Enabling NATO Cyberspace Operations by Building Comprehensive Cyberspace Situational Awareness. In: LOPEZ JR, Juan; PERUMALLA, Kalyan; SIRAJ, Ambareen (Eds.). **ICCWS 2021: Proceedings of the 16th International Conference on Cyber Warfare and Security**. [S.l.: s.n.], 2021. p. 509-518.

ENDSLEY, M. R. Toward a theory of situation awareness in dynamic systems. Human Factors. **The Journal of the Human Factors and Ergonomics Society**, v. 37, n. 1, p. 32-64, 1995.

HUTCHINS, Eric; CLOPPERT, Michael; AMIN, Rohan. **Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains**. 2011.

KOŚCIELSKI, M.; MILER, R.K.; ZIELIŃSKI, M. Maritime Situational Awareness (MSA). **Zeszyty Naukowe Akademii Marynarki Wojennej**, v. 48, n. 4 (171), p. 79–88, 2007.

KUEHL, D.T. From cyberspace to cyberpower: Defining the problem. In: KRAMER, F. D.; WENTZ, L.K.; STARR, S. H. (Ed.). **Cyberpower and National Security**. Dulles, VA: Potomac Books, Inc., 2009.

LEVIN, D.; TENNEY, Y.; HENRI, H. Issues in human interaction for cyber command and control. In: DARPA Information Survivability Conference, 1., 2001. **Anais** [...]. [S.l.: s.n.], 2001. p. 141–151.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Framework for Improving Critical Infrastructure Cybersecurity.** Version 1.1. NIST Cybersecurity Framework, April 2018. Disponível em: <https://doi.org/10.6028/NIST.CSWP.04162018>. Acesso em: 30 jan. 2024.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). NATO Standardization Office (NSO). **Allied Joint Doctrine for Cyberspace Operations**. AJP-3.20, Edition A, Version 1, 2020a.

_____·_____· **NATO Glossary of Terms and Definitions** (English and French): AAP-06. Page 119. Edition 2020b.

STONE, Steve. Data to Decisions for Cyberspace Operations. **Military Cyber Affairs**, v. 1, n. 1, Article 6, 2015.

TYWORTH, M.; GIACOBE, N. A.; MANCUSO, V. M. Cyber situation awareness as distributed socio-cognitive work. In: **Cyber Sensing - Proceedings of SPIE**, v. 8404, 2012.

UNITED STATES DEPARTMENT OF DEFENSE (US DOD). Joint Chiefs of Staff. Joint Publication 3-32: **Joint Maritime Operations**. June 8, 2018. Disponível em: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32ch1.pdf>. Acesso em: 30 jan. 2024.

A necessidade da virtualização em *Software* Livre em proveito das Operações Cibernéticas na utilização do Sistema Naval de Ações Cibernéticas

11

Suboficial (HN) Renato Evaristo **Alfaia**

Ingressou na MB em 1994 por meio da Escola de Aprendizes-Marinheiros do Espírito Santo (EAMES). Realizou os cursos de Especialização e Aperfeiçoamento em Hidrografia e Navegação, além do Curso de Assessoria de Estado-Maior para Suboficiais (CASEMSO). Graduado em Sistemas de Informação e pós-graduado em Segurança da Informação. Integrou a turma pioneira de praças no Curso de Guerra Cibernética para Sargentos do Exército no CIGE. Em sua trajetória profissional, foi Administrador de Redes no Navio Oceanográfico Almirante Câmara, na Diretoria de Hidrografia e Navegação e no Navio Hidrográfico Sirius; Supervisor de Segurança da Informação na Diretoria de Hidrografia e Navegação; Encarregado da Seção de Segurança da Informação e Comunicações e Defesa Cibernética no CLTI do Centro de Hidrografia da Marinha; e Operador de Segurança da Informação nas Olimpíadas do Rio de Janeiro em 2016. Participou de várias operações na área de Cibernética (Cibersecuritas, Baluarte, Octopus e Guardião Cibernético) e de operações conjuntas com o Ministério da Defesa (Amazônia, Ágata Norte e Ágata Oeste).

Introdução

A virtualização, um termo proeminente na Tecnologia da Informação e Comunicações, possibilita criar múltiplos ambientes sem a necessidade de *hardware* exclusivo, o que é fundamental para soluções computacionais diversas. Na era de interconexão e dependência da Internet, as organizações devem se precaver contra falhas de *hardware* que afetam decisões estratégicas.

Segundo o Plano Estratégico da Marinha (PEM 2040), a Cibernética é um elemento-chave no contexto naval. O espaço cibernético, um teatro de operações militares sem fronteiras físicas, requer o preparo das Forças Armadas para responder de modo eficaz às ameaças contemporâneas. Assim, a criação de um ambiente concebido para treinamento e o fornecimento de equipamentos e artefatos adequados voltados para a esfera cibernética tornam-se imperativos.

> O espaço cibernético não possui fronteiras físicas, permeia todos os setores (marítimo, terrestre, aéreo e espacial) e é considerado um teatro de operações militares. A vulnerabilidade nesse espaço é uma ameaça contemporânea a ser enfrentada (BRASIL, 2020, p. 31).

É imprescindível, portanto, que as Forças estejam devidamente preparadas para fazer frente a esse tipo de ameaça, respondendo com eficácia e resiliência.

Figura 1: Aspecto básico da virtualização.

Fonte: Truenet Blog, [s.d.].

1. Histórico

Antes mesmo da concepção do PEM 2040, a Marinha do Brasil já desenvolvia iniciativas para testar e preparar as Equipes de Ataque e Defesa Cibernética em suas respectivas áreas de atuação. Em 2011, foram implementadas as Operações Baluarte e Ciber Securitas, cada uma com seus contextos e escopos bem definidos. A primeira tinha como foco principal avaliar as defesas da Rede de Computadores Integrada da Marinha (RECIM) por meio de ataques e explorações reais

em sua infraestrutura, enquanto a segunda criava um ambiente virtual com múltiplas interações, simulando situações quase realistas.

Todas essas operações demandavam considerável capacidade dos recursos computacionais disponíveis, garantindo a condução eficaz dos exercícios e a conclusão satisfatória de seus objetivos. Até 2018, a Divisão de Guerra Cibernética do Comando de Operações Navais (ComOpNav) supervisionava esses exercícios, mas, com a criação do Comando Naval de Operações Especiais (CoNavOpEsp) em 2019, essa responsabilidade foi transferida para a nova organização.

Desde então, a virtualização passou a ser utilizada como um componente adicional, aproveitando-se dos diversos recursos físicos disponíveis na época para criar ambientes adequados às missões propostas, tendo alcançado relativo sucesso em sua execução.

2. O problema da continuidade com a falta de padronização

Apesar dos êxitos alcançados, surgia a impressão de que a criação de cenários e artefatos carecia de continuidade. A diversidade de sistemas e a falta de um padrão pré-estabelecido resultavam em soluções que pareciam não se harmonizar, dando a sensação de que cada operação exigia um recomeço, o que acarretava um considerável retrabalho para as equipes da Divisão de Guerra Cibernética.

Como resposta a essa situação, juntamente com a fundação do CoNavOpEsp, foi criado o Laboratório de Ações Cibernéticas. Subordinado ao Departamento de Operações de Informação, o Laboratório é dedicado à centralização do desenvolvimento de artefatos e infraestrutura para a condução das atividades de Guerra Cibernética.

No entanto, persistiam desafios a serem enfrentados. A proliferação de soluções e a ausência de padronização exigiam que os desenvolvedores se especializassem em diversas tecnologias para criar os artefatos necessários. Além disso, eram consideráveis os custos para manter múltiplas infraestruturas operacionais (tanto físicas quanto virtuais) atualizadas e plenamente funcionais.

3. A solução em *Software* Livre: o Proxmox

Entre as tecnologias disponíveis no Laboratório, uma que não recebia a devida atenção era o Proxmox, uma solução de virtualização fundamentada no GNU/Linux, distribuída sob a licença *GNU Affero General Public License* (AGPL).

Essa solução engloba duas tecnologias essenciais: o *Kernel-based Virtual Machine* (KVM) e os *Linux Containers* (LXC). O hipervisor oferece suporte tanto para a virtualização total quanto para a virtualização assistida por *hardware* fornecida pelo KVM. A empresa mantenedora do projeto, *Proxmox Server Solutions GmbH*, disponibiliza licenças de suporte empresarial que incluem acesso ao repositório empresarial. No entanto, vale ressaltar que a versão gratuita do projeto é robusta e respaldada por uma comunidade ativa.

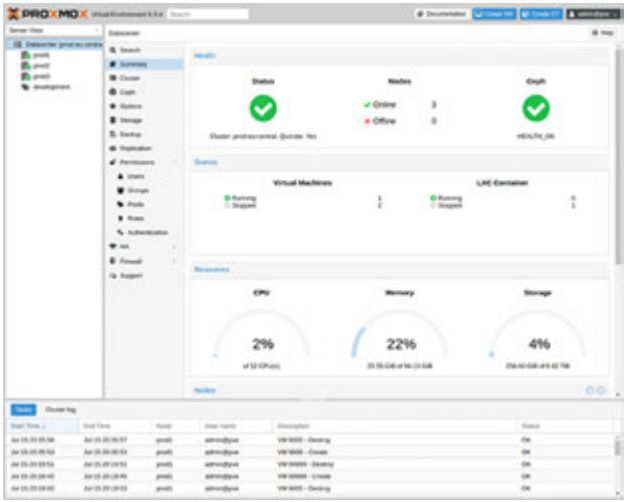
Uma das principais vantagens do Proxmox é sua natureza de código aberto, que se baseia em tecnologias similares. Isso permite o acesso a recursos avançados sem a necessidade de desembolsar quantias vultosas em licenças, em contraste com outras soluções que impõem custos significativos.

Suas características primordiais estão descritas nos subitens a seguir.

3.1. Interface de gerenciamento baseada na *web*

O Proxmox pode realizar todas as tarefas de gerenciamento com a interface gráfica do usuário (GUI) integrada, não havendo necessidade de instalar uma ferramenta de gerenciamento separada. A interface *web* central é baseada na estrutura JavaScript e pode ser acessada a partir de qualquer navegador moderno.

Figura 2: Interface *web* – GUI do Proxmox.



Fonte: Proxmox.

Além das tarefas de gerenciamento, também fornece uma visão geral do histórico de tarefas e dos *logs* do sistema de cada nó. Isso inclui: execução de tarefas de *backup*, migração em tempo real, armazenamento definido por *software* ou atividades acionadas por alta disponibilidade. A ferramenta multiusuário permite o gerenciamento de todo o *cluster* a partir de qualquer nó, não sendo necessário um nó gerenciador dedicado.

3.2. Interface de linha de comando (CLI)

Para usuários avançados acostumados com o conforto do Shell Unix ou do Windows Powershell, o Proxmox VE fornece uma interface de linha de comando para gerenciar todos os componentes do ambiente virtual. Essa interface possui preenchimento inteligente de guias e documentação completa na forma de páginas de manual do Unix.

3.3. Sistema de arquivos de *cluster* Proxmox (PMXCFS)

O Proxmox VE usa o *Proxmox Cluster File System* (PMXCFS), um sistema de arquivos baseado em banco de dados que permite sincronizar arquivos de configuração em seu *cluster*. Ao usar o sistema Corosync, esses arquivos são replicados em tempo real para todos os nós do agrupamento. O sistema de arquivos armazena todos os dados dentro de um banco de dados persistente em disco; no entanto, uma cópia desses dados reside na RAM. O tamanho máximo de armazenamento atualmente é de 30 MB – mais que suficiente para armazenar a configuração de vários milhares de máquinas virtuais.

3.4. Migração ao vivo/online

Com o recurso integrado de migração ao vivo/online, é possível mover máquinas virtuais em execução de um nó do *cluster* Proxmox VE para outro sem qualquer tempo de inatividade ou efeito perceptível por parte do usuário final.

Os administradores podem iniciar esse processo pela interface da *web* ou pela linha de comando, o que permite minimizar o tempo de inatividade caso seja necessário colocar o sistema *host* inativo para manutenção.

3.5. Administração baseada em funções

O acesso é granular a todos os objetos (como máquinas virtuais, armazenamento, nós, etc.) usando o sistema de gerenciamento de permissões baseado em função. Isso permite definir privilégios e ajuda a controlar o acesso aos objetos. Esse conceito também é conhecido como listas de controle de acesso: cada permissão especifica um assunto (um grupo de usuários ou *token* de API) e uma função (conjunto de privilégios) em um caminho específico.

3.6. *Cluster* de alta disponibilidade (HA) Proxmox VE

Um *cluster* Proxmox VE de vários nós permite a criação de servidores virtuais altamente disponíveis. O Proxmox VE HA *Cluster* é baseado em tecnologias Linux de alta disponibilidade comprovada, fornecendo um serviço estável e confiável. Todo o *cluster* Proxmox VE HA pode ser facilmente configurado a partir da interface de usuário integrada baseada na *web*.

O Proxmox também oferece uma solução empresarial para *backup* e restauração de máquinas, contêineres e *hosts* físicos. O Proxmox Backup Server não só garante mais segurança de dados, com criptografia forte e métodos de garantia de integridade, como também economiza espaço de armazenamento nos servidores físicos.

3.7. Redes em ponte (*bridge*)

O Proxmox usa um modelo de rede em ponte também chamado de *bridge*. Cada *host* pode ter até 4.094 pontes. Essas interfaces são como *switches* de rede física, implementados em *software* no *host* Proxmox. Todas as máquinas podem compartilhar uma ponte, como se os cabos de rede virtuais de cada convidado estivessem todos conectados ao mesmo *switch*. Para conectar máquinas virtuais (VMs) ao mundo externo, elas são anexadas a placas de rede físicas atribuídas a uma configuração TCP/IP.

Para maior flexibilidade, são possíveis VLANs (IEEE 802.1q) e ligação/agregação de rede. Dessa forma, é possível construir redes virtuais complexas e flexíveis para os *hosts* virtualizados, aproveitando todo o poder da pilha de rede Linux.

O Proxmox também suporta Open vSwitch (OVS) como alternativa às pontes, ligações e interfaces VLAN do Linux. O OVS fornece recursos avançados, como suporte RSTP, VXLANs e OpenFlow, e suporta múltiplas VLANs em uma única conexão.

3.8. Benefícios

Considerando as características descritas anteriormente, o Proxmox apresenta o melhor custo-benefício para virtualizar tanto a infraestrutura de TI quanto as infraestruturas operativas, uma vez que otimiza os recursos existentes e aumenta a eficiência com despesas mínimas.

Nesse sentido, ele oferece gerenciamento descomplicado e interface simples, que reduz a quantidade de horas de trabalho e, ao mesmo tempo, garante segurança na operação e em *backups*.

4. Emprego Operacional

A utilização do Proxmox mudou o paradigma das soluções utilizadas no ambiente das operações cibernéticas. Utilizando somente essa ferramenta para a virtualização de sistemas, foi possível criar uma padronização na operacionalização dos diversos artefatos e cenários componentes das várias necessidades operativas dentro do ambiente computacional.

4.1. Operação Baluarte

Dentro dessa operação, uma série de configurações de ativos se faz necessária, abrangendo desde a criação de estações de trabalho operacionais até sistemas de roteamento diferenciados, destinados a auxiliar os operadores cibernéticos na condução de suas missões conforme estabelecido no contexto da atividade.

Em operações anteriores, essas configurações eram realizadas em vários hipervisores, demandando um tempo considerável para reunir as diversas características necessárias em diferentes ambientes. Isso acarretava atrasos para a equipe de desenvolvedores do Laboratório, uma vez que algumas configurações poderiam estar ausentes ou desatualizadas, o que resultava em retrabalho e atrasos na implantação das estruturas essenciais do exercício. Graças à facilidade de manutenção do Proxmox e à familiaridade dos desenvolvedores com essa solução devido à sua padronização, esse tempo foi reduzido quase a zero.

4.2. Operação Ciber Securitas

Operação criada para ser um ambiente virtualizado a ser utilizado na instrução de militares de diversas Organizações Militares no contexto da Segurança e da Defesa Cibernética. As edições de 2020 e 2021 do evento utilizaram o paradigma do Proxmox na criação do exercício.

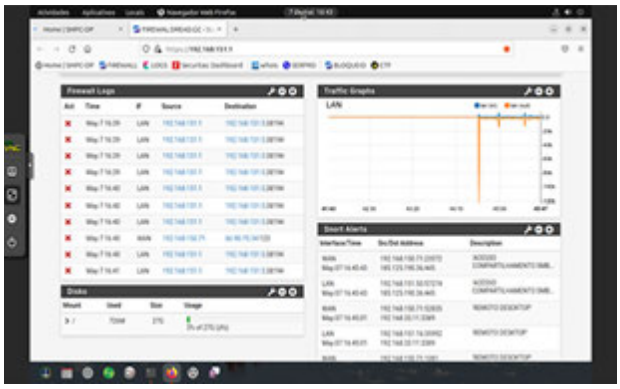
Figura 3: Desenvolvedores do ambiente virtual com o Proxmox.

Fonte: Defesa em Foco, 2021.

No ano de 2023, o ambiente virtualizado pelo Proxmox proposto pelo Laboratório de Ações Cibernéticas do CoNavOpEsp contou com mais de 3800 instâncias virtuais, nas quais os militares puderam se capacitar não somente em *hardening* de servidores, mas também na operação do Sistema Militar de Proteção Cibernética (SMPC – conhecido como *Dreadnought*) via seus módulos (Firewall, IDS, Zabbix, web), na análise de tráfego de rede e em outros aspectos relevantes da Segurança de Informações e Comunicações.

Nesse ambiente, os militares puderam participar de uma competição de *Capture-the-Flag* (CTF) na qual foram submetidos a desafios separados por temas, com várias ações ofensivas via simuladores de tráfego. Os participantes deveriam identificar e bloquear diversos incidentes computacionais e ataques cibernéticos simulados, defendendo, assim, a rede de interesse do exercício. Todos esses eventos puderam ser criados graças às estruturas de desenvolvimento e compartimentação existentes no virtualizador.

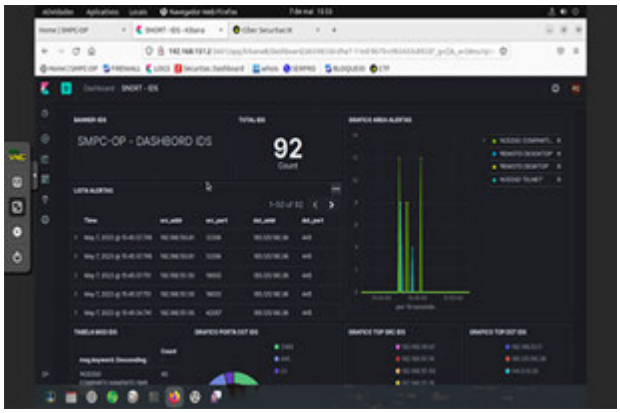
Figura 4: Tela de operação do SMPC virtualizada no Proxmox.



Fonte: O autor.

Esses são apenas alguns exemplos notáveis das aplicações que podem ser efetuadas com a adoção dessa interface de virtualização.

Figura 5: Tela de Operação do SMPC virtualizada no Proxmox.



Fonte: O autor.

Conclusão

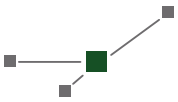
Partindo da premissa estabelecida no início deste artigo, a robustez e a segurança são imperativas tanto para os sistemas cibernéticos navais quanto para qualquer outro sistema. No ambiente operacional, essa necessidade se torna ainda mais premente, pois essas soluções serão submetidas a cargas máximas, podendo ser utilizadas para a execução de ações no contexto da Defesa Naval de ativos, na instrução de militares em relação a novas tecnologias essenciais ou na formulação de novas doutrinas e técnicas para o gerenciamento de questões militares.

Como componente fundamental do Sistema Naval de Guerra Cibernética, o CoNavOpEsp está equipado com um sistema de vanguarda e faz uso eficaz dos recursos

computacionais. O novo paradigma introduzido pela adoção do Proxmox não fica aquém de outros sistemas comerciais que têm a mesma abordagem. Somando-se a isso, a presença de desenvolvedores e operadores competentes aptos a administrar e manter a ferramenta de maneira eficaz abre portas para diversas possibilidades, permitindo a criação e o aprimoramento contínuo dentro desse ambiente.

À medida que a Era da Informação desponta, a convergência de recursos humanos, *hardware* e *software* cria um ambiente propício para o desenvolvimento das capacidades não apenas da Marinha do Brasil, mas também, em um contexto mais amplo, da sociedade como um todo. O Proxmox contribui nesse cenário e incorpora as melhores práticas tanto na virtualização quanto na criação de um modelo integrado de pessoal, programa e máquina, o que pode resultar em inúmeros benefícios no presente e no futuro, facilitando significativamente a integração de sistemas, práticas, técnicas e paradigmas utilizados pelo Poder Naval Operacional.

É esse o caminho que buscamos e almejamos para aprimorar ainda mais o sucesso de nossa Força diante dos desafios que surgem com o advento e o avanço das novas tecnologias.



Referências Bibliográficas

4SYSOPS. **Snapshots in Proxmox VE**. By Surender Kumar. 25 jan. 2023. Disponível em: <https://4sysops.com/archives/snapshots-in-proxmox-ve/>. Acesso em: 09 set. 2023.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Doutrina Cibernética da Marinha (EMA 419)**. Brasília, DF: EMA, 2021.

_____._____._____. **Plano Estratégico da Marinha (PEM 2040).** Brasília-DF: EMA, 2020. Disponível em: <https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/book.html>. Acesso em: 07 mar. 2024.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M-07: Doutrina Militar de Defesa Cibernética**. Brasília, DF: EMCFA, 2014.

CLOSS, T. A. **Virtualização em ambiente corporativo com ferramentas de *open source***. Trabalho de Conclusão de Curso (monografia). Bacharelado em Engenharia de Computação. Instituto Federal de Educação, Ciência e Tecnologia, Cuiabá, Mato Grosso, 2021.

DEFESA EM FOCO. **CoNavOpEsp realiza Operação "Ciber Securitas VIII"**. Por Marcelo Barros. 30 out. 2021. Disponível em: <https://www.defesaemfoco.com.br/conavopesp-realiza-operacao-ciber-securitas-viii/>. Acesso em: 09 set. 2023.

LAUREANO, M. A. P.; MAZIERO, C. Virtualização: conceitos e aplicações em segurança. In: **Minicursos do Simpósio Brasileiro de Segurança da Informação e Sistemas** (SBSeg). Sociedade Brasileira de Computação, 2008. p. 151-200. Disponível em: <https://www.researchgate.net/publication/237681120_Virtualizacao_Conceitos_e_Aplicacoes_em_Seguranca>. Acesso em: 09 set. 2023.

MOTA JUNIOR, S.; MARTINS, N.L. Sistema *Dreadnought* na Vanguarda da Proteção Cibernética Operativa. In: **Revista Passadiço**, ano 35, ed. 42, 2022. Marinha do Brasil. Centro de Adestramento Almirante Marques de Leão. Niterói, Rio de Janeiro. Disponível em: <https://www.marinha.mil.br/caaml/sites/www.marinha.mil.br.caaml/files/flipping_book/passadio_digital_2022_0/index.html#p=52>. Acesso em: 09 set 2023.

PROXMOX SERVER SOLUTIONS GMBH. **Proxmox Virtual Environment – Features**. Disponível em: <https://www.proxmox.com/en/proxmox-virtual-environment/features>. Acesso em: 09 set. 2023.

TRUENET. Blog. **Tipos de virtualização**. Disponível em: <https://blog.truenet.pt/tipos-de-virtualizacao/>. Acesso em: 04 fev. 2024.

A importância das Operações Psicológicas no desempenho das missões realizadas pela Marinha do Brasil

12

Capitão-Tenente Daniel Tomaz **Galrão**

Ingressou na MB em 2005 como aluno do Colégio Naval. É graduado em Ciências Navais pela Escola Naval com habilitação em Mecânica. Foi designado para servir na Força de Minagem e Varredura no 2º Distrito Naval, onde permaneceu embarcado no Navio-Varredor Albardão. Após o Curso de Aperfeiçoamento em Máquinas, foi Encarregado das Divisões de Eletricidade e Máquinas Auxiliares e, posteriormente, Chefe do Departamento de Máquinas na Fragata União. Ao longo da sua carreira, realizou os Cursos Expeditos de Varredura, de Controle de Avarias e de Oficial de Manobra, além do Estágio de Qualificação Técnica Especial de Operações Psicológicas e do Curso Especial de Segurança Orgânica.

Introdução

Essencialmente, é imperativo destacar que a Marinha do Brasil, assim como outras forças militares globais, reconhece a primordialidade das Operações Psicológicas como elemento intrínseco às suas estratégias de defesa e atuação. Tais operações desempenham um papel crucial na promoção dos interesses nacionais, na salvaguarda da segurança e na construção de relações internacionais sólidas. Assim, este artigo se propõe a explorar a marcante relevância das Operações Psicológicas (OpPsc) na condução das diversas operações que contam com a participação da Marinha do Brasil.

1. Histórico

A narrativa histórica nos revela que as ações psicológicas vêm sendo efetivamente empregadas desde as mais remotas épocas, quando o homem começou a se comunicar. O mais antigo emprego clássico de que se tem notícia parece ter sido o da tomada da cidade de Aratta pelo rei sumério Enmerkar 3.000 anos antes de Cristo.

Querendo para si a cidade vizinha, bastante rica, Enmerkar enviou ministros com a proposta autoritária de que a cidade lhe fosse entregue voluntariamente para, assim, evitar a guerra e o derramamento de sangue. Diante da rejeição a essa "investida diplomática", infiltrou diversos espiões em Aratta, os quais relatavam as desavenças locais e a euforia geral daquela sociedade nunca ameaçada. Enmerkar preparou, então, uma equipe de agitadores e sabotadores com instruções para informar ao povo como as pessoas seriam ainda mais felizes sob seu domínio e quão imponentes e numerosas eram as forças sob seu comando.

Simultaneamente, Enmerkar interceptava caravanas de suprimentos, envenenava os poços e perpetrava assassinatos seletivos daqueles capazes de perceber suas intenções enquanto ampliava as naturais desavenças no governo local. Seu exército, em constante exercício e desfile, exibia sua força diante do público-alvo (Pub A)[1], que começava a sentir as agruras do bloqueio. Quando Aratta estava à beira do esgotamento, Enmerkar enviou 1.000 camelos repletos de presentes, mantimentos e água, que seriam distribuídos diretamente ao povo pelos agentes agitadores/sabotadores, os quais se revelaram como enviados de Enmerkar e o apresentaram como a única salvação possível. Em seguida, o próprio povo compeliu seu rei a se render sem combate.

2. Operações Psicológicas

A incumbência do operador psicológico reside na análise das motivações de líderes, forças militares, populações e outros agentes relevantes visando, posteriormente, moldar suas percepções e vontades na direção dos objetivos propostos. Nesse contexto, as Operações Psicológicas (OpPsc), aliadas a outras capacidades da força, podem compensar a escassez de recursos, equipamentos modernos e outros meios materiais.

[1]É o segmento social que compartilha determinadas características e para o qual serão direcionados os esforços motivadores das OpPsc.

Entretanto, é imperativo ter ciência de que as OpPsc só lograrão efeitos favoráveis se forem coordenadas pelas Operações de Informação[2], as quais sincronizam as OpPsc, sobretudo, com as comunicações sociais e outras Capacidades Relacionadas à Informação (CRI)[3].

Consoante a Doutrina Militar Naval, as Operações Psicológicas (que abarcam ações psicológicas e guerra psicológica) englobam atividades políticas, militares, econômicas e psicossociais planejadas e conduzidas para criar em grupos (inimigos, hostis, neutros e/ou amigos) emoções, atitudes ou comportamentos favoráveis à consecução dos objetivos nacionais. Essas operações contemplam medidas preventivas de caráter permanente que têm como propósitos evitar o emprego prematuro da força e impedir ou dificultar a eclosão e o agravamento de situações de perturbação da ordem. Normalmente, englobam atividades de preparo de tropa, inteligência e comunicação social. Vale destacar que as ações psicológicas não se restringem à persuasão ou à manipulação, abrangendo, também, a disseminação de informações verdadeiras e relevantes visando alcançar resultados sem necessariamente recorrer à força física.

Portanto, as Operações Psicológicas representam a aplicação da Psicologia na condução da guerra, compreendendo, em um sentido mais restrito, o uso da propaganda contra o inimigo conjuntamente com as medidas militares necessárias. Nesse contexto, a propaganda é definida como a persuasão por meios não violentos.

3. As Operações Psicológicas na Marinha do Brasil

A Marinha do Brasil, à semelhança de qualquer instituição, depara-se com desafios no âmbito da comunicação e da imagem pública. Em vista disso, as Operações Psicológicas podem desempenhar um papel fundamental na construção e na manutenção da credibilidade da Marinha ao transmitir informações precisas e gerenciar percepções. Tal empreendimento revela-se crucial não apenas para consolidar a confiança interna entre as distintas equipes e lideranças da Marinha, mas também para cultivar uma relação confiável com a sociedade civil e os parceiros internacionais. Isso se torna premente, visto que, por trás do véu da globalização, as mídias despontam como instrumentos psicológicos de poder com veículos que transportam variados tipos de propaganda para qualquer local e a qualquer momento.

A intensidade e a constância das informações difundidas pelos veículos que atendem às diversas esferas da mídia tendem a saturar a mente humana, impregnando-a e inibindo a capacidade de pensamento e a realização de atividades criativas. Esse fenômeno distorce a opinião pública, além da própria estruturação e funcionalidade da mentalidade social.

Em um mundo no qual o ser humano vive imerso em um oceano de informações, a probabilidade de ser afetado inconscientemente por mensagens é substancial. Consciente desse paradigma, a Marinha do Brasil orquestra suas ações psicológicas durante Operações de Paz ou

Figura 1: Sinergia Informacional.

Fonte: O autor.

[2]Conjunto de ações coordenadas dirigido para alcançar superioridade no ambiente informacional por meio de negação, exploração, degradação ou destruição da informação e das redes associadas oponentes, reais ou potenciais, enquanto protege as suas próprias do ataque adversário.
[3]São aptidões requeridas para afetar a capacidade de oponentes ou potenciais adversários de orientar, obter, produzir e difundir informações em qualquer uma das três perspectivas da dimensão informacional (física, cognitiva ou lógica).

em resposta a desastres visando não apenas desempenhar um papel relevante para a população, mas também consolidar a imagem e a credibilidade da Força.

É pertinente destacar que a Marinha do Brasil frequentemente figura em Missões de Paz e Cooperação ao redor do globo, colaborando com outras nações na resolução de conflitos e na promoção da estabilidade. As Operações Psicológicas, conhecidas como "PSYOPS", desempenham um papel vital na criação de entendimento mútuo e na mitigação de conflitos culturais, contribuindo para estabelecer canais de comunicação eficazes com as populações locais e angariando o apoio necessário para o êxito das operações em curso.

Além disso, é notável que a incidência preponderante das Operações Psicológicas na contemporaneidade ocorra no âmbito do Gerenciamento de Crises e da Resposta a Desastres, revelando-se como uma capacidade distinta e essencial no rol de responsabilidades da Marinha do Brasil. As Operações Psicológicas emergem como instrumento imprescindível para acalmar a população impactada, fornecer informações precisas sobre a situação vigente e coordenar esforços de ajuda humanitária. Essa abordagem não apenas contribui para a preservação de vidas, mas também evidencia a capacidade de resposta eficaz da Marinha em tempos de crise.

Conclusão

Considerando o exposto, as Operações Psicológicas na Marinha do Brasil constituem uma ferramenta versátil e poderosa, capaz de alcançar uma miríade de objetivos estratégicos. Essas operações têm sido amplamente adotadas em conflitos contemporâneos do século XXI pelas forças armadas de diversos países, como os Estados Unidos da América e os integrantes da Organização do Tratado do Atlântico Norte (OTAN). A relevância dessas operações é amplificada pelos avanços nas pesquisas acerca da motivação humana e da tecnologia, tornando a ação militar no domínio informacional uma necessidade imprescindível. O aumento do acesso da população aos meios de comunicação, especialmente à Internet, exerce influência crescente sobre a opinião pública, podendo ser determinante nos rumos de um conflito armado.

As Operações Psicológicas, além de fortalecerem a comunicação interna e externa, desempenham papel vital tanto em Operações de Paz e ações de resposta a crises como na construção de relações internacionais sólidas.

À medida que a Marinha do Brasil se adapta aos desafios de um mundo em constante mutação, as Operações Psicológicas permanecem fundamentais para o êxito de suas missões e para a segurança nacional como um todo.

É relevante observar que, embora a Marinha do Brasil, em sua doutrina, considere a atuação das Operações Psicológicas nos níveis estratégico e tático, nas Operações Conjuntas patrocinadas pelo Ministério da Defesa tem-se notado uma presença cada vez mais expressiva de especialistas qualificados em Operações Psicológicas mobiliando a Seção de Operações de Informação no nível operacional. Essa observação demonstra a importância atribuída pela Marinha a essas atividades, que, nesse nível, contribuem sobremaneira para a conquista do estado final desejado de campanhas militares.

Referências Bibliográficas

BRASIL. Marinha do Brasil. Comando-Geral do Corpo de Fuzileiros Navais. **CGCFN-1-6: Manual de Operações Psicológicas de Fuzileiros Navais**. 1. ed. Rio de Janeiro, 2023.

_____._____. Estado-Maior da Armada. **EMA-305: Doutrina Militar Naval.** Brasília-DF, 2017.

_____._____._____. **EMA-335: Doutrina de Operações de Informação.** Brasília-DF, 2018.

DELMAS, F. M. **Operações Psicológicas**: necessidade de desenvolvimento dessa capacidade no nível operacional na Marinha do Brasil. Rio de Janeiro: Escola de Guerra Naval, 2018.

OLIVEIRA, L. S. P. **Informação ou Propaganda? O que recebemos? O que percebemos?** Brasília, Thesaurus, 1996.

As Operações Psicológicas no nível tático em apoio às ações da Força de Fuzileiros da Esquadra

Capitão de Corveta (FN) Thiago **Das Neves** Barbosa

Ingressou na MB por meio da Escola Naval. Entre os diversos cursos realizados, são dignos de destaque o Curso de Aperfeiçoamento de Oficiais do Corpo de Fuzileiros Navais (CAOCFN), o Curso Especial de Negociação com Tomada de Reféns, Cursos Básicos de Inteligência e Segurança Orgânica, Estágio de Qualificação Técnica Especial em Operações Psicológicas e o *Psychological Operations Qualification Course*, realizado no Exército dos Estados Unidos (US ARMY).

Introdução

Segundo a definição do Ministério da Defesa, Operações Psicológicas são:

> (...) procedimentos técnicos especializados, operacionalizados de forma sistematizada, para apoiar a conquista de objetivos políticos ou militares e desenvolvidos antes, durante e após o emprego da força, visando motivar públicos-alvo amigos, neutros ou hostis a atingir comportamentos desejáveis (BRASIL, 2007).

É possível compreender que as Operações Psicológicas visam desenvolver comportamentos desejáveis, favoráveis aos objetivos preestabelecidos, em públicos-alvo criteriosamente selecionados e em diversos níveis de condução de um conflito. Deve-se, também, considerar que os conflitos são gerenciados em distintos níveis (a saber: político, estratégico, operacional e tático) e que cada um desses níveis possui suas particularidades, resultados esperados e, por conseguinte, os meios adequados para a sua consecução. Quanto mais elevado o nível de condução do conflito, maior é a gama de recursos à disposição do tomador de decisões. Tal realidade não difere das Operações Psicológicas.

1. Operações Psicológicas

As Operações Psicológicas no nível estratégico têm por finalidade prestar apoio a ações nos diversos domínios do Poder Nacional, facilitando a consecução dos objetivos previamente estabelecidos. Sua atuação é duradoura, com resultados em médio e longo prazos.

Nesse contexto, recursos de comunicação em massa, como internet, televisão, rádio e cinema, muitas vezes somente estão disponíveis, com qualidade, no nível estratégico ou mesmo político. Ademais, essa atuação pode contar com a colaboração de vetores de influência, como líderes e formadores de opinião de prestígio tanto nacional quanto internacional.

No nível operacional, as Operações Psicológicas são conduzidas com o intuito de apoiar o comandante do Teatro de Operações no cumprimento de sua missão. Nesse cenário, a colaboração de órgãos civis pode ser necessária; porém, os especialistas militares constituem o principal recurso (BRASIL, 2023).

As Operações Psicológicas nesse nível frequentemente são iniciadas por militares integrantes de um Destacamento de Operações Psicológicas subordinado a um Comando Conjunto, conforme estabelecido por uma diretriz ministerial em situações de crise.

Já no nível tático, conforme a Doutrina Militar Naval (DMN) classifica, as Operações Psicológicas são desenvolvidas em apoio à execução de operações militares, com planejamento e execução de cunho militar e obtenção de resultados em curto e médio prazos. Tais operações são empregadas em apoio à manobra dos comandantes dos diversos escalões envolvidos. Consideram-se as características da área de atuação, a população local e as peculiaridades do local buscando respaldar as tarefas recebidas pelo comandante.

Os Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav), formados por militares da Força de Fuzileiros da Esquadra, atuam no nível tático, inseridos em

contextos de Operações Conjuntas sob a Força Naval Componente ou em exercícios e operações singulares.

É cada vez mais frequente o emprego das Capacidades Relacionadas à Informação, sobretudo as Operações Psicológicas nos GptOpFuzNav. Isso ocorre em virtude da realidade do ambiente operacional contemporâneo, que considera não somente a Dimensão Física, mas também a Dimensão Informacional e Dimensão Humana.

Pode-se mencionar o ano de 2023 como um período no qual algumas operações/exercícios envolvendo Operações Psicológicas foram conduzidas em contextos de operações humanitárias ou ações benignas, proporcionando significativo aprendizado e aprimoramento dessa capacidade recentemente desenvolvida pela Marinha do Brasil.

2. Operações Psicológicas desenvolvidas em 2023

2.1. Operação Abrigo pelo Mar

No mês de fevereiro de 2023, a cidade de São Sebastião, situada no litoral de São Paulo, foi devastada por um desastre natural que acarretou severos danos à população. Durante a madrugada do dia 18 para o dia 19 daquele mês, uma intensa precipitação pluviométrica teve início, resultando em um acumulado de chuvas superior a 640 mm em um período de apenas 24 horas, equivalente à média anual de precipitação em poucas horas. O grande volume de água desencadeou uma série de deslizamentos de encostas, desmoronamentos, inundações e, como consequência, bloqueio de vias e soterramentos.

Como resposta a essa tragédia, a Força de Fuzileiros da Esquadra recebeu a ordem para ativar seu Plano de Apoio à Defesa Civil. Assim, um Grupamento Operativo de Fuzileiros Navais (GptOpFuzNav) foi deslocado para a região a bordo do Navio Multipropósito Atlântico. A missão foi designada como Operação Abrigo pelo Mar.

O GptOpFuzNav foi incumbido de três tarefas específicas como parte de sua resposta à crise. Primeiramente, atuou na desobstrução das vias utilizando equipamentos de engenharia. Em seguida, prestou auxílio logístico no transporte de pessoal e material, incluindo doações de roupas e alimentos. Além disso, operou um Hospital de Campanha (HCamp).

O Estado-Maior do GptOpFuzNav contava com um Oficial de Ligação de Operações Psicológicas (OLig OpPsc) e um destacamento composto por quatro militares responsáveis por assessorar o comando em relação ao ambiente informacional.

Conforme mencionado anteriormente, as Operações Psicológicas atuam no nível tático, proporcionando apoio às tarefas pertinentes ao escalão em questão. Dado que o grupamento estava eficientemente estruturado para a desobstrução das vias e colaborava em coordenação com a Defesa Civil e outras entidades contratadas para essa finalidade, o Destacamento de Operações Psicológicas concentrou-se na tarefa relacionada à operação do HCamp.

Após os primeiros dias de missão, observou-se uma redução no número de atendimentos registrados no Hospital de Campanha, o que suscitou dúvidas no Estado-Maior. A questão era se a diminuição da procura estava relacionada ao desconhecimento, por parte da população local, do local de funcionamento, dos horários de atendimento e das especialidades oferecidas no HCamp, ou se a demanda por serviços médicos emergenciais havia naturalmente diminuído, resultando em um equilíbrio entre oferta e procura no sistema de saúde local.

Diante dessa situação, um estudo de público-alvo foi conduzido e uma Campanha de Operações Psicológicas foi elaborada com o objetivo de aumentar o número de atendimentos no Hospital de Campanha. Isso foi realizado por meio de diversas estratégias de divulgação de informações relevantes para a comunidade local.

Figura 1: Produto visual para mídia social.

Fonte: Destacamento de Operações Psicológicas.

Foram criados materiais visuais para mídias sociais (Figura 1), que foram compartilhados por meio de comunicadores influentes em grupos de aplicativos de mensagens.

Durante o estudo de público-alvo, foram identificados líderes comunitários, como lideranças religiosas, presidentes de associações de moradores e representantes de ONGs, que poderiam contribuir para a disseminação de informações de interesse da Força.

Adicionalmente, foi desenvolvido um conteúdo de áudio, que era transmitido por meio de um Dispositivo Acústico de Longo Alcance (*Long Range Acoustic Device* – LRAD) instalado em uma viatura operativa (Figura 2) com o intuito de alcançar as regiões mais afetadas pelos deslizamentos. Enquanto o áudio era transmitido, membros do destacamento abordavam os moradores locais para fornecer informações sobre a Operação Abrigo pelo Mar e o funcionamento do HCamp, além de orientações relativas às áreas de risco classificadas pela Defesa Civil (Figura 3).

Figura 2: Dispositivo Acústico de Longo Alcance (*Long Range Acoustic Device* – LRAD).

Fonte: Destacamento de Operações Psicológicas.

Figura 3: Militares OpPsc abordando a população em áreas afetadas pelo desastre.

Fonte: Destacamento de Operações Psicológicas.

Após o início da campanha, verificou-se uma estabilização no número de atendimentos diários, que anteriormente estava em declínio. No entanto, após alguns dias, a quantidade de atendimentos voltou a diminuir. Essa observação permitiu ao Comando adquirir maior clareza para tomar decisões quanto à continuidade das operações do HCamp no local, com a compreensão de que a redução nos atendimentos não estava relacionada ao desconhecimento da população sobre o funcionamento do hospital.

2.2. Operação Furnas

Em março de 2023, a Força de Fuzileiros da Esquadra solicitou ao CoNavOpEsp que realizasse uma Campanha de Operações Psicológicas em São José da Barra (MG), visto que o exercício realizado na localidade aumentaria de vulto, dobrando o efetivo de militares, o que gerou preocupação com os desdobramentos que esse aumento poderia causar à população local.

Dessa forma, foram definidos os propósitos e o estado final desejado a ser alcançado:

Propósitos:

- Promover a comunicação efetiva com a população local, explicando os objetivos e os benefícios da Operação;
- Esclarecer dúvidas e receios, reduzindo resistência ou oposição; e
- Identificar, na população e em lideranças, as necessidades locais que podem ser alcançadas por meio de ações da Marinha do Brasil.

Estado final desejado:

Aumento da transferência e da confiança da população na Marinha do Brasil e na Operação, fortalecendo o apoio e o engajamento da comunicação local.

O Destacamento de Operações Psicológicas foi estabelecido e deu início ao seu planejamento com a elaboração de um abrangente Levantamento de Área para Operações Psicológicas. A meticulosa análise da região proporcionou um alicerce sólido para a seleção do público-alvo e a definição dos objetivos psicológicos a serem perseguidos na Campanha de Operações Psicológicas em nível tático.

A primeira medida adotada consistiu em conduzir uma pesquisa inicial, por meio da qual o destacamento pôde avaliar o grau de conhecimento e de aceitação da população em relação às atividades da Marinha e do Corpo de Fuzileiros Navais, conhecer os principais pontos de insatisfação na comunidade e identificar as lideranças e os comunicadores de influência.

Com base nas valiosas informações fornecidas pela pesquisa, deu-se início à divulgação da Operação juntamente com a promoção de eventos com acesso aberto ao público em geral, como a Ação Cívico-Social (ACISO) e a Demonstração Operativa planejada. Conforme a pesquisa revelou, entre as preocupações manifestadas pela população estavam a carência de opções de entretenimento e a escassez de informações acerca da vida militar e das possibilidades de ingresso nas Forças Armadas.

Figura 4: Material de divulgação da ACISO.

Fonte: Destacamento de Operações Psicológicas.

Em vista disso, foram criados materiais visuais e gráficos de mídias sociais (Figura 4), os quais foram amplamente disseminados – tanto em estabelecimentos comerciais locais e escolas quanto por meio de comunicadores influentes na região – com o intuito de promover a ACISO, que incluiria apresentações de banda de música, demonstrações de cães adestrados e outras atividades, transformando a Ação em uma opção de lazer para as famílias.

Figura 5: Divulgação em escolas.

Fonte: Destacamento de Operações Psicológicas.

Os militares do Destacamento OpPsc também visitaram escolas locais (Figura 5), onde divulgaram a Ação Cívico-Social, responderam a perguntas relacionadas ao ingresso na Marinha e convidaram algumas dessas instituições a participarem da Demonstração Operativa que seria realizada no Lago de Furnas.

Adicionalmente, foi produzido conteúdo de áudio contendo informações sobre a Operação e convites à população para comparecer à ACISO. Esse material foi veiculado em diversas rádios locais após contatos diretos com os principais radialistas da cidade.

No início do exercício, com a movimentação de equipamentos e efetivos na pequena cidade de São José da Barra, constatou-se que a população havia compreendido que aquela alteração na rotina local correspondia à Operação que havia sido previamente divulgada. Notou-se um sentimento de normalidade entre os habitantes, o que permitiu concluir que a Operação Psicológica havia alcançado seus objetivos. Esse êxito também se refletiu na expressiva presença de público na ACISO, na Demonstração Operativa e na quantidade de reportagens positivas sobre a Operação veiculadas na mídia local.

Conclusão

As Operações Psicológicas têm como objetivo primordial a alteração de comportamentos específicos em públicos-alvo determinados. No âmbito tático, mais precisamente em apoio à Força de Fuzileiros da Esquadra, busca-se constantemente influenciar os comportamentos que estejam alinhados com as necessidades do Comandante do Grupamento Operativo a fim de facilitar a execução de suas tarefas e, por conseguinte, o cumprimento de sua missão.

Nos exercícios programados no calendário operativo da Força de Fuzileiros da Esquadra, as Operações Psicológicas são meticulosamente planejadas levando em consideração o público-alvo inimigo. Nesses cenários, elas são implementadas com o propósito de atingir objetivos psicológicos específicos, como a redução da vontade de combate do inimigo e o aumento das rendições. Entretanto, é importante destacar que, em operações benignas e em situações de resposta a desastres humanitários reais, ocorre uma interação direta com públicos-alvo neutros e aliados, como a população local.

Esses contextos reais proporcionam oportunidades valiosas para o treinamento de procedimentos e técnicas essenciais aos Operadores Psicológicos, permitindo que eles adquiram experiência prática em ambientes genuínos. Essa experiência raramente pode ser reproduzida com fidelidade em exercícios que envolvem apenas interações com um inimigo fictício, o que ressalta a importância das operações reais e da interação com públicos-alvo reais para o aprimoramento das capacidades de Operações Psicológicas.

Referências Bibliográficas

BRASIL. Marinha do Brasil. Comando-Geral do Corpo de Fuzileiros Navais. **Manual de Operações Psicológicas de Fuzileiros Navais - CGCFN – 1-6.** 1. ed. Rio de Janeiro, 2023.

_____._____. Estado-Maior da Armada. **EMA-305: Doutrina Militar Naval.** Brasília-DF, 2017.

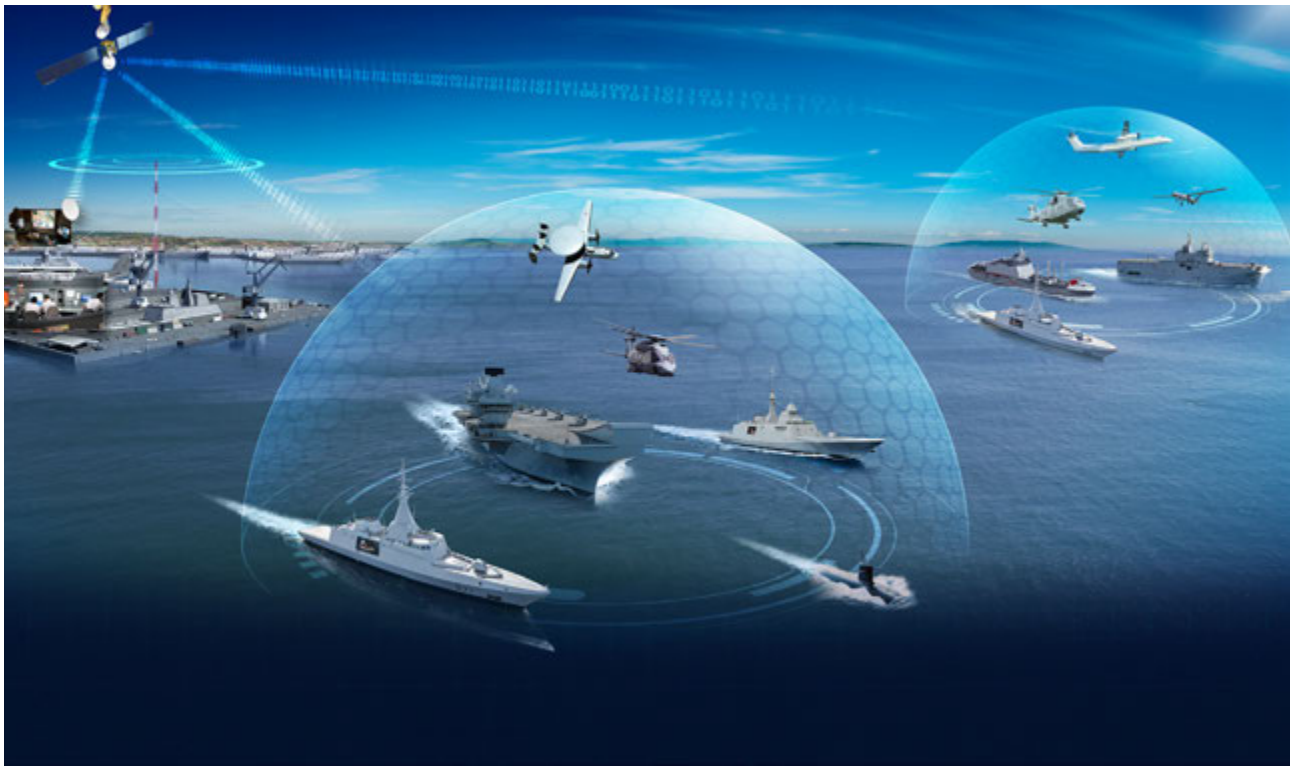
_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD-35-G-01: Glossário das Forças Armadas.** 4. ed. Brasília-DF, 2007.

Inteligência de Comunicações: uma poderosa arma em apoio às Operações Navais

Capitão de Mar e Guerra **Humberto** Ferreira Ramos Junior

Atualmente estagiário do Curso de Altos Estudos de Política e Estratégia (CAEPE), é graduado em Ciências Navais pela Escola Naval com habilitação em Eletrônica. Realizou os cursos de Mestrado em Informática com ênfase em Segurança de Redes e Pós-graduação em Gerência de Redes e Tecnologia Internet. Entre as principais comissões, foi Encarregado da Divisão de Convés do Navio-Patrulha Guaíba, Encarregado da Divisão de Sistema de Armas da Corveta Frontin, Chefe do Departamento de Segurança das Informações Digitais e Encarregado da Central de Tratamento de Incidentes em Redes de Computadores do Centro de Tecnologia da Informação da Marinha (CTIM), Chefe do Departamento de Segurança das Informações Digitais da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) e Diretor do Centro de Guerra Acústica e Eletrônica da Marinha (CGAEM).

Figura 1: Inteligência de Comunicações.



Fonte: Thales Group.

Introdução

No âmbito da Guerra Eletrônica (GE), a Inteligência de Comunicações (*Communications Intelligence* – COMINT) é a atividade que visa à obtenção de informações sobre as comunicações utilizadas pelo inimigo com o objetivo de compreender sua intenção, localização, capacidades e limitações. Essa atividade inclui a interceptação, a análise e a interpretação de sinais de rádio, voz, dados e outros tipos de comunicação. Engloba as atividades voltadas para a proteção de sistemas eletrônicos próprios, bem como aquelas voltadas à perturbação e à degradação dos sistemas eletrônicos do inimigo. Por meio da COMINT, é possível obter informações críticas sobre as atividades do oponente, o que pode se traduzir em vantagens táticas e estratégicas no campo de batalha.

No cenário tecnológico atual, em que os conflitos ocorrem em múltiplos domínios, essa subárea da GE vem ganhando cada vez mais notoriedade como uma capacidade crítica em apoio às ações militares. Neste artigo, busca-se enfatizar sua importância nas Operações Navais, iniciando com um breve histórico sobre sua evolução no contexto mundial. Em seguida, é apresentada a forma como a GE foi inserida na Marinha do Brasil (MB), concluindo com o destaque para algumas ações voltadas à sua efetiva consolidação no âmbito da Força.

1. Breve histórico da Inteligência de Comunicações no mundo

Ao longo da história, a atividade militar serviu para impulsionar a busca e o desenvolvimento de tecnologias que, de alguma forma, levassem uma força a sobrepujar seus inimigos. Especialmente a partir do século XX, os fenômenos eletromagnéticos e sua utilização em prol das comunicações passariam a despertar especial interesse pelo seu emprego nos campos de batalha. À medida que os sistemas eletrônicos avançavam, logo se percebeu a necessidade de serem efetuadas ações tanto de inteligência quanto de contrainteligência nesse novo ambiente. Essa disputa pelo usufruto e/ou pela negação do espectro eletromagnético passou a ser conhecida como Guerra Eletrônica.

A GE foi empregada pela primeira vez na Batalha de Tsushima em 27 de maio de 1905. Durante a madrugada, o cruzador japonês Shinano Maru avistou o navio-hospital russo Orel, que estava iluminado, cumprindo as leis marítimas internacionais. Mais tarde, próximo ao amanhecer e com a dissipação da neblina, os japoneses constataram que o Orel não estava só.

Com o avistamento da frota russa, o Shinano Maru passou a transmitir, para o comando da frota japonesa, a localização da esquadra inimiga. Nesse momento, os operadores de radiotelégrafos russos, aproveitando-se da potência de seus equipamentos, realizaram emissões na mesma frequência das comunicações japonesas, no intuito de torná-las ininteligíveis. Mas, em algum momento, após o comandante da esquadra russa ordenar o fim do bloqueio eletrônico, os japoneses obtiveram a posição de seus oponentes, resultando na vitória da esquadra japonesa do Almirante Togo. Esse foi o primeiro emprego da GE em combate.

Figura 2: Batalha de Tsushima.
Fonte: HistoryNet, 2021.

Com a I Guerra Mundial, mesmo que ainda não empregada de forma sistemática, a COMINT passou a ser utilizada em ações de monitoração, interceptação e interferência em transmissões de radiofrequência. Já na II Guerra, vale destacar o papel das unidades americanas nos esforços conjuntos com os britânicos na área de inteligência de sinais. A quebra do código naval japonês JN25b, por exemplo, desempenhou papel decisivo nas batalhas do Mar de Coral e de Midway em 1942. Da mesma maneira, desde as primeiras soluções para as mensagens codificadas pelas máquinas alemãs Enigma em 1940, o esforço aliado no âmbito da inteligência de sinais foi fator decisivo para o encurtamento da guerra.

Na atualidade, podemos citar o conflito Rússia x Ucrânia, no qual fica clara a importância da COMINT, que vem desempenhando um importante papel nos combates travados e no posicionamento das tropas no terreno. Como as comunicações de radiofrequência são essenciais para operações tantos civis quanto militares, as ações realizadas nesse ramo têm se mostrado uma grande arma para a destruição ou a degradação dos sistemas de combate inimigos.

Como exemplo, pode ser citado o *jammer* russo R-330Zh Zhitel, que supostamente consegue interferir em todos os equipamentos de comunicações via satélite, em redes celulares, no GPS e em transmissões nas faixas de VHF/UHF dentro de um raio de 25 km. Além disso, em sua estação de comando e controle, há equipamentos para detecção, localização de direção e análise de sinais de radiocomunicação usando a tecnologia baseada em Rádio Definido por *Software* (RDS).

Figura 3: Jammer R-330Zh Zhitel.

Fonte: Defense Express, 2023.

As forças ucranianas, por sua vez, vêm se utilizando de sistemas fornecidos pelos Estados Unidos (EUA). Há relatos de que a Rússia não possui um sistema de comando e controle robusto, dependendo de telefones celulares ou rádios não criptografados suscetíveis a ações de geolocalização e interferência ucranianas. Muitos celulares russos, supostamente seguros, falharam por dependerem de canais de dados 3G/4G. Além disso, a falta de adesão a uma política rígida de COMINT levou muitos combatentes russos, inclusive generais, a utilizarem celulares comuns, contribuindo para o sucesso de algumas medidas adotadas pelos ucranianos.

2. A Inteligência de Comunicações na Marinha do Brasil

Nos anos 1970, entravam no serviço ativo as Fragatas Classe Niterói. Na época, os navios chamaram a atenção da imprensa naval, inclusive no exterior. O livro *Modern Naval Combat* (MILLER & MILLER, 1986) menciona a Fragata Constituição nos seguintes termos: "Fragatas, como as da Classe Niterói, tornaram-se os navios de guerra modernos mais amplamente utilizados, com capacidades muito superiores aos seus similares da II Guerra Mundial".

No contexto da COMINT, foi efetuada a incorporação de um equipamento de Medida de Apoio de Guerra Eletrônica (MAGE) que possibilitava o monitoramento de sinais de comunicações conhecido como radiogoniômetro CDL-160.

Mas as ações da MB nesse campo estão registradas desde a II Guerra Mundial, com a implantação da Rede de Radiogoniométrica de Alta Frequência (RRGAF), inicialmente composta por duas Estações Radiogoniométricas de Alta Frequência (ERGAF): a primeira instalada em Pina (Pernambuco) e a segunda, em Salinas da Margarida (Bahia). Por ocasião da Guerra da Lagosta, quando chegou ao Brasil o relato de que um navio de guerra francês havia iniciado seu deslocamento em direção à nossa costa, tais estações foram empregadas na busca por emissões eletromagnéticas oriundas de navios franceses navegando no Atlântico.

Hoje, as estações pertencentes à MB que desempenham o papel de monitorar e obter a localização de sinais de comunicações em alta frequência (*High Frequency* – HF) ao longo da nossa costa estão localizadas nas áreas de jurisdição dos Comandos dos seguintes Distritos Navais (DN):

- 1º DN – Estação Radiogoniométrica da Marinha em Campos Novos/RJ (ERMCN);
- 3º DN – Estação Radiogoniométrica da Marinha em Natal/RN (ERMN);
- 4º DN – Estação Radiogoniométrica da Marinha em Belém/PA (ERMBe).
- 5º DN – Estação Radiogoniométrica da Marinha em Rio Grande/RS (ERMRG).

No âmbito do Corpo de Fuzileiros Navais (CFN), em 1990 foi criada a Companhia de Guerra Eletrônica (CiaGE) como subunidade do Batalhão de Comando da Tropa de Reforço (BtlCmdoTrRef). Mais adiante, em 2003, em virtude da reestruturação da Força de Fuzileiros da Esquadra, foi ativado o Batalhão de Comando e Controle (BtlCmdoCt), composto por: Companhia de Comunicações, Companhia de Comando da Divisão Anfíbia e Companhia de Guerra Eletrônica. Coube à CiaGE a tarefa de realizar Medidas de Guerra Eletrônica (MGE) em apoio ao Grupamento Operativo de Fuzileiros Navais (GptOpFuzNav). Nesse cenário, entra em utilização o Sistema de Guerra Eletrônica Tadiran, que tem capacidade de atuar como Centro Controlador de Inteligência de Sinais (CECOIS).

Figura 4: Sistema de Guerra Eletrônica Tadiran.

Fonte: Acervo interno do BtlCmdoCt.

3. Incrementos em nossas capacidades

Uma ação futura de modernização e integração de nossas ERGAF ao atual Sistema de Radiogoniometria e Monitoramento em HF de uso do Centro Gestor e Operacional do Sistema de Proteção da Amazônia (CENSIPAM), com sítios localizados em Boa Vista e Porto Velho, alavancaria a capacidade de inteligência de comunicações da MB nos níveis tático, operacional e estratégico em virtude da disponibilidade de informações quanto à localização de uma fonte emissora, contribuindo, dessa maneira, para o aumento da consciência situacional e da inteligência marítima.

Quanto aos meios navais, tanto os novos Submarinos Classe Riachuelo como as Fragatas Classe Tamandaré (FCT) foram contemplados com equipamentos MAGE de Comunicações (MAGE-COM), que são capazes de monitorar canais de radiocomunicação. Em que pese o efeito primordial desejado de uma ação de submarinos ser a destruição dos navios inimigos – compreendendo medidas contra o tráfego marítimo e contra unidades navais de superfície e submarinos –, de acordo com a Doutrina Militar Naval (DMN), o emprego desse aparato aumenta sua capacidade de realizar operações de esclarecimento em áreas controladas pelo inimigo, caso sejam necessárias.

No caso das FCT, o equipamento possibilitará o alerta antecipado graças à sua capacidade de detecção de sinais de comunicação de ameaças em longo alcance, auxiliando na autoproteção do navio. Ademais, será possível geolocalizar sinais de comunicação emitidos, complementando a capacidade similar fornecida pelo sensor MAGE-Radar, contribuindo, assim, para o incremento da consciência situacional marítima.

Na atualidade, uma boa opção tecnológica de baixo custo a ser utilizada em atividades COMINT é o Rádio Definido por *Software* RTL-RDS quando integrado com sistemas baseados em *software* livre. Esse dispositivo pode ser utilizado como um *scanner* de frequências capaz de atuar na faixa de 25 kHz a 1,75 GHz. Após testes conjuntos envolvendo o Centro de Guerra Acústica e Eletrônica da Marinha (CGAEM) e o Batalhão de Comando e Controle (BtlCmdoCt), vislumbrou-se seu emprego em apoio aos Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav) nas operações e ações de guerra naval e em demais situações de emprego que lhe são afetas. Além disso, o dispositivo também mostrou ser eficaz em atividades de escuta de comunicações digitais e na identificação de embarcações pesqueiras atuando no limite da Zona Econômica Exclusiva (ZEE).

Figura 5: RTL-RDS conectado a um *laptop*.

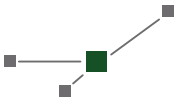
Fonte: DesktopSDR.com, [s.d.].

Conclusão

Atualmente, a guerra moderna é cada vez mais dependente do espectro eletromagnético. Negar seu uso a uma força oponente e, por meio desse ambiente, obter informações críticas sobre suas atividades torna-se cada vez mais crucial.

Nesse contexto, a COMINT atua sobre as comunicações utilizadas pelo inimigo com os objetivos de compreender suas intenções de movimento e localização, conhecer suas limitações e, possivelmente, degradar e/ou neutralizar sua capacidade de Comando e Controle (C^2).

Estar preparado para esse atual cenário tecnológico contribuirá para que a MB tenha superioridade em Teatros de Operações que venham a se desvelar, de forma a permitir ao Brasil o exercício do protagonismo internacional proporcional à grandeza de nossas potencialidades.



Referências Bibliográficas

AFCEA INTERNATIONAL. **Russia versus Ukraine and the Role of Software-Defined Radios**. 2023. Disponível em: <https://www.afcea.org/signal-media/cyber-edge/russia-versus-ukraine-and-role-software-defined-radios>. Acesso em: 07 set. 2023.

BRASIL. Marinha. Estado-Maior da Armada. **EMA-305: Doutrina Militar Naval**. Brasília, 2017.

CEPIK, Marco. Origens do Sistema de Inteligência dos Estados Unidos: 1775-1946. **Carta Internacional**, v. 9, n. 1, p. 03-18, 2014.

COELHO, Emilio Reis. **O pensamento naval nas páginas da Revista Marítima Brasileira (1970-1990): no contexto da Guerra Fria e à luz das lições aprendidas com a guerra das Falklands/Malvinas**. 2019. 354 f. Dissertação de Mestrado. Programa de Pós-Graduação em Estudos Estratégicos da Defesa e da Segurança. Instituto de Estudos Estratégicos, Universidade Federal Fluminense. Niterói, 2019. Disponível em: <https://app.uff.br/riuff/handle/1/25135>. Acesso em: 16 jan. 2024.

DEFENSE EXPRESS. **Ukrainian Defenders Destroyed the R-330Zh Zhitel Jamming Station, a Technical Support Vehicle and a Tank**. August 17, 2023. Disponível em: <https://en.defence-ua.com/news/ukrainian_defenders_destroyed_the_r_330zh _zhitel_jamming_station_a_technical_support_vehicle_and_a_tank-7651.html>. Acesso em: 20 ago. 2023.

DESKTOPSDR.COM. **RTL-SDR and Computer Hardware Requirements**. [s.d.]. Disponível em: <https://www.desktopsdr.com/hardware>. Acesso em: 27 set. 2023.

HISTORYNET. **Japan's Trafalgar: the Battle of Tsushima Strait**. By Alan George. December 27, 2021. Disponível em: <https://www.historynet.com/battle-of-tsushima/>. Acesso em: 19 ago. 2023.

KIFFER, André Geraque. **Batalha Naval de Tsushima, 1905**. Clube de Autores, 2011.

MILLER, David; MILLER, Chris. **Modern Naval Combat**. Crescent Books, 1986.

PODER NAVAL. **A classe 'Niterói' foi destaque na imprensa internacional**. 2018. Disponível em: <https://www.naval.com.br/blog/2018/01/22/classe-niteroi-foi-destaque-na-imprensa-internacional>. Acesso em: 07 set. 2023.

SOARES, Anderson Silva. Inteligência de Comunicações e sua importância como suporte às operações navais. **Revista Passadiço**, v. 34, n. 42, p. 18-18, 2022.

THALES GROUP. **Fleet Communications**. [s.d.] Disponível em: <https://www.thalesgroup.com/en/markets/defence-and-security/radio-communications/naval-communications/fleet-communications>. Acesso em: 27 set. 2023.

Emprego de Telemetria Acústica Terrestre na localização de disparos e fogo de contrabateria

15

Capitão de Corveta Guilherme Ferreira **Murmel** Liali

Ingressou na MB por meio do Colégio Naval. Ao longo de sua carreira, realizou diversos cursos, com destaque para o Curso de Aperfeiçoamento em Submarinos para Oficiais (CASO), o Curso de Operação e Manutenção do Sistema de Combate Integrado AN/BYG-501 e o Mestrado em Engenharia de Defesa pelo Instituto Militar de Engenharia. Entre as principais comissões, foi Encarregado da Divisão de Operações, Chefe do Departamento de Operações no Submarino Tikuna e Instrutor do CASO no Centro de Instrução e Adestramento Almirante Átilla Monteiro Aché. Em 2022, assumiu a Divisão de Análise de Campo em Guerra Acústica do CGAEM.

Introdução

A telemetria de peças de artilharia, ou posições de armas inimigas por métodos acústicos, visa estimar a sua localização através do som produzido, predominantemente, pelos disparos realizados. Outra abordagem para essa estimativa consiste na análise da onda de choque gerada pelo projétil durante a fase supersônica de sua trajetória.

Inicialmente, os métodos acústicos, associados à mensuração temporal da recepção, emergiram antes da Primeira Guerra Mundial. Essa metodologia engloba a identificação do ruído proveniente do disparo de uma peça, a estimativa de sua direção e a mensuração da diferença de tempo de chegada entre dois receptores distanciados por alguns quilômetros. Embora os alemães tenham empregado esse método durante a guerra, ele foi prontamente descartado por ser considerado ineficaz pelas nações da Tríplice Entente, que desenvolveram os fundamentos científicos para a telemetria acústica, ainda vigente.

A base científica para a telemetria acústica é a utilização de sensores compostos por vários microfones visando à obtenção de linhas de posição (LDP) do disparo e sua origem. Essas LDPs são derivadas das diferenças temporais na chegada do sinal aos microfones (*Time Difference of Arrival* – TDoA). Tipicamente, cada sensor é equipado com três microfones, dispostos triangularmente com uma separação de aproximadamente 10 metros, medida necessária para alcançar a relação sinal-ruído ideal na faixa de frequência mais baixa (infrassom, abaixo de 20 Hz), característica dos disparos de peças de artilharia.

Após um período de suspensão ao término da Segunda Guerra Mundial, quando sistemas de radares terrestres e aéreos dominaram a tarefa de localização de artilharia, a década de 2010 testemunhou uma nova abordagem, ainda em desenvolvimento, que utiliza os denominados Sensores Acústicos Multimissão. Eles incorporam microfones vinculados a sensores de velocidade de partículas capazes de proporcionar a direção de chegada para sinais de banda larga e baixa frequência, reduzindo substancialmente as dimensões dos sensores e consolidando-os em uma única unidade.

1. Histórico

A Primeira Guerra Mundial coincide com o advento da Acústica como ciência em um período que reuniu sensores, tecnologia de medição precisa de tempo e recursos de análise necessários para a obtenção de uma telemetria acústica eficaz. Como muitos conceitos tecnológicos, a ideia de utilizar o som para localizar peças de artilharia inimigas surgiu de várias iniciativas individuais quase simultâneas.

O conflito proporcionou o ambiente propício para o desenvolvimento da telemetria acústica, pois o processamento de sinais elétricos de microfones estava amadurecendo devido ao início do desenvolvimento da telefonia, assim como das tecnologias para a gravação de sons. Esses avanços permitiram a medição precisa da diferença de tempo de chegada na ordem de centésimos de segundo. Dessa forma, a necessidade de suprimir a artilharia, central na guerra estática das

trincheiras, automaticamente gerou a opção mais viável: o fogo de contrabateria.

Embora o exército britânico não tenha sido o primeiro a testar a telemetria acústica para artilharia, foi ele que efetivamente implementou o primeiro sistema eficaz para essa tarefa durante a Primeira Guerra Mundial. Em meados de 1915, os britânicos atribuíram ao cientista australiano e ganhador do Prêmio Nobel, Sir William Lawrence Bragg, a responsabilidade pelo desenvolvimento de uma solução.

A primeira tarefa de Bragg foi investigar trabalhos existentes, especialmente as iniciativas francesas que, apesar de relevantes, careciam de aplicabilidade prática em combate. Bragg concentrou-se na natureza dos sons da artilharia e na necessidade de isolar o infrassom do ruído (relacionado à detonação do propelente do projétil) da fase supersônica de sua trajetória. Esse desafio foi resolvido em meados de 1916 por um membro da equipe de Bragg, o cabo William Sansome Tucker, militar ex-integrante do Departamento de Física da Universidade de Londres. Tucker desenvolveu um microfone de baixa frequência para separar o som do disparo da arma do estrondo supersônico do projétil. Outras questões foram igualmente resolvidas, resultando em dispositivos operacionais eficazes já em 1917.

Durante a Segunda Guerra Mundial, a tecnologia de alcance do som estava madura e foi amplamente empregada nas ilhas do Pacífico, especialmente pela Inglaterra, pioneira nesse campo, e pelos Estados Unidos – notadamente pelos fuzileiros navais. Em 1944, o radar iniciava, de maneira limitada, sua incursão na detecção de projéteis e na localização de baterias, inaugurando uma nova fase que se estenderia pelas décadas seguintes. Vale destacar que, tanto antes quanto durante a Batalha da Inglaterra, a detecção e a telemetria acústica foram utilizadas de forma alternativa para a defesa aérea das ilhas britânicas, complementando a então recente tecnologia de radar.

Na Guerra Fria, o emprego generalizado de radares terrestres e aéreos foi acompanhado pelo desenvolvimento da microeletrônica e da computação. A detecção de projéteis e suas trajetórias possibilitava a localização dos lançadores, bem como a determinação da direção dos disparos da contrabateria e dos primeiros sistemas de defesa de ponto.

2. Modernidade: Pós-Guerra Fria e dias atuais

No Pós-Guerra Fria, a telemetria acústica ressurgiu e se destacou novamente graças à Inglaterra, sendo empregada até os dias atuais. O salto tecnológico que propiciou esse ressurgimento foi o advento dos sensores multimissão, que integram sensores de velocidade e microfones, permitindo uma significativa redução no tamanho dos arranjos de sensores.

O pioneirismo dessa reinserção foi evidenciado no protótipo do sistema HALO (*Hostile Artillery Locating* – localização de artilharia hostil), utilizado em Sarajevo em 1995. A versão de produção, também denominada ASP (*Advanced Sound Ranging Project* – projeto avançado de alcance sonoro), foi adotada pelos britânicos em 2001 e alega-se que, em 2003, no Iraque, foi capaz de localizar artilharia hostil a uma notável distância de 50 km. Atualmente, essa tecnologia vem sendo adotada por diversos outros operadores, incluindo os fuzileiros navais dos Estados Unidos.

Países como Rússia e Alemanha também desenvolveram sistemas semelhantes. A versatilidade dos sensores multimissão possibilita a sua instalação em diversos tipos de veículos, o que confere capacidade de telemetria acústica para escalões inferiores, proporcionando, assim, maior sobrevivência e disponibilidade espacial e temporal desse recurso.

O cenário atual contempla, ainda, técnicas de processamento de sinais acústicos que incorporam significativos avanços motivados por mudanças nas peças de artilharia contemporâneas. Com armamentos de alcances cada vez maiores, o processamento do estampido do disparo torna-se proibitivo devido às atenuações sofridas durante a propagação, o que dificulta a sua detecção em longas distâncias. Adicionalmente, a velocidade do som no ar e a elevada mobilidade de peças autopropulsadas contribuem para que a detecção e a localização ocorram tarde demais, inviabilizando o efetivo emprego do fogo de contrabateria antes que o inimigo reposicione sua própria artilharia. Nesse contexto, os lançadores múltiplos de foguetes ganham destaque e se tornam cada vez mais difundidos, complementando e substituindo a artilharia de tubo, pois a propulsão contínua dos foguetes ao longo de sua trajetória elimina o ruído do disparo.

Dessa forma, a telemetria acústica contemporânea concentra-se não mais no ruído do disparo, mas sim nas ondas de choque geradas pelo deslocamento supersônico dos projéteis e foguetes. As características singulares desse sinal acústico o tornam mais propenso a ser explorado no cenário moderno, uma vez que é mais intenso, possui maior duração e sofre menor atenuação na propagação. É importante ressaltar que as ondas de choque apresentam um nível sonoro inicial mais elevado, sofrendo atenuações apenas em duas dimensões (ao contrário da propagação esférica do estampido), e geralmente possuem um ângulo de chegada em elevação mais obtuso. Vale destacar que o tempo de aquisição do alvo não é mais ditado pela velocidade do som, mas sim pela velocidade supersônica do projétil,

resultando na localização mais rápida da origem do disparo e na maior efetividade do fogo de contrabateria.

Por fim, é de suma importância salientar que, em determinados sistemas acústicos modernos, as capacidades de telemetria acústica mencionadas anteriormente estendem-se à localização de disparos de armas portáteis de pequeno calibre. Essas capacidades tornam-se primordiais nos dias atuais, marcados pela proliferação de conflitos de baixa intensidade, assimétricos e em áreas urbanizadas. Em tais cenários, é comum ver forças convencionais, inclusive em Operações de Paz, enfrentarem agentes irregulares que utilizam uma variedade de armas leves em ambientes urbanos ou que impedem qualquer tipo de detecção por linha de visada (*Non-Line of Sight* – N-LOS).

3. Vantagens e desvantagens da Telemetria Acústica Terrestre

A variação do som oferece uma série de vantagens em relação a outros métodos: a detecção acústica é um método passivo caracterizado pela ausência de emissões rastreáveis até o receptor, diferentemente de sistemas como radares ou sensores ativos. Os equipamentos de telemetria acústica terrestre, comparados a radares desempenhando funções semelhantes, tendem a ser mais compactos e leves, conferindo maior mobilidade e disponibilidade. Além disso, dispensam a necessidade de extensos arranjos de sensores ou significativas quantidades de energia.

Essas vantagens, contudo, implicam uma solução de compromisso: a velocidade do som varia consideravelmente em função da temperatura e de outras condições atmosféricas, como a intensidade e a direção do vento. Para a detecção em longas distâncias, o som gerado por uma arma não se traduz em um estampido discreto, mas sim em um estrondo de duração considerável, resultado da propagação multipercurso. Isso torna desafiadora a medição precisa do tempo exato de chegada da frente de onda por correlação cruzada do sinal entre diferentes sensores.

4. Sistemas atualmente em serviço

4.1. HALO

O Sistema de Localização de Artilharia Hostil, conhecido como HALO, encontra-se atualmente em operação nas forças armadas do Reino Unido, dos Estados Unidos e do Canadá, entre outros países. O HALO utiliza técnicas avançadas de processamento de dados acústicos para realizar a localização rápida, precisa e confiável de peças de artilharia, morteiros pesados e lançadores múltiplos de foguetes. O sistema é composto por até 12 conjuntos de sensores não tripulados autônomos, denominados *Sensor Posts* (SP), que são distribuídos com espaçamento de dois a quatro quilômetros de distância.

Cada conjunto SP é constituído por sensores meteorológicos e grupos de microfones georreferenciados por GPS, o que proporciona uma redundância eficiente contra falhas de equipamento ou ações inimigas. Os dados coletados pelo SP são transmitidos para o Posto de Comando (CP – *Command Post*), onde a localização da arma é calculada com um erro inferior a 1% em alcance e quase em tempo real, ou seja, praticamente instantaneamente para transmissão subsequente. Esse sistema vem sendo submetido a testes em situações reais de combate desde os anos 1990, tendo demonstrado sua eficácia nos conflitos da Bósnia, do Kosovo, do Iraque e do Afeganistão.

Figura 1: Postes de suporte dos sensores acústicos e de velocidade de partículas (sensores multimissão) do sistema HALO.

Fonte: Military Periscope, [s.d.].

4.2. AZK-7M e WLS POLOZHENNYA-2

O sistema russo AZK-7M é utilizado tanto para localizar armas e morteiros inimigos quanto para direcionar o fogo da própria artilharia contra alvos inimigos. É composto por um Posto de Comando (CP) e três Pontos-Base (BP – *Base Point*), que são transportados por viaturas de cinco toneladas. O AZK-7M opera de maneira eficiente no campo de batalha: cada BP é equipado com duas Estações de Som (SS) e cada SS é composta por três microfones.

O sistema é capaz de localizar projéteis de morteiros ou de canhões em distâncias que variam de 8 km a 16 km, respectivamente, com um erro de apenas 1% em alcance e em um rápido intervalo de 15 segundos. A cobertura efetiva de três BPs abrange uma frente de até 12 km.

Uma versão modernizada do AZK-7M, conhecida como Polozhennya-2, apresenta configuração e capacidade semelhantes, mas se destaca por sua maior mobilidade, sendo instalada em diversos tipos de veículos.

Originado na Ucrânia, o Polozhennya-2 é considerado um Sistema Automatizado de Localização Acústica de Armas (*Weapons Localization System* – WLS). Alega-se que esse sistema possui a notável capacidade de localizar disparos em distâncias de até 35 km em apenas 5 segundos, além de dirigir o fogo da própria artilharia a uma distância máxima de 15 km. Essas características destacam a avançada tecnologia empregada no Polozhennya-2, tornando-o uma ferramenta eficaz para a moderna gestão do campo de batalha.

Figura 2: Viatura URAL de transporte do Posto de Comando do Sistema AZK-7M.

Fonte: Russian Defence Export.

4.3. SL2A

O Sistema de Localização Acústica de Artilharia SL2A (*Système de Localisation de l'Artillerie par l'Acoustique*) foi desenvolvido pelo Grupo Thales da França. Esse sistema autônomo proporciona cobertura de 360° em uma área de 2.000 m². Sua capacidade de detecção e localização automática abrange uma ampla gama de tipos de disparos, desde tiros de artilharia até bombas, minas, armas leves e dispositivos explosivos improvisados.

Composto por um posto de comando e oito conjuntos de sensores autônomos, cada um equipado com três microfones, o SL2A é capaz de oferecer uma resposta abrangente em cenários variados. A integração eficiente desses conjuntos de sensores é coordenada por um posto de comando central, proporcionando uma gestão unificada e precisa das informações coletadas. Essa configuração permite uma rápida e precisa localização acústica de eventos de interesse em um amplo espectro de situações operacionais.

Figura 3: Sistema SL2A. À esquerda: elemento sensor acústico portátil. Centro: arranjos triangulares de elementos sensores. Direita: Posto de Comando (CP) portátil.

Fonte: Lemer; Ywanne, 2006.

Conclusão

Os modernos sistemas de telemetria acústica superaram eficazmente as limitações associadas à sua utilização em campos de batalha dinâmicos e de ritmo acelerado graças aos complexos esforços e ao tempo despendidos para essa finalidade. Avanços notáveis em sensores, técnicas de processamento de sinais e miniaturização de componentes do sistema resultaram em elevados níveis de mobilidade e disponibilidade. Essas inovações permitiram que a telemetria acústica não apenas se integrasse de forma complementar, mas também superasse as soluções tradicionais baseadas em sistemas de radar.

Recentemente, surgiram sistemas dedicados à detecção de disparos provenientes de armas portáteis e de pequeno calibre. Essa evolução reflete tanto a adaptação a conflitos *near-peer* convencionais como a capacidade para enfrentar cenários não convencionais ou assimétricos. Esses avanços, portanto, destacam a versatilidade e a capacidade de resposta da telemetria acústica em um espectro diversificado de contextos operacionais contemporâneos.

Referências Bibliográficas

ARMED FORCES – the website for UK defence information. The British Army. Artillery. **Sound Ranging**. Disponível em: <http://www.armedforces.co.uk/army/listings/l0144.html>. Acesso em: 06 mar. 2024.

LEMER, A.; YWANNE, F. Acoustic/Seismic Ground Sensors for Detection, Localization and Classification on the Battlefield. In: **Battlefield Acoustic Sensing for ISR Applications. Meeting Proceedings RTO-MP-SET-107**, Paper 17, p. 1-12, 2006. Disponível em: <https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/RTO-MP-SET-107/MP-SET-107-17.pdf>. Acesso em: 06 mar. 2024.

MACLEOD, R. Sight and Sound on the Western Front: Surveyors, Scientists, and the 'Battlefield Laboratory' 1915-1918. **War & Society**, 2000, 18(1), p. 23-46. DOI: 10.1179/072924700791201405

MEYER, G. J. **A World Undone: the story of the Great War, 1914 to 1918**. New York: Bantam Books, 2006.

MILITARY PERISCOPE. **HALO - Hostile Artillery Location System**. [s.d.]. Disponível em: <https://www.militaryperiscope.com/weapons/sensorselectronics/ground-radars/halo-hostile-artillery-location-system/overview/>. Acesso em: 28 fev. 2024.

MITCHELL, A. J. **Technology for Artillery Location, 1914-1970**. Glasgow, UK: Lulu Press Inc., 2012.

MUIR, T. G.; BRADLEY, D. L. Underwater acoustics: a brief historical overview through World War II. **Acoustics Today**, 2016, 12(3), p. 40-48.

NAMORATO, M. V. A concise history of acoustics in warfare. **Applied Acoustics**, 2000, 59, p. 101-135.

RUSSIAN DEFENCE EXPORT. Catalog. Land Forces. **AZK-7M Automatic Sound Ranging System**. Disponível em: <http://roe.ru/eng/catalog/land-forces/automated-artillery-fire-control-systems/azk-7m >. Acesso em: 28 fev. 2024.

STEFFENS, H.; SCHUTTE, M.; EWERT, S.D. Acoustically driven orientation and navigation in enclosed spaces. **Journal of the Acoustical Society of America**. Sep. 2022; 152(3): 1767. DOI: 10.1121/10.0013702. PMID: 36182293.

STORZ, D. Artillery. In: **1914-1918 Online – International Encyclopedia of the First World War**. Daniel, U.; Gatrell, P.; Janz, O.; (Eds.). Trad. (inglês): Christopher Reid. Freie Universität Berlin, 2014. Disponível em: <https://encyclopedia.1914-1918-online.net/article/artillery?version=1.0>. Acesso em: 06 mar. 2024.

THOMPSON, S. C. As we enter the second century of electroacoustics... **Acoustics Today**, 2019, 15(4), 55-63. Disponível em: <https://acousticstoday.org/issues/2019AT/Winter2019/index.html#p=55>. Acesso em: 06 mar. 2024.

TROWBRIDGE, A. (1920). Sound ranging in the American Expeditionary Forces. In: YERKES, R. M. (Ed.). **New World of Science**. New York: The Century Co., 1920. p. 63-88.

VAN DER KLOOT, W. (2005). Lawrence Bragg's role in the development of sound-ranging in World War I. **Notes and Records of the Royal Society of London**, vol. 59(3), Sep. 2005, p. 273-284. Disponível em: <https://www.jstor.org/stable/30041503>. Acesso em: 06 mar. 2024.

Figura 4: ComAnf em Furnas.
Fonte: Acervo MB.

Além do campo de batalha: o papel crucial dos Assuntos Civis na Guerra Russo-Ucraniana

Capitão de Corveta (FN) **Daniel** Gomes e **Silva** de Macedo

É graduado pela Escola Naval e realizou diversos cursos, com destaque para o Curso Especial de Comandos Anfíbios. Entre as principais comissões, foi Comandante de Pelotão e Imediato de Companhia no 1ºBtlInfFuzNav (Batalhão Riachuelo), serviu na Companhia de Ação de Comandos no Batalhão de Operações Especiais de Fuzileiros Navais, foi Imediato do Componente de Combate Terrestre do 26º Contingente Haiti, exerceu o comando da Companhia de Ação de Comandos no Batalhão de Operações Especiais de Fuzileiros Navais, foi Encarregado do Departamento de Pesquisa de Inteligência no CIM-RJ e Oficial de Operações do Comando da Tropa de Desembarque.

Introdução

A análise cultural do conflito entre Rússia e Ucrânia revela nuances profundas e multifacetadas. Compartilhando a mesma origem eslava e um passado histórico entrelaçado desde a Idade Média, a relação entre esses dois países é marcada por complexidades históricas, políticas e econômicas.

Geopoliticamente, a Ucrânia ocupa uma posição estratégica para a Rússia, que frequentemente a considera um "Estado-tampão" que oferece proteção a Moscou. Após a dissolução da União Soviética em dezembro de 1991, a Rússia tem buscado incessantemente manter sua influência sobre a Ucrânia. Geograficamente, a Ucrânia é delimitada pela Rússia a leste, enquanto ao norte faz fronteira com a Polônia e Belarus, e a oeste com a Eslováquia, a Hungria, a Moldávia e a Romênia.

As tensões entre Rússia e Ucrânia se intensificaram significativamente com a anexação da Crimeia pela Rússia em 2014, uma região de importância estratégica tanto para o transporte marítimo quanto para a defesa territorial devido às suas águas quentes. A ação de Moscou gerou ampla condenação internacional, mas a Rússia defendia a anexação como uma reivindicação legítima de um território historicamente russo. Esse evento desencadeou o aumento das tensões, levando a um conflito prolongado que resultou em um grande número de deslocados e refugiados, com efeitos significativos na economia global.

O conflito tornou-se uma luta geopolítica envolvendo as principais potências mundiais: por um lado, membros da OTAN apoiando a Ucrânia com armamentos e logística, e, por outro, a Rússia enfrentando severos embargos econômicos.

A complexidade do conflito é acentuada por narrativas e perspectivas divergentes. Enquanto a Rússia é frequentemente retratada como a agressora que violou a soberania da Ucrânia e desestabilizou a região, alguns argumentam que as ações do Ocidente, especialmente a expansão da OTAN em direção às fronteiras russas, provocaram a Rússia e contribuíram para a escalada do conflito. Essa perspectiva sugere que a representação ocidental da Rússia como única agressora pode ser uma forma de propaganda que obscurece as dinâmicas complexas e o papel das potências ocidentais na origem do conflito.

Essa análise evidencia que o conflito é moldado por uma combinação única de memória histórica, ideologia política e interesses estratégicos, tornando-o uma questão multifacetada e altamente complexa.

O conflito russo-ucraniano teve importantes implicações globais, afetando as relações entre grandes potências e representando riscos para a segurança regional e global. As tensas relações entre Estados Unidos e Rússia, o risco de um conflito europeu mais amplo e o potencial de futura cooperação em questões críticas – como controle de armas, cibersegurança e não proliferação nuclear – são influenciados pelo conflito em curso. Além disso, essa guerra expôs as vulnerabilidades do direito internacional e das instituições, desafiando a capacidade do mundo de gerenciar e resolver conflitos em uma paisagem geopolítica em rápida mudança. À medida que a guerra continua, ela serve como um lembrete contundente do poder duradouro de agravos históricos, dos perigos da competição geopolítica e da necessidade urgente de mecanismos eficazes de resolução de conflitos.

1. Compreendendo o Ambiente Operacional

1.1. Guerra não linear

Empregada pela Rússia na Guerra Russo-Ucraniana, a guerra não linear é uma estratégia multifacetada que ultrapassa ações militares convencionais. Ela inclui táticas políticas, econômicas, informativas e humanitárias visando criar um cenário de conflito amplo e complexo. O objetivo é explorar divisões sociais, gerar confusão e impedir uma resposta eficaz do inimigo, combinando medidas para desestabilizar em diversos níveis.

Essa abordagem vai além do combate direto, uma vez que enfatiza a manipulação de informações, as pressões econômicas e as operações assimétricas para maximizar a incerteza e a desordem. Enfim, o propósito é criar um cenário de guerra confuso e imprevisível, dificultando a capacidade do inimigo de montar uma resposta eficaz e coerente. Essa estratégia busca tirar proveito das vulnerabilidades do adversário, tanto internas quanto externas, e operar em um espectro de conflito que vai além do campo de batalha tradicional.

1.2. "Pequenos homens verdes"

A expressão "pequenos homens verdes" é utilizada para descrever os soldados não identificados que a Rússia empregou na Crimeia e no leste da Ucrânia durante a anexação da Crimeia. Esses soldados, vestidos em uniformes sem insígnias ou distintivos claros, operaram de modo a não serem diretamente associados às forças armadas russas, permitindo à Rússia negar oficialmente seu envolvimento no conflito. Eles tiveram um papel-chave na ocupação de instalações estratégicas e no suporte a movimentos separatistas pró-Rússia, contribuindo significativamente para a desestabilização da região.

Figura 1: "Pequenos homens verdes".

Fonte: EuroDefense-Portugal, 2017.

1.3. Guerra de informação

Durante o conflito russo-ucraniano, a Rússia empregou uma guerra de informação estratégica ao se valer do controle sobre a mídia estatal e as plataformas de comunicação digitais para disseminar desinformação e propaganda. O principal objetivo dessa tática era influenciar a opinião pública, tanto internamente quanto no cenário global.

Por meio de veículos de comunicação controlados pelo Estado, a Rússia promoveu narrativas falsas e deturpadas visando exacerbar tensões, criar divisões e enfraquecer a confiança nas instituições ucranianas. Além disso, procurou desacreditar os esforços da comunidade internacional para resolver o conflito, moldando a percepção pública para atender aos seus interesses geopolíticos.

1.4. Guerra cibernética

A capacidade da Rússia para conduzir ataques cibernéticos foi notavelmente demonstrada durante a Guerra Russo-Ucraniana. Esses ataques focaram em alvos estratégicos dentro da Ucrânia visando infraestruturas críticas como redes de energia, sistemas de comunicação e serviços essenciais. As consequências desses ataques cibernéticos incluíram interrupções significativas e danos extensos, ilustrando o uso eficaz da guerra cibernética como uma ferramenta para alcançar objetivos militares e políticos.

Ataques cibernéticos como esses patrocinados por Estados emergem como armas modernas na guerra e na propaganda. Um dos desafios em lidar com tais ataques é a dificuldade para rastrear sua autoria devido à natureza anônima e sofisticada da tecnologia cibernética. Essa característica torna mais complexo o processo de atribuição de responsabilidade, permitindo que os perpetradores operem com um grau de negação plausível.

1.5. Adaptação e resposta

A resposta da Ucrânia e de seus aliados às táticas não convencionais da Rússia durante o conflito exigiu uma adaptação rápida e estratégica. Para enfrentar a guerra de informação, a Ucrânia fortaleceu suas defesas cibernéticas, desenvolvendo capacidades aprimoradas para analisar e reagir a ataques cibernéticos. Além disso, implementou estratégias eficazes para combater a desinformação, que incluíram aumentar a conscientização do público e promover fontes de informação confiáveis. Esses esforços visaram não apenas proteger a infraestrutura digital do país, mas também preservar a integridade da informação e combater a propaganda.

Simultaneamente, a Ucrânia se empenhou em fortalecer a resiliência social e promover a unidade nacional, elementos fundamentais para resistir às táticas de guerra híbrida empregadas pela Rússia. Essas medidas foram cruciais para manter a coesão social e o moral da população diante das complexas ameaças impostas pelo conflito.

1.6. Abordagem abrangente de segurança

A Guerra Russo-Ucraniana ressaltou a necessidade de uma abordagem abrangente de segurança que transcenda as tradicionais estratégias de defesa militar. Essa perspectiva holística reconhece que a segurança engloba áreas críticas como a Informação e a Cibernética, enfatizando a importância de se proteger contra ameaças híbridas através de uma estratégia multidimensional.

Diante dessa realidade, a Ucrânia e seus aliados concentraram esforços para fortalecer suas capacidades de defesa cibernética. Isso envolveu não apenas a melhoria das infraestruturas tecnológicas, mas também a coordenação aprimorada entre os setores militar e civil. Ao reconhecer que a guerra híbrida pode impactar todos os aspectos da sociedade, essas nações também promoveram a resiliência social.

Estratégias para aumentar a resiliência social incluíram conscientização pública sobre as ameaças, educação abrangente sobre segurança digital e engajamento ativo das comunidades. Essas medidas objetivavam não somente preparar a população para lidar com desafios de segurança, mas também fortalecer a coesão social e a confiança nas instituições, elementos cruciais para a manutenção da estabilidade em tempos de conflito.

1.7. Mudança na natureza da guerra

A Guerra Russo-Ucraniana é um exemplo claro da evolução na natureza dos conflitos modernos. Nesta era, as guerras vão além dos campos de batalha convencionais e envolvem uma variedade de domínios, incluindo Informação, Cibernética e Diplomacia, além de provocarem impactos sociais mais amplos. Essa realidade multifacetada dos conflitos contemporâneos reflete uma complexidade crescente na condução e na resolução de guerras.

A mudança na natureza da guerra reforça a importância de entender as táticas não convencionais utilizadas por atores estatais e não estatais. Isso implica a necessidade de estratégias que não se limitem ao aspecto militar, mas que também abarquem a Segurança da Informação, a Defesa Cibernética, a Diplomacia ativa e a estabilidade social.

Para responder eficazmente a essa nova realidade, é crucial uma abordagem abrangente que integre diferentes setores, tanto militares quanto civis, e que envolva todas as dimensões do conflito. Isso inclui não apenas preparação e resposta a ataques físicos e digitais, mas também gestão da informação, manutenção da coesão social e construção de alianças diplomáticas. Essa perspectiva integrada é essencial para entender plenamente o panorama contemporâneo dos conflitos e para desenvolver respostas eficazes a desafios cada vez mais complexos.

2. Os conceitos de Assuntos Civis e sua relevância no conflito

2.1. Assuntos Civis

Conjunto de atividades conexas à relação do comandante e de outros componentes de uma Organização Militar ou Força com as autoridades civis e a população da área ou território sob responsabilidade ou jurisdição desse comandante. Essas atividades incluem comunicação social, ação comunitária e assuntos governamentais.

2.2. Assuntos Governamentais

Atividade de assuntos civis que, em uma situação de guerra ou agitação interna, prevê que as relações mantidas pelo comandante militar e as forças subordinadas a ele com as autoridades e a população da área submetida à condução de ações por força devem ser regulamentadas no que diz respeito à administração local, considerando as atividades governamentais e econômicas de serviços públicos e especiais.

2.3. Ações preventivas

São ativadas de forma permanente com os objetivos de evitar o uso prematuro da força e de prevenir ou dificultar o surgimento e o agravamento de uma situação de desordem.

Normalmente, abrangem atividades de preparação de tropas, Inteligência, Operações Psicológicas e Comunicação Social.

2.4. Ações não cinéticas

São ativadas dentro da área de operações e não envolvem movimentos (ações de Guerra Eletrônica, Operações Psicológicas, ações de Assuntos Civis, ações no espaço cibernético), mas produzem resultados intangíveis (interferências eletromagnéticas, bloqueios, percepção positiva da população em relação às forças amigas e suas operações) e contribuem para o sucesso da operação.

3. O papel dos Assuntos Civis na guerra moderna

3.1. Ações não cinéticas e seu valor estratégico

No contexto do conflito russo-ucraniano, os Assuntos Civis podem desempenhar um papel crucial na mitigação do impacto sobre os civis e ajudar a restaurar a estabilidade e a segurança.

As ações não cinéticas estão relacionadas ao uso de meios não letais para alcançar objetivos estratégicos, o que pode incluir operações de Informação, Operações Psicológicas, Operações Cibernéticas e outras atividades que não envolvam o uso de força física. As ações não cinéticas têm um valor estratégico significativo em conflitos modernos, pois podem ajudar a moldar percepções e comportamentos de atores-chave e populações sem recorrer à violência.

Ao usar uma combinação de meios cinéticos e não cinéticos, as forças militares podem lidar de forma mais eficaz com desafios complexos e apoiar a paz e a estabilidade em longo prazo.

3.2. Calibrando as forças de Assuntos Civis para letalidade em operações de combate em grande escala

3.2.1. O papel dos Assuntos Civis na letalidade

Os assuntos civis desempenham um papel crucial no aumento da letalidade da força, especialmente no contexto de Operações de Múltiplos Domínios. Os assuntos civis são responsáveis pelo reconhecimento civil e pela análise e o desenvolvimento da rede civil, que são essenciais para combater a guerra híbrida do inimigo.

3.2.2. Guerra híbrida e Assuntos Civis

Adversários de mesma capacidade têm investido pesadamente na guerra híbrida, que combina várias camadas de guerra irregular, econômica, de informações, sócio-política e cibernética. Os Assuntos Civis, com suas capacidades únicas, são posicionados como a arma de escolha da força para combater essas ameaças de guerra híbrida.

3.2.3. Assuntos Civis como plataforma de Inteligência, Vigilância e Reconhecimento (ISR)

Os Assuntos Civis são descritos como a principal capacidade do comandante do componente de combate terrestre para reconhecimento tático do componente civil no campo de batalha. O reconhecimento civil pode fornecer informações significativas sobre os elementos civis de uma rede de ameaça de guerra híbrida.

3.2.4. Análise da rede civil

As futuras forças de Assuntos Civis precisam aprimorar sua capacidade de fornecer aos comandantes a análise da rede civil. Essa análise investiga aspectos da geografia humana para caracterizar tendências, relacionamentos e redes em relação ao tempo e ao espaço.

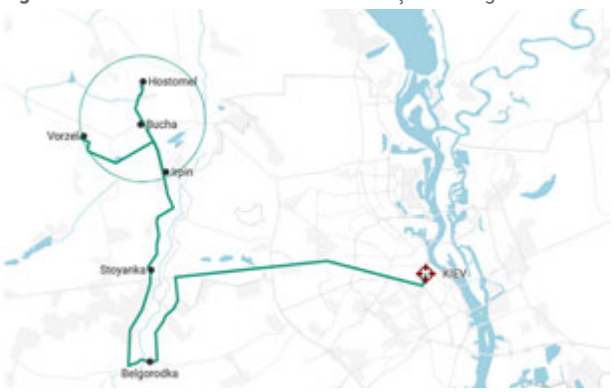
3.2.5. Contraposição às redes de ameaça híbrida inimiga com redes civis

É necessário usar redes para combater redes. O papel único dos Assuntos Civis é desenvolver e conectar parceiros locais. Através do engajamento, as forças de Assuntos Civis podem fortalecer parcerias com a população civil.

4. Os Assuntos Civis na Guerra Russo-Ucraniana e seus impactos

A Guerra Russo-Ucraniana, assim como qualquer conflito armado, tem gerado uma crise humanitária significativa, com um aumento potencial nos números de refugiados e deslocados internos. A criação e a manutenção de corredores humanitários são fundamentais para a evacuação segura da população civil das zonas de conflito. Esses corredores atuam como áreas de trégua temporária e são vitais para proteger os civis durante os confrontos.

Figura 2: Corredor Humanitário – evacuação na região de Kiev.

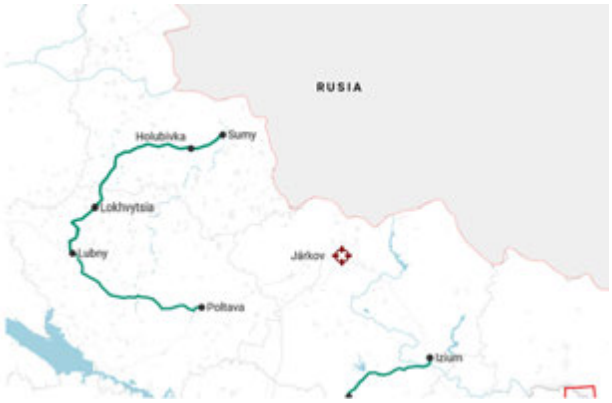


Fonte: RTVE, 2022.

Figura 3: Corredor Humanitário – evacuação na região de Mariupol.

Fonte: RTVE, 2022.

Figura 4: Corredor Humanitário de retorno à Rússia – evacuação de Sumy e Izium.



Fonte: RTVE, 2022.

No entanto, reportagens indicam que nem a Ucrânia e nem a Rússia estavam completamente preparadas para lidar com as exigências de uma operação humanitária em larga escala. Há uma atuação limitada do componente militar de ambos os países no que tange à segurança nos corredores humanitários, bem como uma deficiência nas ações de natureza humanitária.

Um aspecto distintivo dos conflitos modernos, em comparação com as guerras mundiais do século XX, é o cenário de combate. Atualmente, muitos confrontos ocorrem em ambientes urbanizados, elevando a importância da dimensão humana no conflito. Na Guerra Russo-Ucraniana, observa-se a utilização de forças auxiliares, como policiais estaduais e guardas municipais da Ucrânia, que atuam ao lado de agências internacionais.

Quanto aos Centros de Controle de Evacuados (CCE), nota-se um efetivo militar reduzido. Idealmente, esses locais devem ser bem estruturados e organizados para facilitar a redistribuição e o direcionamento adequado dos civis que fogem da guerra.

Um exemplo eficaz de um centro de acolhimento bem gerenciado pode ser encontrado na Operação Acolhida, em Roraima (Brasil), destinada a auxiliar a população venezuelana que escapa das condições desumanas impostas por uma ditadura.

Esse cenário reforça a necessidade de uma abordagem mais abrangente e bem preparada para lidar com as consequências humanitárias dos conflitos contemporâneos e garantir a proteção e o bem-estar dos civis afetados.

5. Desafios e oportunidades para Assuntos Civis na Guerra Russo-Ucraniana

A Rússia anexou os territórios de Donetsk, Luhansk, Zaporizhzhia e Kherson após a realização de um referendo. Entretanto, a Ucrânia afirma que o governo russo coagiu os moradores a votarem. Esse impasse nos indica que essas regiões são locais em potencial para a eclosão de movimentos insurgentes tanto do lado ucraniano quanto do lado russo.

Figura 5: Luhansk, Donetsk, Zaporizhzhia e Kherson – territórios da Ucrânia anexados pela Rússia.

Fonte: Wikipédia, 2022.

Em vista disso, observa-se, nesse momento da guerra, a importância dos Assuntos Civis para os russos. Será que eles realizaram um estudo dos aspectos políticos, econômicos e psicossociais antes de entrarem em guerra? Será que os russos prepararam tropas de Assuntos Civis e especialistas em diversos campos (economistas, engenheiros, administradores, etc.)? Essas respostas serão importantes para a redução de movimentos insurgentes nas regiões anexadas pelo Kremlin.

Conclusão

A partir da análise dos conflitos contemporâneos, como a Guerra Russo-Ucraniana, fica evidente que a guerra moderna requer uma eficaz interoperabilidade envolvendo civis e militares. Essa coordenação é crucial para minimizar os danos colaterais que afetam a população civil durante os conflitos. A colaboração entre os setores civil e militar assegura que as operações de combate e as ações humanitárias sejam conduzidas de maneira integrada e eficiente, abordando tanto as necessidades militares quanto as humanitárias.

Além disso, a realização de exercícios militares focados na evacuação de refugiados e deslocados internos é fundamental. Esses treinamentos preparam as tropas para lidar com situações complexas de evacuação, garantindo a segurança e o bem-estar dos civis afetados. O treinamento deve incluir cenários que simulam condições reais de evacuação, envolvendo a logística necessária para a movimentação segura de grandes grupos de pessoas, bem como a provisão de assistência médica e psicológica.

Por fim, é imperativo que os planejadores militares integrem o planejamento de ações humanitárias em suas estratégias. A negligência em considerar a proteção de civis em conflitos de nova geração pode levar a consequências graves, incluindo o surgimento de movimentos insurgentes e a exacerbação de crises humanitárias. O respeito e a proteção da população civil não são apenas imperativos morais e legais, mas também elementos estratégicos essenciais para a estabilidade em longo prazo de qualquer região afetada por conflitos.

Figura 6: Corredor humanitário.
Fonte: RTVE, 2022.

Figura 7: Corredor humanitário.
Fonte: RTVE, 2022.

Figura 8: Corredor humanitário.
Fonte: RTVE, 2022.

Figura 9: Envio de ajuda humanitária aos desalojados da guerra na Ucrânia em 2022.
Fonte: Fotografia de Teo Cury / CNN Brasil, 2022.

Referências Bibliográficas

AMERICAN SOCIETY OF ASSOCIATION EXECUTIVES (ASAE). **Strategies for Measuring Government Relations Achievements**. By Ann Weber. June 11, 2019. Disponível em: <https://www.asaecenter.org/resources/articles/an_plus/2019/june/strategies-for-measuring-government-relations-achievements/>. Acesso em: 27 jan. 2024.

BIANCHI, Carmine; NASI, Greta; RIVENBARK, William C. Implementing collaborative governance: models, experiences, and challenges. (2021). **Public Management Review**, 23:11, 1581-1589. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/14719037.2021.1878777>. Acesso em: 27 jan. 2024.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (CSIS). **Russia's War in Ukraine: identity, history, and conflict**. Report by Jeffrey Mankoff. April 22, 2022. Disponível em: <https://www.csis.org/analysis/russias-war-ukraine-identity-history-and-conflict>. Acesso em: 27 jan. 2024.

_____. **The civilian impacts of a possible Russian invasion of Ukraine**. by Jacob Kurtzer, Catherine Nzuki, Erol Yayboke and Andrew Lohsen. Feb. 02, 2022. Disponível em: <https://www.csis.org/analysis/civilian-impacts-possible-russian-invasion-ukraine>. Acesso em: 27 jan. 2024.

_____. **The longer-term impact of the Ukraine Conflict and the growing importance of the civil side of war**. By Anthony H. Cordesman. June 06, 2022. Disponível em: <https://www.csis.org/analysis/longer-term-impact-ukraine-conflict-and-growing-importance-civil-side-war>. Acesso em: 27 jan. 2024.

CNN BRASIL. **Brasil envia alimentos e remédios para vítimas da guerra na Ucrânia**. Por Fabiana Lima e Thayana Araújo, 07 mar. 2022. Disponível em: <https://www.cnnbrasil.com.br/internacional/brasil-envia-alimentos-e-remedios-para-vitimas-da-guerra-na-ucrania/>. Acesso em: 28 fev. 2024.

CORPORACIÓN DE RADIO Y TELEVISIÓN ESPAÑOLA (RTVE). **Ucrania evacúa a civiles de varias localidades mientras Mariúpol y Járkov denuncian bombardeos**. 2022. Disponível em: <https://www.rtve.es/noticias/20220309/guerra-ucrania-rusia-corredores-humanitarios-combates/2306061.shtml>. Acesso em: 28 fev. 2024.

COUNCIL ON FOREIGN RELATIONS (CFR). Global Conflict Tracker. **War in Ukraine**. Disponível em: <https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine>. Acesso em: 27 jan. 2024.

EURODEFENSE-PORTUGAL. **A guerra híbrida russa dos "pequenos homens verdes" e o impacto na NATO**. Por Amaral Mota, 15 fev. 2017. Disponível em: <https://eurodefense.pt/a-guerra-hibrida-russa-dos-pequenos-homens-verdes-e-o-impacto-na-nato/>. Acesso em: 28 fev. 2024.

GLOBAL PUBLIC POLICY INSTITUTE (GPPI). **Civil Affairs and Local Conflict Management in Peace Operations**. By Sarah Brockmeier and Philipp Rotmann. Disponível em: <https://www.gppi.net/media/Brockmeier__Rotmann__2016__Civil_Affairs_and_Conflict_Management_in_Peace_Operations.pdf>. Acesso em: 27 jan. 2024.

ROYAL UNITED SERVICES INSTITUTE FOR DEFENCE AND SECURITY STUDIES (RUSI). **Preliminary Lessons from Russia's unconventional operations during the Russo-Ukrainian War**, February 2022–February 2023. Authors: Jack Watling; Oleksandr V. Danylyuk; Nick Reynolds. Special Report – March 29, 2023. Disponível em: <https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf>. Acesso em: 27 jan. 2024.

THE RED TEAM ANALYSIS SOCIETY. **Ukraine Crisis package: understand the roots of the crisis**. By Helene Lavoix. Disponível em: <https://redanalysis.org/product/ukraine-crisis-package-understand-the-roots-of-the-crisis-2/>. Acesso em: 27 jan. 2024.

UNITED NATIONS MISSION IN SOUTH SUDAN (UNMISS). **Civil Affairs**. Disponível em: <https://unmiss.unmissions.org/civil-affairs>. Acesso em: 27 jan. 2024.

UNITED NATIONS PEACEKEEPING. **Civil Affairs**. Disponível em: <https://peacekeeping.un.org/en/civil-affairs>. Acesso em: 27 jan. 2024.

UNITED STATES ARMY MANEUVER CENTER OF EXCELLENCE. Joint Chiefs of Staff. **Joint Publication 3-57: Civil-Military Operations**. Sep. 11, 2013. Disponível em: <https://www.moore.army.mil/infantry/doctrinesupplement/atp3-21.8/PDFs/jp3_57.pdf>. Acesso em: 27 jan. 2024.

UNITED STATES ARMY RESEARCH LABORATORY. **Understanding Civil Affairs Operations: a qualitative exploration of self-reported Civil Affairs operational experiences**. Authors: David R. Scribner, et al. Sep. 2018. Disponível em: <https://apps.dtic.mil/sti/pdfs/AD1061341.pdf>. Acesso em: 27 jan. 2024.

WIKIPÉDIA. **Referendos sobre a adesão à Rússia dos territórios ocupados da Ucrânia (2022)**. Última atualização em 16 mar. 2023. Disponível em: <https://pt.wikipedia.org/wiki/Referendos_sobre_a_adesão_à_Rússia_dos_territórios_ocupados_da_Ucrânia_%282022%29>. Acesso em: 28 fev. 2024.

ZAALBERG, T. W. B. Substituting the Civil Power: Civil Affairs and Military Government in World War II. (2006). In: **Soldiers and Civil Power: Supporting or Substituting Civil Authorities in Modern Peace Operations** (p. 25-44). Amsterdam University Press. Disponível em: <https://www.jstor.org/stable/j.ctt46mxbz.5>. Acesso em: 27 jan. 2024.

Ameaças Híbridas x Ameaças Comuns: por que é importante saber diferenciar

17

Capitão de Mar e Guerra (FN) **Luiggi** Campany de Oliveira

Atualmente, é Adido Naval na Colômbia. Durante sua carreira, foi Ajudante de Operações na *Fuerza de Infantería de Marina de la Flota del Mar*, na Argentina; Comandante da Companhia de Polícia do Batalhão Naval, onde foi responsável pela segurança dos deslocamentos durante os Jogos Mundiais Militares Rio 2011; Oficial de Ligação no *US Southern Command*; Comandante da Base de Fuzileiros Navais da Ilha do Governador, onde obteve, pela primeira vez, o Selo de Qualidade nas Melhores Práticas de Gestão do Instituto de Pesquisas da Marinha (IPQRio); e Imediato do Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais.

Introdução

Em 23 de março de 2021, o grande navio mercante porta-contêineres *Ever Given* ocupou as principais manchetes dos jornais mundiais ao colidir com uma das margens e ficar atravessado no Canal de Suez. Esse episódio interrompeu o fluxo de navios mercantes entre os mares Mediterrâneo e Vermelho por seis dias, resultando em um prejuízo de centenas de milhões de dólares. Com o canal obstruído, cerca de quatrocentos navios foram afetados, tendo que adotar tempos de espera não planejados, o que gerou um efeito cascata em toda a cadeia de suprimentos.

Os estudiosos de guerras híbridas já haviam vislumbrado cenários tanto de fechamento quanto de obstrução de um canal de um importante porto, uma vez que se trata de uma ação típica de exploração de vulnerabilidades de uma infraestrutura crítica, cujos prejuízos são potencializados pelo efeito multiplicador da interrupção dessa infraestrutura. Mas será que esse acidente do *Ever Given*, operado pela empresa taiwanesa *Evergreen*, pode ser considerado um exemplo de ameaça híbrida?

Este breve artigo procura responder a essa pergunta apresentando alguns elementos que diferenciam as ameaças híbridas das ameaças comuns, segundo a definição utilizada pelo Centro de Excelência em Guerra Híbrida (*Hybrid CoE*) da União Europeia. Essa diferenciação é muito relevante, pois é necessário se contrapor a cada tipo de ameaça adequadamente. Ainda que difíceis de detectar, as ameaças híbridas são combatidas de forma diferente de crimes comuns ou acidentes.

1. O caso *Ever Given*

Analisando o ocorrido no Canal de Suez, de acordo com a avaliação de um experiente oficial da marinha alemã publicada em um artigo da revista *Marine-Pilots.com* (2021), antes de o *Ever Given* finalmente bloquear o Canal de Suez, uma sequência de decisões equivocadas teria sido tomada pelo seu Comandante e pelo Prático que nele estava embarcado.

Tudo começou com uma forte ventania que atingiu o navio de través. Nesse momento, eles confiaram apenas nos instrumentos de bordo e deixaram de compensar essa influência – um vetor lateral ao movimento – no rumo. Tal erro levou o navio a se aproximar de uma das margens do Canal. Naquele momento, o Comandante teria dado ordem para aumentar a velocidade para 13 nós, que é muito acima da permitida para o Canal (oito nós). Assim, os efeitos hidrodinâmicos presentes nesse ambiente de navegação em águas restritas, somados à inércia do navio, levaram ao forte impacto em uma das margens, seguido do bloqueio do canal egípcio (MARINE-PILOTS, 2021).

Figura 1: Navio *Ever Given* encalhado no Canal de Suez.

Fonte: Daily Motion, 2021.

A descrição do ocorrido e as condições do acidente contribuem para o entendimento de que tudo foi resultado de falhas humanas e, aparentemente, não havia, por parte do Comandante ou do Prático, a intenção de obstruir o Canal de Suez.

2. O incidente no Estreito de Kerch

Outro incidente recente envolvendo o bloqueio de um canal foi o ocorrido em novembro de 2018, quando um navio mercante russo fechou o Estreito de Kerch, que une o Mar de Azov ao Mar Negro. Essa ocorrência impediu o acesso de navios ucranianos aos seus portos localizados naquele mar. Na ocasião, helicópteros militares russos sobrevoavam o Estreito como forma de intimidação.

Esse episódio foi precedido por um incidente no qual navios da guarda costeira russa tentaram impedir navios ucranianos de contornarem a Península da Crimeia em direção aos portos no Mar de Azov. Em seguida, houve acusações mútuas e uma forte propaganda (REUTERS, 2018).

Figura 2: Trajeto das embarcações da Ucrânia atacadas por navios da Rússia.

Fonte: G1, 2018. Foto: Fernanda Garrafiel/G1.

3. Características da ameaça híbrida

Comparando os dois casos, percebe-se que o efeito foi o mesmo: o bloqueio de um canal, cortando uma linha de comunicação marítima. Mas é possível inferir que há uma importante diferença: as intenções por trás do ocorrido. No caso do *Ever Given*, ao que tudo indica, tratou-se de um acidente. No Estreito de Kerch, pelo contrário, houve a intenção de bloquear o acesso ao Mar de Azov a fim de contribuir para ampliar a influência russa na região, a qual, posteriormente, viria a ser anexada com a invasão de 2022 na região de Dombas.

Outra diferença entre os dois exemplos é que, no Canal de Suez, identifica-se apenas um acidente isolado. Já no Estreito de Kerch, observa-se uma combinação de diversas ações hostis, como a ameaça militar com o uso de helicópteros militares sobrevoando o local e a campanha informacional perpetrada pela Rússia, além do posicionamento de um navio mercante fechando o Estreito.

Os elementos citados encontram-se presentes na definição utilizada pelo *European Centre of Excellence for Countering Hybrid Threats* (*Hybrid CoE* – Centro Europeu de Excelência para o Combate a Ameaças Híbridas), qual seja: "ameaças híbridas são ações desencadeadas por um ator, seja ele estatal ou não, cujo objetivo é causar um dano ou degradar um alvo, influenciando o processo decisório local, regional, institucional ou estatal."

Diferentemente de uma ação militar direta, que tem um custo político e nem sempre possui legitimidade, uma ameaça híbrida se vale de agentes *proxy* (ou intermediários), tornando mais difícil a identificação do real ator e de suas intenções. Além disso, ameaças híbridas exploram a vulnerabilidade dos alvos, tornando os resultados não lineares e com um custo-benefício bastante aceitável.

É digno de nota que, atualmente, diversos atores não estatais acumularam poder suficiente para ameaçar estados. Conforme destaca Moisés Naím, estamos testemunhando uma mudança radical na dinâmica do poder com o aparecimento de micropoderes em vários setores. Não se trata apenas do *poder bélico* (uso da força): há, também, o *poder informacional* (mensagem), como as grandes redes sociais e as redes de notícias; o *poder econômico* (recompensa), como, por exemplo, as enormes somas movimentadas pelos cartéis do narcotráfico; e até o *poder do código*, como o das religiões (NAÍM, 2013).

Figura 3: Ameaças Híbridas.

Fonte: Hybrid CoE.

Assim, as ameaças híbridas buscam explorar vulnerabilidades políticas, sociais, econômicas, tecnológicas e de infraestruturas críticas. Por isso, é importante mapear tais vulnerabilidades a fim de tornar o sistema considerado mais resiliente a ataques e capaz de identificar a ocorrência das ameaças híbridas, diferenciando-as das ameaças comuns com o propósito de mapear eventuais atores e suas intenções e possibilitando uma resposta

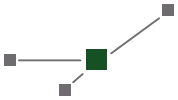
adequada por parte do Estado (CULLEN; REICHBORN-K-JENNERUD, 2021; CAMPANY, 2021).

As estratégias de defesa contra essas ameaças envolvem, além da sua detecção, a dissuasão e uma resposta apropriada por parte do estado a fim de demover o agressor da intenção de realizar novos ataques ou lhe infringir um alto custo, fazendo-o mudar (MCDC, 2021).

Conclusão

A discussão desses aspectos requer um artigo à parte, uma vez que o assunto extrapola o escopo deste trabalho. Apesar disso, é importante ressaltar que a defesa contra ameaças híbridas demanda a integração de várias capacidades estatais para a identificação dos prováveis agressores e a adoção de medidas pertinentes. Além de identificar e punir o agressor, é necessário mapear o eventual patrocinador dos ataques. Como sugerido por Campany (2021), para isso, é importante relacionar os potenciais atores entre aqueles que são beneficiados pelos ataques e apontar quais foram os seus ganhos com os desdobramentos das ações.

Por isso, tratar uma ameaça híbrida como um crime comum pode ser uma resposta insuficiente que poderá, ainda, ensejar ao ator híbrido a possibilidade de perpetrar as hostilidades em outras modalidades até alcançar seus objetivos.



Referências Bibliográficas

CAMPANY, Luiggi. **Ameaças Híbridas e a Segurança Marítima do Século XXI**. Rio de Janeiro, EGN: 2021.

CULLEN, Patrick J.; REICHBORN-KJENNERUD, Erik. Understanding Hybrid Warfare. In: Norwegian Institute of International Affairs. **MCDC Countering Hybrid Warfare Project**. Oslo, 2017. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf>. Acesso em: 03 mar. 2021.

DAILY MOTION. **Navio bloqueia durante horas o Canal de Suez**. Vídeo, 24 de março de 2021. Disponível em: <https://www.dailymotion.com/video/x805t0z>. Acesso em: 23 fev. 2024.

G1. **Rússia teme escalada na tensão na região da Crimeia após Ucrânia aprovar lei marcial**. 27 de novembro de 2018. Disponível em: <https://g1.globo.com/mundo/noticia/2018/11/27/russia-teme-escalada-na-tensao-na-regiao-da-crimeia-apos-ucrania-aprovar-lei-marcial.ghtml>. Acesso em: 23 fev. 2024.

HYBRID COE. **Hybrid threats as a concept**. Disponível em: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>. Acesso em: 03 mar. 2021.

MARINE-PILOTS.COM. **More details and an analysis of the Ever Given accident**. October 2021. Disponível em: <https://www.marine-pilots.com/articles/315948-more-details-and-analysis-of-ever-given-accident>. Acesso em: 03 mar. 2021.

MULTINATIONAL CAPABILITY DEVELOPMENT CAMPAIGN (MCDC). Countering Hybrid Warfare (CHW) Project. **Countering Hybrid Warfare**. Oslo: Norwegian Institute of International Affairs, 2019. Disponível em: <https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding- hybrid-warfare>. Acesso em: 21 fev. 2021.

NAÍM, Moisés. **O Fim do Poder**: nas salas da diretoria ou nos campos de batalha, em Igrejas ou Estados, por que estar no poder não é mais o que costumava ser? Tradução Luis Reyes Gil. São Paulo: LeYa, 2013.

REUTERS. Europe News. **Russia blocks Ukrainian navy from entering Sea of Azov:** Russian State TV, Nov. 25, 2018. Disponível em: <https://www.reuters.com/article/us-ukraine-crisis-russia-kerch-idUSKCN1NU0LA>. Acesso em: 03 mar. 2021.

TERRA NOVA LOGÍSTICA. Blog. **Canal de Suez: impactos mundiais**. Por Marcia Hashimoto, 15 de julho de 2021. Disponível em: <https://terranovalogistica.com.br/blog/canal-de-suez-impactos-mundiais/>. Acesso em: 23 fev. 2024.

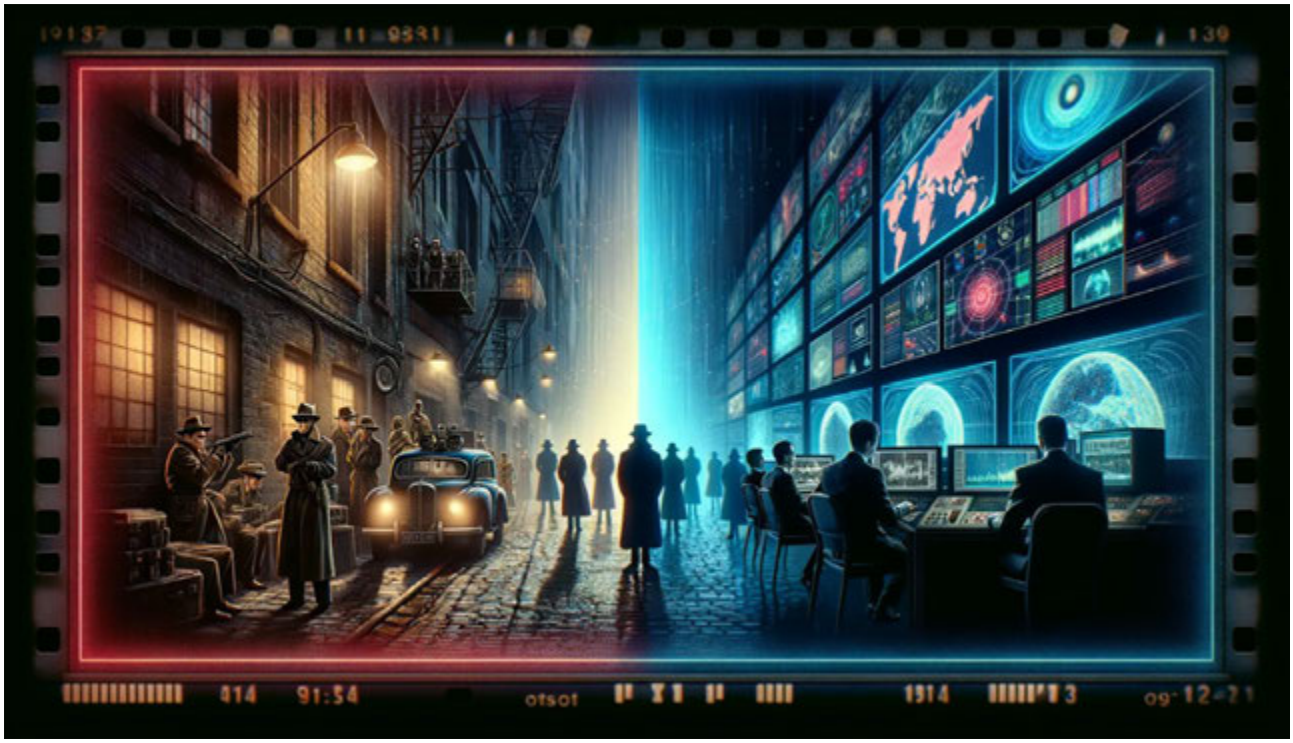
Atividade de Inteligência em transformação: desafios, mudanças tecnológicas e necessidade de adaptação às novas realidades

18

Terceiro-Sargento (AD) **Tamyris Salgueiro** Santana Almeida

Ingressou na MB em 2013 por meio do Curso de Formação do Corpo Auxiliar de Praças, realizado no Centro de Instrução Almirante Alexandrino no Rio de Janeiro. Entre os diversos cursos realizados, destacam-se: o Curso Especial de Pesquisa de Inteligência, o Curso Especial Avançado de Inteligência para Praças e o Curso Especial de Inteligência para Praças.

Figura 1: A evolução dos serviços de Inteligência.



Fonte: A autora.

Introdução

Este artigo explora a evolução dos serviços de Inteligência no século XXI – um período já marcado por provocações inéditas e sucessivas transformações tecnológicas –, analisando como essas mudanças afetam a eficiência, a eficácia e as práticas éticas da atividade. Aborda, ainda, o impacto da digitalização, discutindo tanto os riscos quanto as oportunidades que ela apresenta.

No decurso deste estudo, é possível perceber uma complexidade crescente no campo da Inteligência a exigir uma gestão de recursos mais profissionalizada, que considere variáveis cada vez mais amplas, desde a gestão de recursos humanos até a aceitação de riscos tecnológicos para ações de busca de dado negado. O uso futuro da Inteligência Artificial (IA) poderá servir como um propulsor para a atividade, enquanto a

transparência, crucial para a relação com a sociedade, apresenta-se como um impasse, dado que a ação de analistas e agentes deve ser inerentemente discreta, silenciosa e anônima.

Assim, são levantadas questões sobre o impacto das novas tecnologias: a necessidade de adaptação estratégica e operacional dos serviços de Inteligência em resposta a essas novas realidades é o foco central deste estudo.

Figura 2: A evolução dos serviços de Inteligência.

Fonte: A autora.

1. Desafios atuais

O cenário da atividade de inteligência sempre esteve em um estado de fluxo contínuo, enfrentando desafios crescentes tanto em complexidade e escopo, quanto em amplitude. A habilidade de se adaptar a tais complexidades é essencial para o sucesso.

No entanto, no contexto atual, a multiplicidade de ameaças, que vão desde o ciberespaço, passando pelo crime organizado infiltrado em instâncias do Estado, o ativismo radical social e até questões geopolíticas, exige uma abordagem mais detalhada para identificar e mitigar riscos, além de uma análise abrangente das hostilidades emergentes e já existentes. Dessa forma, torna-se crucial direcionar recursos para áreas consideradas prioritárias para a Segurança Nacional.

Historicamente, os serviços de Inteligência dependiam de profissionais altamente especializados em riscos, geografia, estratégias nacionais e relações internacionais. Embora essa especialização tenha sido efetiva, a variedade de riscos atuais e o advento de novas tecnologias demandam uma reavaliação.

No século XXI, os serviços de Inteligência enfrentam obstáculos significativos devido às mudanças no contexto global e ao avanço da digitalização. A evolução da atividade está condicionada à sua capacidade de responder às transformações no ambiente estratégico, particularmente na transição para uma sociedade interconectada e digital, o que implica uma necessidade de adaptação e antecipação proativa para manter a eficácia. A crescente proliferação de riscos introduz novas exigências, como um foco maior na análise e na prevenção de que na reação. Além disso, a conectividade global facilita a disseminação de perigos para setores anteriormente mais isolados e protegidos, desafiando os profissionais de segurança a se concentrarem tanto na segurança física quanto na informacional. Acelera, ainda, a propagação de ameaças, encurta os tempos de resposta e alerta e intensifica os riscos sistêmicos. Portanto, a atividade de Inteligência precisa se adaptar e evoluir para enfrentar de maneira efetiva essa nova realidade.

2. A transformação tecnológica e a Inteligência

Avanços disruptivos em IA, aprendizado de máquina, computação quântica, análise de *big data* e *internet* das coisas estão redefinindo o panorama da Inteligência moderna, oferecendo mais meios para aprimorar a coleta e a análise de dados.

Essas tecnologias não apenas facilitam percepções mais profundas e rápidas, mas também suscitam questões críticas acerca da confiabilidade dos dados e exigem um novo conjunto de habilidades especializadas. A integração eficaz dessas inovações exigirá uma adaptação contínua de práticas e estratégias para manter os serviços de Inteligência um passo à frente das ameaças, que evoluem rapidamente. O que antes se ocultava sob camadas de criptografia avançada agora se aproxima de uma era de acessibilidade sem precedentes, transformando radicalmente a dinâmica da segurança e da tomada de decisões.

Por outro lado, a enorme quantidade de dados gerados diariamente torna mais difícil distinguir informações úteis de ruídos irrelevantes. Além disso, a dependência crescente de sistemas digitais aumenta a vulnerabilidade a ataques cibernéticos, que podem comprometer informações sensíveis ou interromper operações críticas.

Outra preocupação é com a ética e a privacidade na era digital. À medida que a capacidade de vigilância dos serviços de Inteligência se expande, cresce também a necessidade de equilibrar segurança e privacidade, exigindo políticas e regulamentações claras para evitar abusos de administrações eventuais e lideranças circunstanciais sem apreço pelas liberdades individuais.

Figura 3: As novas tecnologias ampliam a capacidade de coleta e análise de dados.

Fonte: A autora.

Essa transformação tecnológica requer que os serviços de Inteligência não apenas atualizem suas ferramentas e métodos, mas também reformulem suas estratégias e políticas para se adaptarem a um ambiente em constante mudança. Isso inclui investir em formação e treinamento para desenvolver as habilidades necessárias para lidar com as novas tecnologias, além de estabelecer colaborações com o setor privado e outras organizações com a finalidade de acessar inovações tecnológicas e compartilhar informações de modo eficaz.

Caberá aos serviços desenvolverem novos métodos para integrar diferentes ambientes de trabalho (como redes, operações conjuntas e combinadas), compatibilizar tecnologias díspares e agregar novas. Também deverão estar atentos a novos instrumentos de análise, criando e adaptando novos procedimentos internos e construindo novas curvas de aprendizado a fim de entender toda uma nova combinação de fontes de dados. Nesse caso, deve-se dar especial atenção à enorme gama de conhecimentos que poderão ser construídos exclusivamente a partir de fontes abertas, particularmente as redes sociais.

Em resumo, a transformação tecnológica representa uma dupla face para os serviços de Inteligência, oferecendo melhorias significativas em capacidades enquanto traz novas provocações em termos de segurança cibernética, ética e gestão de informações. A adaptação a essas mudanças será crucial para garantir que os serviços de Inteligência continuem a desempenhar seu papel vital na proteção da Segurança Nacional.

3. Adaptação às novas realidades: exemplos em curso

Em resposta ao dinamismo da evolução tecnológica e às transformações globais, agências de Inteligência, exemplificadas pela CIA nos Estados Unidos e pelo MI5 no Reino Unido, estão em um processo de reinvenção mediante o desenvolvimento de IA, análise de *big data* e emprego de *drones*.

A iniciativa da *Open Source Center* (OSC) da CIA[1] ilustra a ênfase em coleta e análise de informações oriundas de fontes abertas, tais como mídias sociais e *websites*, visando à identificação e ao monitoramento de atividades extremistas e outras ameaças potenciais. Tal estratégia almeja expandir suas capacidades por meio da análise de dados abertos para o reconhecimento de padrões.

O MI5, por sua vez, concentra esforços na análise de redes sociais como estratégia para combater o extremismo. O *Joint Terrorism Analysis Centre* (JTAC) reúne informações de diversas agências e oferece uma análise abrangente da ameaça terrorista. A responsabilidade do JTAC pela avaliação do nível e da natureza

[1] Inteligência de código aberto (*Open Source Intelligence* – OSINT) é a coleta e a análise de dados de fontes abertas para produzir conhecimento. A OSINT distingue-se da pesquisa na medida em que aplica o processo de Inteligência para criar conhecimento personalizado que apoie uma decisão específica de um indivíduo ou instituição. Disponível em: <https://irp.fas.org/dni/osc/index.html>. Acesso em: 12 mar. 2024.

da ameaça do terrorismo internacional foi descrita no CONTEST, estratégia do Reino Unido para combater o terrorismo publicada pelo governo britânico em julho de 2011 que visa prevenir o extremismo e a radicalização por meio da integração de medidas de segurança e políticas sociais.

Ambas as iniciativas representam exemplos atuais de engajamento nessa área e delineiam uma tentativa contínua e fundamental de enfrentar ameaças em um contexto internacional cada vez mais complexo, sublinhando a importância crescente da colaboração interagências e da inovação.

4. Evolução estratégica e operacional

A evolução estratégica e operacional nos serviços de Inteligência, que envolve a adoção de novas abordagens alinhadas com as mudanças tecnológicas e contextuais atuais, é fundamental no século XXI. Esse imperativo é impulsionado pela rápida evolução das ameaças, que exigem respostas mais ágeis e adaptativas.

E o campo interno parece evoluir notavelmente com a crescente necessidade de monitorar potenciais agressores e focar em fontes de fratura e radicalização interna, como desigualdade, marginalização, imigração e urbanização, que afetam a coesão social e a identidade nacional. O descontentamento, o ativismo radical e o ressentimento desafiam os sistemas de controle social e facilitam a desestabilização de sociedades antes consideradas seguras e democráticas. Nesse mister, avultará em importância o estudo do campo informacional para acompanhar o conhecimento variável de atores, estados de opinião, tendências e cenários, tanto de agressores potenciais quanto de usuários e beneficiários. Além disso, a exposição a desinformação, operações de influência e manipulação da mídia tradicional e nas redes sociais exige monitoramento constante.

As novas abordagens na Inteligência incluem o uso de análise de dados avançada, IA e técnicas de aprendizado de máquina para prever e prevenir ameaças. A integração de fontes de dados diversificadas e a colaboração entre diferentes agências e organizações internacionais também se tornam essenciais.

A inovação não se limita apenas à tecnologia, mas também envolve a atualização de doutrina de emprego, políticas e normas internas, estratégias e procedimentos operacionais, assim como a exigência de novos perfis profissionais com formação em tecnologias emergentes. A capacidade de se adaptar rapidamente a novos contextos será crucial e requer uma cultura organizacional que valorize a flexibilidade, a aprendizagem contínua e a colaboração interdisciplinar. Um analista que atualmente não conta com o suporte de Grandes Modelos de Linguagem (*Large Language Models* – LLM) na sua vasta gama de ferramentas já se encontra em descompasso com as exigências contemporâneas.

Essa transformação profunda é vital para que a atividade de Inteligência mantenha sua efetividade em um mundo em constante mudança, no qual novas ameaças e oportunidades surgem continuamente. A inovação e a adaptação são, portanto, não apenas desejáveis, mas necessárias para a sobrevivência e o sucesso desses serviços. Portanto, a escolha entre abordagens proativas e reativas não apenas moldará nossa capacidade de adequação, mas também determinará nossa proficiência em antecipar e neutralizar perigos futuros, assegurando, assim, a continuidade e a eficácia da atividade diante das incessantes mudanças.

5. Dilemas de eficiência e eficácia na Inteligência moderna

A eficiência e a eficácia são vitais para a inteligência moderna, desafiadas tanto por novos cenários quanto pelo impacto das tecnologias emergentes. A otimização da coleta e da análise de dados em grande escala, viabilizada por avanços tecnológicos, é fundamental para a tomada de decisões fundamentadas e rápidas.

No entanto, essa eficiência é desafiada pela complexidade e pelo volume crescente de dados coletados. A eficácia, por sua vez, depende da habilidade de interpretar corretamente esses conhecimentos e aplicá-los de maneira efetiva.

Em um panorama no qual a eficiência e a eficácia delineiam o cerne da Inteligência moderna, a interseção entre tecnologia avançada e habilidade analítica emerge como um campo fértil para inovações. À medida que nos debruçamos sobre as complexidades e o volume expansivo de dados, torna-se cada vez mais premente a necessidade de refinar nossas capacidades interpretativas. Esse desafio abre portas para a próxima fronteira da atividade: a IA.

6. Inteligência Artificial

A IA se tornará um elemento central nos serviços de Inteligência, revolucionando tanto a coleta quanto a análise de dados. A IA permite a automação de tarefas repetitivas, liberando recursos humanos para tarefas mais complexas e estratégicas. Ela oferece a capacidade de processar e analisar grandes volumes de dados com velocidade e precisão superiores, o que é essencial no cenário atual, em que o volume de informações é vasto e, muitas vezes, esmagador.

A aplicação de IA no cenário de Inteligência não se limita à análise de dados; ela também se estende ao campo da previsão e da identificação de padrões, o que é crucial para antecipar ameaças e oportunidades. Algoritmos de aprendizado de máquina, por exemplo, podem ser treinados para identificar sinais de atividades suspeitas ou mudanças de padrões em comunicações, movimentos financeiros ou comportamentos de grupos.

Entretanto, a integração da IA traz complicações próprias, incluindo questões sobre confiabilidade e interpretação dos dados gerados pela IA, assim como preocupações éticas relacionadas ao uso de sistemas automatizados em decisões críticas. A necessidade de supervisão humana e de entendimento dos algoritmos utilizados é vital para garantir que as decisões baseadas em IA sejam acuradas, pois há uma tendência de o ser humano se acomodar e transferir sua responsabilidade para a máquina, assumindo como inquestionável o seu resultado.

A IA, por ser um instrumento de uso civil, permite que outros produtores e usuários busquem nichos de excelência e criem conhecimentos especializados. Em vez de competir com esses produtores, os serviços deveriam criar formas de incorporar seu trabalho como fontes fidedignas.

Por exemplo: um dos estudos mais sofisticados em Inteligência – a Estimativa – pode tirar proveito dos modelos de aprendizado automático já existentes, como ChatGPT, Claude.AI ou Gemini. Essas plataformas são capazes de simular especialistas em variados campos do saber, ou até mesmo indivíduos específicos, mediante a inserção de seus escritos, estudos e análises.

Contudo, a adoção de IA envolve desafios específicos, tais como dúvidas sobre a confiabilidade e a interpretação dos dados gerados por esses sistemas, além de dilemas éticos acerca da utilização de tecnologias automatizadas em decisões fundamentais. A presença de supervisão e compreensão humanas sobre os algoritmos é essencial para assegurar a precisão das decisões orientadas por IA, evitando a complacência humana de delegar indiscriminadamente responsabilidades à máquina e aceitar seus resultados sem questionamentos.

Em resumo, a IA está remodelando o campo da Inteligência, oferecendo possibilidades inovadoras para melhorar a coleta e a análise de informações ao mesmo tempo em que apresenta novos dilemas éticos e operacionais que precisam ser cuidadosamente gerenciados.

7. Propostas inovadoras: fazendo a informação fluir

A adaptação às novas tecnologias e a incessante busca por soluções inovadoras emergem como pilares para a manutenção da eficácia dos serviços e das agências de Inteligência no contexto do século XXI. As propostas subsequentemente delineadas visam contribuir para o fomento do debate por um aparato de Inteligência atualizado, eficaz e apto a confrontar as imposições do mundo contemporâneo.

Primeiramente, sugere-se a criação de uma plataforma digital segura destinada à facilitação do intercâmbio de informações e Inteligência entre agências de distintas instituições nacionais. Tal plataforma funcionaria como um vetor essencial para a colaboração interagências, a partilha de dados e a coordenação de esforços conjuntos no combate a ameaças internas, tais como o terrorismo, o ativismo radical, o tráfico de entorpecentes e a cibercriminalidade. E ainda, como efeito colateral, contribuiria para mitigar a desconfiança e o preconceito que hoje contamina as relações institucionais.

Inegavelmente, essa iniciativa resultaria na geração de um volumoso acervo de dados, o que conduz à segunda proposição: a instituição, sob os auspícios do Sistema Brasileiro de Inteligência (SISBIN), de um sistema compartilhado de análise de *big data* com total capilaridade, que seria um mecanismo autóctone baseado em inteligência artificial capacitado para o escrutínio de vastas quantidades de dados oriundos de múltiplas fontes e agências especializadas. O sistema teria o intuito de identificar padrões e detectar atividades suspeitas nos campos interno e externo, abrangendo células ativistas, grupos terroristas e redes de crime organizado, como, por exemplo, o narcotráfico. Essa nova conjuntura demandaria, por sua vez, a disponibilidade de recursos humanos altamente especializados. Dessa forma, propõe-se a implementação de um programa de treinamento interdisciplinar: um esquema abrangente que integre conhecimentos e experiências de diversas instituições com o objetivo de formar profissionais de Inteligência dotados de competências multidisciplinares e capazes de atuar de maneira sinérgica e conjunta.

Essas medidas, se implementadas, provavelmente tendem a elevar significativamente a capacidade de resposta das agências de Inteligência diante das complexidades emergentes no panorama atual.

8. Transparência e ética

Transparência e ética nos serviços de Inteligência são características cada vez mais enfatizadas na era moderna. O dilema central é equilibrar a necessidade de segurança com a demanda por transparência e o respeito à privacidade. Com a crescente capacidade de vigilância proporcionada pela tecnologia, surgem preocupações éticas significativas, principalmente em relação à coleta e ao uso de informações dos cidadãos. Os serviços

de Inteligência devem operar dentro de um quadro legal e ético claro, garantindo que suas ações sejam justificáveis e proporcionais às ameaças enfrentadas.

A eficácia dos serviços de Inteligência muitas vezes depende da discrição e do segredo, mas a sociedade moderna exige maior transparência e responsabilidade, o que requer a criação de mecanismos de supervisão e fiscalização robustos para equilibrar a necessidade de segredo com a responsabilidade pública. As agências de Inteligência devem, portanto, encontrar maneiras de manter a confiança pública sendo, na medida do possível, transparentes em suas operações sem comprometer suas capacidades operacionais.

Uma das formas de realizar isso é diminuir o grau de sigilo hoje existente. Por que uma apreciação, que toma por base exclusivamente fontes abertas, deve ser reservada? O mesmo questionamento deve ser feito quando um informe, que, em algumas situações, é *ipsis litteris* um artigo de jornal, também recebe o mesmo tratamento e caráter sigiloso. Será que os centros já não necessitariam ter estudos de caráter ostensivo?

No contexto atual de expansão da vigilância digital, torna-se crucial estabelecer políticas robustas de proteção de dados para preservar a privacidade individual. A transparência no processo de coleta, uso e proteção de dados é fundamental para sustentar a confiança pública e prevenir violações. É imperativo evitar a emergência de uma realidade *orwelliana*, na qual figuras de autoridade possam empregar dados pessoais para consolidar projetos de poder específicos. Assim, os serviços de Inteligência enfrentam o desafio de balancear meticulosamente a segurança com a ética e a privacidade, uma tarefa preponderante no cenário do século XXI.

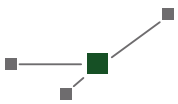
Conclusão

No século XXI, marcado por transformações tecnológicas incessantes e desafios sem precedentes, os serviços de Inteligência encontram-se navegando em águas encapeladas da era informacional, que exige uma abordagem mais sofisticada e integrada, impulsionando a busca por soluções inovadoras e reinvenção estratégica, além da abertura para novas ferramentas e metodologias.

O ambiente em rápida mudança exige uma transformação estrutural que pode envolver mudanças organizacionais, implementação de novas tecnologias para otimização da coleta e da análise de dados, revisão da doutrina e dos métodos operacionais, bem como a interconexão entre diferentes agências. Tal transformação é vital para manter a relevância em um mundo cada vez mais complexo e incerto.

Tanto a eficiência e a eficácia na reorganização de recursos (gestão, talento, inovação, cooperação, integração), quanto a transparência e a ética surgem como pilares fundamentais nesta nova era. Com o avanço das tecnologias como a IA, os serviços de inteligência enfrentam oportunidades e obstáculos inéditos.

Olhando para o futuro, o campo da Inteligência está em um momento decisivo, requerendo inovações e adaptações organizacionais para enfrentar os desafios do século XXI, mantendo o equilíbrio entre segurança, privacidade e molduras éticas a fim de mitigar dilemas operacionais.



Referências Bibliográficas

HOME OFFICE IN THE MEDIA. Blog. **CONTEST 2023 Factsheet**. By Home Office news team, 18 July 2023. Disponível em: <https://homeofficemedia.blog.gov.uk/2023/07/18/contest-2023-factsheet/>. Acesso em: 12 mar. 2024.

SCIENCES ET AVENIR. **La CIA en open source: 13 millions de pages accessibles au public sur le web**. Loïc Chauveau, 24 jan. 2017. Disponível em: <https://www.sciencesetavenir.fr/high-tech/informatique/la-cia-en-open-source-13-millions-de-pages-accessibles-au-public-sur-le-web_109907>. Acesso em: 12 mar. 2024.

SECURITY SERVICE MI5. **Introduction to Joint Terrorism Analysis Centre (JTAC)**. Disponível em: <https://www.mi5.gov.uk/joint-terrorism-analysis-centre>. Acesso em: 12 mar. 2024.

VITÓRIA nas Sombras
Revista do Comando Naval de Operações Especiais

APOIO

Comando de Operações Navais

Comando-Geral do
Corpo de Fuzileiros Navais

Grupamento de
Mergulhadores de Combate

Batalhão de Operações Especiais
de Fuzileiros Navais
Batalhão Tonelero

Centro de Guerra Acústica
e Eletrônica da Marinha

Revista Tecnologia & Defesa

Revista do Comando Naval de Operações Especiais

Comando Naval de Operações Especiais
Praça Barão de Ladário, s/nº - Edifício Almirante Tamandaré, 7º andar
Centro - Rio de Janeiro/RJ - CEP: 20091-000