

ISSN 2317-6350

DOUTRINA MILITAR

Publicação do Exército Brasileiro | Ano 010 | Edição nº 032 | Outubro a Dezembro de 2022

www.coter.eb.mil.br

www.cdoutex.eb.mil.br

coter_exercito

COMANDANTE DE OPERAÇÕES TERRESTRES
General de Exército Estevam Cals **Theophilo** Gaspar de Oliveira

CHEFE DO CENTRO DE DOUTRINA DO EXÉRCITO
General de Brigada **Marcelo** Pereira Lima de Carvalho

CONSELHO EDITORIAL
General de Brigada **Marcelo** Pereira Lima de Carvalho
Coronel Marcelo Eduardo **Anacleto**
1º Tenente Cláudio César **Marques** Simões
1º Sargento **Alexandre** André Lussani

EDITOR-CHEFE
Coronel Marcelo Eduardo **Anacleto**

EDITOR-ADJUNTO
1º Tenente Cláudio César **Marques** Simões
1º Sargento **Alexandre** André Lussani

SUPERVISOR DE PRODUÇÃO
Coronel Marcelo Eduardo **Anacleto**

REDAÇÃO E REVISÃO
2º Tenente Patrícia Fátima Soares **Fernandes**

PROJETO GRÁFICO
Cabo Douglas **Vitor Pereira** da Silva

DIAGRAMAÇÃO E ARTE FINAL
Cabo Douglas **Vitor Pereira** da Silva

IMPRESSÃO GRÁFICA
Gráfica do Exército
Al. Mal. Rondon s/nº - Setor de Garagens
Quartel-General do Exército
Setor Militar Urbano
CEP 70630-901 - Brasília/DF
Fone: (61) 3415-5815
RITEX: 860-5815
www.graficadoexercito.eb.mil.br
divcmcl@graficadoexercito.eb.mil.br

TIRAGEM
200 exemplares

DISTRIBUIÇÃO
Gráfica do Exército

VERSÃO ELETRÔNICA
Portal de Doutrina do Exército: www.cdoutex.eb.mil.br
portal.cdoutex@coter.eb.mil.br
Biblioteca Digital do Exército: www.bdex.eb.mil.br

CENTRO DE DOUTRINA DO EXÉRCITO
Quartel-General do Exército – Bloco H – 3º Andar
Setor Militar Urbano
CEP 70630-901
Brasília – DF
Fone: (61) 3415 6275/5014/6967
RITEX: 860 6275/5014/6967
www.cdoutex.eb.mil.br

Envie a sua proposta de artigo para:
dmtrevista@coter.eb.mil.br

Ano 010, Edição 032, 4º Trimestre de 2022

DISTRIBUIÇÃO GRATUITA

SUMÁRIO

O COMANDO DE FOGOS DO TEATRO
Tenente-Coronel Laraia **04**

O ASPECTO POLÍTICO-ECONÔMICO DA MODERNIZAÇÃO DO NORAD PELO CANADÁ
Coronel Celso **18**

A EXPLORAÇÃO E O ATAQUE CIBERNÉTICO
Major Diogo Luiz **30**

A CAPACIDADE CIBERNÉTICA NO EXÉRCITO DO CHILE
38
Tenente-Coronel Jerônimo

DEMANDAS DOUTRINÁRIAS PARA UMA OPERAÇÃO CONJUNTA DE AVIAÇÃO
Tenente-Coronel Marcus Gomes **46**

O EMPREGO DE DRONES NO EXÉRCITO FRANCÊS
Coronel Glaidson **56**

A RELEVÂNCIA DOS COMBATES URBANOS NA 1ª FASE DO CONFLITO NA UCRÂNIA
Major Tiago França **64**

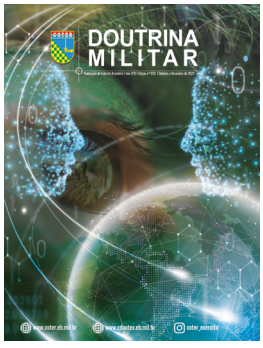


Foto de Capa: Composição ilustrando imagens relacionadas ao ambiente cibernético.
Autor: Cb Vitor Pereira.

"As ideias e conceitos contidos nos artigos publicados nesta revista refletem as opiniões de seus autores e não a concordância ou a posição oficial do Exército Brasileiro. Essa liberdade concedida aos autores permite que sejam apresentadas perspectivas novas e, por vezes, controversas, com o objetivo de estimular o debate de ideias."

APRESENTAÇÃO

Caro leitor,

Ao findar o ano de 2022, o Comando de Operações Terrestres (COTER) reafirma sua atuação como o órgão de direção operacional do Exército Brasileiro, ciente dos desafios que se apresentam nos cenários externo e interno ao nosso país.

O conflito na Ucrânia, que teve início em fevereiro deste ano, mostra a necessidade e a relevância de se dispor de forças armadas adestradas, aptas para o cumprimento de sua missão e focadas nos conflitos de alta intensidade. Nesse diapasão, foi criado o Observatório de Doutrina, grupo multidisciplinar composto por mais de uma centena de integrantes de diversas especialidades das três forças singulares brasileiras, com o propósito de acompanhar o conflito, realizar análises sob a óptica da doutrina militar e difundir os conhecimentos de interesse da Força Terrestre (F Ter). Fruto desse trabalho, ao longo do ano, foram apresentadas diversas indicações ao Alto Comando do Exército, com reflexos nos diversos fatores, tais como: Doutrina, Organização (e/ou Processos), Adestramento, Material, Educação, Pessoal e Infraestrutura (DOAMEPI), que compõem as capacidades operacionais necessárias para a atualização do Braço Forte de nossa Instituição.

No campo interno, manteve-se o foco no preparo e no emprego da F Ter, com intensa participação em exercícios e operações militares. Cabe destacar as operações de segurança em nossas fronteiras terrestres (Operação Ágata), as ações humanitárias em Roraima (Operação Acolhida), a distribuição de água potável no semiárido brasileiro (Operação Pipa), as ações de garantia da votação e apuração das eleições, o exercício combinado ARANDU (ciclo 2021 – 2023), com o Exército da Argentina, e o exercício combinado CORE 2022, realizado com o Exército dos Estados Unidos da América (EUA), entre tantos outros, que contribuem grandemente para a prontidão da tropa.

Além disso, por meio das organizações operacionais da F Ter, o COTER tem colaborado para a segurança anbiental e nacional, orientando diversas ações em prol do combate aos crimes ambientais e transfronteiriços e no apoio ao desenvolvimento nacional, com as obras de cooperação, nos mais diversos rincões do país.

No que se refere à produção doutrinária, o COTER, órgão central do Sistema de Doutrina Militar Terrestre (SIDOMT), por meio do Centro de Doutrina do Exército, atingiu a marca histórica de vinte e quatro manuais de caráter doutrinário aprovados, o maior indicador registrado desde a criação deste centro, em 2010.

Alinhados com a necessidade de se promover a discussão doutrinária, os artigos apresentados nesta edição trazem, em sua maioria, uma reflexão sobre a dinâmica que impele o COTER e a F Ter a se ajustarem às demandas do combate moderno, nos múltiplos domínios onde se desenvolvem as operações militares.

Considerando a evolução da doutrina militar nos demais exércitos, o aumento do alcance e do poder de fogo dos sistemas de armas, o incremento de ações na dimensão informacional, a evolução no emprego dos meios de guerra eletrônica nas operações, bem como o desenvolvimento das ações na área da cibernética, há necessidade de se incrementar o comando e controle e a coordenação desses diferentes vetores que impactam os resultados no combate moderno e pontecializam seus efeitos.

Dessa forma, visando a obter maior sinergia, propõe-se um novo desenho para o Sistema Operacional Militar Terrestre (SISOMT), que será aperfeiçoado, de modo a favorecer o planejamento e o emprego dos elementos do Exército Brasileiro que já atuam no desenvolvimento dessas capacidades.

O COTER, por seu turno, terá sua estrutura readequada, a fim de atender às demandas operacionais contemporâneas e se transformar em um órgão de comando operacional, subordinando as organizações militares que possuem capacidades únicas no Exército Brasileiro em um Comando Multidomínio [1], com potencial para interferir profundamente no emprego da Força Terrestre na defesa da pátria. Essa transformação provocará atualização na nossa doutrina militar, além de apresentar uma configuração atual que vem sendo empregada nos principais exércitos do mundo, o que contribuirá para o fortalecimento da estratégia da dissuasão.

Finalizando este prólogo, em nome do COTER, manifesto o compromisso irrestrito e inabalável com o povo brasileiro, com a democracia e com a harmonia política e social do Brasil, ratificado pelos valores e pelas tradições das Forças Armadas, sempre presentes nos mais importantes momentos de nossa história. Permanecemos vigilantes, atentos e focados no papel constitucional outorgado ao Exército na garantia de nossa soberania, da ordem e do progresso, sempre em defesa de nosso povo.

Lembrai-vos da Guerra!

General de Exército Estevam Cals **THEOPHILO** Gaspar de Oliveira
Comandante de Operações Terrestres



[1] O Sistema Multidomínio, que se encontra em estudo, será responsável pelo preparo e pela geração de capacidades relacionadas aos diversos vetores de nível estratégico a serem disponibilizados para emprego. Integrarão esse sistema as seguintes estruturas: Comando de Operações Especiais; Comando de Artilharia de Exército; Unidade de Busca de Alvos; Comando de Comunicações e Guerra Eletrônica; e Centro de Defesa Cibernética).



TENENTE-CORONEL LARAIA
Oficial de Ligação junto ao Centro de Excelência de Fogos do Exército dos EUA.

O COMANDO DE FOGOS DO TEATRO

A Estratégia Nacional de Defesa dos Estados Unidos da América (EUA), publicada em 2018, aponta significativas mudanças no cenário internacional que ameaçam a, até então, incontestável superioridade militar norte-americana.

De acordo com o texto, a atual desordem global, caracterizada pelo declínio da ordem mundial estabelecida ao término da Guerra Fria, deu origem a um ambiente internacional mais complexo e volátil, marcado pela competição [1] interestatal.

China e Rússia implementaram programas de modernização no campo militar. O estabelecimento de sofisticados sistemas de antiacesso [2] e negação de área [3] (A2/AD, sigla em inglês para *anti-access and area denial*), bem como o desenvolvimento de capacidades de guerra eletrônica, cibernética e espacial, limita a liberdade de ação de tropas norte-americanas nos teatros de guerra [4] da Europa e do Pacífico.

Diante desses novos desafios, o Departamento de Defesa dos EUA estabeleceu uma abordagem estratégica de longo prazo, visando a garantir superioridade militar decisiva e duradoura para o país, por meio do desenvolvimento de Forças Armadas (FA) mais letais, incentivo à inovação tecnológica e estabelecimento de alianças e parcerias.

A formação de FA aptas a enfrentar as ameaças atuais passa pela recuperação da prontidão e da operacionalidade, bem como pela modernização de capacidades fundamentais para atuar em ambientes contestados e desenvolver operações em múltiplos domínios [5] (MDO, sigla em inglês para *Multi-Domain Operations*).

O Exército dos Estados Unidos da América (EEUA), em alinhamento com a estratégia do Departamento de Defesa, apresentou sua visão para o ano de 2028, primeiro marco temporal do processo de modernização. O exército de 2028 deverá estar pronto para se deslocar, combater e vencer qualquer adversário, a qualquer momento e em qualquer lugar, em um conflito de alta intensidade e em múltiplos domínios, como parte de uma força conjunta ou combinada.

A fim de atingir os objetivos futuros, a Estratégia do Exército, publicada em 2018, estabeleceu quatro linhas de esforço a serem seguidas simultaneamente: Prontidão, Reforma, Fortalecimento de Alianças e Modernização.

A linha de esforço Prontidão tem por objetivo a geração de forças organizadas, treinadas e equipadas para pronta resposta. A linha de esforço Reforma busca readequação do orçamento destinado ao EEUA de modo a favorecer os projetos prioritários e as unidades mais importantes. Já a linha de esforço Fortalecimento de Alianças visa a ampliação da interoperabilidade entre forças norte-americanas e tropas aliadas.

Por fim, a linha de esforço Modernização, prioritária a partir do ano de 2022, visa a atualizar doutrina, equipamentos e formações, por meio de desenvolvimento e pesquisa em seis áreas prioritárias: Fogos de Longo Alcance, Nova Geração de Veículos de Combate, Defesa Aérea e Contra Mísseis, Letalidade do Soldado, Redes e Plataformas de Decolagem Vertical.

Em 2019, a Estratégia de Modernização do Exército, por sua vez, ampliou o conceito de modernização e incorporou a esse processo o desenvolvimento de novos conceitos e a atualização de doutrina, organizações, treinamento, liderança, educação e gestão de pessoal.

Corroborando com essas ideias, o General James P. Mcconville, Chefe do Estado-Maior do EEUA, em discurso para o Subcomitê de Defesa do Congresso norte-americano em 2021, afirmou que "os conflitos futuros ocorrerão em grandes distâncias, em todos os domínios e em velocidade muito maior". Para fazer face a esses desafios, "o exército precisa se transformar para prover à Força Conjunta a velocidade, o alcance e a convergência de efeitos provenientes de novas tecnologias que resultarão na superioridade necessária para vencer os combates".

A PRESENÇA GLOBAL DO EEUA

Nesse contexto de competição, todas as ações tomadas antes de um conflito armado são extremamente importantes, pois podem criar determinadas condições no teatro de guerra que contribuam para as opções estratégicas disponíveis para os Comandos Combatentes e Comandos Componentes do Exército (ASCC, sigla em inglês para *Army Service Component Command*).

Os Comandos Combatentes (COCOM, sigla em inglês para *Combatant Command*), também denominados Comandos Combatentes Unificados, constituem o maior escalão de comando possível em operações militares, de acordo com a doutrina militar norte-americana. Suas áreas de responsabilidade [6] e missões são definidas pelo Plano de Comando Unificado, documento elaborado pelo Chefe do Estado-Maior das Forças Armadas.

Os COCOM são encarregados de prover comando e controle para todas as unidades das Forças Armadas dos EUA (Força Aérea, Exército, Marinha, Fuzileiros Navais e Força Espacial), em qualquer local do planeta, em tempos de guerra ou paz.

Os EUA possuem, atualmente, 11 COCOM, divididos em dois tipos: funcional e geográfico. Os comandos funcionais são responsáveis por atividades específicas, como transporte e operações especiais (Op Esp). Já os Comandos Combatentes Geográficos (GCC, sigla em inglês para *Geographic Combatant Command*) são responsáveis pelo planejamento e condução de operações dentro de sua área de responsabilidade. Cada um deles é comandando por um Oficial General do mais alto posto da hierarquia militar norte-americana, sob ordens diretas do Secretário de Defesa.

Os quatro comandos funcionais são:

– Comando Cibernético (USCYBERCOM – *United States Cyber Command*);

– Comando Estratégico (USSTRATCOM – *United States Strategic Command*);

– Comando de Op Esp (USSOCOM – *United States Special Operations Command*); e

– Comando de Transporte (USTRANSCOM – *United States Transportation Command*).

Os sete comandos geográficos são:

– Comando da África (USAFRICOM - *United States Africa Command);*

– Comando Central (USCENTCOM - *United States Central Command);*

– Comando Europeu (USEUCOM - *United States European Command);*

– Comando do Norte (USNORTHERNCOM - *United States Northern Command);*



Fig 1 - Área de Responsabilidade dos GCC. Fonte: USCENTCOM.

– Comando do Pacífico (USAINDOPACOM - *United States Indo-Pacific Command);*

– Comando do Sul (USSOUTHCOM - *United States Southern Command);* e

– Comando Espacial (USSPACECOM - *United States Space Command).*

Os COCOM, como comandos unificados (comandos operacionais, de acordo com a Doutrina Militar brasileira), reúnem tropas de duas ou mais forças singulares. O EEUA integra todos os comandos geográficos e dois dos comandos funcionais (Transporte e Op Esp). O escalão do exército norte-americano integrante dos COCOM é denominado Comando Componente do Exército (ASCC, sigla em inglês para Army Service Component Command).

Os cinco ASCC associados aos comandos geográficos são:

- Exército Central (USARCENT - *U.S. Army Central*);

- Exército da Europa e África (USAREUR-AF - *U.S. Army Europe and Africa*) [7];

- Exército do Norte (USARNORTH – *U.S. Army North*);

- Exército do Pacífico (USARPAC – *U.S. Army Pacific*); e

- Exército do Sul (USARSOUTH – *U.S. Army South*).

O EXÉRCITO DO TEATRO

As forças do exército norte-americano são organizadas e empregadas em escalões, com diferentes missões e funções específicas. Esse tipo de estrutura proporciona grande flexibilidade aos comandantes, visto que o escalão mais adequado pode ser selecionado para cada operação militar.

O mais alto escalão do EEUA é o exército do teatro e, doutrinariamente, sua função primária é atuar como ASCC.

A cada GCC é alocado um exército do teatro. Apesar dessa ligação, o exército do teatro é subordinado diretamente ao Departamento do Exército [8] norte-americano.

A missão do exército do teatro é extremamente complexa. Normalmente, todas as tropas do EEUA desdobradas na área de responsabilidade de um GCC estão sob controle do exército do teatro, resultando em inúmeras atribuições de ordem operacional e administrativa, tais como:

- prover o apoio logístico;
- realizar atividades de recepção, acomodação, apoio ao movimento e integração de tropas;
- integrar tropas em um sistema de C2;
- efetuar estimativas logísticas;
- realizar proteção de tropas e instalações; e
- executar operações de assistência humanitária.

Além disso, como integrante do GCC, o exército do teatro deve apoiar elementos de outras Forças Armadas dos EUA desdobrados na área de responsabilidade do GCC; conduzir operações de cooperação de segurança, operações de contingência e operações de assistência humanitária; contribuir com o desenvolvimento da infraestrutura local; elaborar planos operacionais; prover indicativos de modificações do ambiente operacional e estabelecer relações diplomáticas bilaterais e multilaterais.

Como parte do nível operacional, o exército do teatro pode atuar como Força Terrestre Componente (FTC), em caso de conflito, integrando o comando operacional (C Op) constituído pelo GCC. Pode, ainda, constituir uma força-tarefa conjunta, recebendo tropas de outras forças singulares.

O escalão tem capacidade de coordenar o emprego, por tempo limitado, de elementos subordinados em operações de contingência [9], de acordo com a necessidade do GCC. Porém, no caso de operações de combate de larga escala, caso não ocorra a ativação de um exército de campanha [10], o exército do teatro requer que suas capacidades sejam ampliadas, visando à coordenação do emprego de múltiplos corpos de exército (C Ex) e divisões de exército (DE).

De acordo com o manual de campanha FM 3-0 Operations, de 2017, o exército do teatro é organizado em comando, estado-maior, batalhão de comando e tropas alocadas ao GCC (sob controle operacional do exército do teatro). As tropas alocadas podem variar, de acordo com a área de responsabilidade e características da missão. De forma geral, o escalão possui estruturas de apoio logístico, comando e controle, saúde, inteligência e assuntos civis representadas pelos seguintes elementos:

- Comando de Sustentação do Teatro;

- Comando de Comunicações do Teatro;

- Comando Médico do Teatro;
- Brigada de Inteligência Militar; e
- Brigada de Assuntos Civis.

No caso de ampliação das capacidades para atuação em operações de combate de larga escala, o exército do teatro pode receber brigadas de aviação, antiaérea, de engenharia, de polícia militar e de defesa química, biológica, radiológica e nuclear (DQBRN), bem como um grupo de operações psicológicas.

No que se refere, em particular, à função de combate fogos, a única estrutura orgânica existente no exército do teatro é a célula de fogos, encarregada da aquisição e engajamento de alvos (atividades denominadas *targeting* pelo EEUA), bem como do planejamento do emprego dos fogos cinéticos e não cinéticos no âmbito desse escalão.

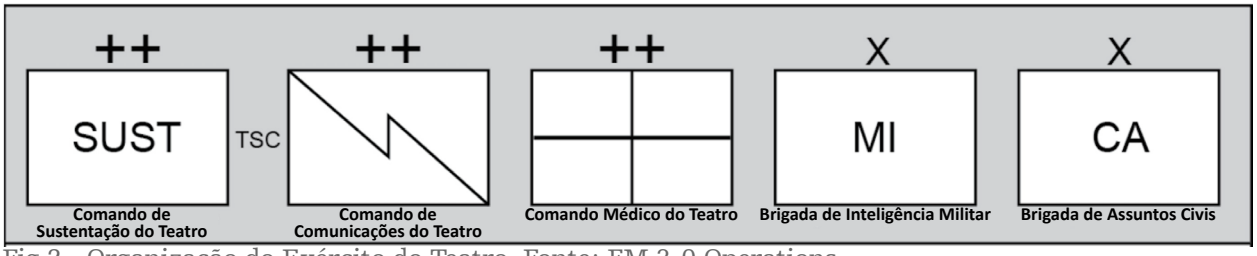


Fig 2 - Organização do Exército do Teatro. Fonte: FM 3-0 Operations.

A CRIAÇÃO DO COMANDO DE FOGOS DO TEATRO

Na década de 1990, ao término da Guerra Fria, o EEUA optou pela desativação dos comandos de artilharia dos C Ex. Posteriormente, durante os anos em que as tropas norte-americanas foram empregadas em operações de contrainsurgência no Iraque e no Afeganistão, as artilharias divisionárias (AD) e algumas brigadas de artilharia (Bda Art) foram desativadas em detrimento da necessidade de emprego de tropas de outra natureza.

Recentemente, a ameaça apresentada pelo surgimento de uma nova potência militar e pela reconstrução da capacidade militar russa exigiu a mudança de postura do EEUA em relação aos combates de larga escala. Nessa conjuntura, foi constatado que a desativação de comandos de artilharia resultou em uma séria deficiência na capacidade de comando e controle da função de combate fogos.

A solução encontrada foi a ativação de comandos de artilharia em todos os escalões da força. Coube ao Centro de Excelência de Fogos do Exército dos Estado Unidos (FCoE, sigla em inglês para *Fires Center of Excellence*) a missão de estruturar as unidades responsáveis por restabelecer as capacidades de planejamento, coordenação e sincronização do emprego de fogos terrestres, conjuntos e multinacionais.

Em 2014, as AD foram reativadas, solucionando parcialmente o problema no escalão DE. Contudo, nos escalões C Ex e exército do teatro, a inexistência de um comando de artilharia delegava às Bda Art alocadas a esses grandes comandos a missão de integrar os fogos e, também, executar as missões de apoio.

Em 2020, a Diretoria de Desenvolvimento e Integração de Capacidades do FCoE publicou o conceito operacional e organizacional do Comando Operacional de Fogos (OFC, sigla em inglês para *Operational Fires Command*), detalhando a estrutura inicial e a concepção de emprego desse comando a ser estruturado nos C Ex em substituição às antigas artilharias de corpo de exército.

No mesmo ano, foi publicado o conceito operacional e organizacional do Comando de Fogos do Teatro (TFC, sigla em inglês para *Theater Fires Command*), com as informações doutrinárias iniciais a respeito da estrutura concebida para planejar, coordenar e empregar os fogos em múltiplos domínios no escalão exército do teatro.

Integrada ao processo geral de modernização do EEUA, a criação dos TFC subordinados aos cinco exércitos do teatro atualmente ativos está prevista para o período de 2028 a 2035. Entretanto, em novembro de 2021, o primeiro TFC foi ativado na Alemanha, no continente europeu, sendo designado 56º Comando de Artilharia (56th AC, sigla em inglês para *56th Artillery Command*) e integrado à estrutura do USAREUR-AF.



Fig 3 - Cerimônia de ativação do 56th Artillery Command. Fonte: U.S. Army.

O TFC NAS OPERAÇÕES EM MÚLTIPLOS DOMÍNIOS

De acordo com o Conceito Operacional e Organizacional do TFC, publicado em 2020, o EEUA busca desenvolver a capacidade de emprego de fogos de longo alcance, nos níveis operacional e estratégico, para apoiar as operações em múltiplos domínios. Em especial, o exército tem o objetivo de neutralizar os sistemas de A2/AD inimigos, a fim de proporcionar liberdade de ação para o emprego da força conjunta.

A criação do TFC visa a atender a essa necessidade, garantindo ao exército do teatro e ao GCC um comando de artilharia que realize o planejamento, a coordenação, o emprego e a sincronização dos fogos em todos os domínios.

Em sua concepção doutrinária, o TFC é alocado ao ASCC, ficando sob controle operacional do exército do teatro, e tem a missão geral de integrar os fogos multidomínio [11], nos níveis operacional e estratégico, em apoio ao comando conjunto em todas as fases das MDO.

O TFC deve estar desdobrado em sua área de responsabilidade com elementos subordinados em posições avançadas, a fim de apoiar ações de segurança, ampliar a interoperabilidade com outras forças e aliados estratégicos, ampliar a consciência situacional e, principalmente, contribuir com a dissuasão.

Com essa postura, durante o período de competição, o TFC elabora planos operacionais e realiza a aquisição e o processamento de alvos, garantindo condições de ataque imediato contra alvos estratégicos de interesse do GCC, como sistemas integrados de defesa antiaérea, meios de apoio de fogo (Ap F), instalações de comando e controle (C2), centros logísticos e infraestrutura crítica.

Em caso de conflito armado, o TFC coordena o desencadeamento de fogos cinéticos e não cinéticos contra os alvos designados, dentro e fora da área de operações do C Op, possibilitando a abertura de janelas de superioridade [12] a serem exploradas pelos elementos de manobra.

Todas essas ações são desenvolvidas a partir de posições interconectadas, porém dispersas na área de operações, atendendo a critérios de segurança, tendo em vista a capacidade de busca de alvos e emprego

de fogos de longo alcance dos potenciais inimigos. A moderna rede de C2 estabelecida garante a segurança das comunicações e permite a realização de reuniões virtuais para planejamento operacional e logístico, processamento de alvos, direção de tiro e coordenação das atividades de guerra eletrônica (GE) e cibernética.

A rede de C2, denominada Rede Integrada de Fogo (IFN, sigla em inglês para *Integrated Fires Network*) permite, ainda, o emassamento de fogos provenientes de sistemas desdobrados em diferentes posições no teatro de operações, criando a superioridade de efeitos que garante a abertura da janela de superioridade a ser explorada pelo comando conjunto.

É importante ressaltar que a IFN é conectada às redes de C2 e sistemas de inteligência, vigilância e reconhecimento (IVR) de outras forças, agências e nações aliadas que atuam no teatro de operações. É ligada, ainda, à Rede de Informações do Departamento de Defesa dos EUA. Assim, valendo-se de inteligência artificial, a IFN acessa informações sobre alvos provenientes de diversos sensores e estabelece a conexão com o sistema de armas mais adequado para o engajamento. O processamento das missões de tiro é realizado por meio do Sistema Avançado de Dados Táticos de Artilharia de Campanha (AFATDS, sigla em inglês para *Advanced Field Artillery Tactical Data System*), principal sistema vinculado à IFN.

ORGANIZAÇÃO

Segundo informações divulgadas, em fevereiro de 2022, pela Diretoria de Desenvolvimento e Integração de Capacidades/Fogos, do Comando do Exército do Futuro (AFC, sigla em inglês para *Army Future Command*) do EEUA, o TFC é composto por um Comando e Batalhão de Comando (HHBN, sigla em inglês para *Headquarters and Headquarters Battalion)* e uma Força-Tarefa Multidomínio (MDTF, sigla em inglês para *Multi-domain Task Force*).

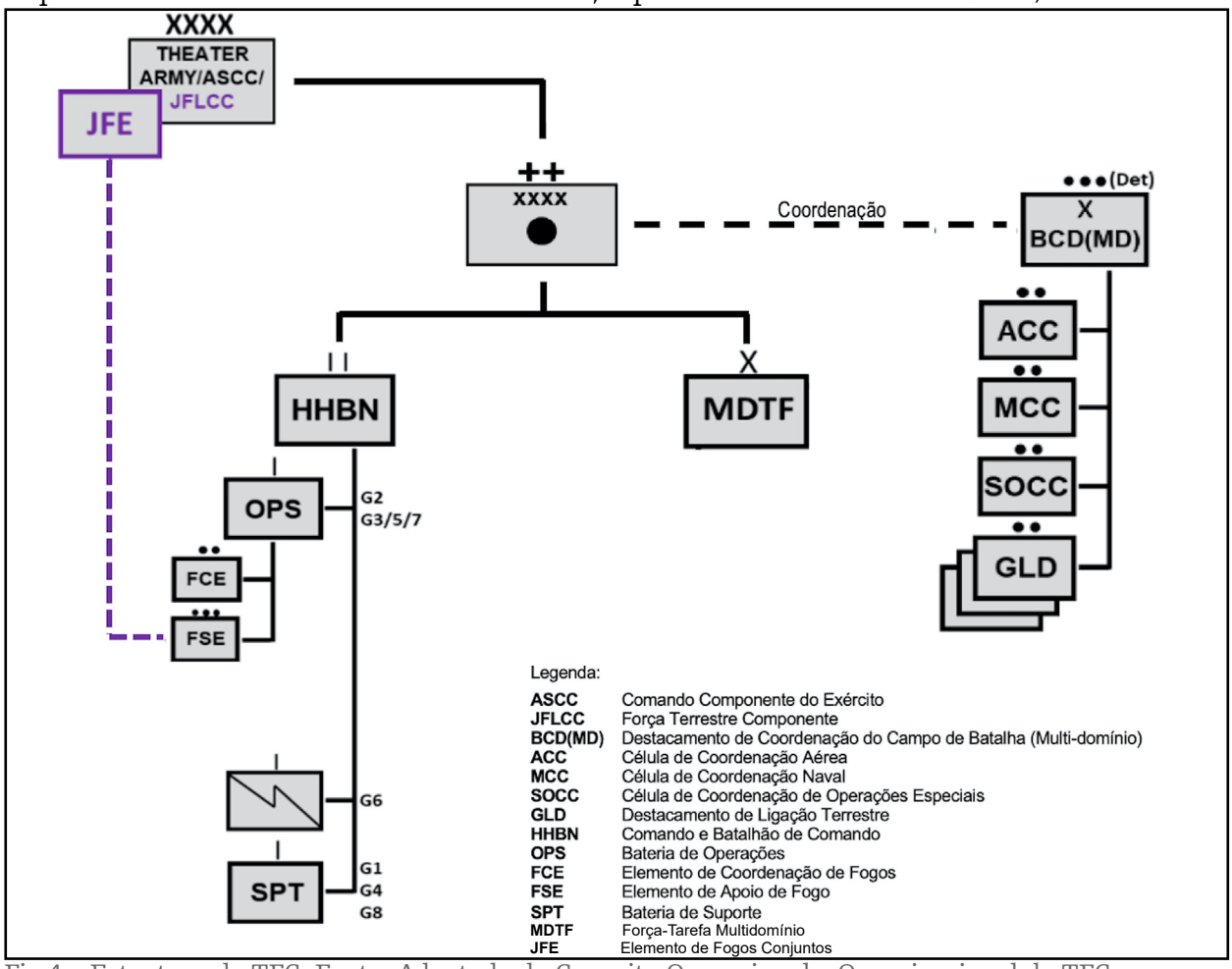


Fig 4 – Estrutura do TFC. Fonte: Adaptado do Conceito Operacional e Organizacional do TFC.

Essa estrutura ainda é conceitual e pode variar de acordo com as características de cada área de responsabilidade. De forma geral, o TFC é inicialmente organizado para atender às demandas específicas do GCC. Em caso de conflito, pode ser reorganizado de acordo com o planejamento do C Op. Tal característica permite que Bda Art, grupos de artilharia e outros atuadores cinéticos ou não cinéticos sejam colocados sob o comando do TFC.

O TFC é comandado por um *Major General* (equivalente a General de Brigada), que também exerce a função de coordenador do apoio de fogo (CAF) do exército do teatro ou FTC. A função de subcomandante é exercida, preferencialmente, por um *Brigadier General* (posto não existente na hierarquia militar brasileira).

O HHBN é organizado em Bateria de Operações, Companhia de Comunicações e Bateria de Suporte. O EM está integrado ao HHBN e mantém a organização funcional padrão normalmente utilizada em grandes escalões do EEUA, com um Chefe do Estado-Maior (posto de Coronel) e seções de pessoal (G1); inteligência (G2); operações, planejamento e treinamento (G3-5-7), apoio logístico (G4), comunicações (G6) e finanças (G8).

Essa estrutura pode ser ampliada com a inclusão de oficiais de ligação do exército (forças especiais, GE, cibernética etc.), de outras forças (Oficial de Ligação de Fogo Naval, Oficial de Ligação Aérea etc.), de agências governamentais (Agências Central de Inteligência, Agência de Segurança Nacional etc.) e de países aliados, visando a ampliar a capacidade de aquisição, análise e processamento de alvos.

Dentro da organização do HHBN, é importante ressaltar as atividades desempenhadas pela Bateria de Operações, por intermédio da Seção de Inteligência e da Seção de Operações, Planejamento e Treinamento.

A Seção de Inteligência é encarregada do levantamento e análise de informações sobre o inimigo e contribui de maneira substancial para o processo de *targeting* no âmbito do TFC. Para tanto, o G2 trabalha com informações oriundas do exército do teatro e, principalmente, do Batalhão de Efeitos Multi-domínio (MDEB, sigla em inglês para *Multi-domain Effects Battalion*) orgânico da MDTF.

A Seção de Operações, Planejamento e Treinamento, por sua vez, executa o planejamento das operações correntes e futuras em coordenação com o exército do teatro. É encarregada do posicionamento das forças subordinadas ao TFC e pela integração dos fogos cinéticos e não cinéticos em combate. Cabe ao G3-5-7, ainda, preparar as tropas de artilharia de campanha (Art Cmp) do EEUA e de países aliados que estejam posicionadas dentro da área de responsabilidade do TFC para atuar de acordo com a doutrina de MDO.

Sob a estrutura do G3-5-7 encontram-se as seguintes células funcionais: Elemento de Apoio Espacial (SSE, sigla em inglês para *Space Support Element*), Elemento de Controle de Fogo (FCE, sigla em inglês para *Fire Control Element*) e o Elemento de Apoio de Fogo (FSE, sigla em inglês para *Fire Support Element*).

O SSE é coordenado por um oficial da Força Espacial dos EUA, responsável por assessorar o comandante do TFC nos assuntos relacionados a esse domínio. A célula agrega importantes capacidades ao TFC, como vigilância e reconhecimento para detecção de alvos, comunicação satelital, alerta contra mísseis e dados precisos de localização e navegação sem a possibilidade de interferência de GE inimiga.

O FSE é encarregado da integração dos fogos cinéticos e não cinéticos, provenientes de todos os domínios, em apoio às ações do C Op e, para isso, é subdividido em três seções: GE e Cibernética, Operações de Informações e *Targeting*. A célula é desdobrada junto ao posto de comando (PC) do exército do teatro/FTC, onde atua sob a coordenação do Elemento de Fogos Conjuntos (JFE, sigla em inglês para *Joint Fires Element*) e integra o esforço conjunto de aquisição e processamento de alvos.

Por sua vez, o FCE é responsável do planejamento de fogos, em coordenação com o FSE (seção de *Targeting*, principalmente), e pelo controle da direção de tiro no âmbito do TFC. Cabe aos integrantes da célula a supervisão do processo de desencadeamento de fogos, garantindo que os elementos táticos e técnicos selecionados pelo AFATDS estejam

de acordo com os protocolos em vigor para a operação.

O TFC possui, ainda, uma relação funcional com o Destacamento de Coordenação do Campo de Batalha - Multidomínio (BCD-MD, sigla em inglês para *Battlefield Coordination Detachment – Multi-domain*). Essa unidade subordinada ao ASCC tem a missão de realizar a ligação, física e/ou virtual, entre o TFC e os componentes aéreo, naval e de Op Esp do C Op, visando a estabelecer os ajustes necessários para o emprego de fogos conjuntos.

Cabe ao BCD-MD, entre outras tarefas, integrar o processo de *targeting* conjunto; compartilhar informações de IVR; gerenciar as Medidas de Coordenação de Apoio de Fogo (MCAF) e Medidas de Coordenação e Controle do Espaço Aéreo (MCCEA) junto às demais forças; e coordenar, junto à Força Aérea, as ações de apoio aéreo aproximado, interdição e transporte por meio dos Destacamentos de Ligação Terrestre (GLD, sigla em inglês para *Ground Liaison Detachment*).

MULTI-DOMAIN TASK FORCE

A MDTF é considerada o elemento mais importante da operacionalização do conceito de MDO. É uma organização militar, valor grande unidade, conceitualmente subordinada ao TFC e que atua no nível estratégico-operacional em apoio às ações do C Op.

Sua principal missão é integrar fogos cinéticos e não cinéticos, em todos os domínios, proporcionando ao comandante operacional (Cmt Op) variadas capacidades para atuação contra os sistemas de A2/AD inimigos. Para tanto, a MDTF sincroniza efeitos oriundos de GE, defesa cibernética, operações de informações e operações espaciais com fogos de longo alcance.

A primeira MDTF do EEUA foi ativada em 2017, como uma unidade experimental, na Base Conjunta *Lewis-McChord*, no estado de Washington e tem sua atuação alinhada com a área de responsabilidade do USAINDOPACOM. Já incorporando os ensinamentos colhidos, a segunda MDTF foi ativada em 2021, na

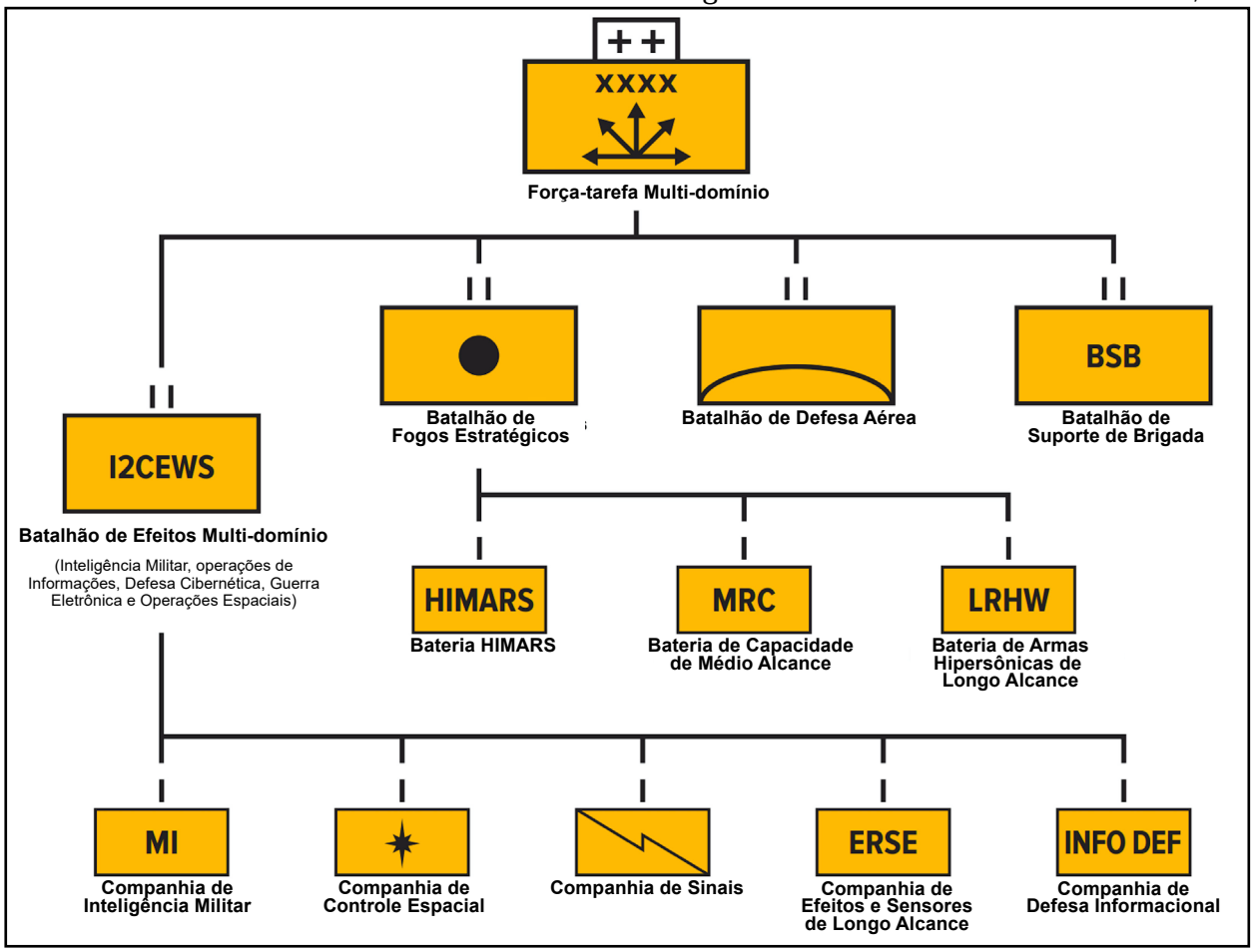


Fig 5 - Estruturas da MDTF. Fonte: FEICKERT, 2022.

Alemanha. Atualmente, é subordinado ao 56th AC e atua em proveito do USAREUR-AF.

A terceira MDTF, por sua vez, foi ativada em setembro de 2022, no *Fort Shafter*, no estado do Hawaii, e atuará, também, em proveito do USAINDOPACOM, teatro de operações reconhecido como prioritário pelo Departamento de Defesa dos EUA. O EEUA planeja ativar, ainda, mais duas MDTF, sendo uma destinada à região do Ártico e outra para resposta global, podendo ser empregada em qualquer parte do planeta.

De forma geral, a MDTF é organizada de acordo com as necessidades dos GCC. Sua estrutura básica vem sendo modificada desde sua concepção inicial visto que parcela considerável das capacidades que serão integradas às MDTF ainda se encontra em desenvolvimento. De acordo com relatório divulgado pelo Congresso dos EUA, em 31 de maio de 2022, a MDTF é composta por:

- Batalhão de Efeitos Multidomínio (MDEB, sigla em inglês para *Multi-Domain Effects Battalion*);
- Batalhão de Fogos Estratégicos (SFB, sigla em inglês para *Strategic Fires Battalion*);
- Batalhão de Defesa Aérea; e
- Batalhão de Suporte de Brigada.

A essa estrutura devem ser acrescentados, ainda, o Comando e a Bateria de Comando, de acordo com informações do AFC.

Cabe ressaltar que as MDTF atualmente ativas ainda não possuem a estrutura acima descrita. Essas unidades contam com o Comando, Companhia de Suporte e um Destacamento de Inteligência Militar, Defesa Cibernética, GE e Operações Espaciais.

O MDEB é o alicerce da MDTF. Essa unidade integra elementos de C2 com estruturas de inteligência militar, operações de informações, defesa cibernética, GE e operações espaciais. Empregando uma série de sensores, como satélites e sistemas aéreos remotamente pilotados (SARP), o MDEB fornece alvos para o SFB e, ao mesmo tempo, neutraliza redes e sensores inimigos utilizando fogos não cinéticos. Suas capacidades específicas ainda são sigilosas.

Conforme ilustra a figura 5, o MDEB organiza suas diferentes capacidades em cinco subunidades: Companhia de Inteligência Militar; Companhia de Controle Espacial; Companhia de Sinais; Companhia de Efeitos e Sensores de Longo Alcance; e Companhia de Defesa Informacional. Em sua concepção, a unidade possui, ainda, uma Companhia de Comando.

O SFB, por sua vez, tem por missão desencadear fogos de longo alcance para atacar alvos operacionais e estratégicos em apoio às ações do C Op. Para tanto, deverá empregar os sistemas de armas e munições em desenvolvimento pelo EEUA como parte do projeto Fogos Precisos de Longo Alcance (LRPF, sigla em inglês para *Long-Range Precision Fires*), a mais alta prioridade do processo de modernização do EEUA.

A unidade é estruturada em Bateria HIMARS; Bateria de Capacidade de Médio Alcance (MRC, sigla em inglês para *Middle Range Capability*); e Bateria de Armas Hipersônicas de Longo Alcance LRHW, sigla em inglês para *Long-Range Hypersonic Weapon*). Essas subunidades constituem o estado da arte em fogos cinéticos e permitem o ataque a alvos de natureza diversa em território inimigo.

A Bateria HIMARS emprega nove lançadores múltiplos de foguetes M142 *High Mobility Artillery System* (HIMARS). Utilizando esse sistema, a bateria lançará os mísseis de ataque de precisão (PrSM, sigla em inglês para *Precision Strike Missile*), com alcance de 60 a 500 quilômetros, o que confere à MDTF a capacidade de atacar alvos operacionais como radares e sistemas de defesa antiaérea, postos de comando e instalações logísticas. A primeira versão do PrSM, em desenvolvimento pela empresa norte-americana *Lockheed Martin,* encontra-se em fase final de testes e deverá ser entregue ao EEUA em 2023. A segunda versão, mais avançada e com capacidade de neutralizar



Fig 6 - Teste do lançamento do PrSM no M142 HIMARS. Fonte: Lockheed Martin.

embarcações e alvos móveis, deverá estar disponível a partir de 2027.

A Bateria MRC foi concebida para engajar alvos operacionais e estratégicos, em uma faixa de alcance intermediária, entre o PrSM e as armas hipersônicas. Para tanto, deverá empregar o sistema de armas denominado *Typhon* pelo EEUA e, atualmente, em desenvolvimento pela empresa *Lockheed Martin*. Cada bateria, em sua concepção, possui quatro viaturas lançadoras controladas por um centro de operações. De acordo com relatório apresentado ao Congresso norte-americano, a previsão é de que o EEUA receba quatro baterias MRC, sendo a primeira no 2º semestre de 2023 e as demais nos anos subsequentes (sendo uma por ano).

O sistema *Typhon* empregará os mísseis de cruzeiro SM-6 (supersônico) e *Tomahawk* (subsônico), ambos produzidos pela empresa norte-americana *Raytheon* e já em uso pela Marinha dos EUA. O SM-6 possui alcance aproximado de 400 quilômetros. Embora não esteja na faixa de emprego desejada, possui a capacidade de engajar alvos navais, o que atende aos interesses do EEUA na área responsabilidade do USINDOPACOM. Já o Tomahawk possui alcance máximo de 1.600 quilômetros, sendo utilizado para ataque a alvos terrestres estratégicos.

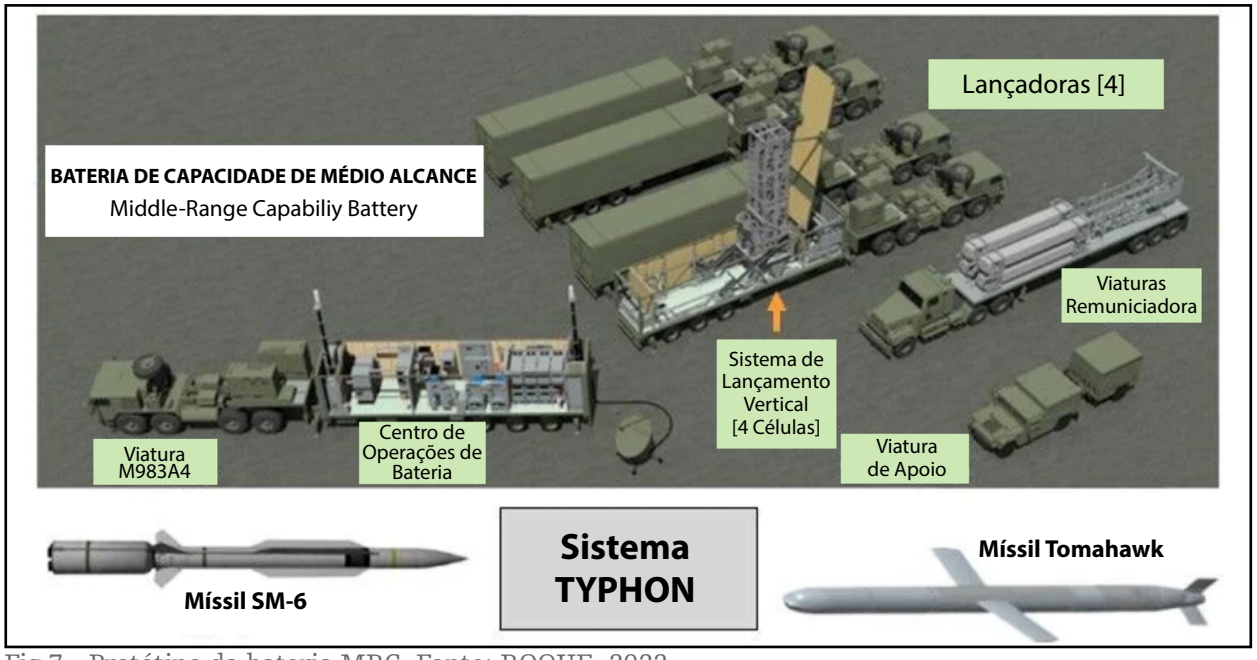


Fig 7 - Protótipo da bateria MRC. Fonte: ROQUE, 2022.

A bateria LRHW consiste em um importante elemento dissuasório ao conferir à MDTF a capacidade de engajar alvos estratégicos em território inimigo. A subunidade é constituída por quatro viaturas lançadoras (cada uma com capacidade de disparo de dois mísseis) e um centro de operações.

Parte desse sistema, denominado *Dark Eagle* pelo EEUA e desenvolvido pelas empresas *Lockheed Martin* e *Northrop Grumman*, já foi entregue, em 2021, à primeira bateria LRHW ativada junto ao 5-3 FA Bn, garantindo condições de treinamento e desenvolvimento de doutrina. Os mísseis hipersônicos deverão ser entregues a partir de 2023. Existe, ainda, a previsão de ativação de mais duas baterias LRHW nos anos de 2025 e 2027.

Os mísseis hipersônicos do sistema *Dark Eagle* terão alcance máximo de 2.800 quilômetros e um custo aproximado de 106 milhões de dólares a unidade. Após o lançamento, o míssil viajará a uma velocidade de 6 mil quilômetros por hora até atingir o topo da atmosfera terrestre, onde permanecerá fora do alcance das defesas antiaéreas inimigas. Quando determinado, o corpo comum de voo hipersônico (C-HGB, sigla em inglês para



Fig 8 – Protótipo da bateria LRHW. Fonte: Lockheed Martin.

Common Hypersonic Glide Body) será lançado em direção ao alvo a uma velocidade entre 6 mil e 21 mil quilômetros por hora. A velocidade de ataque do C-HGB aliada à sua capacidade de manobra torna sua detecção e interceptação muito difíceis por parte dos sistemas de DAAe inimigos.

O C-HGB, ilustrado na figura 9, é desenvolvido pela empresa *Dynetics* e deverá ser utilizado, também, pela Marinha dos EUA.

O 5º Batalhão do 3º Regimento de Artilharia (5-3 FA Bn, sigla em inglês para *Field Artillery Battalion)* é o primeiro SFB a ser ativado no EEUA. A unidade é subordinada à 1ª MDTF.

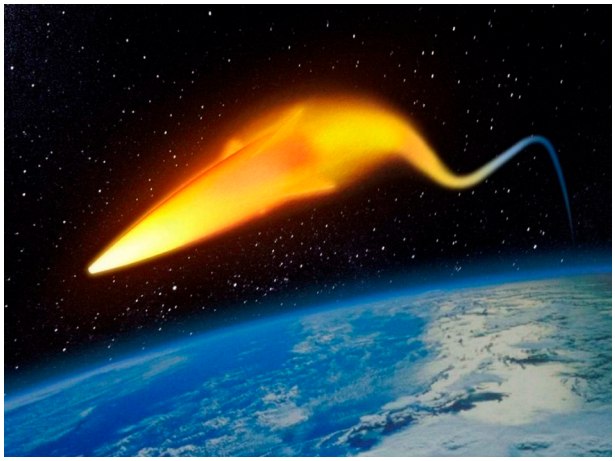


Fig 9 – *Common Hypersonic Glide Body.* Fonte: *Lockheed Martin.*

56º COMANDO DE ARTILHARIA

Conforme relatado anteriormente, o primeiro TFC foi ativado em novembro de 2021, na Alemanha, e integrado à estrutura do USAREUR-AF. A designação de 56th *Artillery Command* (56th AC) reporta ao comando de artilharia ativado, em 1983, com a missão de coordenar o emprego das unidades de Art Cmp responsáveis pelos mísseis nucleares de médio alcance MGM-31A *Pershing,* e desativado, em 1991, ao término da Guerra Fria.

O atual 56th AC tem a missão de planejar, coordenar, integrar e executar fogos cinéticos e não cinéticos na área de responsabilidade do USEUCOM e USAFRICOM, em apoio ao Cmt Op. Nesse contexto, o TFC funciona como comando de artilharia e elemento de coordenação do fogo do USAREUR-AF (ou exército de campanha/FTC, caso sejam ativados).

O 56th AC, como Comando de Artilharia de Campanha da Força (FFA-HQ, sigla em inglês para *Force Field Artillery Headquarters*), tem a missão de organizar a Art Cmp para o combate no escalão exército do teatro e coordenar o emprego de todas as Bda Art e elementos de fogos não cinéticos alocados ao USAREUR-AF, permitindo, dessa forma, a sincronização dos fogos com a manobra de forma eficaz.

Como mais alto escalão de coordenação do Ap F do USAREUR-AF, o 56th AC coordena o processo de *targeting* do componente

terrestre em sua área de responsabilidade, com especial atenção para o desenvolvimento das capacidades do Centro de Processamento de Alvos (TWC, sigla em inglês para *Targeting Work Center*) do ASCC. Deve ainda, atuar de forma coordenada com a Força Aérea dos EUA, em ligação com o 19º Destacamento de Coordenação do Campo de Batalha (19th BCD), no planejamento do emprego de fogos de longo alcance.

O 56th AC pode ainda, mediante ordem, exercer as mesmas funções anteriormente descritas para a FTC da Organização do Tratado do Atlântico Norte (OTAN), no caso de emprego de forças combinadas na Europa. Em consequência, dever trabalhar em coordenação com os países integrantes da OTAN, visando a ampliar interoperabilidade e desenvolver uma estrutura integrada de fogos.

Com esse objetivo, desde sua ativação, o 56th AC busca desempenhar um papel de liderança no âmbito da Art Cmp no continente europeu, organizando exercícios multinacionais com países aliados da OTAN e outras nações amigas. Como exemplo, o exercício Frente Dinâmica (*Dynamic Front*, em inglês) realizado na Alemanha, no ano de 2022, reuniu cerca de 3 mil militares de 19 países, sob a coordenação desse TFC, com o propósito de desenvolver a capacidade de executar fogos em múltiplos escalões e testar a interoperabilidade do sistema de fogos nos escalões operacional e tático.

Atualmente, o 56th AC possui, como unidade subordinada, a 2ª MDTF. Ativada em setembro de 2021, a 2ª MDTF é organizada em: Comando; Companhia de Suporte; e Destacamento de Inteligência Militar, Operações Cibernéticas, GE e Operações Espaciais.

Sua missão principal é sincronizar o emprego de fogos não cinéticos em apoio à consecução dos objetivos do USEUCOM e USAFRICOM. No futuro, com a ampliação de sua estrutura e ativação das unidades previstas, deverá ser capaz de planejar e coordenar o emprego de fogos cinéticos de longo alcance, ampliando exponencialmente o poder de combate do 56th AC.

CONSIDERAÇÕES FINAIS

A concepção da doutrina de MDO, em alinhamento com os novos desafios estratégicos visualizados pelo Departamento de Defesa norte-americano, resultou em significativas transformações no EEUA. A fim de garantir a superioridade militar em um conflito futuro, o processo de modernização, iniciado em 2019, possibilitou o desenvolvimento de novos conceitos, armamentos e equipamentos militares, bem como a atualização de doutrina, organizações, treinamento, liderança, educação e gestão de pessoal.

Nesse contexto, a criação do TFC visa a atender à necessidade de um comando de artilharia no escalão exército do teatro com capacidade para planejar, coordenar, empregar e sincronizar os fogos de longo alcance, cinéticos e não cinéticos, em todos os domínios, em apoio à conquista dos objetivos do C Op.

Sua missão principal é neutralizar a capacidade A2/AD inimiga por meio da convergência de fogos, no tempo e no espaço, sobre os sistemas de defesa antiaérea e meios de apoio de fogo, garantindo a abertura de uma janela de oportunidade a ser explorada pela força conjunta. Deve, ainda, a partir desse ponto, garantir a liberdade de ação da força atacante mediante a manutenção da superioridade de fogos sobre o oponente, neutralizando alvos operacionais e estratégicos.

A estrutura do TFC e seu conceito operacional representam uma transformação significativa na forma como o EEUA emprega os meios de apoio de fogo, sejam eles cinéticos ou não cinéticos. O novo comando reunirá capacidades inovadoras de C2 e aquisição e, principalmente, engajamento de alvos. Nesse cenário, a MDTF, organização subordinada ao TFC e componente fundamental da doutrina de MDO, quando definitivamente operacional, empregará mísseis balísticos e de cruzeiro, armas hipersônicas e elementos de inteligência militar, operações de informações, defesa cibernética, GE e operações espaciais, visando a proporcionar múltiplas opções de ataque ao Cmt Op e gerar

múltiplos dilemas para o defensor.

Diferentes áreas de responsabilidade apresentam distintos desafios para a função de combate fogos. Consequentemente, o TFC deverá ser moldado de acordo com as necessidades operacionais de cada Comando Combatente Geográfico, agregando capacidades para prover o alcance e a letalidade necessários para contribuir com a dissuasão e, em caso de conflito, garantir vantagens operacionais e estratégicas para que o C Op obtenha êxito em suas missões.

REFERÊNCIAS

BRASIL. Exército. Estado-Maior. **EB20-MF-10.1022 Doutrina Militar Terrestre**. Brasília, DF: 2014.

CANTWELL, G.L. **Theater Army Role in Multi-Domain Operations. Integrated Research Project**. Disponível em: https://csl.armywarcollege.edu/usacsl/Publications/Theater%20Army%20Role%20in%20Multi-Domain%20Operations.pdf. Acesso em: 17 jul. 22.

DICKEY, C. **56th Artillery Command re-activates as Theater Fires Command in Wiesbaden**. Disponível em:https://www.army.mil/article/251803/56th_artillery_command_re_activates_as_theater_fires_command_in_wiesbaden. Acesso em: 22 jul. 22.

DYSSEAN, T. **What is a Combatant Command**. Disponível em: https://nationalinterest.org/blog/reboot/what-combatant-command-176257. Acesso em: 17 jul. 22.

EUA. Department of Defense. **Summary of the 2018 National Defense Strategy**. Disponível em: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. Acesso em: 15 jul. 22.

EUA. Department of the Army. Fires Center of Excellence. **Theater Fires Command – Separate (TFC-S). Operational and Organizational Concept.** Fort Sill: 2020.

EUA. Department of the Army. Headquarters. **2019 Army Modernization Strategy**. Disponível em: https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf. Acesso em: 15 jul. 22.

EUA. Department of the Army. Headquarters. **ADP 3-0 Operations**. Washington, DC: APD, 2019.

EUA. Department of the Army. Headquarters. **ADP 3-19 Fires**. Washington, DC: APD, 2019.

EUA. Department of the Army. Headquarters. **AR 10-87 Army Commands, Army Service Component Commands, and Direct Report Units.** Washington, DC: APD, 2017.

EUA. Department of the Army. Headquarters. **ATP 3-93 Theater Army Operations**. Washington, DC: APD, 2021.

EUA. Department of the Army. Headquarters. **FM 1-02.1 Operational Terms**. Washington, DC: APD, 2021.

EUA. Department of the Army. Headquarters. **FM 3-94 Armies, Corps and Division Operations**. Washington, DC: APD, 2021.

EUA. Department of the Army. Headquarters. **FM 6-0 Commander and Staff Organization and Operations**. Washington, DC: APD, 2022.

EUA. Department of the Army. Headquarters. **The Army Modernization Strategy**. Disponível em: https://www.army.mil/e2/downloads/rv7/the_army_strategy_2018.pdf. Acesso em: 15 jul. 22.

EUA. Department of the Army. Headquarters. **The Army Strategy**. Disponível em: https://www.army.mil/e2/downloads/rv7/the_army_strategy_2018.pdf. Acesso em: 17 jul. 22.

EUA. Department of the Army. TRADOC. **Pamphlet 525-3-1 The U.S. Army in Multi-Domain Operations 2028**. Virginia: 2018.

EVERSDEN, A. **The Army could get its next-gen Precision Strike Missile in FY27**. Disponível em: https://breakingdefense.com/2022/05/the-army-could-get-its-next-gen-precision-strike-missiles-in-fy27/. Acesso em: 20 ago. 22.

FEICKERT, A. **The Army's Mid-Range Capability (MRC) Weapon System** Disponível em: https://crsreports.congress.gov/product/pdf/IF/IF12135. Acesso em: 13 ago. 22.

FEICKERT, A. **The Army's Multi-Domain Task Force (MDTF)**. Disponível em:https://crsreports.congress.gov/product/pdf/IF/IF11797. Acesso em: 10 ago. 22.

FEICKERT, A. **The U.S. Army's Long-Range Hypersonic Weapon (LRHW)**. Disponível em:https://crsreports.congress.gov/product/pdf/IF/IF11991. Acesso em: 15 ago. 22.

MARANIAN, S. J; KABAT, M. K. **The King has Returned**. FA Journal. Fort Sill-OK, Issue 3, p. 23-26, 2022.

McENANY, C. **Multi-Domain Task Forces. A glimpse at the Army of 2035**. Disponível em: https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035. Acesso em: 10 ago. 22.

ROQUE, A. **US Army to receive four Mid-Range Capability battery prototypes, fielding set for 2023.** Disponível em: https://www.janes.com/defence-news/land-forces/latest/us-army-to-receive-four-mid-range-capability-battery-prototypes-fielding-set-for-2023. Acesso em: 26 ago. 22.

SHIMOOKA, RUSSEL K. **Third Multi-Domain Task Force activated for Indo-Pacific duty**. Disponível em:https://www.army.mil/article/260505/third_multi_domain_task_force_activated_for_indo_pacific_duty. Acesso em: 21 nov. 22.
SMITH, R. E; CARPENTER, R. W. **National Commission on the Future of the Army After Six Years**. Disponível em:https://www.ausa.org/publications/national-commission-future-army-after-six-years. Acesso em: 17 jul. 22.
U.S. ARMY EUROPE AND AFRICA. **Dynamic Front 22**. Disponível em: https://www.europeafrica.army.mil/What-We-Do/Exercises/Dynamic-Front/. Acesso em: 25 ago. 22.
U.S. ARMY EUROPE AND AFRICA. **2nd Multi-Domain Task Force**. Disponível em: https://www.europeafrica.army.mil/Units/2ndMDTF/. Acesso em: 25 ago. 22.
WHITLEY, J.E; MCCONVILLE, J.P. **On the Posture of the United States Army**. Statement before the Subcommittee on Defense – House Appropriations Committee – Unites States House of Representatives. Disponível em:https://www.army.mil/e2/downloads/rv7/aps/aps_2021.pdf. Acesso em: 15 jul 22.

NOTAS

[1] Período caracterizado pela incompatibilidade de interesses entre dois ou mais atores do sistema internacional que não pretendem agravar a situação e iniciar um conflito armado.
[2] Ação, atividade ou capacidade, geralmente de longo alcance, destinada a impedir a entrada de forças inimigas no teatro de operações.
[3] Ação, atividade ou capacidade, geralmente de curto alcance, destinada a limitar a liberdade de ação de uma força inimiga dentro do teatro de operações.
[4] É o espaço geográfico, terrestre, marítimo, aeroespacial e cibernético que seja ou possa ser diretamente envolvido nas operações militares de uma guerra. Um Teatro de Guerra pode comportar um ou mais Teatro de Operações.
[5] Operações conduzidas em espaços contestados visando a sobrepujar adversários (ou inimigos) por meio da convergência de efeitos oriundos de diversos domínios e da criação de dilemas táticos e operacionais.
[6] Área geográfica associada a um comando combatente onde o comandante tem autoridade para planejar e conduzir operações militares.
[7] Em 20 de novembro de 2020, o então Exército da África (USARAF) foi integrado ao Exército da Europa (USAREUR), formando o atual USAREUR-AF, responsável pelo emprego de tropas do EEUA nos dois continentes.
[8] Agência governamental federal, subordinada ao Departamento de Defesa dos EUA. É chefiada pelo Secretário do Exército e enquadra o EEUA.
[9] Situação que requer o emprego do poder militar em resposta a atividades terroristas, ações subversivas, desastres naturais ou outras ameaças, de acordo com determinação de autoridade competente, para preservação os interesses nacionais.
[10] Escalão de comando ativado para atuar como Força Terrestre Componente de um Comando Conjunto. Sua organização e estrutura de comando e controle permitem a coordenação do emprego de múltiplos corpos de exército, divisões de exército e brigadas multifuncionais.
[11] Emprego coordenado e sincronizado de fogos cinéticos e não cinéticos convergentes de dois ou mais domínios contra alvos designados em apoio à manobra de uma força conjunta.
[12] Convergência, no tempo e espaço, de efeitos em domínios e ambientes selecionados a fim de garantir o controle ou influência física, virtual e/ou cognitiva sobre uma determinada área, visando a dificultar o uso pelo inimigo e criar condições favoráveis ao uso por forças amigas.

SOBRE O AUTOR

O Tenente-Coronel de Artilharia Luiz Renato Laraia Pinheiro é Oficial de Ligação do Exército Brasileiro junto ao Fires Center of Excellence (FCoE), no Fort Sill, Oklahoma, Estados Unidos da América. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras (AMAN) em 2001. É mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) e possui o curso de Comando e Estado-Maior da Escola de Comando e Estado-Maior do Exército (ECEME). Realizou o Curso de Instrutor de Educação Física da Escola de Educação Física do Exército (EsEFEx) em 2005, o Curso de Operações na Selva – Cat A do Centro de Instrução de Guerra na Selva (CIGS) em 2015 e o Curso de Planejamento de Emprego do Sistema de Mísseis e Foguetes do Centro de Instrução de Artilharia de Mísseis e Foguetes (CI Art Msl Fgt) em 2020 (laraia.renato@eb.mil.br).



CORONEL CELSO
Oficial de Ligação no Centro de Doutrina e Treinamento do Exército Canadense, sediado em Kingston, província de Ontário – Canadá.

O ASPECTO POLÍTICO-ECONÔMICO DA MODERNIZAÇÃO DO NORAD PELO CANADÁ

O NORAD

O Comando de Defesa Aeroespacial Norte-americano (*North American Aerospace Defence Command*, NORAD, na sigla em inglês) é um órgão bilateral entre os Estados Unidos da América (EUA) e o Canadá, responsável pela defesa aeroespacial e alerta marítimo na América do Norte. As atividades tocantes aos espaços aéreo e sideral incluem a detecção, identificação e alerta de ataque contra a América do Norte, pelos mais diversos meios, como aeronaves, mísseis, veículos espaciais, dentre outros, bem como o engajamento contra a(s) ameaça(s). Essa atividade é realizada em conjunto com outros órgãos, como o *United States Northern Command* (USNORTHCOM, na sigla em inglês) [1], por exemplo. O NORAD tem papel central na segurança da América do Norte e importância relevante quanto à defesa do Ártico.

Em que pese o Comandante do USNORTHCOM também comandar o NORAD, há compartilhamento e participação do *Canadian Joint Operations Command* (CJOC, na sigla em inglês) [2] na estrutura de comando. Essa bilateralidade, com funcionamento desde os primeiros anos da década de 1950, tem peso significativo na esfera política canadense em relação a sua parceria com os EUA em matéria de defesa do país, de forma que o governo canadense reconhece que o nível de proteção proporcionado pelo NORAD não seria possível de ser alcançado individualmente.

No tocante ao sistema de alerta aeroespacial, o NORAD utiliza rede de satélites, estações de radares terrestres, radares acoplados em plataformas móveis e aeronaves de combate para detectar, interceptar e engajar a(s) ameaça(s), caso necessário. Quanto à detecção e ao monitoramento, o NORAD apoia agências civis no tocante a atividades aéreas suspeitas de tráfico de drogas. Embora o comando também esteja voltado para ameaças marítimas, o foco deste artigo será na modernização do sistema de detecção, monitoramento e alerta aeroespacial, sobretudo na região do Ártico e a cargo do Canadá.

O NORAD é divido em três regiões, a saber: a região do Alasca, *Alaskan NORAD Region* (ANR, na sigla em inglês); a região canadense, *Canadian NORAD Region* (CANR, na sigla em inglês) e a *Continental U.S. NORAD Region* (CONR, na sigla em inglês); cada uma delas com sede e responsabilidades territoriais distintas. As duas primeiras regiões são as responsáveis pelas ameaças vindas do Ártico. A 1ª Divisão Aérea Canadense, com sede em Winnipeg/Manitoba, é responsável por prover os meios aéreos de combate para a CANR.



Fig 1 - Aviões de combate CF-18 Hornet da Força Aérea Canadense e F-16 Fighting Falcon, F-22 Raptor e 2 B-52 Stratofortress da Força Aérea dos EUA sobre o Alasca em junho de 2021 no exercício Amalgam Dart 21-1, com a finalidade de adestrar as capacidades de Defesa do NORAD. Fonte:www.norad.mil/Images.

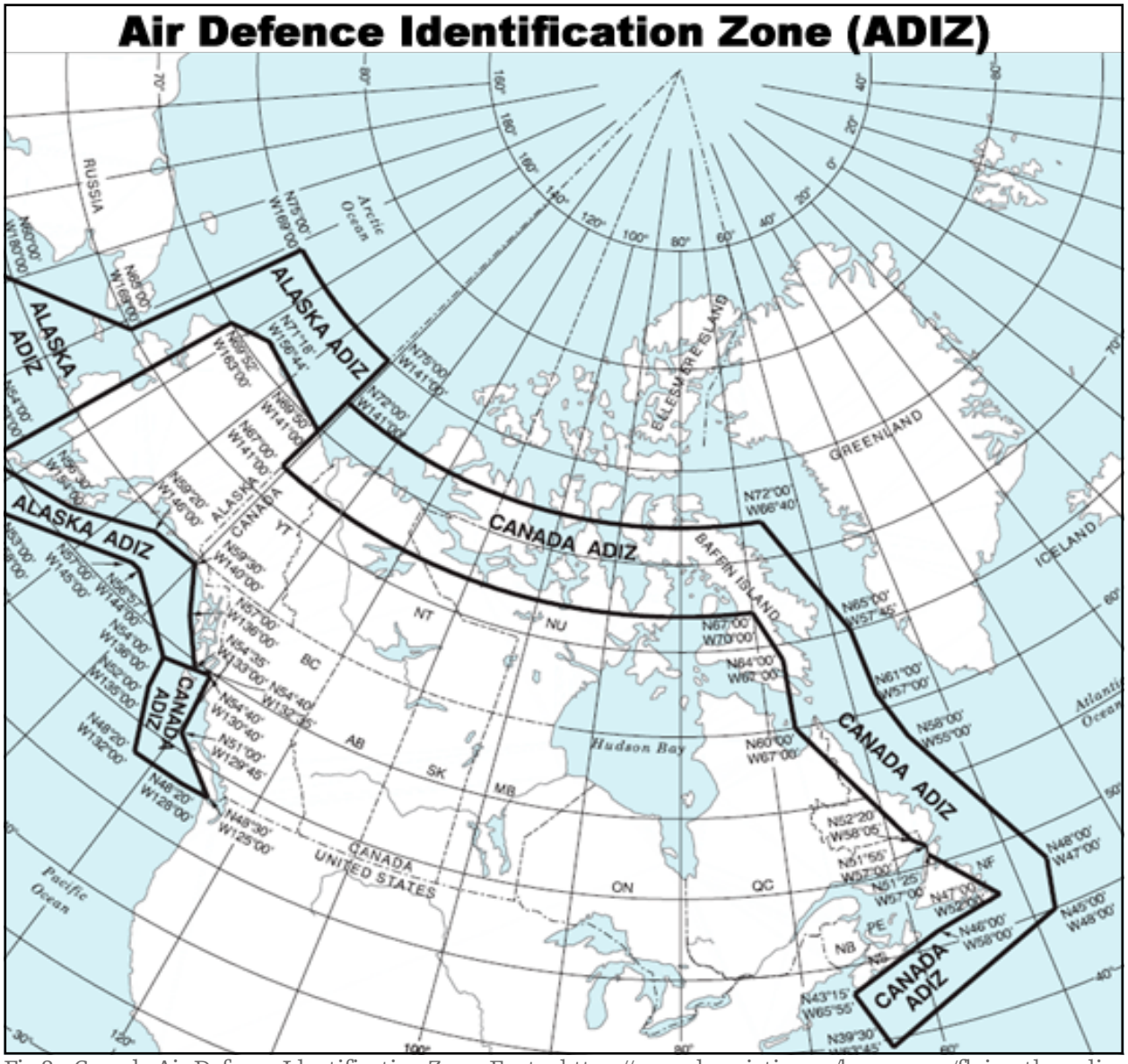


Fig 2 - Canada Air Defence Identification Zone. Fonte: https://www.bcaviation.ca/bcga-news/flying-the-adiz.

A OBSOLESCÊNCIA TECNOLÓGICA DO NORAD E SUAS NECESSIDADES

O NORAD, via *US Strategic Homeland Integrated Ecosystem for Layer Defense* (SHIELD, na sigla em inglês) [3], tem buscado desenvolver suas capacidades de sensoriamento aéreo e marítimo, conjugados com ferramentas de Comando e Controle em todos os domínios, a serem conectados a uma nova geração de sistemas antimísseis. Também foi identificada a necessidade do desenvolvimento das seguintes áreas: consciência situacional no amplo espectro; rápido processamento; análise e compartilhamento de dados; comando e controle; e identificação de alvos/ameaças com eficiência, de forma a proporcionar aos tomadores de decisão a resposta adequada (no tempo, espaço e proporcionalidade), de acordo com o grau e relevância da ameaça.

O NORAD tem lidado com o desafio de novas ameaças tecnológicas que envolvem esforços de modernização em um considerável ambiente de incertezas (VUCA) [4]. As estações de radar do *North Warning System* (NWS, na sigla em inglês) [5] têm mais de 30 anos, tendo seu último *update* nos idos dos anos 80, sob o acordo de modernização da defesa aérea norte-americana [6]. A previsão para essas estações alcançarem o fim de sua

operação é o ano de 2024. É um dos sistemas mais antigos relacionados com a Defesa da América do Norte. O atual sistema de detecção não é capaz de identificar e rastrear projéteis mais modernos, tais como munições hipersônicas, e certas categorias de veículos aéreos não tripulados (VANT) com envelopes de voo particulares (baixa velocidade e altura, por exemplo). Além disso, como foi projetado nos anos 1970, o NWS foi concebido para identificar e rastrear ameaças nucleares com envelopes de voo específicos. Também, devido ao tempo de operação e por não ter passado por modernizações, apresenta deficiências no tocante à proteção eletrônica e cibernética.

Em março de 2021, o NORAD e o USNORTHCOM emitiram um extrato de uma estratégia (princípios estratégicos), alinhado com as políticas de defesa norte-americana e canadense. Os princípios estratégicos e seus campos de atuação são:

1) **Integração Global** (*Global Integration* – GI, na sigla em inglês):

a) geografia (regiões avançadas, direções de aproximação e camadas de proteção);

b) domínios (ar, terra, mar, espaço, cibernético, espectro eletromagnético e cognitivo); e

c) ação governamental.

2) **Superioridade Decisória** (*Decision Superiority* – DS, na sigla em inglês):

a) entendimento dos dados distribuídos para a Consciência Situacional (*Domain Awareness* – DA, na sigla em inglês) e para o Domínio Informacional (*Information Dominance* – ID, na sigla em inglês); e

b) estabelecimento de múltiplas camadas de dissuasão, detecção, negação e, se necessário, contra-ataque a quaisquer agressões.

3) **Consciência Situacional** (*Domain Awareness* – DA, na sigla em inglês):

– investimentos na extensão da vida útil de estruturas ainda em operação, desenvolvimento de novas capacidades e inclusão de capacidades de consciência situacional de outros setores (além da Defesa).

4) **Domínio Informacional** (*Information Dominance* – ID, na sigla em inglês):

a) obtenção do ID, conectando/compartilhando dados/informação de sensores da DA com sensores da DS; e

b) rapidez na coleta, processamento, análise e disseminação de dados/informação por inteligência artificial e *machine learning*.

Do acima exposto, o foco do desenvolvimento tecnológico precisará se concentrar em sensores avançados capazes de detectar, rastrear e identificar diferentes vetores (foguetes, mísseis, VANT, *etc*) e suas plataformas de lançamento, bem como sistemas capazes de se contrapor a essas ameaças, as impedindo de alcançar alvos na América do Norte.

Além disso, o Canadá e os EUA visualizam a necessidade de fortalecer o NORAD com sensores/meios capazes de identificar ameaças abaixo da linha do combate tradicional, tais como ameaças nos campos eletromagnético e cibernético.

O DESCONGELAMENTO DO ÁRTICO

O Ártico, diferentemente da Antártica, que é um continente (com solo) coberto de gelo, é uma massa de água (daí o nome Oceano Ártico) que se apresenta congelada durante todo o tempo, mas que tem variações de tamanho, espessura e altura da área congelada durante o ano, com o gelo encolhendo ou crescendo de acordo com as estações climáticas.

Com as mudanças do clima e, sobretudo, o aquecimento das calotas polares, o Ártico, nos últimos 10 anos, tem perdido a característica de um obstáculo natural para embarcações de outros continentes em direção às Américas. Com o degelo anormal na região, novas passagens marítimas surgiram com o passar dos anos, abrindo caminho para o comércio de cargas, incremento da pesca, bem como para a possibilidade de exploração econômica de recursos minerais, sobretudo o petróleo e gás. Em 2009, uma pesquisa geológica norte-americana estimou que cerca de 30% de todo o gás e 13% do petróleo ainda não descobertos no planeta provavelmente estejam em latitudes acima do Círculo Polar Ártico.

Diversas expedições civis e militares têm se intensificado no Ártico nos últimos anos. Em setembro de 2017, um grupo de oficiais



Fig 3 - Militares do U.S. Army Northern Warfare Training Center em treinamento no Alasca.
Fonte: www.norad.mil/Images.

do alto escalão da Força Aérea e do Exército dos EUA, bem como outros especialistas, foram à região para verificar *in loco* os efeitos das mudanças climáticas, potenciais ameaças, presença de outros países e desafios logístico-operacionais na região. O grupo passou pelo Alasca, Groelândia e uma estação de alerta no extremo norte do Canadá, constatando o aumento da atividade humana na área.

Em outubro de 2020, a missão *Multidisciplinary Drifting Observatory for the Study of Arctic Climate* (MOSAiC, na sigla em inglês) [7], a maior e mais relevante expedição científica no Polo Norte, retornou à Alemanha após um ano de coleta de material para estudo sobre as mudanças climáticas e seus impactos no Ártico. A Agência Espacial Europeia (ESA, na sigla em inglês) também contribuiu e participou do estudo, fornecendo imagens do satélite de pesquisa ambiental, CryoSat, e realizando experimentos no gelo marinho no Ártico. A MOSAiC coletou milhares de amostras de gelo, água e ar, bem como realizou outros estudos científicos na região. Em que pese os dados ainda estarem em análise, a equipe identificou que parte do gelo ao norte da Groelândia havia derretido, permitindo que o navio Polarstern alterasse a sua rota, pegando um atalho para o Polo Norte em seu deslocamento.

O documento *Artic and Northern Policy Framework* (ANPF, na sigla em inglês), lançado pelo governo canadense em setembro de 2019, enfatiza que a mudança climática tem afetado o ecossistema no norte do Canadá, sobretudo no tocante à infraestrutura, saúde e bem-estar dos habitantes, bem como impactado as atividades econômicas na região. O ANPF ressalta que a província dos Territórios do Noroeste (*Northwest Territories* – NWT, na sigla em inglês) produziu menos dióxido de carbono que qualquer outra província canadense em 2016, mas, no entanto, o clima na região está esquentando de duas a quatro vezes mais rápido que a média do aumento da temperatura global.

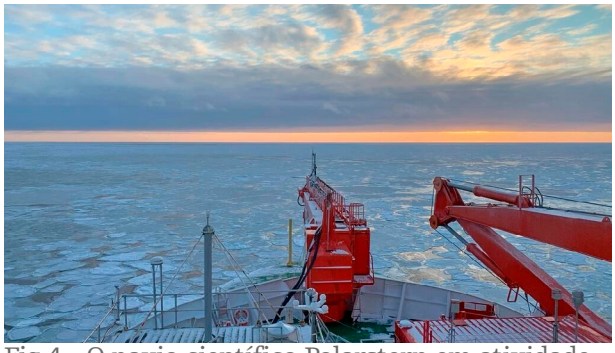


Fig 4 - O navio científico Polarstern em atividade.
Fonte: www.rfi.fr/en/science-and-technology/20201012-polarstern-world-s-biggest-arctic-expedition-returns-with-tales-of-dying-ice-mosaic-esa-climate-change.



Fig 5 - Vista de parte do arquipélago de Franz Josef Land. Fonte: www.thearcticinstitute.org.

BREVE CONTEXTO GEOPOLÍTICO E O AVANÇO MILITAR CHINÊS E RUSSO

Oito países possuem território ao norte do paralelo 60. São eles: Canadá, Dinamarca, EUA, Finlândia, Islândia, Noruega, Rússia e Suécia. Desses, apenas a Rússia, Finlândia e Suécia não fazem parte da Organização do Tratado do Atlântico Norte (OTAN), sendo que a Finlândia e a Suécia caminham para a entrada na Aliança. Em julho de 2022, os protocolos de adesão desses dois países foram assinados, marcando uma importante etapa no processo de entrada no Grupo.

Em 2007, a Rússia, a poucas milhas do Polo Norte, simbolicamente fincou uma bandeira russa no fundo do mar, reivindicando reservas de combustíveis fósseis na região. Desde 2012, os planos russos de modernização de sua capacidade militar no Ártico têm se expandido, com foco nas capacidades marítimas e aéreas, bem como com o aumento de efetivos militares na costa norte russa, de Murmansk à Chukotka. Em 2020, aproximadamente 15 incursões aéreas russas no espaço aéreo do Alasca foram registradas. Muito provavelmente, essas incursões tiveram como objetivo testar o nível de prontidão das defesas aeroespaciais norte-americana e canadense. Mais recentemente, em setembro de 2022, ainda durante o conflito entre a Rússia e a Ucrânia, a Rússia realizou manobras navais (exercício Umka-2022) no Mar de Chukchi, região à margem do Oceano Ártico, disparando mísseis de cruzeiro antinavio de dois submarinos nucleares, Omsk e Novosibirsk, em um navio-alvo localizado, aparentemente, no Ártico. A Defesa russa informou que esse exercício serviu para adestrar a prontidão do país em defender o Ártico russo.

Nas últimas décadas, a China tem emergido como uma nova superpotência econômica e militar, com aspirações políticas em diversas partes do globo. Em 2020, o Contra-Almirante Yin Zhin aconselhou autoridades políticas chinesas que o país deveria ter um papel de destaque na exploração econômica do Ártico, tendo em vista eles possuírem um quinto da população mundial. De forma que, além da Rússia, conforme abordado anteriormente, a China também tem aumentado a sua presença no Ártico.

Ainda em 2020, o Brigadeiro norte-americano Terrance O'Shaughnessy, ex-comandante do USNORTHCOM e do NORAD, relatou a um comitê do Senado dos EUA que as ameaças sobre o país e o Canadá eram reais e significativas, e que o Ártico não era mais uma muralha de proteção contra adversários; que os oceanos se tornaram eixos de progressão para sistemas avançados de armas convencionais, sendo o Ártico a nova fronteira de defesa do território norte-americano, provendo aos países inimigos uma nova direção de aproximação, representando uma mudança estratégica no tocante a área de responsabilidade norte-americana.

Nos últimos anos, com a saída dos EUA de diversos tratados que restrigiam o emprego de mísseis balísticos [8], a Rússia e a China tem buscado, em contrapartida, se equiparar às capacidades norte-americanas nesse campo, modernizando os seus arsenais nucleares, de forma a sobrepujar as defesas antimísseis dos EUA. Recentemente, o Centro de Estudos Internacionais e Estratégicos (*Center for Strategic and International Studies*), nos EUA, afirmou que as ameaças balísticas externas têm se desenvolvido em alcance, quantidade e eficiência. Soma-se a esse panorama o fato de, nos últimos anos, outros países inimigos dos EUA, como a Coreia do Norte e o Irã, seguirem com seus programas nucleares, de forma que o primeiro alcançou êxito em 2006. Seguindo na linha temporal, em 2010, os EUA e a OTAN iniciaram a colocação de mísseis balísticos e sistemas de defesa contra mísseis

> **A guerra entre Rússia e Ucrânia, iniciada em fevereiro de 2022, no campo político, foi o evento externo que fortemente contribuiu para acelerar o processo decisório da modernização do NORAD, por parte do Canadá.**

na Europa, sob a narrativa de proteção dos países da OTAN contra eventuais foguetes/mísseis lançados pelo Irã.

Dessa forma, com esse ambiente geopolítico pouco favorável em relação à restrição de desenvolvimento de capacidades balísticas estratégicas, a Rússia, antes mesmo da invasão do território ucraniano em fevereiro de 2022, havia desenvolvido mísseis de cruzeiro avançados, hipersônicos [9], capazes de atingir o território canadense e norte-americano via Ártico, saindo do norte da Rússia. A edição (*volume*) 19.2 do *Canadian Army Journal* ilustra, como exemplo, que um míssil de cruzeiro supersônico russo Kalibr-M, lançado de território russo, com a finalidade de atingir o território norte-americano, muito provavelmente teria como trajetória o Ártico e o espaço aereoespacial canadense.

Até o final de 2020, em que pese a questão da modernização do NORAD ser uma das prioridades da política da Defesa Canadense (*Strong, Secure, Engaged* – SSE, na sigla em inglês), não havia dotação orçamentária para ela. Durante anos, o governo canadense vinha se valendo dos investimentos e gastos militares proporcionados pelos EUA quanto à defesa da América do Norte. No entanto, a partir da administração Donald Trump [10], a disposição do governo norte-americano em contribuir desequilibradamente em acordos binacionais e/ou multinacionais diminuiu, de forma que a atenção canadense quanto à Defesa começou a mudar de maneira mais significativa. No começo de 2021, o Presidente norte-americano, Joe Biden, em conversa com o Primeiro-Ministro (PM) canadense, Justin Trudeau, reforçou a importância da defesa continental e da modernização do NORAD.

Todavia, os anos de 2020 e 2021 prejudicaram o início do investimento público nessa modernização, tendo em vista a pandemia da Covid-19, que canalizou os gastos públicos no Canadá, bem como em muitos outros países, para o combate à doença e seus reflexos socioeconômicos.

A guerra entre Rússia e Ucrânia, iniciada em fevereiro de 2022, no campo político, foi o evento externo que fortemente contribuiu para acelerar o processo decisório da modernização do NORAD, por parte do Canadá. Muitos dos cenários que planejadores e especialistas sobre o NORAD vinham alertando aos decisores canadenses, nos últimos anos, têm ocorrido no conflito.

Por exemplo, o emprego de mísseis hipersônicos e mísseis de cruzeiro avançados por parte da Rússia, bem como a demanda da Ucrânia aos EUA e OTAN, por material de emprego militar avançado, relacionado à defesa antiaérea/aérea. Assim, em maio de 2022, poucos meses após o início do conflito, a Ministra da Defesa Canadense (MDC), Anita Anand, anunciou que o Canadá está estudando a possibilidade de se juntar ao BMD *program* [11], uma vez que o país havia rejeitado o convite no passado. Em junho de 2022, o governo canadense declarou que irá investir cerca de US$ 5 bilhões no NORAD nos próximos 6 anos, em torno de 40% do total, enquanto os EUA irão investir cerca de US$ 7 bilhões.

O ESFORÇO DE MODERNIZAÇÃO DO NORAD PELO CANADÁ E OS ÚLTIMOS EVENTOS RELACIONADOS

O Canadá, com aproximadamente 40% de seu território acima do paralelo 60° e com 162.000 km de costa com o Oceano Ártico, é um país com forte interesse na região, sobretudo quando se leva em conta o aspecto psicossocial, bem como a dimensão socioeconômica, tendo

em vista que considerável proporção de indígenas canadenses habitam o norte do país, sejam aqueles que originalmente viviam na região (*Inuit*), sejam aqueles que foram deslocados para o norte ao longo do tempo (*First Nations* e *Métis*).

O governo canadense reconhece que a qualidade de vida dos habitantes de regiões mais ao norte do país é menor daqueles que vivem mais ao sul, de forma que a falta de investimentos em infraestrutura de transporte, energia e comunicações no norte canadense torna a vida mais dispendiosa na região, bem como não atrai investimentos privados. Há cinquenta anos, o governo canadense tem reconhecido a necessidade de desenvolver economicamente o norte do país, bem como tem buscado meios de fazê-lo de forma sustentável, respeitando o meio ambiente, os direitos dos povos indígenas e as especificidades das culturas e meios de subsistência locais.

O Canadá se comprometeu a modernizar o *North Warning System* em parceria com os EUA, desenvolvendo um novo sistema de monitoramento espacial capaz de rastrear ameaças acima da linha do horizonte, especificamente na região ártica, bem como um sistema de comunicações mais eficiente que cubra toda a região. No entanto, especialistas afirmam que, para isso, serão necessárias criatividade e novas abordagens pelo governo canadense, tendo em vista os grandes desafios ligados à infraestrutura, logística, vigilância, detecção e interceptação. Por exemplo, a necessidade dos equipamentos (de apoio e finalísticos) serem capazes de suportar condições climáticas hostis (temperatura negativa extrema, nevascas, ventos, *etc*) encarece a empreitada. Uma característica que se busca alcançar ao longo desse processo de modernização é que, dentro do possível, suas estruturas tenham uso dual, devido às situações já abordadas anteriormente. Existe, também, a previsão de que o novo sistema seja capaz de monitorar as alterações climáticas no Ártico.

A modernização do NWS precisará também estar consonante com uma rede de detecção multicamadas ao redor do mundo, uma vez que projéteis, inteligentes ou não, hipersônicos ou não, podem ser lançados de diferentes plataformas (aéreas, terrestres, marítimas, subaquáticas, móveis ou estacionárias) e de diferentes lugares. Recentes conversas no alto nível político entre os EUA e Canadá sinalizaram que os EUA estão dispostos a compartilhar *know-how* de sistemas/tecnologias restritas (*very classified systems*) com o Canadá, bem como incrementar a troca de inteligência no mais alto nível, via *Five Eyes* [12]. Nos últimos anos, o Canadá vinha adotando uma postura mais isolada do grupo, de forma que o compartilhamento de inteligência no mais alto nível era mais significativo entre os EUA, Reino Unido e Austrália.

A modernização do NWS também estará alinhada com investimentos na estrutura física de comunicações no Canadá, sobretudo mais ao norte, bem como na aquisição/desenvolvimento de modernos MEM, tais como aeronaves (Lockheed Martin F35, Airbus A310-300), belonaves, armas e instalações físicas de maneira geral.

Outra questão que impacta na modernização do sistema foi levantada na SSE, que identificou tendências chaves que continuarão a impactar e moldar os eventos, sendo a rápida evolução tecnológica um problema a ser considerado. A modernização de sistemas e sensores que compõem o NORAD, além de vultosa, levará anos para se concretizar. Um problema decorrente que especialistas têm dado atenção é sobre o descompasso tecnológico, onde se questiona se, ao final do processo de modernização, a estrutura final estará adequada para enfrentar as ameaças/desafios tecnológicos do momento futuro.

Em junho de 2022, a MDC anunciou que o Canadá irá investir 38,6 bilhões de dólares canadenses (CAD) nos próximos 20 anos na modernização das capacidades canadenses do NORAD. Desse montante, aproximadamente 16 bilhões serão alocados

para a construção de nova infraestrutura e modernização da infraestrutura de operações aéreas já existentes. Além disso, juntamente com o Chefe do Estado-Maior da Defesa canadense, em agosto de 2022, a Ministra Anita Anand visitou a 5ª Base Aérea de Goose Bay, unidade cuja missão principal é apoiar as operações do NORAD. Durante a visita, ela destacou que a unidade e outras quatro ao norte do país serão modernizadas nos próximos anos.

Os CAD 22 bilhões restantes serão distribuídos, aproximadamente, da seguinte forma: 7 bilhões na modernização do sistema de vigilância (NWS) mais 4,3 bilhões no *update* no C3 (comando, controle e comunicações) desse sistema; 6,4 bilhões na modernização do sistema de armas da Força Aérea canadense, via aquisição de novos mísseis ar-ar para a nova geração de caças (Lockheed Martin F35); por fim 4,3 bilhões voltados para a P&D na área da Defesa.



Fig 6 - Passagem do Noroeste. Fonte: https://www.britannica.com/topic/Hudsons-Bay-Company.

Em agosto de 2022, o Secretário-Geral da OTAN, Jens Stoltenberg, esteve no Canadá por 3 dias, visitando uma estação de radar do NWS e uma estação de pesquisa no Ártico, em Cambridge Bay/Nunavut, e a Base Aérea canadense em Cold Lake/Alberta. Na ocasião, o PM canadense e o representante da OTAN ressaltaram a importância do Ártico como proteção do flanco norte e oeste da Aliança, em um ambiente de crescimento da competição geopolítica mundial, em que pese ainda existir alguma divergência sobre a soberania do Canadá em parte do Ártico (Passagem do Noroeste) [13] entre o Canadá, os EUA e a OTAN.

Na primeira semana de setembro de 2022, o navio HMCS Max Bernays foi entregue à Real Marinha Canadense (RCN, na sigla em inglês). A embarcação, construída pelo estaleiro Irving Inc em Halifax/Nova Escócia, é o terceiro de seis navios patrulhas costeiras e do Ártico (*Artic and Offshore Patrol Ship* – AOPS, na sigla em inglês). Eles são resultado da Estratégia Nacional de Construção Naval, bem como de aumento da presença do país no Ártico (alinhamento com a SSE). Os AOPS aumentarão a capacidade da presença armada da RCN em águas canadenses, incluindo o Ártico.



Fig 7 - Cerimônia de entrega do navio HMCS Max Bernays à Real Marinha Canadense. Fonte: Disponível na página oficial do Facebook das Forças Armadas Canadenses – Canadian Armed Forces – publicação de 01/09/2022.

CONSIDERAÇÕES FINAIS

Há algumas décadas, o cenário internacional dava indícios de que a Rússia caminhava para um regime democrático nos padrões ocidentais e a China estabeleceria bons laços diplomáticos e políticos com a América do Norte. As mudanças geopolíticas dos últimos anos acabaram por contribuir com a disposição do governo canadense em aumentar parte do orçamento nacional destinado à Defesa. O Canadá já vinha sendo pressionado pelos membros da OTAN, sobretudo pelos EUA, nesse quesito nos últimos anos. No entanto, como não havia ameaça relevante no horizonte, também não havia disposição política para o incremento das despesas públicas no campo militar.

A ofensiva russa na Ucrânia, em fevereiro de 2022, que na percepção ocidental sinalizou que a Rússia não tem respeitado os limites estabelecidos pelas normas internacionais, provocou a centelha que faltava para o governo canadense mostrar disposição em modernizar o NORAD, inclusive desequilibrando a abordagem política mais defensiva e não-cinética do país diante de possíveis ameaças externas. Nesse tópico, em 2015, o PM canadense, Justin Trudeau, havia declarado que o desenvolvimento do sistema de defesa de mísseis balísticos estava fora de cogitação. Em 2017, ele ratificou essa oposição. No entanto, em 2022, com a sinalização do montante financeiro para a modernização do NORAD, bem como declarações públicas da alta administração do país sobre o assunto, verifica-se uma abordagem mais proativa em relação à Defesa, que pode, inclusive, mudar a política canadense em relação ao desenvolvimento e estabelecimento de armas cinéticas de longo alcance em seu território.

O NORAD, bem como a sua modernização, mostra a importância de parcerias internacionais no tocante a grandes projetos, quando esses buscam atingir objetivos convergentes de diferentes países. É natural e compreensível que cada Estado busque independência plena em matéria relacionada à sua soberania. No entanto, a realidade vem imprimindo restrições aos gastos com

a Defesa, sobretudo nos países democráticos e, mais especificamente, nos países em desenvolvimento, como o Brasil. Isso se deve ao fato da opinião pública ter, cada vez mais, pressionado seus governos em questões relacionadas com a segurança pública, educação, saúde, infraestrutura e programas de transferência de renda. O exemplo do NORAD, principalmente por parte do Canadá, ilustra a busca da otimização da aplicação dos recursos destinados à Defesa no país.

O caso em tela pode servir de estímulo para o Brasil e países da América do Sul buscarem algumas soluções conjuntas no tocante à defesa de seus territórios. O Sistema Integrado de Monitoramento de Fronteiras (SISFRON) [14] é um exemplo de estrutura de grandes proporções destinada à Defesa Nacional, via vigilância da fronteira terrestre brasileira; e de Segurança Pública, via ações governamentais contra delitos transfronteiriços e ambientais. No entanto, seu custo recai sobre o Exército Brasileiro, consumindo considerável montante do orçamento anual da Força. É possível que nos campos político, militar e socioeconômico existam interesses convergentes com outros países sul-americanos no monitoramento da fronteira terrestre ou parte dela.

O NORAD também ilustra a interação e cooperação entre forças singulares e órgão civis em atividades ligadas à Defesa e à Segurança dos EUA e Canadá. Soma-se a isso, o caráter dual que a modernização terá que alcançar, sobretudo no tocante ao acompanhamento da mudança climática na região. Não obstante, a modernização do sistema, por parte do Canadá, buscará ir ao encontro de anseios econômicos e sociais das comunidades mais isoladas do país, em destaque para comunidades indígenas que, nos últimos anos, têm aumentado a sua participação política, levando seus problemas e anseios para o debate nacional.

Como dito anteriormente, a modernização do NORAD, por parte do Canadá, enfrentará grandes obstáculos, sendo alguns bem correlatos com aspectos geoeconômicos brasileiros, como o desafio logístico e a busca pelo desenvolvimento socioeconômico de região remota do país, atendendo aos anseios de comunidades locais e indígenas. Há, também, o caráter dual que se pretende alcançar, com o sistema monitorando o clima. Ou seja, o Canadá terá que lidar com questões que são similares às do Brasil, não na mesma proporção e intensidade, mas de relevância considerável para o país, como as dificuldades logísticas no estabelecimento/manutenção do monitoramento de extensa área.

A temática da modernização do NORAD também reforça a importância que deve ser dada à manutenção da vida útil e o constante aperfeiçoamento de estruturas ligadas à Defesa Nacional. Em que pese, por vezes, a ameaça ou o perigo parecer distante, mudanças no tabuleiro geopolítico internacional, como o surgimento de novos atores, ou ações estatais expansionistas, sobretudo aquelas conduzidas à margem do arcabouço jurídico internacional, ressaltam a importância de um país estar sempre apto a defender a sua soberania. A recuperação (modernização, desenvolvimento ou aquisição) de determinada capacidade relacionada à Defesa, há muito ultrapassada, poderá demandar certo lapso temporal, do qual o País talvez não venha a dispor, quando a ameaça se apresentar.

REFERÊNCIAS

BRASIL. **Integrando capacidades na vigilância e na atuação em nossas fronteiras.** EPEx. Disponível em: http://www.epex.eb.mil.br/index.php/sisfron. Acesso em: 08 de set. 22.

BRASIL. **Rússia realiza exercícios militares no mar Ártico em frente ao Alasca.** CNN Brasil. Disponível em https:// www.cnnbrasil.com.br/internacional/russia-realiza-exercicios-militares-no-mar-artico-em-frente-ao-alasca/. Acesso em: 21 de set. 22.

BRITANNICA. **Northwest Passage.** Disponível em: https://www.britannica.com/topic/Hudsons-Bay-Company. Acesso em: 1º de set. 22.

CANADA. **Artic and Northern Policy Framework**. 2019. Disponível em: https://www.rcaanc-cirnac.gc.ca/eng/1560523306861/1560523330587. Acesso em: 24 de ago. 22.

CANADA. **Canada considering actively defending against intercontinental ballistic missiles**.

CTV News. Disponível em: https://www.ctvnews.ca/politics/canada-considering-actively-defending-against-intercontinental-ballistic-missiles-anand-1.5896519. Acesso em: 30 de ago. 22.
CANADA. **Defence Minister Anita Anand visits 5 Wing Goose Bay and highlights NORAD modernization**. National Defence. Disponível em: https://www.canada.ca/en/department-national-defence/news/2022/08/defence-minister-anita-anand-visits-5-wing-goose-bay-and-highlights-norad-modernization.html?utm_campaign=dnd-mdn-dt-news-22-23&utm_medium=eml&utm_source=dtnews-aug-30&utm_content=nr-norad-en-220830. Acesso em: 1º de set. 22.
CANADA. **The Five Eyes**. Public Safety Canada. Disponível em: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-en.aspx. Acesso em: 8 de set. 22.
CANADA. **Royal Canadian Navy Announces Ship's Sponsor for HMCS Max Bernays**. National Defence. Disponível em: https://www.canada.ca/en/department-national-defence/news/2022/05/royal-canadian-navy-announces-ships-sponsor-for-hmcs-max-bernays.html. Acesso em: 2 de set. 22.
CANADA. **Strong, Secure, Engage - Canada's Defence Policy**. 2017. Disponível em: https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf. Acesso em: 24 de ago. de 22.
CANADA. **The Canadian Army Journal**. Volume 19.2. Kingston: Army Publishing Office, 2021. Disponível em: https://publications.gc.ca/collections/collection_2021/mdn-dnd/D12-11-19-2-eng.pdf. Acesso em: 08 de set. 22.
CANADIAN ARMED FORCES. Royal Canadian Navy. **Our Navy Family is growing!** Canadá, 01/09/2022. Disponível em www.facebook.com/CanadianForces. Acesso em 02/09/2022.
CANADIAN JOINT OPERATIONS COMMAND. National Defence. Disponível em: https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-joint-operations-command.html. Acesso em: 23 de ago. 22.
CANADIAN NORAD REGION.]. Disponível em: https://www.norad.mil/About-NORAD/Canadian-NORAD-Region/. Acesso em: 31 de ago.22.
KORDA, Matt. **Joining the U.S missile defence program would be a big mistake**. Toronto Star. Disponível em: https://www.thestar.com/opinion/contributors/2022/05/20/joining-the-us-missile-defence-program-would-be-a-big-mistake.html. Acesso em: 8 de set. 22.
LACHENBAUER, Paul W; BOUFFARD, Troy; TEEPLE Nancy. **The Artic and North American Defence.** revista VANGUARDA The Forum for Canada's Security and Defence Community, volume 28, número 2, abril e maio de 2021. East Gwillimbury, Canadá.
MARCH, Bill. **Continental Air Defence and NORAD Modernization.** revista VANGUARDA The Forum for Canada's Security and Defence Community, volume 29, número 3, junho e julho de 2022. East Gwillimbury, Canadá.
MORROW, Amanda. **Biggest ever Artic expedition returns with tales of dying ice**. RFI. 12/10/2020. Disponível em: https://www.rfi.fr/en/science-and-technology/20201012-polarstern-world-s-biggest-arctic-expedition-returns-with-tales-of-dying-ice-mosaic-esa-climate-change. Acesso em: 3 de ago. 22.
NATO. **Finland & Sweden Accession.** Disponível em: https://www.nato-pa.int/content/finland-sweden-accession. Acesso: 24 de ago. 22.
NATO. **NATO Secretary General wraps up visit to Canada**. Disponível em: https://www.nato.int/cps/en/natohq/news_206960.htm. Acesso em: 31 de ago. 22.
NORAD. Disponível em: https://www.norad.mil/About-NORAD/. Acesso em: 4 de ago. 22.
POWER AND POLITICS WITH VASSY KAPELOS. **Canada spending nearly $5B to modernize NORAD**. Gen Tom Lawson. CBC LISTEN. 20/06/2022. Disponível em: https://www.cbc.ca/listen/cbc-podcasts/123-power-and-politics/episode/15920292-canada-spending-nearly-dollar5b-to-modernize-norad?featuredPodcast=true&. Acesso em: 24 de ago.22.
POWER AND POLITICS WITH VASSY KAPELOS. **NATO secretary general tours Canada's North**. CBC LISTEN. 26/08/2022. Disponível em: https://www.cbc.ca/listen/cbc-podcasts/123-power-and-politics/episode/15933175-nato-secretary-general-tours-canadas-north. Acesso em 31 de ago. 22.
SHERMAN, Jason. **Forging a SHIELD for the homeland.** Air Force Magazine, janeiro de 2021. Disponível em: https://www.airforcemag.com/article/forging-a-shield-for-the-homeland/. Acesso em: 22 de ago.22.
SHERMAN, Jason. **The Arctic heats up.** Air Force Magazine, novembro de 2017. Disponível em: https://www.airforcemag.com/article/the-arctic-heats-up/. Acesso: 22 de ago. 22.
VAZQUES, Rafael. **O que é a OTAN e quais são os países que fazem parte da Organização.** Valor, fevereiro de 2022. Disponível em: https://valor.globo.com/mundo/noticia/2022/02/25/o-que-e-a-otan-e-quais-sao-os-paises-que-fazem-parte-da-organizacao.ghtml. Acesso em: 24 de ago. 22.
US NORTHERN COMMAND. Disponível em: https://www.northcom.mil/About/. Acesso em: 22 de ago. 22.

NOTAS

[1] *United States Northern Command,* USNORTHCOM em inglês - é o Comando estadunidense que planeja, organiza e cumpre missões de Defesa e apoia operações civis. Forças podem ser atribuídas ao USNORTHCOM sempre que necessário, uma vez que o órgão tem poucas forças subordinadas permanentemente. O Comandante do órgão também comanda o NORAD.
[2] *Canadian Joint Operations Command,* CJOC em inglês - é a estrutura militar, subordinada à Defesa Canadense (Ministério da Defesa do Canadá), permanentemente ativada, que comanda as Forças Armadas Canadenses em operações domésticas e internacionais. O órgão também trabalha em estreita cooperação com outros elementos em operações, tais como departamentos e agências do Governo Canadense, Forças Armadas de países aliados ou que compartilhem objetivos comuns de Defesa, e organizações multinacionais, como a OTAN e as Nações Unidas.
[3] *US Strategic Homeland Integrated Ecosystem for Layer Defense,* SHIELD em inglês - é a estratégia dos EUA em relação ao NORAD, que visa fortalecer os setores aéreos e marítimos dos EUA, a fim de aumentar a dissuasão contra invasores externos sobre o território norte-americano.
[4] VUCA – O termo, cunhado nos EUA no século passado, é um acrônimo das palavras volátil/volatilidade (*volatile/volatility*), incerto/incerteza (*uncertain/uncertainty*), complexo/complexidade (*complex/complexity*) e ambíguo/ambiguidade (*ambiguous/ambiguity*). Tem sido muito utilizado para descrever o cenário mundial contemporâneo, que tem se apresentado com essas características, bem como para vislumbrar o futuro.
[5] *North Warning System,* NWS em inglês - foi criado nos anos 1980, no contexto da Guerra Fria e da modernização do sistema anterior, o *Distant Early Warning* (DEW). O NWS é um sistema estacionário e de defesa passiva, composto por um conjunto de estações remotas automáticas de radares, cobrindo o norte do Canadá, do Alasca e a costa oeste da Groelândia. O NWS é vital para o controle do espaço aéreo no NORAD.
[6] *North American Air Defence Modernization*, NAADM em inglês.
[7] Missão MOSAiC (*Multidisciplinary Drifiting Observatory for the Study of Arctic Climate* – Observatório Multidisciplinar para o Estudo do Clima Ártico). A missão custou aproximadamente 140 milhões de euros e envolveu 600 pesquisadores de vários países.
[8] Tratado *Anti-Ballistic Missile* (ABM, na sigla em inglês), Tratado de Forças Nucleares de Alcance Intermediário (*Intemediater-Range Nuclear Forces Treaty*) e do Tratado dos Céus Abertos (*Open Sky Treaty*).
[9] Nos últimos anos, a Rússia desenvolveu uma nova categoria de mísseis balísticos (*hypersonic glide vehicles*, HGV em inglês), tanto lançados de plataformas aéreas (*air-launched cruise missiles*), como lançados de plataformas terrestres (*ground-lauched cruise missiles*). Eles podem alcançar velocidades acima de *Mach* 5 e são manobráveis.
[10] Donald Trump foi o 45º Presidente dos EUA, de janeiro de 2017 a janeiro de 2021.
[11] *US (Homeland) Ballistic Missile Defence program* – Programa Norte-americano de Defesa contra Mísseis Balísticos.
[12] *Five Eyes* é a aliança no campo da Inteligência entre os EUA, Austrália, Canadá, Nova Zelândia e Reino Unido.
[13] *Northwest Passage* - Passagem do Noroeste: trecho marítimo que liga a região do Mar do Labrador, a NE do Canadá, ao Mar de Bering, região a W do Alasca e NE da Rússia.
[14] Sistema Integrado de Monitoramento de Fronteiras, SISFRON - sistema de sensoriamento e apoio à decisão em suporte ao emprego operacional, cujo objetivo é fortalecer a presença e a capacidade de monitoramento e ação do Estado brasileiro na faixa de fronteira terrestre.

SOBRE O AUTOR

O Coronel de Artilharia Leonardo Celso de Almeida Alves é Oficial de Ligação do Exército Brasileiro no Centro de Doutrina e Treinamento do Exército Canadense. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras (AMAN) em 1996. Concluiu o Curso de Piloto de Aeronaves no Centro de Instrução de Aviação do Exército (CIAvEx) em 2001, o Curso de Aperfeiçoamento de Oficiais na Escola de Aperfeiçoamento de Oficiais (EsAO) em 2004 e o Curso de Comando e Estado-Maior na Escola de Comando e Estado-Maior do Exército (ECEME) em 2016. É Mestre em Ciências Militares pela EsAO. Foi observador militar das Nações Unidas na Costa do Marfim em 2008. Serviu na Aviação do Exército por mais de 10 anos. Comandou o 2º Centro de Geoinformação (2º CGEO) em 2018 e 2019 (celso.alves@eb.mil.br).



MAJOR DIOGO LUIZ
Oficial de Operações do Centro de Defesa Cibernética.

A EXPLORAÇÃO E O ATAQUE CIBERNÉTICO

Muito se comenta sobre como o domínio cibernético tem se ampliado e como ele também é intrínseco aos demais domínios naturais: terra, mar, ar e espaço. O fluxo constante de dados pelo ciberespaço faz parte do cotidiano da sociedade brasileira, que está cada dia mais conectada. Uma nova fronteira, até então inexistente, foi aberta, sendo imperativo guarnecê-la. Temas ligados à atuação estatal e não estatal nesse ambiente têm sido tratados por uma ampla gama de entidades e assuntos, como soberania, legalidade e legitimidade das ações cibernéticas, estando na ordem do dia de instituições e indivíduos.

As Forças Armadas, acompanhando a evolução dos tempos, têm buscado garantir que o poder nacional brasileiro seja também manifestado no domínio cibernético. Esse ambiente possui particularidades específicas e necessita de capacidades e competências peculiares para sua efetiva utilização no âmbito de operações militares.

A Doutrina de Operações Conjuntas, referência doutrinária brasileira mais atual sobre a Guerra Cibernética, divide a Capacidade Cibernética em três capacidades operativas [1]: proteção cibernética, exploração cibernética e ataque cibernético.

A proteção cibernética é o conceito que causa menos dificuldade de compreensão. Ela representa o escudo que garante o funcionamento dos dispositivos computacionais do teatro (TO) ou área de operações (A Op) e que provê a proteção contra ações de exploração e ataque do oponente. A proteção é uma atividade de caráter permanente.

Por outro lado, exploração e ataque cibernéticos possuem conceitos distintos em diferentes referências. É de suma importância que os planejadores e executantes conheçam os limites de cada atividade para que haja um correto exercício do comando e para que limites estabelecidos não sejam transpostos.

Por estar em um domínio essencialmente artificial, a doutrina da defesa e da guerra cibernética obedecem a uma dinâmica de evolução mais veloz. Enquanto a ordem natural possui leis consideradas imutáveis do ponto de vista humano, o espaço cibernético está em permanente transformação, exigindo que os guerreiros que atuam nesse ambiente estejam em constante atualização. É plenamente compreensível que táticas, técnicas e procedimentos (TTP) cibernéticos devam se atualizar em uma frequência mais rápida que a de TTP aplicáveis aos outros domínios e que conceitos estabelecidos possam e devam ser revisados continuadamente.

ATAQUE CIBERNÉTICO

O ataque cibernético é uma capacidade operativa [2] que guarda estreita relação com a Função de Combate Fogos. Sua definição é dada pela doutrina de operações conjuntas: "conduzir ações sobre dispositivos, redes de computadores e comunicações do oponente para causar efeitos cinéticos e não-cinéticos". De acordo com o manual, o ataque cibernético busca atingir os seguintes objetivos ou efeitos:

> 1) destruir ou degradar equipamentos e sistemas, provocando baixas e/ou danos permanentes ou temporários, que sejam favoráveis à operação do TO/A Op;
> 2) degradar a capacidade de operação do oponente no campo de batalha, reduzindo a eficácia de funcionamento dos seus sistemas;
> 3) corromper dados de sistemas do oponente, manipulando informações de interesse do TO/A Op;
> 4) negar o acesso do oponente a sistemas de interesse do TO; e
> 5) interromper o funcionamento de sistemas do oponente que tragam vantagem ao TO.

Em virtude das características da guerra cibernética, para que o ataque cibernético seja realizado, faz-se necessária a exploração do ambiente cibernético de maneira a se obter o comando e controle de um sistema inimigo. Essa situação demanda o investimento de tempo, recursos financeiros e a aplicação de uma expertise sobre o espaço cibernético.

Normalmente, algumas etapas são seguidas para que seja possível julgar que determinada tropa cibernética é capaz de realizar um ataque, a saber:

1) **Reconhecimento:** o alvo é analisado de maneira a se encontrar uma ou mais vulnerabilidades que possam ser exploradas. Nessa etapa, os dados e informações encontradas em fontes abertas (*Open Source Inteligence* – OSINT, na sigla em inglês) são fundamentais. Um trabalho de engenharia social deve ser executado para levantar costumes e características do alvo ou de indivíduos ligados a ele ou, ainda, forçá-lo a proporcionar informações, tudo com o fim de se levantar uma vulnerabilidade passível de ser explorada. Essa etapa demanda um longo tempo e não deve ser desprezada. Quanto melhor for o reconhecimento executado, maiores serão as chances de êxito de um ataque cibernético.

2) **Armamento:** uma arma cibernética é desenvolvida para explorar a vulnerabilidade encontrada, objetivando provocar um determinado efeito. Um *exploit* específico é utilizado carregando consigo um *payload* para executar o efeito desejado. O *malware* desenvolvido precisa ser específico e suficientemente eficaz para escapar das defesas existentes no ambiente lógico a ser atacado.

3) **Entrega:** o artefato é disponibilizado ao alvo. Entendendo o alvo como um sistema [3], busca-se fazer com que o alvo tenha acesso ao *malware* desenvolvido. Diversas estratégias são empregadas para que a rede ou o ativo visado seja colocado em contato com o artefato desenvolvido. Muitas vezes, o ser humano é o vetor a ser explorado a fim de se acessar uma rede. Uma campanha de *phishing* ou mesmo *spear-phising* pode ser empregada para que determinado ator, previamente identificado, receba um e-mail com conteúdo malicioso. Em algumas vezes, uma vulnerabilidade até então desconhecida (e para qual ainda não há correção) é identificada e a entrega é realizada sem a necessidade da interação com um alvo humano.

4) **Exploração:** a ativação do *payload* é realizada e o *malware* é instalado no objetivo. Normalmente, essa etapa é dependente da participação do usuário, que habilita involuntariamente o código malicioso.

5) **Instalação:** O *malware* se consolida no alvo. Uma conexão com o exterior da rede visada é garantida por uma *backdoor* e a persistência dentro do alvo é estabelecida.

6) **Comando e Controle:** o atacante se estabiliza completamente dentro do alvo aproveitando o canal de comunicação estabelecido. A capacidade de realizar movimentos laterais na rede é explorada e a possibilidade de se fazer busca e exfiltração de dados e informações se torna uma realidade.

7) **Ações Objetivas:** uma vez que o comando e controle é estabelecido, o atacante pode executar ações para conseguir os efeitos desejados. Os efeitos de destruir, degradar, corromper dados, negar o acesso ou impedir o funcionamento podem ser plenamente alcançados.

O modelo apresentado toma por base o conceito da *cyber kill chain* e foi elaborado pela empresa fabricante de produtos de defesa *Lockheed Martin* para identificar e prevenir a atividades cibernéticas intrusivas. Esse *framework* ilustra muito bem os passos que um atacante precisa executar até conseguir provocar um efeito sobre um alvo. O ataque é somente a ação final de "detonar uma bomba", que foi customizada para penetrar nas defesas de um determinado alvo particular. A capacidade operativa de ataque cibernético só pode ser considerada factível por um



Fig 1 - Cyber Kill Chain® Lockheed Martin. Fonte: https://danieldonda.com/cyber-kill-chain/

decisor, se o comando e controle já tiver sido providenciado. Toda a ação anterior que prepara o terreno para a detonação da bomba, pela doutrina mais atual, não faz parte do ataque, mas sim da exploração cibernética.

> **“Assim como uma Bateria de Busca de Alvos dotada de radares e sistemas remotamente pilotados está intrinsecamente ligada à função de combate fogos, mas age como um vetor importantíssimo na função de combate inteligência, a tropa que realiza a exploração cibernética também atua nas duas funções de combate.”**

EXPLORAÇÃO CIBERNÉTICA

Segundo o MD30-M-01 – Doutrina de Operações Conjuntas (2020), toda a cadeia anterior às ações objetivas (ataque cibernético) está inserida no conceito da Exploração Cibernética, a saber: “mapear sistemas e ativos de informação presentes no Espaço Cibernético de interesse do TO/A Op [4], identificar vulnerabilidades e realizar a preparação para futuras ações ofensivas.”

Faz-se necessário desconflitar esse conceito com o previsto no manual do Exército EB70-MC-10.232 – Guerra Cibernética (2017). Enquanto o manual do Exército Brasileiro (EB), mais antigo, identifica a exploração cibernética como uma capacidade de “conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados”, igualando a exploração à inteligência cibernética; o manual do Ministério da Defesa (MD), mais atual, conceitua a exploração como uma etapa a ser realizada para a execução de um ataque.

Vale salientar que o manual EB70-MC-10.244 – Corpo de Exército (2020) já define a exploração cibernética em consonância com o manual do MD, ampliando o escopo da atividade e afastando-se do que postula o manual Guerra Cibernética.

A definição do MD está alinhada com o que prevê a doutrina conjunta dos Estados Unidos da América. O JP 3-12 – Cyberspace Operations, descreve uma gama de atividades incluídas nas ações de exploração do ciberespaço (*cyberspace exploitation)*. Para aquela nação, a exploração engloba tanto as atividades afetas a inteligência quanto as atividades preparatórias para a obtenção de um efeito (afetas ao ataque cibernético).

> A exploração cibernética inclui operações correntes e futuras por meio de ações como obter e manter acesso a redes, sistemas e nós com valor militar, manobrar para posições vantajosas e posicionar capacidades cibernéticas para facilitar operações futuras. [tradução nossa]

A Junta Interamericana de Defesa (JID) descreve o funcionamento de um ataque cibernético utilizando o modelo da *cyber kill chain*, ilustrando as diversas etapas que devem acontecer para que a obtenção de um efeito seja conseguida.

De acordo com a doutrina interamericana, o ataque cibernético se caracteriza pelo uso deliberado de uma arma cibernética para gerar um efeito prejudicial nas redes e sistemas de informação de um adversário, podendo ter efeitos indiretos no âmbito de operações convencionais.

Quando se refere aos tipos de operações, a JID define que a exploração cibernética se refere a procedimentos passivos ou ativos orientados a obtenção da informação necessária para a planificação e condução de operações cibernéticas defensivas e ofensivas ou outras operações convencionais. Dado que as operações cibernéticas ofensivas são definidas como aquelas executadas nas redes de adversários ou terceiros com a finalidade de causar um efeito cibernético ou um efeito físico, elas são dependentes de uma exploração

prévia, que permita a obtenção desses efeitos.

Em resumo, as doutrinas mais atuais, tanto do Brasil como de outros países, vinculam a possibilidade de um ataque cibernético à necessidade de uma exploração prévia. Da mesma maneira que um avião precisa ser armado, que uma bateria precisa entrar em posição e possuir um sistema de busca de alvos e que um torpedo precisa ser acondicionado no navio para que esses atuadores cinéticos possam atingir seus alvos e obter os efeitos desejados, uma tropa cibernética precisa explorar o ambiente cibernético para possibilitar a obtenção de um efeito do ataque do atuador não cinético. Vale salientar que a exploração já possui um caráter ofensivo e que a tropa opera em um "terreno inimigo".

A exploração, no entanto, pode se limitar a um reconhecimento em fontes abertas, agindo de maneira passiva. Nesse caso, não cumprirá sua missão precípua de preparar o terreno para a realização de um ataque. Essa preparação terá que, invariavelmente, realizar ações intrusivas.

Assim como uma Bateria de Busca de Alvos dotada de radares e sistemas remotamente pilotados está intrinsecamente ligada à função de combate fogos, mas age como um vetor importantíssimo na função de combate inteligência, a tropa que realiza a exploração cibernética também atua nas duas funções de combate. Quando se obtém o comando e controle para se realizar um ataque, o sistema do alvo já é plenamente conhecido e a extração de dados e informações passa a ser inteiramente possível.

Convém ressaltar que, muitas vezes, o decisor terá que optar entre obter um efeito (cinético ou não cinético) sobre um alvo ou permanecer com o comando e controle [5] de um determinado sistema para extrair dados e informações. Tem-se um exemplo prático: após instalar um *back door* em um sistema de comando e controle, ou mesmo de comunicações inimigo, um invasor pode apagar todos os dados do sistema, obtendo o efeito de degradar a capacidade de operação do inimigo, ou permanecer oculto no ambiente invadido para coletar informações sobre as posições das tropas inimigas no terreno. Uma escolha é feita: a cibernética será um atuador não cinético na função de combate fogos ou um vetor de busca de informações na função de combate inteligência. Ambas as ações exigem do guerreiro cibernético a adoção dos mesmos TTP, percorrendo toda a *cyber kill chain,* o que muda é apenas a provocação ou não de um determinado efeito na fase das ações objetivas.

A experiência tem mostrado que o sucesso de uma exploração cibernética é função do tempo investido nessa exploração, da expertise dos profissionais designados para essa tarefa e do volume de recursos financeiros disponibilizados para que os TTP possam ser executadas corretamente. Dessas variáveis, o tempo tem sido o fator com maior coeficiente. Quanto maior for a antecedência na designação de alvos para a cibernética, maior será a probabilidade de sucesso na coleta de dados e levantamento de informações, principalmente quando a atuação se limita a ações não intrusivas.

A CIBERNÉTICA COMO ATUADOR NÃO CINÉTICO DE FOGOS

No contexto do planejamento de fogos conjunto, a tropa cibernética é enquadrada como mais um atuador/vetor de fogos capaz de provocar efeitos sobre alvos previamente determinados. A etapa decidir do processo Decidir, Disparar, Detectar e Avaliar (D3A) busca definir, de antemão, quais os efeitos são desejados sobre quais alvos e quais são as tropas vocacionadas para obter esses efeitos. Como já explicitado, a possibilidade de ataque cibernético é diretamente dependente da exploração cibernética, o que demanda o investimento de tempo e recursos. Essa exploração, muitas vezes, terá de ser realizada desde os tempos pré-crise, o que acarreta a adoção de medidas para mitigar os riscos de se atuar no que se tem chamado de combate em zona cinzenta [6].

A Subseção de Guerra Cibernética, presente na Seção de Operações do Estado Maior Conjunto, é responsável por se integrar com os outros elementos de coordenação de fogos presentes nessa célula do Estado Maior Conjunto, a fim de apresentar as reais possibilidades de ataque dos Destacamentos de Guerra Cibernética presentes na campanha ou operação. A Proposta de Lista de Alvos da FCj G Ciber é, portanto, muito dependente da exploração cibernética previamente realizada.

Na reunião de Coordenação de Fogos, os alvos serão priorizados e será decidido qual o vetor de ataque será empregado sobre cada alvo, gerando a Lista Preliminar Integrada Priorizada de Alvos (LPIPA). Aspectos, como custo, tempo, possibilidades de cada tropa e riscos envolvidos, serão considerados para determinar qual meio provocará o efeito desejado sobre os alvos.

Após aprovação do comandante operacional (Cmt Op), a LPIPA deixa de ser provisória, tornando-se a Lista Integrada e Priorizada de Alvos (LIPA), e pode ser decomposta em Listas Priorizadas de Alvos (LPA) para cada Força Componente existente no TO ou A Op. A FCj G Ciber também receberá uma LPA contendo os alvos que devem ser batidos pelo atuador não cinético, a fim de cooperar com a obtenção do estado final desejado (EFD) estabelecido pelo Cmt Op.

PRIORIZAÇÃO DE ALVOS

A definição sobre qual atuador deverá bater cada alvo representa, em termos de força, espaço e tempo, como o comandante operacional visualiza a obtenção dos efeitos desejados que conduzem o esforço conjunto ao atingimento do EFD. Aspectos, como economicidade, riscos envolvidos para a tropa e para o cumprimento da missão, probabilidade de sucesso da investida, efeitos colaterais, além de vários outros fatores, são considerados para a escolha de um atuador em detrimento de outro.

Um ataque cibernético é normalmente mais econômico e envolto em menos riscos para a tropa. Em contrapartida, efeitos colaterais podem também existir no domínio cibernético, caso um *malware* destinado a um ativo escape para a rede mundial de computadores, afetando

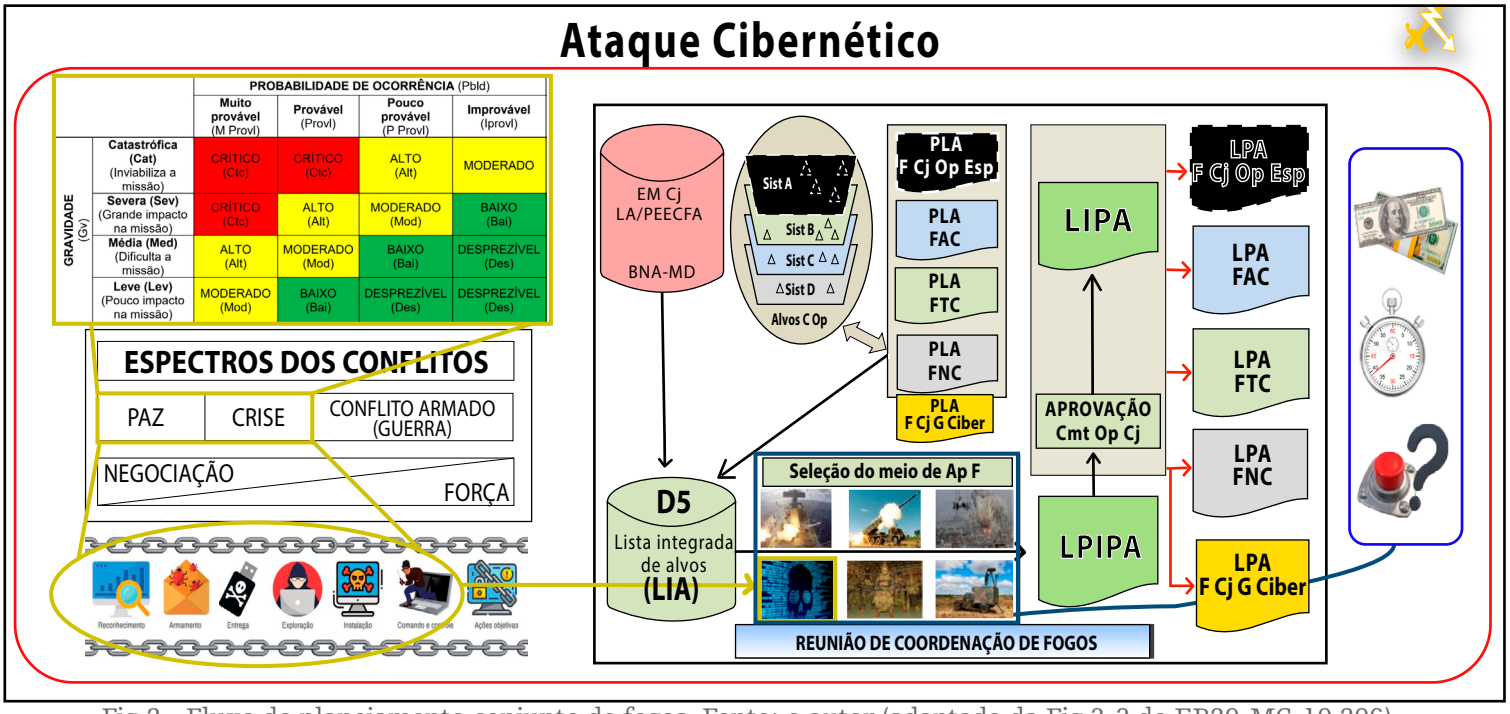


Fig 2 - Fluxo do planejamento conjunto de fogos. Fonte: o autor (adaptado da Fig 3-3 do EB20-MC-10.206).

Estados neutros, por exemplo. Em razão da artificialidade e da consequente mutabilidade do espaço cibernético, a probabilidade de sucesso de um ataque cibernético é um dado momentâneo e depende da exploração que foi realizada.

A Subseção de Guerra Cibernética é responsável por informar ao comandante qual a real capacidade da tropa cibernética para atingir os efeitos desejados. Enquanto os alcances da artilharia e o raio de ação dos aviões e navios são obtidos em função de dados reais, a capacidade da tropa cibernética só é conhecida após a realização da exploração. Daí a necessidade de se explorar o espaço cibernético desde os tempos pré-crise, tal qual faz-se necessário adquirir canhões e mísseis antes de a guerra começar.

CONSIDERAÇÕES FINAIS

A evolução tecnológica deixa um legado aos seres humanos ao ampliar a sua capacidade.

As limitações impostas pelo ambiente natural vão sendo vencidas e as Nações passam a contar com capacidades diversas para alcançar seus objetivos. O espaço cibernético foi desenvolvido como resposta da humanidade para lidar com o processamento de dados e com a automação de processos, gerando um ambiente que consolidou a globalização e possibilitou a alteração benéfica no modo de vida das pessoas.

Os interesses nacionais precisam ser mantidos também nesse novo domínio. A proteção dos ativos é uma necessidade constante e deve ser executada por cada ator que interage no ambiente cibernético.

As capacidades operativas de exploração e ataque representam a possibilidade de um país ampliar sua dissuasão para além do ambiente físico. Uma Nação não pode prescindir de seus canhões mesmo quando passa décadas sem travar guerras. Da mesma maneira, não se pode prescindir da capacidade de se obter efeitos no espaço cibernético e por meio dele.

REFERÊNCIAS

BRASIL. MINISTÉRIO DA DEFESA. GABINETE DO MINISTRO. **Portaria normativa Nr 3.010/MD, de 18 de novembro de 2020.** Aprova a Doutrina Militar de Defesa Cibernética (MD31-M-07).
BRASIL. MINISTÉRIO DA DEFESA. ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS**. Portaria normativa Nr 84/GM-MD, de 15 de setembro de 2020.** Aprova a Doutrina de Operações Conjuntas – MD30-M-01/Volumes 1 e 2 (2. ed. Brasília. 2020.
BRASIL. MINISTÉRIO DA DEFESA. EXÉRCITO BRASILEIRO. COMANDO DE OPERAÇÕES TERRESTRES. **Portaria Nr 42 – COTER, de 8 de junho de 2017.** Aprova o Manual de Campanha EB70-MC-10.232 Guerra Cibernética, 1ª ed. Brasília. 2017.
BRASIL. MINISTÉRIO DA DEFESA. EXÉRCITO BRASILEIRO. COMANDO DE OPERAÇÕES TERRESTRES. **Portaria Nr 66 – COTER, de 3 de junho de 2020.** Aprova o Manual de Campanha EB70-MC-10.244 Corpo de Exército, Edição Experimental. Brasília. 2020.
BRASIL. MINISTÉRIO DA DEFESA. EXÉRCITO BRASILEIRO. ESTADO MAIOR DO EXÉRCITO. **Portaria Nr 003-EME, de 5 de janeiro de 2015.** Aprova o Manual de Campanha EB20-MC-10.206. Fogos, 1 ed. Brasília. 2015.
EUA. SPECAL OPERATIONS COMMAND. **White Paper – The Gray Zone. 2015.** Disponível em: https://publicintelligence.net/ussocom-gray-zones/ Acesso em 11 set. 22.
EUA. Joint Chiefs of Staff. **Doctrine for the Armed Forces of the United States.** JP 3-12 Cyberspace Operations. Washington, DC: Joint Chiefs of Staff, 2018.
JUNTA INTERAMERICANA DE DEFENSA. **Guía de Ciberdefensa – Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.** Canadá, 2020.

NOTAS

[1] O Exército Brasileiro também chama essas Capacidades Operativas de Atividades.
[2] Segundo o Glossário das Forças Armadas, capacidade operativa é o conjunto de capacidades específicas de unidades/elementos constituintes de uma Força, orientadas para a obtenção de um efeito estratégico, operacional ou tático.
[3] O alvo é percebido com um conjunto de elementos interconectados. Muitas vezes o objetivo final é uma peça que não possui um acesso disponível, mas possui ligação com outras partes cujo acesso é mais facilitado. O servidor de uma empresa é muito seguro, mas às vezes é colocado em rede com um laptop de um agente que utiliza a mesma máquina na rede de sua residência. A entrega não será feita ao servidor, mas ao agente, para que, por meio de futuros movimentos laterais (manobra), seja possível acessar o servidor.
[4] Teatro de Operações ou Área de Operações.
[5] Referindo-se à penúltima etapa da ciber kill chain. Etapa que antecede às ações objetivas.
[6] A zona cinzenta é definida pelo US Special Operation Command como interações competitivas entre e dentro de atores estatais e não estatais que se situam entre uma guerra tradicional e uma paz dual.

SOBRE O AUTOR

O Major de Artilharia Diogo Luiz Oliveira de Andrade é Oficial de Operações do Centro de Defesa Cibernética. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras em 2005. Concluiu o Bacharelado em Ciências Econômicas pela Associação Educacional Dom Bosco em 2010, o Mestrado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) em 2013 e a Pós-Graduação em Ciências Militares pela Escola de Comando e Estado Maior do Exército (ECEME) em 2021. Realizou cursos na área segurança de rede de computadores e Artilharia de Mísseis e Foguetes. Cursou o Field Artillery Captains Career Course, em Fort Sill, EUA, o Curso de Armas Combinadas, na Escuela Superior Tecnológica del Ejército, Bolívia e realizou a capacitação em Ciberdefensa, da Junta Interamericana de Defesa (JID) (diogoluiz@cdciber.eb.mil.br).

Produção Doutrinária













Manuais aprovados no 4º trimestre de 2022

do C Dout Ex



“ A VITÓRIA TERRESTRE COMEÇA AQUI! ”



TENENTE-CORONEL JERÔNIMO
Instrutor da Academia de Guerra do Exército do Chile e Oficial de Ligação de Doutrina.

A CAPACIDADE CIBERNÉTICA NO EXÉRCITO DO CHILE

O ciberespaço ganha cada vez mais relevância no complexo cenário mundial. A globalização e o exponencial progresso tecnológico proporcionaram um avanço na era digital nunca experimentado.

Com esse avanço, iniciaram-se também as atividades ilícitas, criminosas e ofensivas no espaço cibernético, consubstanciando-se em uma nova ameaça para os estados-nação e demais organizações, afetando setores vitais dos países e, por consequência, atingindo também os cidadãos comuns.

A obra *La ciberguerra: sus impactos y desafíos*, publicada em 2018 pelo Centro de Estudos Estratégicos da Academia de Guerra (CEEAG) do Exército chileno, afirma que, em nível regional, os países que se destacaram como alvos de ciberataques, na América Latina, foram Brasil, Argentina, Colômbia, México e Chile. O acesso ou roubo de informações de um computador infectado predomina na região. Como exemplo, o autor cita uma família de códigos maliciosos – *Dorkbot* – que, em meados de 2016, gerou mais de 80.000 ações contra sistemas virtuais, concentrados no Chile (44%), Peru (15%) e Argentina (11%).

Assim, evidencia-se que a América Latina se configura como palco de inúmeros ataques cibernéticos, demonstrando ser uma região instável e insegura quanto à proteção de ativos no domínio cibernético.

Como consequência, o quinto domínio das operações militares – o ciberespaço – tem imprimido uma mudança no rol de atribuições das forças armadas, reorientando esforços e recursos para geração de novas capacidades para se contraporem às novas ameaças no ciberespaço, somado aos conceitos de zona cinza dos conflitos armados e guerra híbrida, com predominância de atores não estatais e ameaças difusas.

O Exército do Chile, visando gerar capacidades em face das necessidades atuais, projetou sua nova estrutura superior. Essas mudanças respondem aos novos cenários já mencionados, abarcando diferentes capacidades militares, otimizando recursos e sincronizando os respectivos atuadores.

Dentre essas mudanças, destaca-se o Comando de Operações Especiais (COPE), no final de 2020. O COPE está organizado com três brigadas operativas: Brigada de Operações Especiais (BOE), Brigada de Aviação do Exército (BAVE) e Brigada de Inteligência (BINTE). Trata-se de uma solução *sui generis*, pois reúne sob o mesmo comando as capacidades relacionadas às operações especiais, montanha, aviação, inteligência, guerra eletrônica e cibernética – sendo essas unidades preexistentes, mas que sob a égide de um comando único tem a expectativa de gerar uma sinergia e aumento dessas capacidades.

Cabe relembrar que se entende por capacidade como a aptidão requerida a uma força ou organização militar para cumprir determinada missão ou atividade. Essa aptidão é exercida sob condições e padrões determinados, pela combinação de meios para desempenhar uma gama de tarefas.

Ademais, a capacidade é obtida a partir de um conjunto de sete fatores determinantes, interrelacionados e indissociáveis: Doutrina, Organização (e/ou processos), Adestramento, Material, Educação, Pessoal e Infraestrutura – que formam o acrônimo DOAMEPI (Brasil, 2019).

Dessa forma, o objetivo do presente artigo é apresentar a atual situação da capacidade cibernética do Exército do Chile, segundo os fatores DOAMEPI.

> **Em nível regional, os países que se destacaram como alvos de ciberataques, na América Latina, foram Brasil, Argentina, Colômbia, México e Chile.**

O SETOR CIBERNÉTICO NO EXÉRCITO DO CHILE

O Chile adota um modelo, de forma similar à doutrina brasileira, onde a segurança cibernética representa um conceito mais amplo e abrangente, englobando as ações de defesa cibernética, de forma análoga à conhecida relação entre segurança e defesa nacional.

A defesa cibernética é a vertente do sistema segurança cibernética, a nível nacional, que reúne as capacidades das Forças Armadas para executar operações no ciberespaço. Assim, está focada na defesa e sobrevivência dos sistemas militares, bem como daqueles que são vitais para o bom funcionamento de diferentes órgãos estatais.

Outra importante observação é que suas

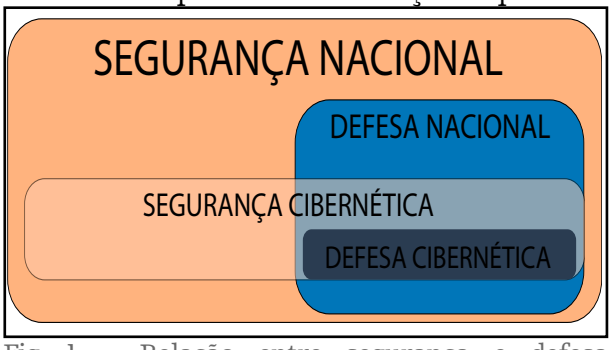


Fig 1 – Relação entre segurança e defesa cibernética. Fonte: o autor – adaptado de apresentação do Batalhão de Defesa Cibernética.

ações são respaldadas do ponto de vista jurídico, com base no princípio de legítima defesa, que permite o uso de capacidades militares de defesa cibernética ativa para lidar com ataques cibernéticos contra o Estado (MIRANDA, 2021).

Além disso, o Exército do Chile optou por subordinar a cibernética à função de combate inteligência, conforme o manual de defesa cibernética:

> As unidades e organizações de "Defesa Cibernética" constituem a parte dos meios institucionais de inteligência que são dedicados ao desenvolvimento de tarefas destinadas a proporcionar a devida segurança e proteção das informações institucionais que são armazenadas, processadas ou transmitidas pelos sistemas de informação do Exército, a fim de garantir disponibilidade, confidencialidade e integridade. (Regulamento RDI 20008 – Defesa Cibernética, 2016, p. 65)

Dessa maneira, a Diretoria de Planejamento de Informação do Exército (DIPLINE) representa o órgão de direção setorial de inteligência, contrainteligência, operações de informação e cibernética, sendo o escalão de mais alto nível do setor cibernético no exército. Cabe à DIPLINE aconselhar o Chefe do Estado-Maior no controle e coordenação das atividades executivas que, sob a autoridade da Brigada de Inteligência do Exército (órgão executivo), são realizadas pelas unidades de inteligência do Exército. (Ministério da Defesa Nacional, Decreto 305, 2021). Por sua vez, a BINTE é subordinada ao Comando de Operações Especiais.

Do exposto, infere-se que as atividades do setor cibernético estão concentradas na Brigada de Inteligência do Exército, subordinada ao Comando de Operações Especiais. Ou seja, não existe um órgão, no nível direção ou execução, que seja exclusivo para as atividades cibernéticas. Como efeito, pode-se gerar uma limitação da atuação e abrangência do setor cibernético, que em teoria deveria atuar de forma transversal com outras diretorias e órgãos, principalmente no tocante às ações de proteção cibernética, onde o usuário final também se torna protagonista do processo, representando o elo mais frágil ante uma tentativa hostil contra os sistemas próprios.

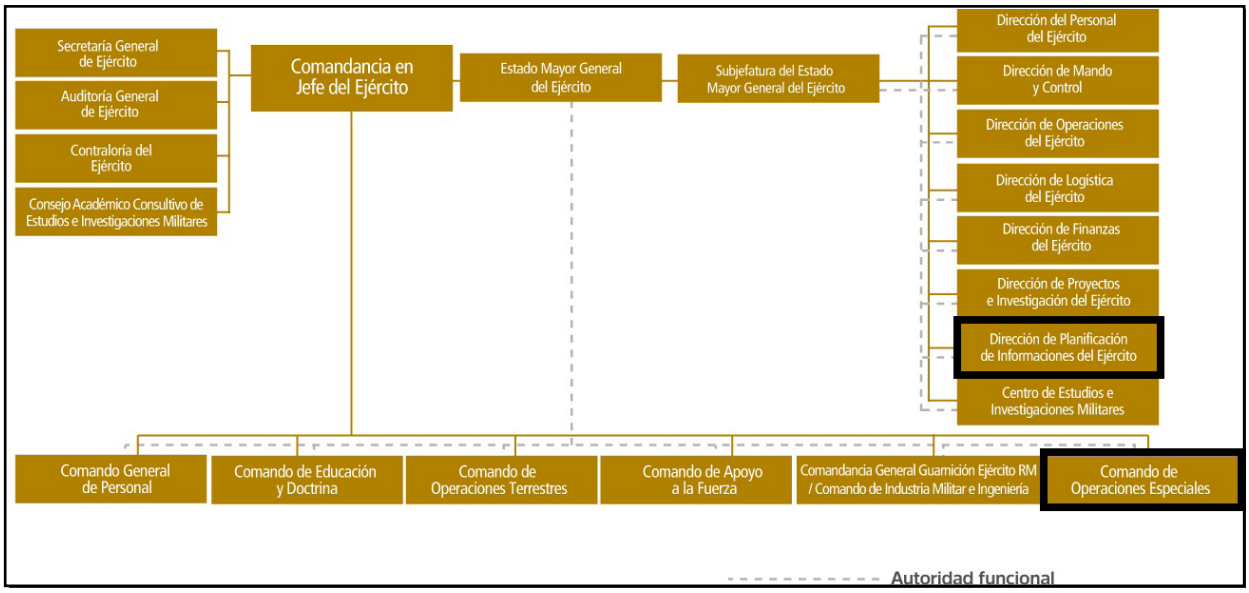


Fig 2 – Organização do Exército do Chile, com destaque para a DIPLINE e o COPE.
Fonte: Exército do Chile https://www.ejercito.cl/estructura-y-organizacion.

Outro fator importante é a fonte de recursos, que pode ter uma limitação em virtude da possível concorrência com outras áreas, como é o caso específico da inteligência, que está – pelo menos sob a ótica da organização – abrangendo a atividade cibernética.

Além disso, as Forças Armadas do Chile têm expressivo desenvolvimento das atividades conjuntas, sendo o Estado-Maior Conjunto (EMCO) o responsável pelo emprego das capacidades geradas pelas forças singulares. Entretanto, a capacidade cibernética, a nível conjunto, está em fase preliminar de implantação, não tendo uma estrutura organizada.

FATORES DOAMEPI - DOUTRINA

Segundo o manual Doutrina Militar Terrestre do Brasil, a doutrina é base para os demais fatores, estando materializado nos produtos doutrinários. Desse modo, a geração de capacidades de uma unidade ou força inicia-se com a formulação de sua base doutrinária, que considera a gama de missões (traduzida nas capacidades operativas), atividades e tarefas que essa unidade cumpre em operações.

A defesa cibernética, em nível institucional, tem sua base doutrinária no regulamento RDI - 20008 Defesa Cibernética, definindo a estrutura para a defesa cibernética no Exército do Chile.

Esse marco legal aborda os conceitos e definições próprios da cibernética, estipula o quadro jurídico sob o qual as ações relacionadas à defesa cibernética são enquadradas, estabelece a infraestrutura crítica a ser protegida e estipula os órgãos de ciberdefesa do exército. Além disso, relaciona a defesa cibernética com as funções primárias, enquadra a defesa cibernética no processo de planejamento militar e estabelece as tarefas a serem realizadas pela instituição em matéria de defesa cibernética.

Esse manual assegura a realização de operações cibernéticas ofensivas, contra pessoas, redes de computadores e sistemas C4I [1] adversário. Segundo Plum (2020), a previsão doutrinária de ataque cibernético outorga liberdade de ação à força, impactando positivamente na sua capacidade. Soma-se a isso, o emprego sistêmico previsto na doutrina em voga, que vislumbra tarefas para a capacidade cibernética em todas as operações – relacionando-as com as demais funções de combate e enquadrando-as dentro do contexto das operações de informação.

Observa-se que a doutrina abrange o nível mais alto da instituição, contudo existe uma lacuna para as ações táticas da Força Terrestre, com manuais e regulamentos voltados para as ações defensivas, que

abrange os usuários e sistemas empregados pela força e, também, ações ofensivas, para normatizar e orientar tais ações, visando o público alvo especializado.

ORGANIZAÇÃO E/OU PROCESSOS

Esse fator é materializado por intermédio da estrutura organizacional dos elementos de emprego da Força Terrestre (F Ter). Algumas capacidades são obtidas por processos, com vistas a evitar competências redundantes, quando essas já tenham sido contempladas em outras estruturas (Brasil, 2019).

Como mencionado, a Brigada de Inteligência é o órgão executivo do setor cibernético. Essa Grande Unidade de Inteligência possui dois regimentos de inteligência, sendo que o Regimento de Inteligência Nº 2 "Llaitún" reúne as capacidades cibernética e guerra eletrônica, materializadas pelo Batalhão de Defesa Cibernética (Figura 3) e o Batalhão de Guerra Eletrônica.

missão executar operações militares no ciberespaço, com o propósito de garantir o livre uso do domínio cibernético de interesse militar e manter a proteção das infraestruturas críticas institucionais, bem como obter informações relevantes para o sistema de inteligência do exército.

A Companhia de Operações Cibernéticas Defensivas cumpre um rol duplo de atribuições, pois além de ser uma estrutura voltada para a guerra, também desempenha o papel de centro de tratamento de incidentes de rede ou CSIRT - Computer Security Incident Response Team (CSIRT, na sigla em inglês), sendo uma estrutura permanentemente ativada.

O setor cibernético, no Exército do Chile, a nível de direção, está organizado com uma estrutura não vocacionada especificamente para atividade no domínio cibernético. Porém, no nível tático, o Batalhão de Defesa Cibernética se destaca de maneira positiva.

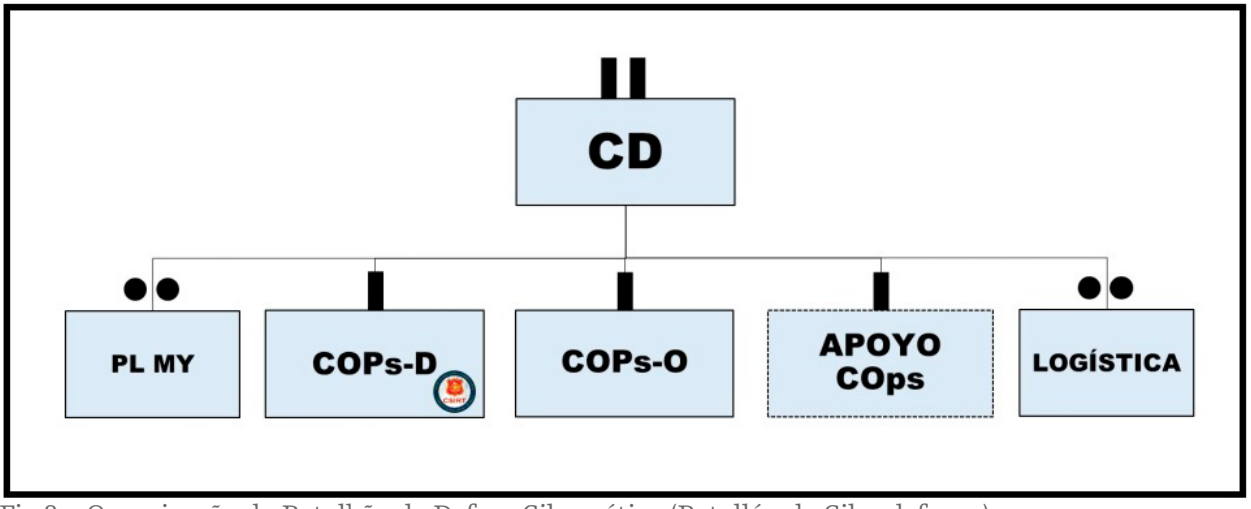


Fig 3 – Organização do Batalhão de Defesa Cibernética (Batallón de Ciberdefensa).
Fonte: Batalhão de Defesa Cibernética – palestra institucional.

O Batalhão de Defesa Cibernética está organizado a uma companhia de operações cibernéticas defensiva (COPs-D), uma companhia de operações cibernéticas ofensiva (COPs-O), uma companhia de apoio às operações cibernéticas (Apoyo COps), uma seção de estado-maior e uma seção logística. Essa OM Ciber tem como

ADESTRAMENTO

Compreende as atividades de preparo, obedecendo a programas e ciclos específicos, incluindo a utilização de simulação em todas as suas modalidades: virtual, construtiva e viva.

O adestramento das subunidades do Batalhão de Defesa Cibernética chileno

é realizado, principalmente, por meio da participação de suas subunidades em exercícios militares. O ciclo de adestramento é uma das áreas que se encontra em fase inicial de desenvolvimento, não se observando programas padrão de adestramento como em outras capacidades.

Além disso, a Companhia de Operações Cibernética Defensiva participa do Exercício de Simulação de Gestão de Segurança Cibernética para Funcionários Públicos, organizado pelo CSIRT governamental, realizado em parceria com a empresa de segurança cibernética Kaspersky e aberto aos funcionários do Estado e empresas membros do Sistema de Empresas Públicas (CHILE, 2022). Trata-se de uma simulação realista de um incidente de cibersegurança, guardando semelhanças com o Exercício Guardião Cibernético, realizado pelo Comando de Defesa Cibernética (ComDCiber), do Exército Brasileiro.

MATERIAL

A Doutrina Militar Terrestre (2019) preconiza que o fator material compreende todos os materiais e sistemas para uso na F Ter, acompanhando a evolução de tecnologias de emprego militar e com base na prospecção tecnológica. É expresso pelo quadro de distribuição de material dos elementos de emprego e inclui as necessidades decorrentes da permanência e sustentação das funcionalidades desses materiais e sistemas durante todo o seu ciclo de vida.

Segundo Miranda (2021), o Batalhão de Defesa Cibernética aumentou sua capacidade em termos do material implementado para realizar suas funções – hardware e principalmente softwares, porém, sua principal dificuldade é representada pela obsolescência tecnológica em parte da infraestrutura crítica a ser salvaguardada, definida pela instituição. Tudo isso porque existem diferentes organizações encarregadas dos dados de pessoal, planejamento de operações militares e administração dos recursos que, como resultado dessa obsolescência, não conseguiram migrar para plataformas mais modernas e seguras. E isso se traduz em uma maior exposição às ameaças cibernéticas.

Por outro lado, em relação aos recursos financeiros destinados à aquisição de materiais e outros investimentos e custeio do setor cibernético, existe um Plano de Desenvolvimento Estratégico do Exército que priorizou a capacidade cibernética, garantindo um fluxo contínuo de recursos.

EDUCAÇÃO

Compreende todas as atividades continuadas de capacitação e habilitação, formais e não formais, destinadas ao desenvolvimento do integrante da Força Terrestre quanto à sua competência individual requerida. Essa competência deve ser entendida como a capacidade de mobilizar, ao mesmo tempo e de maneira interrelacionada, conhecimentos, habilidades, atitudes, valores e experiências para decidir e atuar em situações diversas.

No Exército do Chile, a vertente educação é de responsabilidade setorial do Comando de Educação e Doutrina (CEDOC), que tem, por um lado, a responsabilidade pela geração de doutrina por meio da Divisão de Doutrina (DIVDOC) e, por outro, é responsável pelo sistema de educação militar através da Divisão de Educação (DIVEDUC).

Contribuindo com o setor cibernético, a Academia Politécnica Militar (ACAPOMIL) ministra o Curso Técnico Avançado de Defesa Cibernética, fornecendo pessoal permanente com competências necessárias para atuar como administradores da rede de defesa cibernética, bem como no Batalhão de Defesa Cibernética. O curso é destinado a engenheiros militares, com conhecimentos avançados na área e constitui um nível superior de educação militar sobre o assunto.

O Exército do Chile estabeleceu uma linha de carreira para os cabos profissionais [2], na linha de ensino militar bélico, na área de defesa cibernética, que inclui cursos ministrados tanto pela Escola de Telecomunicações (ESCTEL) como pela Escola de Inteligência (ESCINT). A ESCTEL está vocacionada para as atividades de proteção cibernética, visando preservar os

ativos próprios do Exército do Chile. Assim, essa instituição de ensino possui um centro de treinamento em telecomunicações, que inclui em suas instalações o Centro de Treinamento CISCO e o Laboratório de ensino e treinamento de rede – onde são ministrados cursos de treinamento e especialização. Como exemplo, cita-se os cursos CISCO CCNA [3], que são orientados para a entrega de habilidades para desenvolver redes seguras, reconhecer ameaças e vulnerabilidades de rede e mitigá-las, mantendo a integridade, confidencialidade e disponibilidade de dados e serviços. Ao mesmo tempo, esse pessoal tem especialização secundária em guerra eletrônica e, uma vez que tenham recebido ambos os treinamentos, estão prontos para serem treinados pela Escola de Inteligência.

Após concluir os treinamentos específicos de cibernética e guerra eletrônica, os militares seguem para ESCINT, onde frequentam o curso básico de inteligência militar, que será uma especialização orientada para os conhecimentos preconcebidos na área de cibernética e guerra eletrônica. Dessa forma, o ciclo de educação está completo e os militares estão aptos para aplicar os conhecimentos adquiridos. Com o treinamento fornecido em ambas as escolas, a instituição recebe um cabo da arma de Telecomunicações, especialista em guerra eletrônica e inteligência, que desenvolveu as habilidades técnico-profissionais para trabalhar em redes e sistemas de defesa cibernética.

Infere-se que o Exército do Chile desenvolveu uma adequada solução para o aperfeiçoamento técnico-profissional das praças, gerando uma linha de carreira para os sargentos da instituição no campo da defesa cibernética. Porém, não há medidas similares com relação à especialização de oficiais.

PESSOAL

Abrange todas as atividades relacionadas aos integrantes da força, nas funcionalidades: plano de carreira, movimentação, dotação e preenchimento de cargos, serviço militar, higidez física, avaliação, valorização profissional e moral. É uma abordagem sistêmica voltada para a geração de capacidades, que considera todas as ações relacionadas com o planejamento, a organização, a direção, o controle e a coordenação das competências necessárias à dimensão humana da Força.

No âmbito do fator pessoal, o Exército do Chile conta com um plano de carreira para os cabos profissionais, como descrito no fator educação, que visa ao preenchimento de cargos no setor cibernético, principalmente na área de proteção cibernética. Da mesma forma, a ACAPOMIL desenvolve um programa com o Curso Técnico Avançado de Defesa Cibernética, que permite habilitar pessoal em um nível mais avançado para atividades no setor cibernético.

Contudo, no Exército do Chile não existe a previsão para uma carreira de oficiais dedicados ao domínio cibernético. Assim, o fluxo de pessoal na direção e controle, que é desempenhado pelos oficiais, não apresenta uma sistemática ou padronização.

INFRAESTRUTURA

Engloba todos os elementos estruturais (instalações físicas, equipamentos e serviços necessários) que dão suporte ao preparo e ao emprego dos elementos da F Ter, de acordo com a especificidade de cada um e o atendimento aos requisitos do exercício funcional.

Cabe ressaltar que a infraestrutura de proteção cibernética é mais ampla e transversal a todo exército. De modo contrário, a infraestrutura relacionada às ações ofensivas são mais específicas e restritas a unidades militares de cibernética.

A implementação da infraestrutura física relativa ao setor cibernético tem sido gradual, de acordo com o Plano de Desenvolvimento Estratégico já mencionado. Tudo isso, refletiu-se em um aumento considerável no número de instalações do Batalhão de Defesa Cibernética, desde sua criação. Miranda

(2021) afirma que a infraestrutura é um dos pontos fortes da unidade, devido ao fato de que a instituição tem feito um esforço significativo para melhorar as condições da unidade, materializados pela construção dos pavilhões das companhias de operações cibernéticas.

CONSIDERAÇÕES FINAIS

Em síntese, ao término da análise dos fatores DOAMEPI, é possível consolidar os principais fatores positivos e negativos, evidenciados no presente artigo, relativos à capacidade cibernética no Exército do Chile, sintetizada por uma matriz SWOT [4].

Exército do Chile adotou, subordinando o setor cibernético ao sistema de inteligência. A implantação de uma área estratégica sob a direção da DIPLINE e execução do COPE é sublinhada com ressalvas, pois a especificidade do setor cibernético certamente exigirá uma estrutura com maior vocação para essa atividade. Soma-se a isso a falta de um curso de especialização para oficiais no aspecto educação e pessoal.

Sob a óptica dos fatores externos, ressalta-se como fator positivo o marco legal, representado pela Política Nacional de Defesa Cibernética e o conteúdo do Plano de Desenvolvimento do Exército, que estão impulsionando a capacidade

	FATORES POSITIVOS	FATORES NEGATIVOS
Fatores Internos	**STRENGTHS (Fortalezas)** - Cursos de especialização para sargentos; e - Recursos de forma sistêmica: materializados na infraestrutura em ampliação e material.	**WEAKNESSES (Debilidades)** - Organização: não conta com um órgão de direção ou gestão dedicado à cibernética; e - Falta de um plano de carreira para os oficiais.
Fatores Externos	**OPORTUNITIES (Oportunidades)** - Marco legal sólido.	**THREATS (Ameaças)** - Falta de capacidade conjunta.

Tabela 1 – Principais fatores relativos à capacidade cibernética no Exército do Chile.

Considerando os fatores internos, há força no fator educação, representada pela sólida formação das praças, que passam pelo curso de guerra eletrônica, cibernética e inteligência. Deduz-se que a educação tem uma forte relevância ao fornecer profissionais qualificados para o desempenho de tarefas no setor cibernético. Além disso, os aspectos de infraestrutura e material demonstram fortalezas, principalmente pelo fluxo contínuo de recursos financeiros para essas áreas.

Por outro lado, como debilidade, destaca-se a peculiar estrutura que o

cibernética. Como ameaça, elenca-se a falta de capacidade no nível conjunto.

Por fim, conclui-se que a capacidade cibernética no Exército do Chile está em fase de implantação, sendo sua maturação compatível com a realidade regional. Além disso, o Exército Brasileiro tem demonstrado interesse em contribuir com o setor cibernético do Chile, uma vez que as Conferências Bilaterais entre Estados-Maiores (CBEM) de 2020 e 2022, realizado entre ambos os exércitos, expressaram vários entendimentos no setor – fato esse que contribuirá para o aumento da segurança cibernética no cone sul.

REFERÊNCIAS

BRASIL. Ministério da Defesa. Exército Brasileiro. **Doutrina Militar Terrestre.** 2ª. ed. Brasília, 2019.
BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014.
CARNEIRO, João M. E. **A Guerra Cibernética**: **uma proposta de elementos para formulação doutrinária do Exército Brasileiro**. 2012. 204 f. Tese (Doutorado em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.
CHILE. *Política de Ciberdefensa.* Santiago, Región Metropolitana, Chile: Diario Oficial de la República de Chile, 8 de Marzo de 2018.
CHILE. Exército do Chile. **Regulamento RDI 20008 - Defesa Cibernética**. Santiago, Región Metropolitana, Chile: División Doctrina. 2016.
CHILE. Ministério da Defesa Nacional. **Doctrina de Ciberdefensa Conjunta DNC 2-11**. Santiago, Región Metropolitana, Chile: Estado Mayor Conjunto. 2018.
CHILE. Ministério da Defesa Nacional. **Decreto 305 – Extingue a Direção de Inteligência e cria a Direção de Planejamento de Informações do Exército**. Santiago, Chile: MINDEF 2021.
CHILE. Ministério do Interior e Segurança Pública. **Política de Segurança Cibernética**. Santiago, 2020.
CHILE. MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA DE CHILE**. Segundo exercício de simulação em gestão da segurança cibernética.** Disponível em: https://www.ciberseguridad.gob.cl/noticias/segundo-ejercicio-de-simulacion-en-gestion-de-ciberseguridad-para-funcionarios-publicos-reune-mas-de-380-participantes/. Acessado em: 10 de set. 22.
CORREA FILHO, Ivan de Souza. **A segurança cibernética no Brasil – uma análise da situação atual.** Trabalho de Conclusão de Curso. Escola Superior de Guerra. Brasília, 2016.
MIRANDA, Cristian Aguilera. **Estrategia de Ciberdefensa Institucional.** Memória para obtenção do título de Oficial de Estado-Maior. Academia de Guerra do Exército do Chile. Santiago, 2021.
ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE. **NATO Cyber Defence**. Bruxelas: *Public Diplomacy Division*. 2019.
PLUM, Thiago Itamar. **Proposta de metodologia para avaliação da capacidade cibernética de Estados-Nação**. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.
VALENZUELA, Gonzalo Burgos. *La Política Nacional y su relación con el ciberespacio***.** Memória para obtenção do título de Oficial de Estado-Maior. Academia de Guerra do Exército do Chile. Santiago, 2021.

NOTAS

[1] Sistemas C4I: Sistemas de Comando, Controle, Comunicações, Computadores e Inteligência.
[2] Cabos profissionais: início da carreira das praças - equivalente ao 3º Sargento no Exército brasileiro
[3] A certificação **CCNA** (**Cisco Certified Network Associate**) é uma prova da **CISCO** SYSTEMS, uma companhia sediada em San Jose, na Califórnia, cuja principal atividade é oferecer soluções para redes e comunicações, fabricando roteadores e switches, além da prestação de serviços de manutenção através de empresas parceiras.
[4] O termo SWOT é um acrônimo para *Strengths, Weaknesses, Opportunities and Threats* (Forças, Fraquezas, Oportunidades e Ameaças). A análise SWOT é uma ferramenta de diagnóstico estratégico para empresas, governos ou entidades em um determinado ambiente. A técnica é atribuída a Albert Humphrey, que foi um líder de pesquisa na Universidade de Stanford nos anos 60 e 70.

SOBRE O AUTOR

O Tenente-Coronel de Comunicações Lúcio Jerônimo é instrutor da Academia de Guerra do Exército do Chile e Oficial de Ligação de Doutrina junto à Divisão de Doutrina do Exército do Chile. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras (AMAN) em 2002. É mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO/2010). Concluiu o curso de Comando e Estado-Maior (ECEME) em 2019. Comandou a 20ª Companhia de Comunicações Páraquedista, no Rio de Janeiro, no biênio 2016-2017. Desempenhou a função de instrutor do Centro de Instrução de Guerra Eletrônica (CIGE). Possui especialização em Análise do Ambiente Eletromagnético pelo Instituto Tecnológico de Aeronáutica (ITA). Realizou os seguintes cursos: Básico de Guerra Eletrônica, Intermediário de Guerra Eletrônica, Doutrinário de Guerra Eletrônica (FAB), Expedito de Guerra Eletrônica (MB), Básico de Paraquedista, Mestre de Salto, Operações na Selva Cat "B", Avançado de Comunicações (EUA) e Regular de Estado-Maior (Chile) (jeronimo.lucio@eb.mil.br).



TENENTE-CORONEL MARCUS GOMES
Oficial do Estado-Maior do Comando de Aviação do Exército.

DEMANDAS DOUTRINÁRIAS PARA UMA OPERAÇÃO CONJUNTA DE AVIAÇÃO

Segundo Clausewitz,

> o principal objetivo de qualquer teoria é esclarecer conceitos e ideias que se tornaram, por assim dizer, confusos e emaranhados. Até que os termos e conceitos tenham sido definidos, pode-se esperar fazer algum progresso no exame da questão de forma clara e simples e esperar que o leitor compartilhe suas opiniões. (CLAUSEWITZ, *apud* McBeth, 2003, p. 445, tradução nossa).

Ao longo do século XX, pôde ser observada a importância da aviação para as operações militares. Do emprego incipiente na 1ª Guerra Mundial à aplicação ostensiva nos conflitos armados atuais, sua doutrina e organização evoluíram constantemente.

Os primeiros aviões do Exército datam de 1913, mas as operações aéreas angariaram uma importância incontestável na evolução das operações no século XX. Para Douhet (1988, p. 19) "o domínio do ar é o fator determinante da vitória".

Dentro dessa importância e sob a influência de teóricos do Poder Aéreo, como Giulio Douhet, Billy Mitchell e Hugh Trenchard, somadas às decisões de países europeus que deram independência para a arma aérea, o Brasil, em 1941, decide pela criação do Ministério da Aeronáutica (BRASIL, 1941a).

O nome Aeronáutica é influência direta de Giulio Douhet, que destacava a necessidade de uma organização central que unisse as aviações sob uma única direção, uma "cabeça suprema", cujo nome deveria ser Ministério da Aeronáutica (DOUHET, 1988, p. 122-125).

Portanto, em 1941, nasce o Ministério da Aeronáutica no Brasil, integrando

> [...] os elementos existentes nas aeronáuticas do Exército e da Marinha e no Departamento de Aeronáutica Civil [...], ou seja, [...] as instituições, repartições, órgãos e serviços [...] subordinados aos Ministérios da Guerra, da Marinha e Viação e Obras Públicas. (BRASIL, 1941a, art. 4º e 5º).

O Decreto-Lei 2.961 (BRASIL, 1941a, art. 8º), ainda traz uma importante novidade, pois ao integrar as aeronáuticas do Exército e da Marinha, cria "uma corporação única, subordinada ao Ministério da Aeronáutica [...]" que, nessa data, foi denominada de "Forças Aéreas Nacionais".

A denominação para Força Aérea Brasileira (FAB) foi feita por meio do Decreto-Lei 3.302, de 22 de maio de 1941 (BRASIL, 1941b, art. 2º).

O Decreto-Lei que estabelecia a organização da FAB em tempo de paz, no seu Capítulo I, também definia a Concepção de Emprego e já destacava que a Força Aérea era "organizada e instruída tendo em vista a participação em: a) operações puramente aéreas; b) **em operações combinadas com o Exército e a Armada;** e c) na defesa aérea do território." (BRASIL, 1942, art. 3º, grifo nosso).

Em 1946, o Decreto-Lei 9.889 estabelecia nova organização para a FAB e, onde, no decreto anterior, definia que a FAB deveria ser empregada na defesa do território, passa a estabelecer que a Força Aérea deveria executar ações para "a defesa aérea do país". (BRASIL, 1946, art. 1º).

Portanto, a FAB foi criada como braço operacional da Aeronáutica, ficando sob sua responsabilidade a execução das ações militares necessárias à defesa aérea do país, o domínio do ar, essencial para a defesa do território nacional, bem como para as operações do Exército e da Marinha.

Essa responsabilidade da FAB foi atualizada, acompanhando a evolução da doutrina e documentos, como a Missão da Aeronáutica (ICA 11-1), a Política Militar Aeronáutica (DCA 14-5), a Estratégia Militar da Aeronáutica (DCA 15-1) e a Doutrina Básica da Força Aérea (DCA 1-1), que evoluíram no tempo e acompanharam publicações, como a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END).

Nesse fator, a Doutrina Básica da Força Aérea de 1958 [1], descreve os componentes do Poder Militar e as Forças Singulares (FS) que os compõem (Exército, Marinha e Força Aérea), destacando que "[...] as Forças Armadas são

distintas e equivalentes, nenhuma é organização auxiliar da outra, mas **interdependentes no seu emprego e conjugam seus esforços onde e quando necessário**". (BRASIL, 1958, item 1.8, grifo nosso).

Portanto, desde o início da Força Aérea, a visão de operações integradas com as Forças Singulares já estava presente, no que hodiernamente é tratado como interoperabilidade.

Mas, para a aplicação do Poder Aéreo, Santos (1989, p. 15-16, grifo nosso) destaca como ponto importante que o "fenômeno do Poder Aéreo é composto, dentre outros, por ideias, conceitos e **doutrina**, acentuando o seu caráter dinâmico."

Santos acentua a importância da doutrina ao destacar que "[...] o impacto que as descobertas tecnológicas produzem sobre as doutrinas [...], nem sempre são percebidas com a desejada rapidez". (SANTOS, 1989, p. 16).

Em 2005, a doutrina da FAB, DCA 1-1/2005 destacava as operações com outras Forças, nacionais ou internacionais, já dentro de um conceito de interoperabilidade e enfatizava o aspecto da Doutrina Militar de Defesa (DMD):

> 3.10 INTEROPERABILIDADE - UM FATOR PREPONDERANTE
> 3.10.1 É exigida para garantir a operação efetiva de uma Força ao lado de instituições e países diferentes, dentro de um ambiente nacional ou internacional. Não só é alcançada pela existência de sistemas que aglutinem interesses comuns, mas **também pela implementação de doutrinas** e procedimentos convergentes. **Aumenta com a execução de operações e exercícios combinados** que foquem a unidade de comando, permitindo aprimorar procedimentos na busca da sinergia através da união de esforços.
> 3.10.2 No caso brasileiro, a efetividade e a coerência das operações militares **têm respaldo na existência da Doutrina Militar de Defesa**, da qual derivam as doutrinas específicas para cada Força, prevendo-se que **os meios nacionais possuam capacidade para operar dentro de disposições compatíveis com a referida Doutrina.** (BRASIL, 2005, p. 16, grifo nosso).

Santos destacou (1989, p. 16) que as doutrinas nem sempre evoluem na rapidez desejada, principalmente quando se trata de operações conjuntas, ensejando possíveis mudanças nos documentos das Forças envolvidas.

A Doutrina de Operações Conjuntas, MD30-M-01/2020, estabelece que "as operações Conjuntas (Op Cj) se caracterizam pelo emprego coordenado de elementos de mais de uma força singular, com propósitos interdependentes ou complementares **voltado a um objetivo ou propósito comum** [...]". (BRASIL, 2020c, p. 41, v. 1, item 3.1.2, grifo nosso).

Observa-se que, nessa descrição, o MD30-M-01/2020 caracteriza as operações conjuntas dentro da visão já observada pela doutrina da FAB de 1958, onde esse tipo de operação deve ser caracterizado por propósitos interdependentes (no seu emprego) e com objetivo comum (onde e quando necessário).

A Aviação do Exército, ao ser recriada, em 1986, para proporcionar aeromobilidade [2] à Força Terrestre, constituiu-se de meios (instalações, aeronaves e recursos humanos) e capacidades que poderão ser de interesse para o Poder Aeroespacial [3] e por meio de operações conjuntas.

Para a Força Terrestre, a possibilidade de trabalhar de forma integrada é visualizada no seu Plano Estratégico 2020-2023, quando atribui e incentiva a interoperabilidade entre Forças Armadas, por meio de exercícios e operações conjuntas, voltados para o mesmo objetivo (BRASIL, 2019a, p.15, item 2.2.3.2).

> No caso das Forças Armadas, **a interoperabilidade é a capacidade de operar de maneira integrada, coordenada e harmônica com as outras FA,** órgãos e agências governamentais, bem como em operações multinacionais, de modo a **cumprir a missão atribuída** (BRASIL, 2018a, p. 28, item 4.4.2, grifo nosso).

Mesmo com outras palavras, a descrição do Exército Brasileiro (EB) se alinha com a Doutrina Militar de Defesa e com a DCA 1-1/2020 da FAB ao destacar a operação integrada das Forças, bem como o objetivo comum (a missão atribuída).

"Nos últimos anos, ocorreu um incremento gradativo da necessidade de operar em conjunto com as demais Forças ou mesmo com órgãos e agências governamentais" (BRASIL, 2018a, p. 28, item 4.4.4).

Nesse sentido, o Exército Brasileiro instituiu, dentro da estratégia de estabelecimento de uma doutrina militar compatível com uma força transformada, a ação estratégica de "[...] aperfeiçoar a doutrina singular e contribuir com o aperfeiçoamento da doutrina conjunta" (BRASIL, 2019a, p. 25, item 6.1.1).

Assim, a Força Terrestre também demonstra sua perspectiva no interesse das operações conjuntas, viabilizando e incentivando a

interoperabilidade e a atualização doutrinária.

A interoperabilidade perpassa todo o planejamento estratégico militar e diante da sua importância, está presente em documentos de nível nacional, elaborado pelas mais altas autoridades do país, de nível setorial, que engloba os documentos produzidos pelo Ministério da Defesa, e de nível subsetorial, na doutrina e legislações das Forças Armadas, tendo como ponto importante a convergência da doutrina e dos procedimentos.

INTEROPERABILIDADE E OPERAÇÕES CONJUNTAS NA DOUTRINA DA FAB

O entendimento da Organização do Tratado do Atlântico Norte sobre o conceito de interoperabilidade, engloba tanto diferentes Forças Armadas (FA) quanto diferentes nacionalidades, ou ambas distinções e o referido conceito permite que forças, unidades ou sistemas operem juntos, **compartilhando doutrinas**, procedimentos, infraestruturas, bases e informações entre si (NATO, 2006, p.1, tradução nossa, grifo nosso) [4].

Sobre os níveis de operações que englobam a interoperabilidade, Moon *et al*. (2008, p. 5, tradução nossa) esclarece que a

> [...] definição de interoperabilidade engloba todos os níveis de operações militares, do tático ao estratégico, do combate às operações de apoio, além de acomodar vários elementos, como, por exemplo, das plataformas às instalações militares, dos sistemas de comunicação até o de suprimento das unidades militares.

O conceito de interoperabilidade é encontrado no Glossário das Forças Armadas:

> 1. Capacidade de forças militares nacionais ou aliadas operarem, efetivamente, de acordo com a estrutura de comando estabelecida, na execução de uma missão de natureza estratégica ou tática, de combate ou logística, em adestramento ou instrução. O desenvolvimento da interoperabilidade busca otimizar o emprego dos recursos humanos e materiais, **assim como aprimorar a doutrina de emprego** das Forças Armadas. **A consecução de um alto grau de interoperabilidade está ligada diretamente ao maior ou menor nível de padronização de doutrina**, procedimentos, documentação e de **material** das Forças Armadas. São os seguintes níveis de padronização: compatibilidade, intercambialidade e comunalidade. 2. Capacidade dos sistemas, unidades ou forças de intercambiarem serviços ou informações ou aceitá-los de outros sistemas, unidades ou forças e, também, de empregar esses serviços ou informações, sem o comprometimento de suas funcionalidades. (BRASIL, 2015, p.151, grifo nosso).

A Força Aérea Brasileira tem como visão de futuro: "uma Força Aérea de grande capacidade dissuasória, operacionalmente moderna e **atuando de forma integrada** para a defesa dos interesses nacionais". (BRASIL, 2020a, p. 7, grifo nosso).

Destaca-se, na visão de futuro, o fator integração, que se reflete na interoperabilidade entre as Forças Armadas.

Para atingir seus objetivos, uma força armada deve possuir uma doutrina onde um conjunto de princípios servem de base, dando suporte coerente para ser transmitido ou ensinado.

> A Doutrina, em seu significado mais amplo, é o conjunto de princípios, conceitos, normas e procedimentos, exposto de forma integrada e harmônica, destinado a estabelecer linhas de pensamentos e a orientar ações. A formulação doutrinária é fundamentada principalmente na experiência e deve refletir as melhores práticas até então conhecidas e aprovadas. (Brasil, 2020a, p. 7).

A Doutrina Básica da Força Aérea (2020a) descreve que:

> para alcançar tal nível de operacionalidade, faz-se pertinente identificar e desenvolver o Planejamento Baseado em Capacidades da Força Aérea. Essas Capacidades têm origem na conjugação das características do Poder Aeroespacial com as habilidades inerentes aos Meios Aeroespaciais e de Força Aérea, e traduzem as áreas de especialização do "Emprego da Força Aérea", em campanhas e operações militares, no âmbito de ações independentes, conjuntas ou combinadas. (BRASIL, 2020a, p. 41, item 4.2).

O planejamento baseado em capacidades acaba por demandar constante evolução da doutrina e o emprego de operações conjuntas ou combinadas [5], pois a característica central da guerra normalmente não é o embate das forças militares (WARDEN III, 1995b, p. 46), pois existe toda uma estrutura política, social e econômica envolvida que demanda capacidades para atingir o inimigo em frentes distintas.

Daí, a importância das operações conjuntas ou combinadas, onde a interoperabilidade entre Forças Singulares é essencial para agregar, criar ou multiplicar as capacidades operativas necessárias, obtendo efeitos não só para o combate propriamente dito, mas para atingir outras estruturas importantes, visando o enfraquecimento do inimigo.

A doutrina da FAB de 1958 já destacava o aspecto de operações com elementos de mais de uma força, mas que deveria estar sob um comando único e ter objetivos comuns.

Esses detalhes também são abordados na Doutrina de Operações Conjuntas publicada pelo Ministério da Defesa (MD), quando destaca que elas devem ter um objetivo ou **propósito comum e subordinadas a um Comando Operacional Conjunto**. (BRASIL, 2020c, p. 41, item 3.1.2, grifo nosso).

Observa-se, portanto, a importância, no conceito de Operações Conjuntas, de que é possível adjudicar meios de uma Força Singular para cooperar com outra Força. Contudo, dois pontos são fundamentais: que haja um objetivo ou propósito comum e que estejam subordinados a um comando único.

O que se busca nas ações conjuntas, de forma integrada, é multiplicar o poder de combate por meio do aumento das capacidades de atuação, seja pela diversificação ou maior quantidade, buscando contemplar diversos objetivos e, ao mesmo tempo, um efeito sinérgico.

> O emprego coordenado do Poder Aeroespacial, **juntamente com outras parcelas do Poder Militar,** ou em apoio a elas, **pode produzir efeitos sinérgicos** que excedem as contribuições do emprego estanque de cada uma das Forças Singulares. (BRASIL, 2020a, p. 39, item 3.8.4, grifo nosso).

Esses fatores também são destacados por Teixeira Júnior e Freire:

> De forma objetiva, interoperabilidade diz respeito à medida pela qual organizações e indivíduos conseguem **atuar de forma conjunta para se alcançar um mesmo objetivo**. Visto assim, este seria considerado como a busca por **padronizar procedimentos** e integrar ações, **por meio da sinergia e da cooperação entre as partes envolvidas** (HURA *et al.*, 2000, *apud* Teixeira Júnior e Freire, 2019, p. 31, grifo nosso).

A Doutrina da Força Aérea (BRASIL, 2020a) define que as tarefas são: "funções operacionais exercidas pela FAB, que descrevem as possibilidades de emprego da Força Aérea e definem os propósitos mais amplos da participação do Poder Militar Aeroespacial em uma campanha ou operação militar." (Brasil, 2020a, p. 13, item 1.2.28).

O manual de Doutrina de Operações Conjuntas (BRASIL, 2020c, v. 2), define que uma das tarefas da Força Aérea é o controle do ar, conquanto a Doutrina da FAB (BRASIL, 2020a) a define como "controle aeroespacial", uma vez que inclui o espaço sideral como ambiente de batalha.

A fim de potencializar características como alcance, mobilidade, penetração e pronta-resposta, ampliando o poder de combate dos Meios Aeroespaciais e de Força Aérea e das Forças amigas, foram estabelecidas Ações de Força Aérea (BRASIL, 2020b, p. 26).

A Doutrina Básica da Força Aérea (BRASIL, 2020a) conceitua Ação de Força Aérea como:

> ato de empregar, no nível tático, Meios Aeroespaciais e de Força Aérea para causar um ou mais efeitos desejados em uma campanha ou operação militar. Envolve ações letais e não letais de emprego do Poder Aeroespacial, bem como ações especializadas destinadas a suportar e a complementar a capacidade operacional da Força Aérea. (BRASIL, 2020a, p. 9, item 1.2.1)

Mas, as Ações de Força Aérea são denominadas Missões de Força Aérea ao serem "[...] atribuídas a um comandante de aeronave, líder de formação de aeronaves, comandante de unidade terrestre ou comandante de fração de tropa, com o propósito de atingir um ou mais efeitos desejados." (BRASIL, 2020b, p. 26, item 2.3.2).

Observa-se, na doutrina da FAB e nos conceitos analisados, que a operação conjunta demanda interoperabilidade, que possui como componente a doutrina e esta última exerce um papel importante no grau de consecução.

EVOLUÇÃO DAS DOUTRINAS

Santos destacou (1989, p. 16-17) que as doutrinas nem sempre evoluem na rapidez desejada, principalmente quando se trata de operações conjuntas, ensejando possíveis mudanças nos documentos das Forças envolvidas. O autor destaca, ainda, que a doutrina é um elemento importante, constituída por ideias e conceitos, mas que ela deveria manter-se atualizada "[...] mercê de novas concepções

decorrentes do momento, dos objetivos e dos meios disponíveis [...]". (SANTOS, 1989, p. 17).

A importância da doutrina também é ressaltada na Doutrina Militar de Defesa, enfatizando que as doutrinas representam "[...] uma exposição integrada e harmônica de ideias e entendimentos sobre determinado assunto, com **a finalidade de ordenar linhas de pensamentos e orientar ações**", sendo entendimentos que ordenam, distinguem e qualificam as atividades de organização e, principalmente, **de preparo e emprego das Forças Armadas**. (BRASIL, 2007, p.11, item 1.4.1, grifo nosso).

Daí, a importância da análise das doutrinas para o contexto de interoperabilidade.

A Política Nacional de Defesa cita o contínuo aperfeiçoamento da doutrina, com foco na interoperabilidade, além do adequado aparelhamento das (FA) (BRASIL, 2018b, p. 12).

A atuação conjunta por parte das Forças Armadas é incentivada no manual de Doutrina de Operações Conjuntas (BRASIL, 2020c), explorando elementos como flexibilidade, versatilidade e mobilidade. O manual ainda determina para as FA a soma de esforços, a compatibilização de procedimentos e a integração das ações, com foco na eficiência das operações conjuntas (BRASIL, 2020c, p. 15).

A doutrina é um elemento importante, sendo o fio condutor entre as ideias e conceitos, tendo a finalidade de ordenar linhas de pensamento e orientar ações para o preparo e emprego das Forças Armadas. (Santos, 1989, p. 16).

Essa visão aparece em todos os documentos, seja em nível do MD ou das Forças Singulares. A Doutrina Militar de Defesa destaca que a doutrina integra ideias e entendimentos com "[...] a finalidade de ordenar linhas de pensamentos e orientar ações [...] para o preparo e emprego das Forças Armadas." (BRASIL, 2007, p. 11, item 1.4.1).

Com visão similar, a Doutrina Militar Terrestre e a Doutrina Básica da Força Aérea enfatizam que a doutrina é um conjunto de princípios que apresenta ideias básicas, expostos de forma harmônica e integrada, fundamentadas principalmente na experiência e que procura orientar a ação. (BRASIL, 2019b, p. 1-2; BRASIL, 2020a, p. 9).

Antes de tratar os detalhes de aplicação das respectivas doutrinas do EB e da FAB, considera-se importante demonstrar, sinteticamente, o arcabouço dos documentos que são gerados, desde o nível político, estratégico que envolve o MD, o operacional (das Forças Singulares) e o tático (de comandos operacionais ativados).

Isso porque a Doutrina de Operações Conjuntas destaca que o nível estratégico é competência do MD, sendo o responsável, por meio do Estado-Maior das Forças Armadas (EMCFA), por emitir a Diretriz de Planejamento Estratégico Militar (DPEM) com as orientações gerais que nortearão o Plano Estratégico de Emprego Conjunto das Forças Armadas (PEECFA). (BRASIL, 2020c, v. 1, p. 23, item 2.5.2).

Ou seja, é o primeiro nível onde os conceitos, descritores e definições deverão estar claros para que os demais níveis elaborem os seus respectivos planos.

PLANEJAMENTO	
NÍVEIS	DOCUMENTOS
Político (CS)	Diretrizes Políticas (Diretriz Presidencial de Emprego de Defesa - DPED).
Estratégico (MD)	1. Diretrizes Estratégicas: a. Ministerial - Diretriz Ministerial de Emprego de Defesa (DMED). b. Chefe do Estado-Maior Conjunto das Forças Armadas - Diretriz de Planejamento Estratégico Militar (DPEM). 2. Planos Estratégicos - Plano Estratégico de Emprego Conjunto das Forças Armadas (PEECFA).
Operacional (Comandos Operacionais ativados)	Diretriz de Planejamento (DIPLAN) Planos Operacionais.
Tático (F Cte)	Diretrizes de Planejamentos Táticos. Ordens de Operações. Planos Táticos.

Tabela 1 - Níveis dos documentos de planejamento de Defesa. Fonte: BRASIL (2020c, p. 27).

A Doutrina de Operações Conjuntas destaca que, no nível operacional, o comandante operacional "[...] elabora o planejamento militar da operação/campanha, com base no PEECFA correspondente [...]" e, no nível tático (Força Componente), "são elaborados e detalhados os planos e ordens para a execução das grandes operações [...]". (BRASIL, 2020c, v. 1, p. 23-24).

O MD30-M-01 também define que cabe aos comandantes do Exército, da Marinha e da Aeronáutica "emitirem diretrizes, visando o planejamento operacional do emprego, quando da ativação de um Comando Singular a eles subordinado" e "fornecer os meios adjudicados pelo Ministro da Defesa aos Comandos Operacionais". (BRASIL, 2020c, v. 1, p. 25).

Dessa forma, à medida que os níveis de planejamento se aproximam das Forças Singulares, percebe-se a importância de que os conceitos e descritores tenham a clareza adequada, em função do detalhamento necessário às operações, para evitar interpretações equivocadas, principalmente em operações conjuntas.

Essa preocupação é observada no próprio documento do MD que trata sobre Operações Conjuntas ao destacar que: "o comando de uma operação conjunta, embora semelhante ao de qualquer outra operação, diferencia-se pela **heterogeneidade dos processos de emprego e pelas peculiaridades técnico-profissionais das forças componentes**" e que o Comando Operacional Conjunto deverá buscar observar aspectos como coordenação, flexibilidade e "d) **uniformidade doutrinária:** observância dos preceitos da doutrina de emprego conjunto". (BRASIL, 2020c, v. 1, p. 47, item 4.3.1, grifo nosso).

Em uma operação conjunta, com envolvimento da Aviação do Exército e da Força Aérea Brasileira, tanto a operação como a sua preparação será realizada em conjunto pelas forças envolvidas, sendo incluídos os planos e ordens de operações, bem como os treinamentos.

Portanto, diferenças de conceitos e emprego doutrinário serão fatores contribuintes para o insucesso ou dificultarão o entendimento por parte dos envolvidos.

Assim, é preciso analisar os pontos de convergência e divergência doutrinários, pois há a necessidade de aumentar os níveis de padronização entre as Forças Singulares envolvidas (BRASIL, 2019b, p. 5-10, item 5.7.5), critério já definido no próprio Glossário das FA e na DMD.

A doutrina da FAB também destaca as operações conjuntas, enfatizando que "o emprego coordenado do Poder Aeroespacial, juntamente com outras parcelas do Poder Militar, ou em apoio a elas, pode produzir efeitos sinérgicos que excedem as contribuições do emprego estanque de cada uma das Forças Singulares". (BRASIL, 2020a, p. 39).

Portanto, no que tange à visão de que o emprego conjunto é necessário e redunda em resultados melhores na guerra, há uma convergência doutrinária desde o nível estratégico, isto é, da DMD.

No que tange aos descritores mais específicos, no documento do EB que trata sobre sua doutrina, observa-se que a palavra capacidade é definida como:

> [...] a **aptidão** requerida a uma força ou Organização Militar para cumprir determinada **missão ou atividade.** Essa aptidão é exercida sob condições e padrões determinados, pela combinação de meios para desempenhar uma gama de **tarefas**. (BRASIL, 2019b, p. 3-2, grifo nosso).

Para o EB, uma capacidade é obtida em função de sete fatores determinantes, dentre eles o material, a educação, a infraestrutura e a doutrina. (BRASIL, 2019b, p. 3-3, item 3.3.4, grifo nosso).

A FAB descreve capacidade **"[...] como a aptidão para atingir um efeito desejado, por meio de um conjunto de tarefas [...]".** (BRASIL, 2020a, p. 41, grifo nosso).

Nesse descritor, analisando-se as doutrinas do EB e da FAB, observam-se convergências e distinções. As convergências ficam no que tange à aptidão e ao resultado, uma vez que o EB descreve capacidade como aptidão para cumprir determinada missão e a FAB como aptidão para atingir um efeito desejado. A divergência fica no aspecto de que, para o EB, a capacidade permite cumprir uma missão ou atividade, conquanto para a FAB o efeito desejado (resultado) é atingido por meio de "um conjunto de tarefas".

Outro aspecto é que, para a FAB, as tarefas definem "[...] **objetivos mais abrangentes** de uma campanha ou operação militar, **mormente estratégicos e operacionais**" (BRASIL, 2020a, p. 41, grifo nosso).

No caso do EB, o descritor não define o nível do objetivo a ser alcançado, podendo-se presumir que possa ser no nível estratégico, operacional ou tático.

Verificando-se os documentos do MD, observa-se que esse descritor não é definido, apesar de que a DMD destaca a necessidade de que as Forças Armadas possuam "capacidades" para atuar. O Glossário das FA também não define isoladamente esse descritor.

Descreve Capacidade Militar como sendo o "conceito aplicado ao nível estratégico que representa a aptidão de uma Força Armada para executar as operações que lhe cabem como instrumento da expressão militar do Poder Nacional." (BRASIL, 2015, p. 55).

No que tange, portanto, ao descritor capacidade, há diferenças de entendimento entre a FAB, EB e MD, sendo comum o consenso de ser uma aptidão.

Para Corrêa (2020, p. 31, grifo nosso) capacidade significa "um meio de alcançar os **efeitos desejados**, sob condições e padrões específicos, pela combinação de recursos e formas de executar **conjuntos de tarefas**."

O descritor capacidade assume notável importância ao ser pesquisado na doutrina e em documentos de níveis político, estratégico, operacional e tático.

Começando pelo Livro Branco de Defesa Nacional (LBDN), onde cita que o planejamento é baseado em capacidades tendo como objetivo

> [...] identificar as **capacidades conjuntas e as singulares** de cada Força e elevar o grau de **interoperabilidade**, pela definição das necessidades comuns, em articulação e equipamento, para a Defesa do País. (BRASIL, 2018b, p. 151, grifo nosso).

Já a Estratégia Nacional de Defesa cita que "para cumprir sua destinação constitucional, as Forças Armadas devem conceber suas estruturas organizacionais e operacionais em torno de **capacidades** [...]". (BRASIL, 2018, p. 24, grifo nosso).

No mesmo documento de nível político, encontra-se como objetivo nacional de defesa (OND) "assegurar a **Capacidade** de Defesa, para o Cumprimento das Missões Constitucionais das Forças Armadas" tendo como algumas das ações estratégicas de defesa (AED) "estruturar as Forças Armadas em torno de **capacidades**" e "incrementar as **capacidades** das Forças Armadas para **emprego conjunto**" (BRASIL, 2018b, p. 34, grifo nosso).

Nota-se que o descritor capacidade é enfatizado, contudo não tendo uma definição ou explicação do termo nos documentos e doutrinas publicadas.

Sobre o Planejamento Baseado em Capacidades (PBC), citado no LBDN (nível político), observa-se sua ausência na DMD (2007), no Glossário das FA (2015) e na Doutrina de Operações Conjuntas (2020c), ou seja, nos documentos de nível estratégico.

Coube às Forças Singulares, nível operacional, inserirem o PBC em suas doutrinas:

> O Exército Brasileiro adota a geração de forças por meio do **planejamento baseado em capacidades (PBC)**. O desenvolvimento de capacidades é baseado na análise da conjuntura e em cenários prospectivos, com o objetivo de identificar as ameaças concretas e potenciais ao Estado. (BRASIL, 2019b, p. 3-2, item 3.3.1, grifo nosso).
>
> [...] foram adequadas as Ações de Força Aérea às capacidades funcionais das Forças Armadas, alinhamento necessário para a interoperabilidade entre as Forças e a completa execução do método de **Planejamento Baseado em Capacidades (PBC)**. (BRASIL, 2020a, p. 16, item 2.3.9, grifo nosso).

Supõe-se que a falta de tempestividade de descritores importantes da doutrina, como o caso do PBC, pode estar relacionada com a inexistência de uma sistemática de atualização doutrinária, que envolva os níveis político, estratégico, operacional e tático.

Percebe-se que as atualizações não seguem uma rotina, ocasionando espaços vazios e, por vezes, divergências em conceitos utilizados. No nível político, o LBDN, a PND e a END foram aprovadas em 2018 (Decreto Legislativo nº 137/2018), conquanto, no nível estratégico, a DMD foi editada em 2007, e no nível operacional as doutrinas da FAB (DCA 1-1) e da Aviação do Exército (Av Ex) são de 2020 e 2019, respectivamente.

Apesar de a atualização da PND e END estar prevista na Lei Complementar 136, de 25 de agosto de 2010, (BRASIL, 2010, § 3º, art. 9º), o Congresso tem demorado na aprovação desses documentos, o que também gera efeitos sobre os demais documentos dependentes desta atualização.

Tendo a PND e a END atualização quadrienal prevista em norma, sugere-se que as doutrinas de nível estratégico e operacional acompanhem, de forma escalonada, uma sistemática de atualização, de forma concomitante com a PND e END, evitando-se a defasagem existente.

A atualização sistemática da doutrina poderá

ainda diminuir o lapso temporal entre o impacto das descobertas tecnológicas e a sua desejada percepção na doutrina, conforme abordado por Santos (1989, p. 16).

Esse detalhe também é observado, no documento Cenários de Defesa 2020-2039, ao destacar a necessidade de atualização de doutrinas, pois, em decorrência dos avanços tecnológicos, as "[...] doutrinas das Forças Armadas transitarão no sentido de empregar menores quantidades, com maiores capacidades e operações rápidas, pontuais e evitando danos colaterais [...]". (BRASIL, 2017, p. 22).

Portanto, apesar de observar-se que os documentos destacam a necessidade de atualização das doutrinas, o processo não é realizado de forma conectada, ou seja, mesmo no MD não existe um processo, pois seria esperado que, para emitir um documento como a Doutrina de Operações Conjuntas, a DMD estivesse atualizada.

Como isso não ocorre, observa-se uma DMD de 2007, a doutrina de Operações Conjuntas de 2020 e as doutrinas do EB e da FAB de 2019 e 2020, respectivamente. Ou seja, uma defasagem de mais de dez anos entre o documento que deveria ser o fato gerador e os documentos decorrentes.

Visto o aspecto temporal dos documentos de defesa, analisar-se-á outros descritores, além do descritor capacidade, passíveis de utilização em uma operação conjunta de obtenção de superioridade aérea.

Da análise realizada com outros descritores, verificou-se que não há uma padronização entre os diversos documentos no que tange aos descritores empregados, apesar de observar palavras comuns, como aptidão, tarefa, ação e missão. Mesmo nessas palavras há diferenças, como é o caso da palavra missão que, no caso da DMD e da doutrina da Av Ex, são tarefas, conquanto para a Força Aérea é uma ação.

Observou-se, também, que, por vezes, determinados descritores, como capacidade, não estão descritos nos documentos de maior nível hierárquico (MD), mas são definidos em documentos das Forças Singulares, tendo, inclusive, similaridade nos termos empregados.

Outro aspecto observado na análise dos documentos doutrinários, relaciona-se ao nível (estratégico ou tático) de determinados descritores, como tarefa e ação.

Esses dois descritores, em termos de nível, somente são definidos na doutrina da FAB e da Av Ex, não havendo qualquer menção na DMD ou na doutrina da Força Terrestre. O aspecto distinto é que uma tarefa, para a FAB, é um evento mormente estratégico, conquanto, na doutrina da Av Ex, é um evento tático.

Nessa acepção, para este artigo analisou descritores das doutrinas do EB (Av Ex) e da FAB, ligados ao emprego conjunto de ambas forças.

Como exemplo, pode-se citar o descritor tarefa, há divergências no que tange ao nível de emprego quando as Forças definem esse descritor, sendo estratégico e operacional para a FAB e nível tático para o EB.

Acresça-se o detalhe de que o descritor de tarefa do EB também se assemelha ao descritor capacidade da FAB pelo detalhe que ambos buscam um resultado. No caso da FAB, mais especificamente, um "efeito desejado" e, no caso do EB, um "resultado determinado".

Outro detalhe em relação a esse descritor é que, na doutrina da AvEx, um conjunto de tarefas afins forma uma atividade (BRASIL, 2019b, p. 1-2, item 1.4.1.2), sem que o documento especifique quais são as atividades, citando somente que seus resultados concorrem para o desenvolvimento de uma determinada função de combate.

CONSIDERAÇÕES FINAIS

Ao analisar a interoperabilidade entre a Força Aérea Brasileira e a Aviação do Exército, com relação às doutrinas nos níveis político (PND e END), estratégico (Ministério da Defesa) e operacional (FA) e levando em consideração a análise de cada Força Singular dentro de um contexto de operações conjuntas, a doutrina foi evidenciada com oportunidades de melhoria.

Destarte, do nível político ao operacional, o termo interoperabilidade é citado de forma recorrente nas legislações e doutrinas, com foco para o adequado reaparelhamento das FA e do contínuo aperfeiçoamento da doutrina.

Outro elemento destacado ao longo desse artigo que, apesar da criação do Ministério da Defesa em 1999 e do EMCFA em 2010, as doutrinas das três Forças Armadas ainda possuem aspectos muito peculiares e necessitam de aperfeiçoamentos para o emprego conjunto.

Um dos dilemas do emprego das Forças Singulares em operações conjuntas reside em estabelecer um pensamento conjunto de forma prioritária nas FS, acima da cultura e da doutrina singular, espaço esse de difícil acesso face a história de cada força, sua missão e destinação,

algumas com tradições seculares (MB e EB), aspectos que precisam ser trabalhados para melhor integração e interoperabilidade.

Apesar da intenção do MD em padronizar os conceitos, as Forças Singulares ainda encontram dificuldades para manter a doutrina atualizada e provida da comunalidade necessária para as operações conjuntas, possivelmente devido às suas peculiaridades.

Descritores, como capacidade, ação e tarefa, apresentam divergências que poderão ocasionar dificuldades de compreensão quando empregados em uma Ordem de Operações Conjunta.

A demanda pela padronização doutrinária, respeitada a peculiaridade de cada força, foi identificada como uma oportunidade de melhoria. "A consciência doutrinária é fundamental ao desenvolvimento da Força, em tempos de paz, e ao sucesso, em operações de guerra." (BRASIL, 2020a, p. 39, item 3.2).

Ademais, nota-se que a hierarquia e a utilização dos conceitos doutrinários encontram diferenças que poderão gerar dúvidas quando do emprego em um contexto de operação conjunta.

A sugestão seria que a legislação, principalmente as doutrinas das Forças Singulares, contemplasse de forma objetiva a comunalidade, facilitando a compreensão, sobretudo no que tange à elaboração dos Planos Conjuntos, e minimizando possíveis interpretações equivocadas pelo uso de definições e descritores distintos.

Por fim, este artigo identificou que são necessários aprimoramentos em ambas as Forças, bem como em nível de normas da competência do MD, como é o caso das doutrinas, de forma a propiciar maior interoperabilidade entre a FAB e o EB em operações conjuntas.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Assessoria de Organização, Doutrina, Ensino, Operações e Espaço Aéreo. Portaria nº 1.597/GC3, de 10 de outubro de 2018. Aprova a reedição da **Concepção Estratégica-Força Aérea 100 (DCA 11-45)**. Boletim do Comando da Aeronáutica, Rio de Janeiro, n. 180, 15 out. 2018a.

BRASIL. Comando da Aeronáutica. Portaria nº 1.000/GM2, de 10 de dezembro de 1958. **Doutrina Básica da Força Aérea**. Boletim do MAER nº 4, de 30 de abril de 1959. Diário Oficial da União, Brasília, 5 maio 1959. Arquivo em PDF.

BRASIL. Comando da Aeronáutica. Portaria nº 1.224/GC3, de 10 de novembro de 2020. **Doutrina Básica da Força Aérea DCA 1-1**. Boletim do Comando da Aeronáutica, Brasília, n. 205, v. 1, 12 nov. 2020a.

BRASIL. Comando da Aeronáutica. Portaria nº 1.225/GC3, de 10 de novembro de 2020. **Doutrina Básica da Força Aérea DCA 1-1**. Boletim do Comando da Aeronáutica, Brasília, n. 205, v. 2, 12 nov. 2020b.

BRASIL. Comando da Aeronáutica. Portaria nº 476/GC3, de 28 de abril de 2005. **Doutrina Básica da Força Aérea DCA 1-1**. Diário Oficial da União: seção 1, Brasília, n. 81, p. 12, 29 abr. 2005.

BRASIL. **Decreto-Lei nº 2.961, de 20 de janeiro de 1941**. Cria o Ministério da Aeronáutica. Diário Oficial da União: seção 1, Brasília, 20 jan. 1941a. Disponível em: http://planalto.gov.br/ccivil_03/Decreto-Lei/1937-1946/Del2961.htm. Acesso em: 04 jul. 2020.

BRASIL**. Decreto-Lei nº 3.302, de 22 de maio de 1941**. Dá nova denominação às Forças Aéreas Nacionais e aos seus estabelecimentos. Diário Oficial da União: seção 1, Brasília, p. 10385, 24 mai 1941b. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3302-22-maio-1941-413224-publicacaooriginal-1-pe.html. Acesso em 08 mar. 2021.

BRASIL. **Decreto-Lei n. 3.730, de 18 de outubro de 1941**. Organiza o Ministério da Aeronáutica. Diário Oficial da União: seção 1, Brasília, p. 20209, 21 out. 1941c. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3730-18-outubro-1941-413890-norma-pe.html. Acesso em: 6 mar. 2020.

BRASIL. **Decreto-Lei n. 4.478, de 14 de julho de 1942**. Organiza a Força Aérea Brasileira em tempo de paz e dá outras providências. Diário Oficial da União: seção 1, Brasília, p. 11195, 16 jul. 1942. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-4478-14-julho-1942-414365-publicacaooriginal-1-pe.html. Acesso em: 15 out. 2021.

BRASIL. **Decreto-Lei n. 9.889, de 16 de setembro de 1946**. Lei de organização da Força Aérea Brasileira em tempo de paz. Diário Oficial da União: seção 1, Brasília, p. 13005, 17 set. 1946. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-9889-16-setembro-1946-450059-publicacaooriginal-1-pe.html. Acesso em: 19 out. 2021.

BRASIL. Exército. Estado Maior do Exército. **Plano Estratégico do Exército (PEEx) 2020-2023**. Brasília, DF, 2019a. Disponível em: http://www.ceadex.eb.mil.br/images/legislacao/XI/plano_estrategico_do_exercito_2020-2023.pdf. Acesso em: 20 maio 21.

BRASIL. Exército. Portaria nº 326-EME, de 31 de outubro de 2019. **Manual de Fundamentos da Doutrina Militar Terrestre (EB20-MF-10.102)**. Boletim do Exército, Brasília, n. 45, 08 nov. 2019b.

BRASIL. Ministério da Defesa. **Cenários de Defesa 2020-2039 – Sumário Executivo**. Assessoria Especial de Planejamento. Brasília: Assessoria, 2017. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/revista_cenario_de_defesa.pdf. Acesso em: 22 jun. 2020.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional, Política Nacional de Defesa e**

Estratégia Nacional de Defesa. Brasília, , 2018b. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=5063108&ts=1567531261946&disposition=inline. Acesso em: 29 jun. 2020.
BRASIL. Ministério da Defesa. Portaria Normativa nº 113/SPEAI/MD, de 1º de fevereiro de 2007.
Doutrina Militar de Defesa (MD51-M-04). 2. ed. Boletim do Ministério da Defesa, Brasília, n. 06, 09 fev. 2007.
BRASIL. Ministério da Defesa. Portaria Normativa nº 84/GM-MD, de 15 de setembro de 2020. **Doutrina de Operações Conjuntas (MD30-M-01**), 2. ed. Diário Oficial da União: seção 1, Brasília, v. 1-2, n. 178, 15 set. 2020c.
BRASIL. Ministério da Defesa. Portaria nº 9/GAP/MD, de 13 de janeiro de 2016. **Glossário das Forças Armadas MD35-G-01**. 5ª ed. Diário Oficial da União: seção 1, Brasília, n. 14, de 21 jan. 2015.
CORRÊA, F. G. **Planejamento Baseado em Capacidades e Transformação da Defesa: desafios e oportunidades do Exército Brasileiro.** Artigos Estratégicos, Brasília, DF, v. 8, n. 1, jan./jun., 2020. ISSN: 2525-7099.
DOUHET, G. O Domínio do Ar. **Instituto Histórico Cultural da aeronáutica**. Rio de Janeiro: Itatiaia 1988. Coleção Aeronáutica, v. 2.
McBETH, M. S. A Theory of Interoperability Failures. **8th International or Innovation in Collaborative Networks**. IFIP Advances in Information and Communication Technology, v. 307, 2003.
MITCHELL, W. **Winged defense: the development and possibilities of modern air power, economic and military**. New York: Dover Publications, Inc., 1988.
MOON, T.; FEWELL, S.; REYNOLDS, H. **The what, why, when and how interoperability. Defense & Security Analysis**, v. 24, n. 1, p. 5-17, mar. 2008.
NORTH ATLANTIC TREATY ORGANIZATION (NATO). **Interoperability for joint operations. Backgrounger**. jul. 2006. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120116_interoperability-en.pdf. Acesso em: 08 dez. 2021.
PEREIRA, M. V G. **Poder Aeroespacial: a contribuição da Aviação do Exército para o domínio do ar**. Dissertação (Curso de Mestrado em Ciências Aeroespaciais) – Universidade da Força Aérea, Rio de Janeiro, 2022.
SANTOS, M. **Evolução do Poder Aéreo**. Rio de Janeiro: Edição Instituto Histórico Cultural da Aeronáutica, 1989.
TEIXEIRA JR, A. W. M; FREIRE, M. E. L. S. **A importância da Interoperabilidade como Instrumento de Convergência nas Operações Militares do Brasil**, Brasília, v. 6, n. 1, Artigos Estratégicos, jan/jul, 2019.
WARDEN III, J. A. **O inimigo como sistema**. Airpower Journal, Alabama, 3. trim. 1995b. p. 44-59.

NOTAS

[1] A doutrina da FAB de 1958 foi o primeiro documento dessa natureza, trazendo os conceitos, descritores e ações de Força Aérea pela primeira vez aglutinados em um único documento.
[2] "[...] capacidade que uma força, empregando meios aéreos no campo de batalha, possui para: atuar em profundidade, antecipando-se ao inimigo; localizar e engajar forças da linha de contato; alertar sobre o esforço inimigo; redirecionar a manobra; ampliar o comando e controle; reorganizar o apoio ao combate; controlar as áreas de retaguarda; e assegurar o apoio logístico." (BRASIL, 2019b, p. 1-2, item 1.4.1.1).
[3] O conceito de Poder Aeroespacial engloba uma visão unificada de seus elementos integrantes que é constituída pela Força Aérea, a Aviação Civil, a Infraestrutura Aeroespacial, a Indústria Aeroespacial, Ciência e Tecnologia e Recursos Humanos.
[4] *Interoperability refers to the ability of different military organizations to conduct joint operations. These organizations can be of different nationalities or different armed services (ground, naval and air forces) or both. Interoperability allows forces, units or systems to operate together. It requires them to share common doctrine and procedures, each other's' infrastructure and bases, and to be able to communicate with each other.* (NATO, 2006, p.1).
[5] A operação conjunta envolve capacidade de articulação e atuação conjunta entre Forças Singulares de um mesmo país enquanto a operação combinada utiliza forças multinacionais em prol de um objetivo comum (TEIXEIRA JR; FREIRE, 2019, p. 18-19).

SOBRE O AUTOR

O Tenente-Coronel de Intendência Marcus Vinicius Gomes Pereira é Oficial do Estado-Maior do Comando de Aviação do Exército. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras (AMAN) em 2002. É mestre em Direção Estratégica pela Universidade Iberoamericana, no México, mestre em Ciências Aeroespaciais pela UNIFA e aluno de Doutorado do Programa de Pós-graduação em Pesquisa Operacional do Instituto Tecnológico da Aeronáutica (ITA). Realizou os cursos de Gestão e Assessoramento de Estado Maior (CGAEM), Avançado de Aviação, Governança em Defesa na Escola Superior de Guerra, pós-graduação em Operações Aéreas Combinadas e Curso de Controlador Aerotático na Marinha do Brasil (marcus.gomes@eb.mil.br).



CORONEL GLAIDSON
Oficial de Ligação da Aviação do Exército na Aviação do Exército Francês.

O EMPREGO DE DRONES NO EXÉRCITO FRANCÊS

UM BREVE HISTÓRICO DOS DRONES NO MUNDO

As bombas voadoras alemãs do tipo V-1, fabricadas em 1944, popularmente conhecidas como *buzz bomb,* foram predecessoras dos drones modernos, segundo alguns especialistas no assunto. Tais armamentos foram empregados durante a segunda grande guerra mundial e receberam esse nome devido ao zumbido, semelhante ao de um inseto, que faziam durante o seu voo.

A bomba V-1 foi considerada por muitos especialistas a primeira aeronave armada e sem piloto da história. Essa aeronave podia transportar uma carga de até uma tonelada de explosivos, possuía um reservatório de aproximadamente 680 litros de combustível e outro de oxigênio comprimido. Era equipada com um giroscópio e uma bússola, podendo atingir uma velocidade máxima de até 700 km/h e um alcance aproximado de 230 km.

O projeto inicial do drone, como hoje é conhecido, foi desenvolvido pelo engenheiro espacial israelense Abraham Karem, o qual fundou a empresa Leading System ao chegar nos Estados Unidos da América.

Os primeiros drones armados foram produzidos durante a década de 1990, para serem usados em missões de reconhecimento, vigilância e ataque. Atualmente, podem pesar entre poucas centenas de gramas a várias toneladas, dependendo da finalidade e do alcance pretendido.

A Guerra do Golfo revelou novas doutrinas de emprego das forças militares, armamentos e equipamentos. Um de seus principais ensinamentos para a doutrina militar foi a obtenção de dados de inteligência sobre o inimigo, em tempo real e precisa, destacando que as capacidades operacionais e técnicas dos drones fizeram parte dessa nova lógica de emprego de obtenção de dados no teatro de operações.

A recente Guerra de Donbass, entre russos e ucranianos, é um exemplo onde os drones se chocaram no contexto dos confrontos militares: por um lado, o uso de drones civis pelo exército ucraniano em suas operações, por outro, o uso de drones militares pelo exército russo. Pode-se notar nessa ocasião, o nível de tecnologia alcançado pelos drones civis em relação aos seus equivalentes militares.

Com relação ao conflito na Ucrania, estima-se que o Irã tenha fornecido centenas de drones às Forças Armadas Russas, os quais são utilizados no conflito armado para atacar blindados e a artilharia ucraniana. Nas proximidades da cidade de Kherson, por exemplo, drones kamikazes [1] foram usados para destruir veículos militares e obuses, cabendo ressaltar que infraestruturas civis também foram atacadas nas cidades de Odessa e Mikolaiv.

A HISTÓRIA DOS DRONES NA FRANÇA

O Exército Francês tem uma antiga história em relação aos drones. Há mais de um século, a primeira aeronave não tripulada decolava de uma base militar na cidade de Avord, na região central da França. O capitão francês Max Boucher, em 2 de julho de 1917, decolou um avião Voisin de 150 cavalos de potência (HP) e sem piloto a bordo, percorrendo uma distância de aproximadamente 1 Km e uma altitude de 50 metros.

Em 14 de setembro de 1918, Max Boucher realizou um novo voo com uma aeronave Voisin BN3 durante aproximadamente 50 minutos, percorrendo uma distância de quase 100 km.

Com o fim da 1ª Guerra Mundial os testes foram parados, sendo retomados no ano de 1921. O capitão Max Boucher e o engenheiro Maurice Percheron aperfeiçoaram os sistemas do Voisin BN3, equipando com um piloto automático de três eixos giroscópicos elétricos e servos comandos, dando assim, continuação aos seus testes iniciais.

Em 17 de abril de 1923 novos voos

foram realizados pelos franceses no campo de Étampes, agora pelo capitão Arbanère, contando com a supervisão de Lurent-Eynac, subsecretário de Estado da Aeronáutica. Nesse ano foi apresentado o avião automático "de Boucher", que era capaz de realizar voos de pouso e decolagem sem pilotos a bordo, esses ensaios pararam no ano de 1924.

A França retoma a questão dos drones durante os conflitos dos Balkans. Na década de 1960, o Exército francês pediu à empresa Nord-Aviation que desenvolvesse um engenho voador sem a necessidade de piloto embarcado, para realizar missões de reconhecimento. Foi desenvolvido o R-20 que era controlado por rádio controle e lançado de uma rampa de 10 metros.

A Guerra do Golfo (1990-1991) marcou outra retomada de utilização de drones pelos franceses, principalmente devido a construção do drone MART (Mini Avião de Reconhecimento Telepilotado), o qual foi bastante utilizado para reconhecimentos pelo 61° Regimento de Artilharia (61° RA), situado na cidade francesa de Chaumont.

Desde outubro de 2014, foram registrados, na França, vários sobrevoos de drones civis em pontos sensíveis, por exemplo, usinas nucleares e instalações militares. Em um contexto marcado por uma ameaça terrorista, essas intrusões no território nacional são uma verdadeira fonte de preocupação, tanto para a população civil, como para o poder público.

No ano de 2019, a França realizou sua primeira missão de ataque com drone durante as operações no Mali, onde diversos combatentes foram neutralizados em operações na região central de Mopti.

Mas, o que é um drone? A palavra drone, no idioma inglês, significa zangão, devido ao som do zumbido que esse inseto faz ao voar. Ademais, consiste em ser um veículo aéreo não tripulado (VANT), o qual possui um controle de voo, pilotado a distância e que recebe comandos por meio de radiofrequência, infravermelho ou coordenadas *Global Navigation Satellite System* (GNSS, sigla no inglês), por intermédio de seus sistemas embarcados. Além do mais, Podem ter a aparência de pequenos insetos, helicópteros, aviões ou multirotores com quatro, oito e até 12 motores, podendo utilizar combustível ou eletricidade para seu voo.

Um drone, também denominado Unmanned Aerial System (UAS, sigla em inglês) [2] ou, ainda, Remotely Piloted Aircraft Systems (RPAS, sigla em inglês) [3] é, portanto, uma aeronave não tripulada (tripulação não embarcada), controlada remotamente ou autónoma, que pode eventualmente estar armada, bem como é destinada a cumprir missões de vigilância, reconhecimento, inteligência, combate, transporte, dentre outras.

Para o Ministério da Defesa francês, um drone é um dispositivo móvel terrestre, aéreo ou naval, sem tripulação de bordo, programado ou controlado remotamente e que pode ser reutilizável.

DRONE NAS GUERRAS MODERNAS

Um relatório do Comitê de Defesa do Senado da França concluiu que as Forças Armadas francesas deverão ter sua frota de drones aumentadas até o final de 2025 e que também, devem adquirir a capacidade de proteção, diante do uso desse meio como uma ameaça.

Esse tema ganhou força no ano de 2020, quando foi observado que cerca de 58% dos ataques realizados na faixa do Sahel-Saara foram realizados por drones Reaper armados. A França possui um programa chamado: Drone MALE RPAS (Sistema de Aeronaves Remotamente Pilotada de Média Altitude e Longa Duração), também denominado de EURODRONE [4], o qual visa substituir os Reapers e que contará com a cooperação da Alemanha, Espanha e Itália. Suas principais missões serão: inteligência, vigilância, aquisição de alvos e reconhecimento. A França pretende encomendar inicialmente seis desses sistemas, os quais serão entregues ainda na década de 2020.

A gestão do projeto EURODRONE será confiada à Airbus Defense and Space GmbH (Alemanha), Dassault Aviation (França), Leonardo (Itália) e Air Bus DS SAU (Espanha).

Existe um outro objetivo de que todos os regimentos franceses sejam equipados até meados da década de 2020 com drones NX70 e drones PARROT. Assim, a França busca dar celeridade a compra desses pequenos drones, também denominados drones de contato. Foram adquiridos cerca de 210 nano drones Drop e 67 micro drones NX70, os quais começaram a ser entregues no ano de 2019. O Exército francês planeja adquirir cerca de

3000 drones, os quais serão distribuídos para todos os seus regimentos.

Um relatório do parlamento francês ressalta a importância dos drones no teatro de operações. Vários conflitos recentes, como a guerra de Nagorno-Karabakh em 2020, os combates na Líbia em setembro de 2019 e a campanha turca no norte da Síria em março de 2020, foram marcados pelo uso massivo de drones táticos e pequenos drones para cumprir várias tarefas, dentre as quais: guiar fogos de artilharia, servirem de chamarizes, voos em formação de enxame e ataques suicidas.

Um fato importante na atualidade é que, no ambiente de operações mais complexas e de multidomínio, o Exército francês usa drones para cumprir uma variedade de tarefas. Possuem tamanhos diferentes e, portanto, têm missões específicas e diferenciadas. Os sensores transportados, a tecnologia e a autonomia diferem de acordo com o tamanho e tipo desse material de emprego militar, permitindo realizar missões com segurança e em profundidade.

TIPOS DE DRONES EMPREGADOS PELO EXÉRCITO FRANCES

O Exército francês possui hoje cerca de 739 drones, divididos em: sistemas de mini drones de reconhecimento, nano drones e micro drones, esperando aumentar essa frota até o ano de 2025 em cerca de 3000 drones, conforme mencionado anteriormente.

O nano drone de combate mais utilizado hoje pelos exércitos é o *Black Hornet*. Projetado e produzido pela *Prox Dynamics*, empresa norueguesa que foi adquirida pela *FLIR Systems* em 2016. A partir da década de 2010, o *Black Hornet* passou a equipar as tropas do Exército francês durante a Operação *Barkhane* [5].

A partir do ano de 2019, cerca de 210 sistemas de micro drones operacionais de bolso (DROP) foram entregues ao Exército francês e, em maio de 2021, foram encomendados mais 50 unidades desse equipamento.

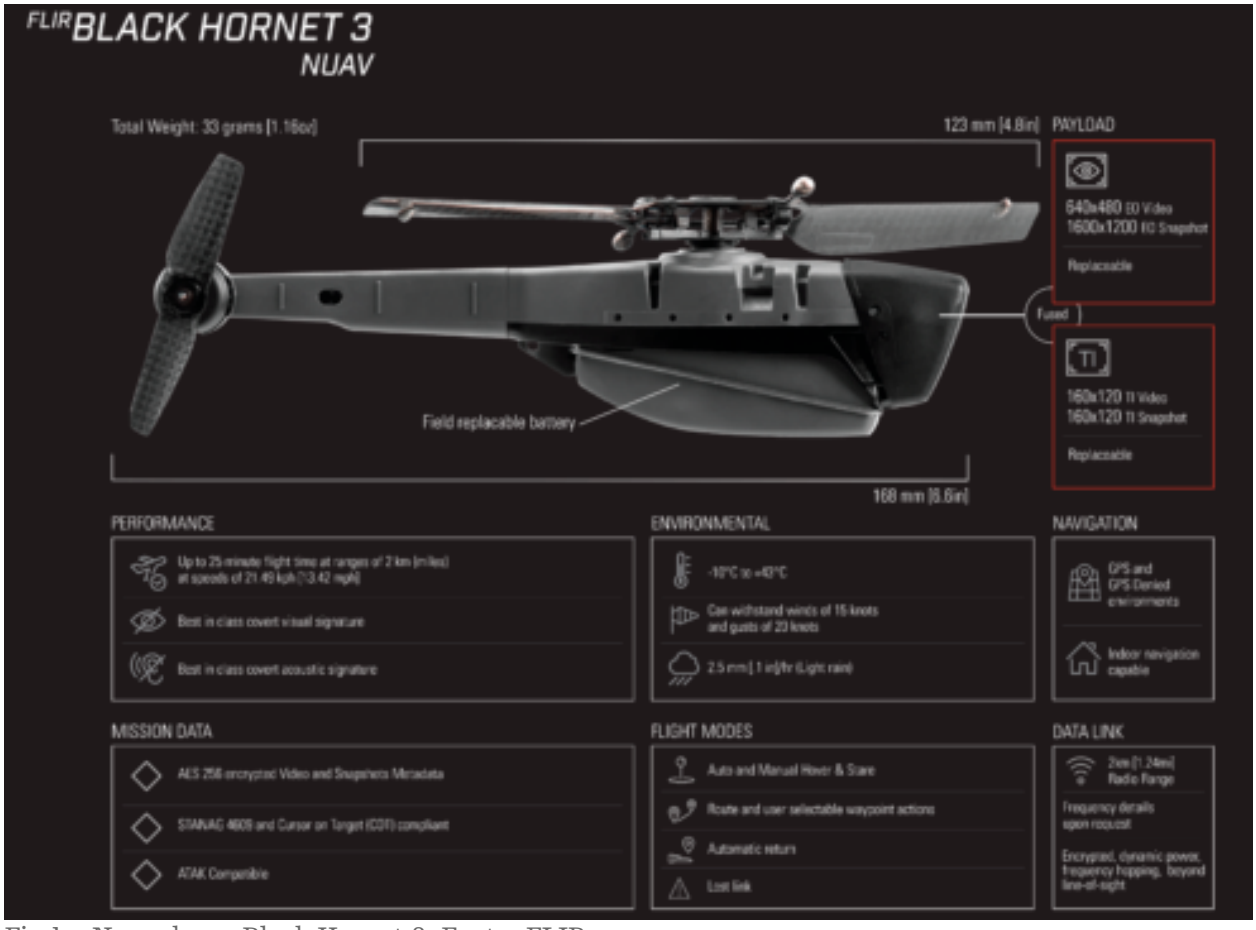


Fig 1 – Nano drone Black Hornet 3. Fonte: FLIR.

O sistema *Black Hornet* 3 é composto por dois nano drones, um controle remoto e uma tela de vizualização. O *Black Hornet* é bastante similar com um helicóptero em miniatura, tem cerca de 16 centímetros de comprimento e pesa próximo de 33 gramas, peso e tamanho que facilitam a realização de missões de reconhecimento e vigilância diurna e noturna de forma discreta, segura e silenciosa.



Fig 2 – Tela Portátil do Black Hornet 3.
Fonte: FLIR.

Em 2021, o Exército francês encomendou 300 microdrones *Parrot Anafi* à empresa francesa *Parrot*, dos quais 150 foram entregues nesse mesmo ano. Esses sistemas de micro drones atendem a uma necessidade operacional das Forças Especiais e das tropas convencionais do Exército francês.

Os drones *Parrot* são usados pelo Exército francês para o cumprimento de diversas missões e tarefas de reconhecimento e de inteligência em proveito da força, podendo realizar essas operações durante os períodos diurno e noturno.



Fig 3 – Micro drone Parrot Anafi:
Fonte: Parrot.

No final de 2020, foram encomendados, também, para o Exército francês, 49 microdrones NX70 à empresa francesa *Novadem*. Os NX70 são aeronaves discretas e de fácil manuseio. Possui, aproximadamente um quilo, tem câmera diurna e sensores térmicos que possibilitam operações com visão noturna. Também possui um *link* criptografado para evitar que seus dados sejam interceptados, autonomia de 45 minutos e opera dentro de um alcance máximo de 3 km.

Em junho de 2020, o 61º RA recebeu seus três primeiros Sistemas de Minidrone de Reconhecimento (SMDR).

Esses drones possuem a capacidade de realizar tarefas como: segurança na escolta de comboios, orientação de fogos de artilharia, detectar engenhos explosivos, dentre outras.

Um SMDR é composto por três drones *Thales Spy'Ranger* e uma estação de terra. É equipado com meios optrônicos e possui



Fig 4 - Système de Mini-Drone de Renseignement Spy Ranger. Fonte: État-Major des Armées.

capacidade de operar durante o dia e a noite. Possui uma autonomia de 2 horas e 30 minutos, podendo realizar transmissão de vídeos ao vivo e com segurança criptografada, pesa cerca de 15 Kg, possibilita a captura de imagens em ótima qualidade a uma distância de 30 Km, o que permite um apoio às unidades de combate francesa por longo tempo e a grandes distâncias.

Em junho de 2020, foram entregues ao Exército francês os três primeiros sistemas de minidrone de reconhecimento SMDR, marcando o início da substituição dos drones de inteligência de contato DRAC, em operação no 61º RA. Em 2021 foram entregues mais uma dúzia desses sistemas.

O Exército francês enviou esse mini drone para o Mali, para apoio das tropas no contexto da Operação *Barkhane*, iniciando uma nova era na capacidade tática, principalmente no que diz respeito à função de combate Inteligência.

O DRONE PATROLLER

O drone *Patroller* substituirá o *Tactical Drone System* (TDIS, sigla em inglês). Esses drones táticos começaram a ser entregues ao Exército francês no primeiro semestre de 2022. Um atraso na entrega ocorreu devido às falhas descobertas após um acidente em dezembro de 2019, quando um drone caiu perto da base aérea de Istres durante um voo de teste, sem causar vítimas. Até o seu recebimento, os pilotos de drones do 61º RA realizavam seus treinamentos no simulador de voo.

O drone *Patroller,* da *Safran Electronics & Defense,* é uma aeronave remotamente pilotada e certificada pela Organização do Tratado do Atlântico Norte (OTAN) [6] . Dotado de versatilidade e multifunções, permitindo realizar missões de monitoramento local a logas distâncias e altitudes, podendo, ainda, realizar missões de reconhecimento de área, detecção, aquisição, identificação, designação de alvos e suporte para manobras em tempo real.



Fig 5 – Drone Patroller. Fonte: 61°RA.

O *Patroller* possui uma autonomia aproximada de 20 horas, pode transportar até 250 kg de carga útil e possui 8,5 metros de comprimento com 18 metros de envergadura. Além disso, permite monitorar uma área dentro de um raio de até 180 Km, a uma altitude de até 16.000 pés. Sua estação terrestre também é interoperável com sistemas e redes de comando da OTAN.

Esse sistema compreende, além dos vetores aéreos, estação de terra, sensores, um sistema de decolagem automática, meios optrônicos Euroflir 410, os quais permitem observação infravermelha, possuindo também *lasers* para designação de alvos.

Um relatório do Senado francês, de junho de 2021, ressaltou a importância em avançar na questão do sistema de armas desses drones táticos ou, pelo menos, possuir essa capacidade, tanto para suprir uma necessidade do Exército francês como também para garantir a competitividade do *Patroller* face aos seus concorrentes americanos, israelenses e turco, os quais podem ser armados.

Assim, o Exército francês, em 2019, demonstrou a intenção de armar o *Patroller*, sendo um dos possíveis candidato a armamento, o foguete guiado a *laser* Thales 68mm.

O CENTRO DE TREINAMENTO DE DRONES E A FUTURA ESCOLA DE DRONES

O Exército conta hoje com um Centro de Treinamento de Drones (CFD) que tem a finalidade de formar os pilotos, pessoal de manutenção, analistas de imagem e demais militares que operarão essas aeronaves.

O centro de treinamento de drones está localizado no 61º RA, o qual possui a capacidade de formar cerca de 900 militares por ano, contando atualmente o Exército francês com cerca de 2600 operadores de drones formados.

Possui como principais missões: treinamento de todos os operadores de todos os tipos de drones, elaboração de cursos e evolução da doutrina, controlar a qualificação dos pilotos de drones, elaboração de manuais, instrução e treinamento das demais equipes que dão suporte à operação, como por exemplo, os operadores de imagem dos regimentos.

A formação ministrada aos militares no CFD compreende assuntos como: técnica de pilotagem, análise de imagens e informações, sua utilização para fins táticos, regras de navegação e segurança de voo.

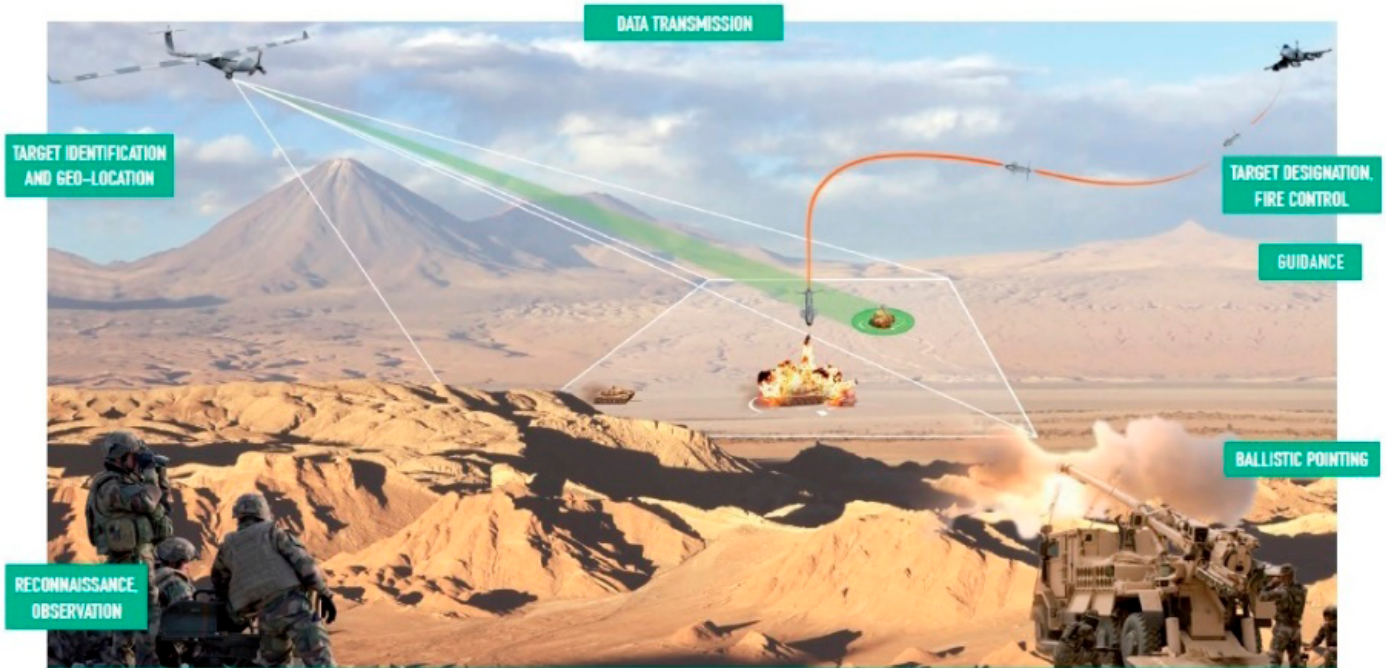


Fig 6 – Emprego do drone Patroller. Fonte: Safran Eletronics & Defense.

Os operadores de drones são treinados de acordo com os diferentes modelos de aeronaves remotamente pilotadas e de acordo com os diferentes tipos de missões que poderão executar nas operações futuras, podendo o ciclo de cada treinamento durar de uma semana até meses.

O CFD é apoiado pelo Comando de Aviação do Exército Francês (COMALAT), por meio da sua Escola de Aviação (EALAT), localizada na cidade de Dax. O COMALAT e a EALAT se ocupam das instruções relativas à segurança de voo e a formação e obtenção da licença para pilotos de aeronaves leve (LAPT).

Devido ao aumento do número de drones e de missões, o Exército francês sentiu a necessidade de criar uma Escola de Drones. Essa escola funcionará a partir do ano de 2023 ao lado do 61º RA , onde todos os meios e pessoal que hoje se encontram nas suas dependências serão alocados para essa escola.

A Escola de Drones será responsável pela formação de todos os operadores e demais especialistas em drones do Exército, na qual serão incluídos também assuntos relacionados à segurança de voo e à formação de pilotos de aeronaves leves, hoje a cargo da EALAT da cidade de Dax.

CONSIDERAÇÕES FINAIS

Há ideia do uso de aeronaves remotamente pilotada não surgiu recentemente, mas sim décadas atrás. Os drones se tornaram, com o passar dos anos, dispositivos de alta tecnologia capazes de realizar observação, adquirir informações e realizar missões de ataque de forma rápida, precisa e em tempo real.

As operações no ambiente multidomínio constituem o novo paradigma técnico-operacional das guerras modernas. Constituem novas táticas operacionais a serem implementadas a fim de que se possa fazer face as novas ameaças presentes no cenário agora geopolítico e não mais reduzido apenas ao campo de batalha, sendo o aumento do uso de drones um exemplo desses novos paradigmas.

Na Guerra na Ucrânia, russos e ucranianos intensificaram o uso de drones para cumprir diversos tipos de missões em proveito de suas forças armadas. Como consequência desse conflito recente, o Exército francês também pretende aumentar e diversificar, até 2025, a sua frota de drones, a fim de possuirem a capacidade para cumprir missões de vigilância, observação, inteligência, levantamento de alvos e ataques a viaturas militares, tropas e a alvos estratégicos.

O Exército francês terá um ganho considerável na sua capacidade de operação com drones com a aquisição do *Patroller e do Eurodrone*. Esses drones possuem uma grande autonomia, versatilidade e possibilidade de ser equipados com um sistema de armas, a fim de ser utilizados em missões de proteção de suas tropas e ataques a alvos compensadores em profundidade.

Nos últimos anos, os drones tornaram-se dispositivos mais complexos com tecnologia e diversos sistemas embarcados, capazes de cumprirem missões diurnas e noturnas em proveito do Exército francês. Assim, o Exército investe cada vez mais na capacitação de seus operadores e equipes de manutenção, no seu Centro de Treinamento de Drones, baseado no 61º Regimento de Artilharia de Chaumont e a partir do ano de 2023, na Escola de Drones, possibilitando assim, o emprego de forma eficaz e eficiente desse equipamento nas suas operações militares, uma vez que, existem diferentes tipos de drones e a técnica de pilotagem e operação, não é a mesma para todos.

Por fim, o drone é um recurso tático importante para o Exército francês que vem evoluíndo com o passar do tempo, tornando-se um ator importante nos teatros de operações terrestre, aéreo e marítimo. Outro entendimento é que, os drones devem ser combatidos caso sejam utilizados por outros exércitos convencionais ou forças não convencionais contra suas tropas, instalações e população civil, crescendo desse modo, a necessidade de se desenvolver sistemas antidrones baseados nas capacidades de detecção, identificação e neutralização dessas ameaças.

REFERÊNCIAS

FRANCE. **Les systèmes de drones de l'armée de terre.** Disponível em: https://defense-zone.com/blogs/news/systemes-drones-armee-de-terre .Acesso em: 22 set. 22.
FRANCE. **L'armée de Terre a déployé le système de mini-drones de reconnaissance Spy'Ranger au Mali.** . Disponível em: http://www.opex360.com/2021/01/17/larmee-de-terre-a-deploye-le-systeme-de-mini-drones-de-reconnaissance-spyranger-au-mali/. Acesso em: 21 set. 22.
FRANCE. Armée de Terre. **Défense. Brochure_PCAT_2020**.
FRANCE. Centre de Renseignement Terre. **La Menace Drone Sur Les Théâtres D'Opérations**. 2018.
FRANCE. Armée de Terre. Défense. **Les chiffres clés de la Défense**. 2021.
FRANCE. **PATROLLER – RPAS. The tactical long-endurance Remotely Piloted Aircraft System**. 2020.
FRANCE. Armée de Terre. Commandement de L'Aviation Légère de L'Armée de Terre. **Étude sur L'Intégration de Drones a L'Engagement Aéromobile**. Villacoublay, 2012.
FRANCE. Ministère de La Défense. Armée de Terre. Centre de Doctrine D'Emploi des Forces. **Concept D'Emploi Des Drones Dans Les Force Terrestres.** Edition 2010

NOTAS

[1] Drones Kamikases – é um drone de combate aéreo, contendo um explosivo. Ele é projetado para evoluir sobre o campo de batalha e destruir alvos, mergulhando sobre eles durante as missões de busca de oportunidade, ou seja, tanto de reconhecimento como combate.
[2] *Unmanned Aerial System* - Veículo aéreo não tripulado (UAV), comumente conhecido como drone, é uma aeronave sem qualquer piloto embarcado, tripulação ou passageiros a bordo.
[3] *Remotely Piloted Aircraft System* (RPAS, na sigla em inglês) –é o termo técnico e padronizado internacionalmente pela OACI para se referir aos sistemas de aeronaves remotamente pilotadas utilizadas com propósitos não recreativos. Drone é o termo utilizado de forma coloquial e popular para se referir aos equipamentos remotamente pilotados.
[4] EURODRONE – O projeto de drone Medium Altitude Long Endurance Remotely Piloted Aircraft System (MALE RPAS, na sigla em inglês) ou Eurodrone visa fornecer um drone de reconhecimento, voando a média altitude e com longa autonomia para as forças aéreas francesas, alemãs e espanholas.
[5] Operação *Barkhane* – Operação *Barkhane* é uma operação anti-insurgente em curso na região do Sahel, na África, iniciada em 1 de agosto de 2014.
[6] A Organização do Tratado do Atlântico Norte (OTAN) – A é uma organização intergovernamental formada por 30 países, que se ajudam mutuamente em termos políticos e militares. Criada no contexto da Guerra Fria, em 1949.

SOBRE O AUTOR

O Coronel de Infantaria Glaidson Santos da Penha é Oficial de Ligação do Exército Brasileiro junto à Aviação do Exército Francês. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras (AMAN) em 1997. Realizou a Escola de Aperfeiçoamento de Oficiais (EsAO) em 2005, o Curso de Comando e Estado-Maior do Exército (ECEME) nos anos de 2015 e 2016, o Curso de Operações na Selva Cat B (CIGS), o Curso de Piloto de Aeronaves, Piloto de Combate e Avançado de Aviação (CIAvEx) e os Cursos de Prevenção e Investigação de Acidentes Aeronáuticos no Cento de Investigação e Prevenção de Acidentes Aeronáuticos (CENIPA). É Bacharel em Direito pela Universidade de Taubaté e possui a especialização em Direito Militar. Comandou o 3° Batalhão de Aviacão do Exército no triênio 2019-2020-2021 (glaidson.santos@eb.mil.br).



MAJOR TIAGO FRANÇA
Comandante do Curso de Infantaria da Escola de Aperfeiçoamento de Oficiais.

A RELEVÂNCIA DOS COMBATES URBANOS NA 1ª FASE DO CONFLITO NA UCRÂNIA

A Guerra entre Rússia e Ucrânia teve início em 24 de fevereiro de 2022. Diferentemente de outros conflitos contemporâneos, esse, ainda em curso, tem tido amplo uso da guerra convencional. Seus principais contendores são as forças russas e ucranianas.

A guerra, até este momento, pode ser dividida em 3 fases [1]. A 1ª Fase, objeto do presente artigo, foi caracterizada por uma ampla ofensiva da Rússia em diversas direções. A 2ª Fase, por sua vez, foi caracterizada pela reorganização das forças russas e pela consequente concentração dos combates no Leste da Ucrânia. A 3ª Fase teve início com a pausa operacional russa e a ampla contraofensiva ucraniana no leste.

Da análise da 1ª Fase, já encerrada, o Centro de Doutrina do Exército Brasileiro, conforme Brasil (2022), dividiu a área de operações em quatro frentes de combate principais: direções operacionais Eixo Sul (Crimeia), Eixo Sudeste (Donbass), Eixo Leste (Kharkiv) e Eixo Norte (Belarus-Kiev). O avanço russo ocorreu sobre tais regiões.

Dentro desse contexto, mesmo com o surgimento de novas táticas, diversos aspectos doutrinários foram confirmados na 1ª Fase. Um desses conceitos pode ser verificado no manual EB70-MC-10.244 - Corpo de Exército, o qual versa que "a finalidade imediata da operação ofensiva resume-se em conquistar áreas ou regiões que lhe proporcionem vantagem marcante, destruição de forças inimigas e a combinação de ambas as finalidades" (BRASIL, 2020). Ainda segundo o mesmo documento, o reflexo de tal conquista seria a ampliação da liberdade de ação nos níveis político, estratégico e operacional.

Na 1ª Fase do atual conflito entre russos e ucranianos, foi verificado amplo emprego de meios de ambos os contendores para a conquista de grandes e médios centros urbanos, como Kharkiv, Kiev, Mariupol, Mykolaiv, Kherson e outros. Os combates nessas cidades foram difíceis, intensos, lentos, com grande quantidade de perdas materiais e humanas e, ainda, com grande exposição perante as operações de informação do inimigo.

Sendo assim, por que as forças russas e ucranianas têm concentrado meios e empreendido grande esforço para dominar os principais centros urbanos? Não seria óbvio para os russos evitar atacar diretamente as principais posições defensivas do inimigo ucraniano?

Segundo o manual EB70-MC-10.223-Operações:

> áreas edificadas caracterizam-se como acidentes capitais, normalmente, em função do controle de vias de transporte e passagem sobre rios obstáculos, de domínio de vias fluviais navegáveis, da existência de um porto ou aeroporto, da existência de parque industrial e tecnológico, dentre outros. (BRASIL, 2017)

Logo, verifica-se que há vantagens significativas no domínio sobre centros urbanos. O presente artigo pretende, portanto, descrever como tal conceito foi aplicado no caso de importantes localidades ucranianas no atual conflito entre Ucrânia e Rússia. Assim, este autor visa a responder a tais questões, no caso específico desta guerra, demonstrando as vantagens obtidas e explicando, de forma contextualizada, algumas razões pelas quais os russos visaram ao domínio de tais cidades na 1ª Fase da Guerra.

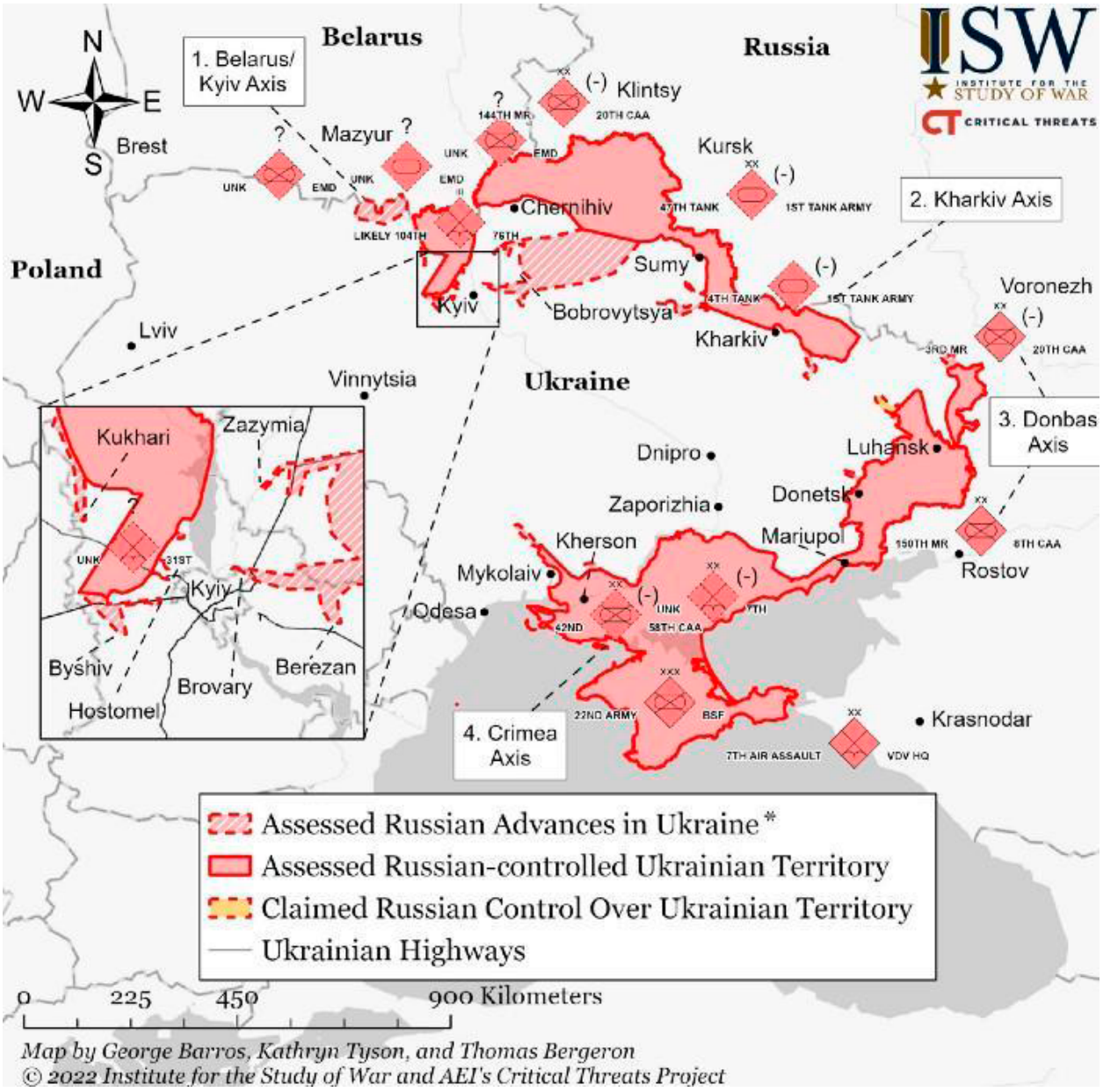


Fig 1- Eixos da 1ª Fase. Fonte:https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-4.

EIXO-SUL (CRIMEIA)

O Eixo Sul caracterizou-se por estar em uma das regiões de maior importância econômica para a Ucrânia, não somente devido à produção, mas, principalmente, por englobar boa parte do litoral ucraniano e seus principais portos, os quais são importantes para a logística tanto em tempos de guerra como em períodos de normalidade.

Nessa região, pode-se destacar as localidades de Kherson, Mykolaiv, Odessa e Melitopol. Além disso, há naquela área, como obstáculo significativo, o Rio Dniepre, que se estende por mais de 2000 km, desde a Rússia, e corta o território ucraniano de norte a Sul.

Odessa é a 4ª maior cidade ucraniana, com pouco mais de 1 milhão de habitantes. Sua área metropolitana engloba dois grandes portos, sendo um homônimo ao município e o outro o de Yuzhny, um importante terminal petrolífero. Segundo Deutsche Welle (2022), o Porto de Odessa é o maior da Ucrânia, com capacidade anual para 40 milhões de toneladas métricas de carga sólida e 25

milhões de toneladas de carga líquida.

Outrossim, a cidade de Odessa ofereceria uma grande vantagem logística à Rússia, com o controle do litoral de seu inimigo, negando-lhe o uso do mesmo e utilizando tal porto para si, como porta de entrada para um grande volume de suprimentos e outros meios necessários à guerra. Além disso, a perda definitiva dessa área degradaria o poderio ucraniano no pós-guerra, devido à sua importância econômica. Pode-se supor, assim, que o domínio de tal localidade fosse um dos objetivos russos do Eixo Sul.

No entanto, duas outras localidades importantes se interpunham entre Odessa e a Crimeia: Kherson e Mykolaiv. A primeira abriga os principais locais de passagem sobre o Rio Dniepre daquela região, e a segunda é um importante nó rodoviário.

Tal afirmação se dá devido ao fato de que a rodovia identificada como M14 se apresentava como um eixo logístico essencial a partir de Nova Kakhovka em direção a Odessa. Essa via passa, justamente, por Kherson. Logo, o domínio dessa área urbana, ou de parte dela, constituiu objetivo decisivo para a evolução da ofensiva russa para o oeste no Eixo Sul.

As passagens próximas a Kherson foram dominadas pelos russos em 26 de fevereiro. Após isso, a ofensiva russa obteve relativo sucesso e só foi contida pelos ucranianos na região de Mykolaiv, 5 horas depois. Essa localidade, como pode ser observado na Figura 2, é um importante nó rodoviário da região. A Rodovia M14, principal ligação rodoviária de Odessa para o Leste, passa por essa cidade.

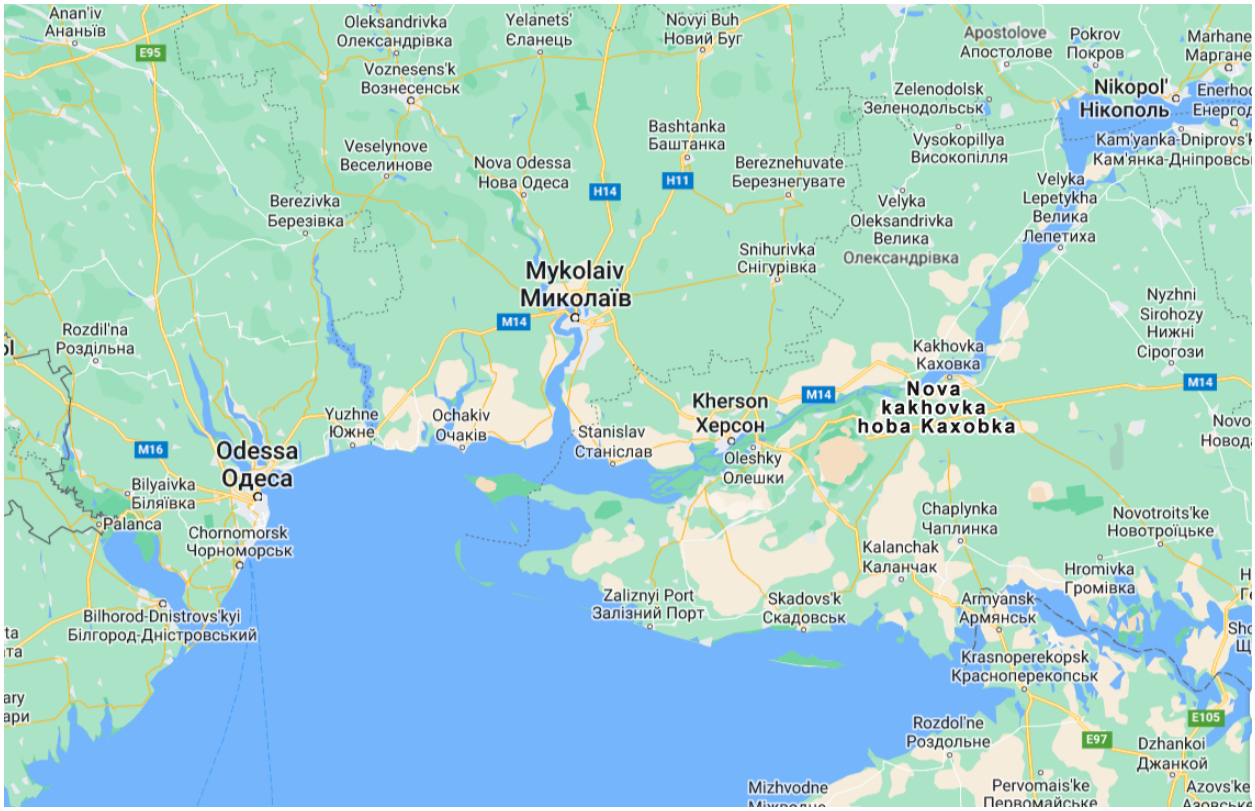


Fig 2- Ligações entre Crimeia, Kherson, Mykolaiv e Odessa. Fonte: Google Maps.

Como pode ser verificado no mapa acima, existem duas principais áreas de passagem rodoviária sobre o Rio Dniepre na região: Kherson e Nova Kakhovka. A segunda, no entanto, não evitaria a passagem pela primeira em uma ofensiva em direção a Odessa.

Kherson foi dominada completamente em 2 de março de 2022.

Outra ligação rodoviária entre Kherson e Odessa pode ser identificada na Figura 2, utilizando estradas mais ao Norte, de menor capacidade, e passando por localidades

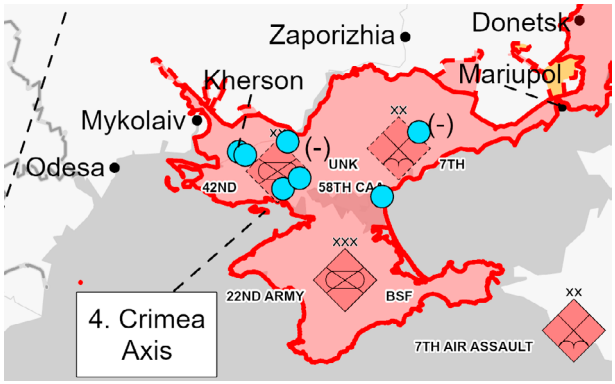


Fig 3- Eixo Sul. Fonte: Instituto para o Estudo da Guerra disponível em https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-8

menores, como Yelanets e Novyi Buh, e totalizando em cerca de 385 km. O caminho por Mykolaiv é de, aproximadamente, 220 km, ou seja, em torno de 165 km menor, e exigiria, então, menos combustível, meios e tempo caso fosse utilizado como eixo logístico na progressão russa para o oeste.

Outrossim, acredita-se que outros fatores possam ter contribuído para a decisão russa de investir sobre Mykolaiv e a escolha dos ucranianos de defendê-la, tais como seu importante porto e seu aeroporto. A cidade possuía, antes do conflito, cerca de 480.000 habitantes, sendo considerada uma cidade média e, consequentemente, uma área favorável à defensiva. Logo, as forças da Ucrânia a escolheram, após a queda de Kherson, como posição de defesa.

O fato é que, no auge do avanço russo na provável direção de Odessa, por volta de 8 de março, os russos ainda estavam contidos em Mykolaiv, a qual estava sob o domínio ucraniano. Como pode ser verificado na Figura 3, houve a tomada das áreas que abrangiam as rodovias ao norte, que desbordavam esta área urbana. No entanto, não houve progresso significativo das forças da Rússia além dessa área. Presume-se, assim, que a posse de Mykolaiv para as forças da Ucrânia contribuiu na contenção de seu inimigo.

Ainda no Eixo Sul, em sua progressão em direção à região de Donbass, destacaram-se os combates na cidade de Melitopol, iniciados no segundo dia da guerra, em 25 de fevereiro.

Melitopol, como é possível verificar na Figura 4, domina todas as rodovias que ligam a Crimeia a Donetsk, já sob domínio russo, e a Mariupol entre o Rio Dniepre e o Mar de Azov. Rapidamente dominado pelos russos, em 1º de março, tal nó rodoviário permitiu rápida progressão até Mariupol, já na região de Donbass.

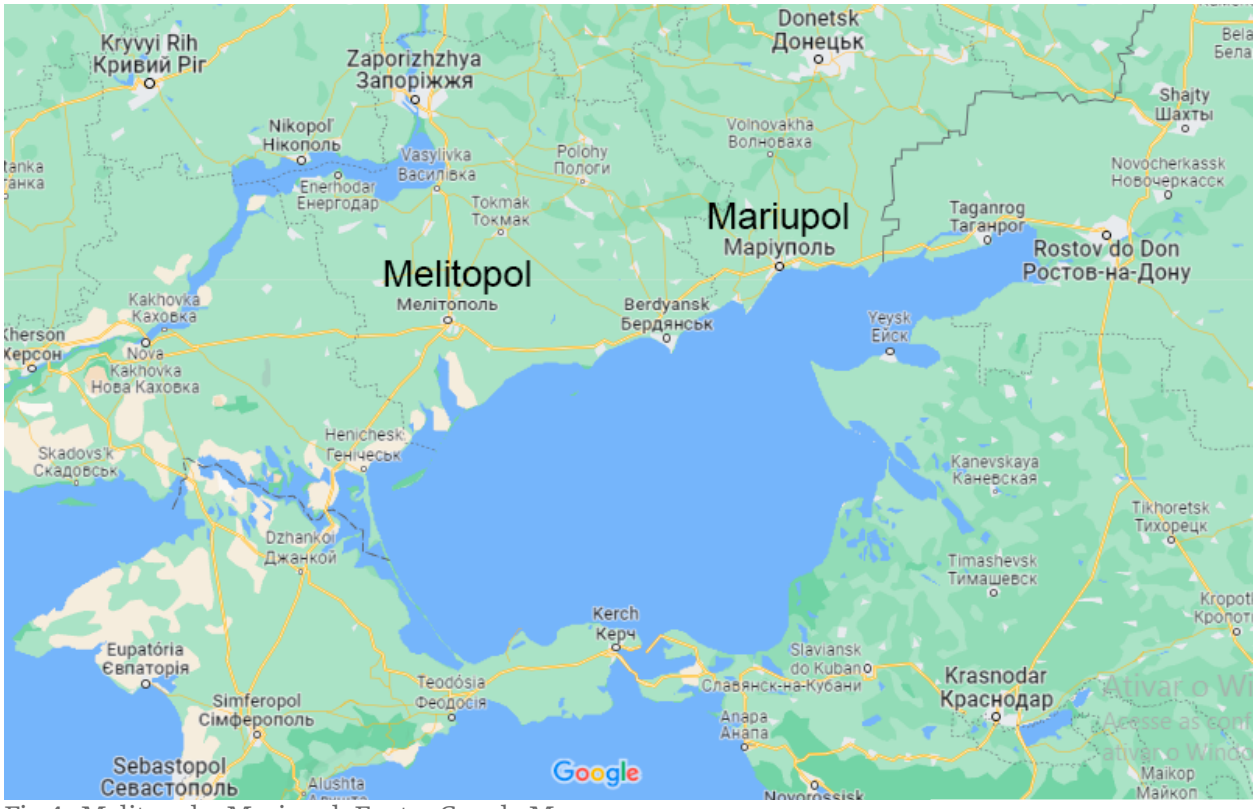


Fig 4- Melitopol e Mariupol. Fonte: Google Maps.

EIXO-SUDESTE (DONBASS)

O Eixo Sudeste (Donbass) se caracterizou por ter se desenvolvido em uma região na qual boa parte do território já estava sob controle russo desde 2014. As principais localidades, Donetsk e Luhansk, já estavam sob domínio dos separatistas e foram utilizadas pela Rússia para a sua progressão.

Mariupol, também na região do Donbass, é uma localidade com cerca de 500 mil habitantes, média para os padrões ucranianos e, então, com simbolismo. Já havia sido alvo de ataques russos em 2014, sem sucesso, nos conflitos separatistas que culminaram com a perda do controle ucraniano sobre parte das regiões vizinhas de Donetsk e Luhansk.

A posse de Mariupol era fundamental para as regiões separatistas por ser uma importante área industrial, com destaque para as siderúrgicas, como a de Azovstal, uma das maiores da Europa e símbolo da defesa ucraniana na cidade. Essas fábricas tinham relevância estratégica para ambos os contendores.

Além disso, o Porto de Mariupol possui ancoradouros profundos e é o maior da região do Mar de Azov. Está localizado a cerca de 85 km do reduto separatista de Donetsk e seu domínio poderia propiciar grande vantagem logística aos russos. O acesso a tal porto propiciaria à Rússia mais uma porta de entrada marítima para os suprimentos necessários às suas tropas que combatiam no Eixo Sudeste.

Além disso, após a queda de Melitopol, não havia mais significativos obstáculos no terreno, entre a Crimeia e Donbass, que favorecessem ao estabelecimento de uma posição defensiva. Logo, presume-se que a área urbana de Mariupol era a área que permitia que as forças ucranianas se interpusessem entre as forças russas dos Eixos Sul e Sudeste.

O sucesso na conquista de Melitopol (Eixo Sul) permitiu, porém, que os russos realizassem um cerco a Mariupol, como pode ser visto na Figura 3, pois passaram a dominar suas ligações terrestres a Sul. As forças do Eixo Sudeste já dominavam as ligações a Norte desde 25 de fevereiro de 2022 e conquistaram o terreno a Oeste da localidade posteriormente. Tal fato colocou as forças ucranianas, que defendiam essa cidade portuária, em grande desvantagem, principalmente pela falta de capacidade de sustentação logística.

Não obstante, houve a recusa das tropas ucranianas daquela cidade em se renderem, dentre as quais estava o Batalhão Azov, famoso pelo seu nacionalismo e acusado pela Rússia de ser difusor da ideologia neonazista. Mariupol era a sede desses militares. Essa, presume-se, tenha sido uma razão importante para a opção russa de tomar aquele centro urbano e impor uma derrota ou, até, destruir a unidade militar mais famosa da Ucrânia. Dessa forma, os combates naquela localidade tinham grande importância para a dimensão informacional, uma vez que Vladimir Putin alegava estar "desnazificando" aquele país, e incluíam uma questão moral para ambos os contendores.

O domínio de Mariupol pela Rússia se concretizou na 2ª Fase do conflito, em meados de maio de 2022, com a intensificação da ofensiva no leste da Ucrânia, após grande resistência ucraniana. Com duração de cerca de 80 dias, foi considerada a batalha mais longa, até então, dessa Guerra e uma das maiores em solo europeu desde a 2ª Guerra Mundial.

EIXO-LESTE (KHARKIV)

O Eixo Leste (Kharkiv), na 1ª Fase do conflito, teve como principais direções de progressão, partindo da fronteira russa: o avanço para Kiev; e o avanço para Donbass, passando por Kharkiv.

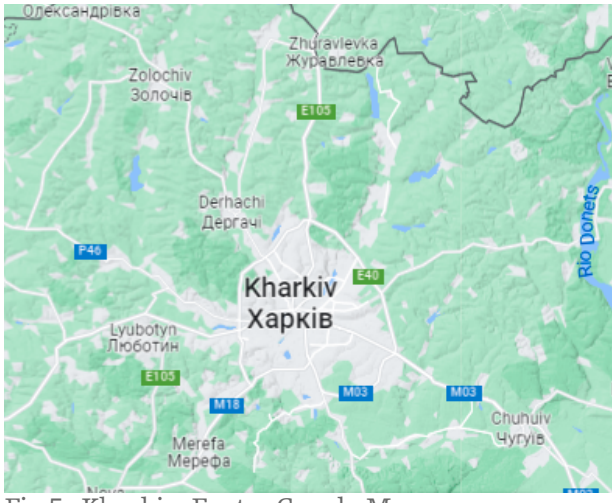


Fig 5- Kharkiv. Fonte: Google Maps

A progressão em direção às proximidades de Kiev, no Eixo Leste, não enfrentou significativa resistência. Em Kharkiv, contudo, a situação foi diferente.

Os combates por Kharkiv foram intensos e começaram logo no início da guerra, em 24 de fevereiro de 2022. Tal fato demonstra que essa cidade era um dos primeiros objetivos russos, visto que está a cerca de 40 km da fronteira.

Outrossim, se levarmos em conta que não há um rio obstáculo entre Kharkiv e o território russo, bem como a proximidade entre ambos, pode-se presumir que esse centro urbano era a área mais favorável à defensiva ucraniana nessa região.

Kharkiv é uma cidade histórica e uma das maiores da Ucrânia, com cerca de 1 milhão e 500 mil habitantes. Esse centro urbano possuía, ainda, importantes indústrias para o país e, principalmente, para a sua defesa, tais como: as fábricas do Grupo Malyshev (indústria de defesa); Khartron (eletrônica de automação de usinas aeroespaciais e nucleares); Turboatom (turbinas para usinas hidrelétricas, térmicas e nucleares); e Antonov (aeronaves de múltiplos propósitos).

A perda de importantes instalações logísticas causaria grandes danos à economia ucraniana e, de forma mais imediata, ao poder de combate de suas forças armadas, tendo em vista a importância das fábricas Malyshev e Antonov, voltadas diretamente ao material de emprego militar. Do ponto de vista russo, por sua vez, a posse de tais instalações traria vantagens à sua logística.

Kharkiv, todavia, não foi conquistada pelos russos durante a 1ª Fase da guerra, mas muitas fábricas da cidade foram destruídas ou danificadas.

EIXO-NORTE (BELARUS-KIEV)

O Eixo Norte se desenvolveu em uma região cujas ações militares, no contexto da 1ª Fase da Guerra entre Rússia e Ucrânia em 2022, tiveram grande repercussão. Isso se deve ao fato de que os combates se concentraram na maior cidade e capital ucraniana, Kiev.

Kiev é uma cidade com quase 3 milhões de habitantes, a pouco mais de 100 km da fronteira com a Rússia. Não há obstáculos naturais significativos entre essa localidade e o território russo. Presume-se, assim, que, por essas razões, a área urbana da capital foi escolhida como principal posição defensiva das forças ucranianas no Eixo Norte.

Além disso, Kiev é o maior nó rodoviário da Ucrânia e concentra importantes



Fig 6- Kiev. Fonte: Google Maps.

passagens sobre o Rio Dniepre. A região metropolitana da capital abriga, ainda, indústrias de alta tecnologia e o Aeroporto e Base Aérea de Hostomel, com capacidade para as aeronaves de carga Antonov, que permitem o rápido transporte de cargas muito pesadas e/ou volumosas, inclusive blindados. Essa estrutura, destaca-se, foi objeto de um ataque aeromóvel russo em 24 de fevereiro, no primeiro dia da invasão, possivelmente para dar mais rapidez à logística das tropas que progrediam em direção àquela grande cidade e negar seu uso pelos ucranianos.

Kiev, no entanto, era mais do que um objetivo dentro da dimensão física do combate. Essa metrópole tem aspectos fortes nas dimensões informacional e humana, pelo que representa para os ucranianos, como sua capital, e, inclusive, para os russos, pois foi a capital da Rússia de Kiev, que é considerada como país ancestral por ambos os contendores.

A Batalha de Kiev, então, teve início em 25 de fevereiro de 2022. Além dos fatores supracitados, muitos acreditam que a principal razão para a decisão russa de investir sobre a capital ucraniana estava ligada diretamente ao suposto objetivo político da Rússia de depor o Presidente da Ucrânia, Volodymir Zelensky, que continuava governando o país e estava presente naquela localidade, e trocá-lo por um governo favorável a Moscou.

Além disso, Kiev, como capital, é o centro político da Ucrânia e abriga as estruturas do governo, tais como a sede do Executivo, o Parlamento e o Banco Central. Um novo governo teria mais legitimidade se estivesse governando a partir desta cidade e com o governante anterior deposto.

Contudo, a Rússia não conquistou a capital na 1ª Fase e começou a se retirar do Eixo Norte em 29 de março de 2022. Tal retirada fez parte da reorganização das forças russas, que deu início à 2ª Fase do conflito.

CONSIDERAÇÕES FINAIS

Da análise da 1ª Fase da Guerra entre Ucrânia e Rússia em 2022, pode-se verificar que o resultado dos combates em médios e grandes centros urbanos ucranianos teve grande relevância para ambos os contendores.

As forças ucranianas utilizaram áreas urbanas importantes, por exemplo Mykolaiv, Mariupol, Karkhiv e Kiev, como suas principais posições defensivas na 1ª Fase e obtiveram relativo sucesso. Os russos, por sua vez, conseguiram rápida progressão e vantagens significativas a partir do domínio de localidades como Kherson e Melitopol.

Diante de todo o acima exposto, conclui-se que há uma grande importância no controle de certos centros urbanos durante um conflito convencional. Devido a isso, tanto as forças russas quanto as ucranianas buscaram o domínio de localidades que oferecessem vantagens às mesmas na 1ª fase da guerra.

Por fim, é relevante frisar que o combate em médios e grandes centros urbanos é uma realidade. Tal possibilidade deve ser considerada pelas principais forças armadas do mundo, dentre as quais inclui-se as brasileiras, na aplicação de exercícios de planejamento e práticos.

REFERÊNCIAS

BRASIL. Centro de Doutrina do Exército. Exército Brasileiro. **Conflito na Ucrânia**: resumo doutrinário nr 10, de 7 de março de 2022. Brasília, 2022.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **EB70-MC-10.244: Corpo de Exército.** Edição Experimental. Brasília, DF, 2020.

BRASIL. Exército Brasileiro. Comando de Operações Terrestres. **EB70-MC-10.223: Operações.** 5ª Edição. Brasília, DF, 2017.

BROWN, David. **Guerra na Ucrânia: o ataque da Rússia em mapas**. 2022. BBC News Brasil. Disponível em: https://www.bbc.com/portuguese/internacional-60517760.amp. Acesso em: 06 maio 2022.

DEUTSCHE WELLE. **A economia da Ucrânia para além do trigo e matérias-primas**. **Istoé Dinheiro**, São Paulo, 15 mar. 2022. Disponível em: https://www.istoedinheiro.com.br/a-economia-da-ucrania-para-alem-do-trigo-e-materias-primas/. Acesso em: 06 maio 2022.

KAGAN, Fredrick W.; BARROS, George; STEPANENKO, Kateryna. **Russian Offensive Campaign Assessment, March 4**. 2022. Institute for the Study of War. Disponível em: https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-4. Acesso em: 15 maio 2022.

NOTAS

[1] Considerou-se, somente, os eventos ocorridos até dezembro de 2022.

SOBRE O AUTOR

O Major de Infantaria Tiago Magalhães França Silva é Comandante do Curso de Infantaria da Escola de Aperfeiçoamento de Oficiais. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras (AMAN) em 2005. É pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) e possui o curso de Comando e Estado-Maior da Escola de Comando e Estado-Maior do Exército (ECEME). Realizou o Curso Básico Paraquedista em 2006, o Curso de Mestre D'Armas da Escola de Educação Física do Exército (EsEFEx) em 2009 e o Curso de Operação da VBTP M113 no Centro de Instrução de Blindados (CIBld) em 2015 (tiagofranca.silva@eb.mil.br).

Aniversário do

GOTEX

6 DE NOVEMBRO

"LEMBRAI-VOS DA GUERRA"



Aceite o desafio de escrever!

Assuntos de interesse

Ações Subsidiárias e Missões de Paz
Sistemas de Armas e Equipamentos
Inteligência e Comando e Controle
Forças Militares Estrangeiras
Manobra, Fogos e Logística
Administração e Liderança
História Militar e Tática
Organização e Doutrina
Política e Estratégia

Colabore com o desenvolvimento doutrinário,
envie sua proposta de artigo para dmtrevista@coter.eb.mil.br
A Doutrina do Exército precisa da sua opinião!