INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO ESTADO MAIOR CONJUNTO

2023/2024

TII

PERSPETIVA DE EVOLUÇÃO DA CAPACIDADE CIBERNÉTICA DO EXÉRCITO BRASILEIRO AO NÍVEL TÁTICO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Samuel Bombassaro Neto

TENENTE-CORONEL, EXE COM

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

PERSPETIVA DE EVOLUÇÃO DA CAPACIDADE CIBERNÉTICA DO EXÉRCITO BRASILEIRO AO NÍVEL TÁTICO

TENENTE-CORONEL, EXE COM Samuel Bombassaro Neto

Trabalho de Investigação Individual CEMC 2023/2024

Pedrouços 2024

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

PERSPETIVA DE EVOLUÇÃO DA CAPACIDADE CIBERNÉTICA DO EXÉRCITO BRASILEIRO AO NÍVEL TÁTICO

TENENTE-CORONEL, EXE COM Samuel Bombassaro Neto

Trabalho de Investigação Individual CEMC 2023/2024

Orientador: TCOR TM EXE Pedro Manuel Monteiro Fernandes

Coorientador: TCOR TOCART FAP João Paulo Ferreira Lourenço

Pedrouços 2024

Declaração de compromisso Antiplágio

Eu, **Samuel Bombassaro Neto**, declaro por minha honra que o documento intitulado **Perspetiva de evolução da capacidade cibernética do Exército Brasileiro ao nível tático** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Estado-maior Conjunto 2023/2024** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 06** de **maio** de **2024**

gov.br
Documento assinado digitalmente
SAMUEL BOMBASSARO NETO
Data: 01/07/2024 07:29:18-0300
Verifique em https://validar.iti.gov.br

Samuel Bombassaro Neto

Agradecimentos

As minhas primeiras palavras são direcionadas ao meu orientador, Tenente-Coronel Fernandes, pelo direcionamento e apoio constante durante o trabalho de investigação. Sua dedicação incansável, contributos valiosos e indicações extremamente objetivas foram cruciais para a conclusão e sucesso deste projeto.

Ao Tenente-Coronel Ferreira Lourenço, meu coorientador, pelas instruções precisas e claras acerca do necessário refinamento do presente estudo. Pequenos ajustes que, sem dúvida, fizeram a diferença.

Ao Diretor de Curso, Sr. Coronel Faria Ribeiro, pelo constante acompanhamento e empenho na solução dos inúmeros percalços durante o percurso, todos transpostos sem maiores problemas graças ao seu apoio. Muito obrigado.

Aos entrevistados, Coronel Nepomuceno, Tenente-Coronel Paulo Barros, Tenente-Coronel Alfredo, Tenente-Coronel Xavier e Tenente-Coronel Ávila, pela disponibilidade e elevado grau de colaboração para este trabalho. As vossas experiências foram imprescindíveis para o atingimento dos objetivos.

Aos nobres companheiros do Curso de Estado-Maior Conjunto 2023/2024, eternos amigos, pela camaradagem, consideração e troca de conhecimentos.

Finalmente, um especial agradecimento à minha amada família, Alexandra, Gabriel e Ana Vitória. Obrigado pela compreensão por todos os momentos de ausência que se fizeram necessários para que este trabalho fosse possível. Obrigado pelo suporte incondicional em todos os períodos de dificuldade. Amo vocês!

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

O setor cibernético, desde a elaboração da Estratégia Nacional de Defesa em 2008, tornou-se ponto fulcral para o Exército Brasileiro. O ambiente operacional atual adaptação diante de inúmeros desafios, dentre os quais a Guerra Cibernética, sublinhando a necessidade de evolução do setor, nomeadamente ao nível tático.

Assim, a presente investigação tem como objetivo selecionar contributos para potenciar a capacidade cibernética do Exército Brasileiro na condução das operações militares, respondendo à seguinte questão: em que medida o Exército Brasileiro pode potenciar a sua capacidade cibernética na condução das operações militares?

A metodologia utilizou-se do raciocínio dedutivo e do método de estratégia qualitativa, calcada em uma rigorosa análise documental e na realização de entrevistas semiestruturadas aos comandantes de estruturas especializadas.

Os contributos selecionados, considerados mais relevantes durante o trabalho, foram a negação de serviços do adversário, a identificação de vulnerabilidades do oponente e a proteção dos sistemas de TIC.

Concluiu-se que para a potenciação dos aludidos contributos, podem ser desenvolvidas as propostas de: (i) manutenção das capacidades cibernéticas através do Programa Estratégico do Exército Defesa Cibernética, (ii) incremento da Capacidade Operativa Exploração Cibernética e (iii) transformação dos Batalhões de Comunicações em Batalhões de Comunicações e Guerra Eletrónica.

Palavras-chave:

Guerra Cibernética, Exército Brasileiro, Estratégia Nacional de Defesa, nível tático.

Abstract

The cyber sector, since the preparation of the National Defense Strategy in 2008, has become a focal point for the Brazilian Army. The current operational environment adapts to numerous challenges, including Cyber War, highlighting the need for evolution in the sector, particularly at a tactical level.

Therefore, the present investigation aims to select contributions to enhance the cyber capacity of the Brazilian Army in the conduct of military operations, answering the following question: to what extent can the Brazilian Army enhance its cyber capacity in the conduct of military operations?

The methodology used deductive reasoning and the qualitative strategy method, based on a rigorous documentary analysis and semi-structured interviews with commanders of specialized structures.

The selected contributions, considered most relevant during the work, were the denial of adversary services, the identification of adversary vulnerabilities and the protection of ICT systems.

It was concluded that to enhance the aforementioned contributions, proposals can be developed for: (i) maintenance of cyber capabilities through the Army's Strategic Cyber Defense Program, (ii) increase in Cyber Exploration Operational Capacity and (iii) transformation of Battalions of Communications in Communications and Electronic Warfare Battalions.

Keywords:

Cyber War, Brazilian Army, National Defense Strategy, tactical level.

Lista de abreviaturas, siglas e acrónimos

A

AED	Ação Estratégica de Defesa

B

BCom	Batalhão de Comunicações
BComGE	Batalhão de Comunicações e Guerra Eletrónica
BComGESl	Batalhão de Comunicações e Guerra Eletrónica de Selva
BGE	Batalhão de Guerra Eletrónica

C

CEMC	Curso de Estado Maior Conjunto
CiaCom	Companhia de Comunicações
CMilA	Comando Militar de Área
CMT	Capacidade Militar Terrestre
CO	Capacidade Operativa
CRFB	Constituição da República Federativa do Brasil

D

DE	Divisão de Exército
DOAMEPI	Doutrina, Organização (e/ou processos), Adestramento, Material, Educação, Pessoal e Infraestrutura

E

ED	Estratégia de Defesa
END	Estratégia Nacional de Defesa

F

FFAA	Forças Armadas
FTer	Força Terrestre
FAC	Força Aérea Componente
FNC	Força Naval Componente
FTC	Força Terrestre Componente

G

GCE	Grupamento de Comunicações e Eletrónica

I

INV	Investigação

IUM	Instituto Universitário Militar
L	
LBDN	Livro Branco de Defesa Nacional
M	
MD	Ministério da Defesa
N	
NEP	Normas de Execução Permanentes
O	
OCCA	Operações de cooperação e coordenação com agências
OE	Objetivo específico
OEE	Objetivo Estratégico do Exército
OG	Objetivo geral
OM	Organização Militar
OND	Objetivos Nacionais de Defesa
ONF	Objetivos Nacionais Fundamentais
P	
PBC	Planejamento Baseado em Capacidades
PCD	Política Cibernética de Defesa
PEE	Programa Estratégico do Exército
PEEx	Plano Estratégico do Exército
PND	Política Nacional de Defesa
PR	Presidência da República
Q	
QC	Questão central
QD	Questão derivada
S	
STIC3	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
T	
TIC	Tecnologia da Informação e Comunicações
TII	Trabalho de Investigação Individual

1. Introdução

A identificação do campo cibernético como uma área vital para a Defesa Nacional[1] brasileira data oficialmente de 2008, ano em que o Estado brasileiro publicou, de modo inédito, a sua Estratégia Nacional de Defesa (END), sendo tal documento objeto de atualizações periódicas, a última realizada em 2016. Trata-se do primeiro grande marco – dentre várias outras etapas que viriam a seguir – que deu início à transformação e ao desenvolvimento efetivo da cibernética na esfera militar no Brasil.

Por conceção, a END está alinhada com outra documentação de nível superior, a Política Nacional de Defesa (PND), que corresponde ao

> […] documento de mais alto nível do País em questões de Defesa […] alinhado às aspirações e aos Objetivos Nacionais Fundamentais (ONF)[2], que consolida os posicionamentos do Estado brasileiro e estabelece objetivos mais elevados neste tema. (Ministério da Defesa, 2018, p. 7)

A END, por sua vez,

> […] orienta os segmentos do Estado brasileiro quanto às medidas que devem ser implementadas para que esses objetivos sejam alcançados. É, portanto, o vínculo entre o posicionamento do País nas questões de defesa e as ações necessárias para efetivamente dotar o Estado da capacidade para preservar seus valores fundamentais. (Ministério da Defesa, 2018, p. 31)

Tem-se, portanto, estabelecida a fundamentação para direcionar as medidas a serem adotadas pelas Forças Armadas (FFAA) brasileiras, ressaltando que o Estado é o garantidor da segurança da população brasileira, bem como o responsável por todas as ações da Defesa Nacional.

Nesse contexto, uma das principais inovações trazidas pela END foi a especificação de três setores estratégicos para a Defesa Nacional: o nuclear, o cibernético e o espacial (Ministério da Defesa, 2018, p. 55). E para o desenvolvimento de cada um dos setores citados foi atribuída responsabilidade a um dos Ramos das FFAA, cabendo ao Exército Brasileiro (EB) o setor cibernético. Estava dado o primeiro grande passo rumo à evolução da cibernética no âmbito do EB.

---

[1] "Conjunto de atitudes, medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas" (Ministério da Defesa, 2015, p. 85).

[2] Os Objetivos Nacionais Fundamentais estão publicados no Art. 3º da Constituição da República Federativa do Brasil (CRFB, 1988).

A partir de então, seguiram-se inúmeras ações que buscaram – e buscam, até os dias atuais – proporcionar o progresso da cibernética no âmbito do EB. Ao nível tático, escopo do presente trabalho, o que se tem são uma série de estruturas com capacidades distintas, que vem sendo modernizadas e capacitadas desde a publicação da END. Tais elementos procuram acompanhar as demandas da Força Terrestre[3] (FTer), principalmente por meio dos programas e projetos estratégicos do EB. Ressalta-se que as capacidades cibernéticas influenciam as operações militares, atuando como multiplicadoras do poder de combate (Kuhn, 2022).

Destaca-se a importância do investimento em uma estrutura cibernética à altura da condição do país, sendo este um ponto fulcral para a nação brasileira – conforme definido na END (2018). A rápida transformação tecnológica e a cada vez maior interdependência da sociedade contemporânea na infraestrutura digital faz com que a Guerra Cibernética se constitua em uma ameaça substancial à segurança nacional, com potencial para causar danos severos em setores críticos, como energia, comunicações e serviços financeiros (Clarke, 2010). Demonstra-se, assim, a relevância do tema estudado não somente para as FFAA, mas também para o Brasil.

É necessário, consequentemente, que a estrutura cibernética atual do EB, ou seja, ao nível tático – cerne do estudo em tela –, esteja apta a contribuir com as operações militares em sua plenitude, moldada às novas características do ambiente operacional. Justifica-se, assim, o propósito do trabalho, que buscou uma perspetiva de evolução dessas capacidades cibernéticas ora citadas, vindo a beneficiar a FTer. Ademais buscou-se a apresentação de propostas ou sugestões que maximizem os contributos da guerra cibernética para o EB e que possam ser compartilhadas com outras FFAA, como por exemplo de Portugal.

Assim, tem-se como objeto de investigação a capacidade cibernética do Exército Brasileiro, sendo que a investigação foi delimitada nos domínios do espaço, do conteúdo e do tempo (Santos & Lima, 2019).

Com relação ao espaço, a investigação foi delimitada ao EB, tendo em vista que o objeto analisado é a capacidade cibernética do Ramo Exército das FFAA do Brasil. Nesse ponto, faz-se necessário uma aclaração específica no que tange ao conceito de espaço para a Guerra Cibernética: "as ações de guerra cibernética não se limitam a fronteiras geograficamente definidas, pois os agentes podem atuar a partir de qualquer local e

[3] "Instrumento de ação do Exército Brasileiro organizado por módulos de combate, com base em capacidades […]" (Exército Brasileiro, 2018, p. 166).

provocar efeito em qualquer lugar" (Exército Brasileiro, 2017c, pp. 2–4). Não obstante, o espaço "fisicamente" delimitado foi o território do Brasil, pois as estruturas a serem analisadas encontram-se instaladas nos sítios em solo brasileiro.

Quanto ao conteúdo, delimitou-se o trabalho à organização da Guerra Cibernética ao nível tático, isto é, do EB. Os demais fatores geradores de capacidade não foram analisados por motivo de constituírem objeto de estudo já investigado (como o fator Doutrina, no que concerne à Guerra Cibernética brasileira) ou ainda a ser analisado em fase posterior (como o fator Pessoal, de modo a avaliar as estratégias para distribuição de efetivo especializados após uma possível reestruturação de organizações), compondo eventualmente outro trabalho a ser realizado.

Finalmente, em termos temporais, foi analisada a capacidade cibernética do EB a partir da publicação da primeira versão da END, em 2008, até os dias atuais. Ressalta-se que antes desta data já existiam iniciativas relativamente ao nível tático, nomeadamente por parte de algumas organizações militares (OM) de ensino do Exército Brasileiro; porém, nada ainda com a sustentação de um documento definido pelo nível político / estratégico do Brasil.

O objetivo geral (OG) deste estudo é selecionar contributos para potenciar a capacidade cibernética do EB na condução das operações militares. Tendo o OG como base, bem como as delimitações elencadas, foram elaborados três objetivos específicos (OE), sendo o OE1 analisar a organização da Guerra Cibernética do Exército Brasileiro, o OE2 examinar a atuação da Guerra Cibernética do Exército Brasileiro para a condução das operações militares, e o OE3 analisar o impacto da capacidade cibernética na condução das operações militares do Exército Brasileiro.

Para se atingir o OG acima exposto, foi elaborada a seguinte questão central (QC): em que medida o Exército Brasileiro pode potenciar a sua capacidade cibernética na condução das operações militares?

Já para serem atingidos os OE do estudo, foram identificadas três questões derivadas (QD), sejam elas: QD1 Como está organizada a Guerra Cibernética no Exército Brasileiro? QD2 De que forma a Guerra Cibernética do Exército Brasileiro atua em proveito das operações militares? e QD3 Quais os contributos da capacidade cibernética do Exército Brasileiro na condução das operações militares?

Para responder aos OG e OE, a presente investigação foi organizada em oito capítulos, sendo que o atual capítulo enquadra o assunto em tela. No segundo capítulo, são

delineados os conceitos e a literatura pertinentes ao objeto de estudo. O terceiro capítulo detalha a metodologia empregada na pesquisa, juntamente com o método selecionado. Os capítulos quatro, cinco, seis e sete abarcam a análise e a discussão dos resultados obtidos tanto da análise documental quanto das entrevistas realizadas, respondendo às questões da investigação. Finalmente, no oitavo capítulo são apresentadas as conclusões derivadas da investigação realizada e suas limitações, bem como alguns possíveis cenários e sugestões, levando em conta o vasto conjunto de informações relacionadas à Guerra Cibernética do EB.

2. Enquadramento teórico e concetual

De modo a enquadrar este trabalho, assim como caracterizar os conceitos mais relevantes relacionados ao objeto de estudo elencado, proceder-se-á à identificação do contexto e à definição dos conceitos básicos da presente investigação.

2.1 Estado da arte e conceitos estruturantes

2.1.1. Política Nacional de Defesa e Estratégia Nacional de Defesa

O documento norteador dos rumos da Defesa no Brasil é a PND, que apresenta o conceito dos Objetivos Nacionais de Defesa (OND) – alinhados aos já citados ONF. É imperativo a compreensão de alguns desses objetivos, haja vista que as ações desencadeadas para a sua consecução estão constantes da END. São eles:

> I. Garantir a soberania, o patrimônio nacional e a integridade territorial;
>
> II. Assegurar a capacidade de Defesa, para o cumprimento das missões constitucionais das Forças Armadas;
>
> III. Salvaguardar as pessoas, os bens, os recursos e os interesses nacionais, situados no exterior;
>
> IV. Contribuir para a preservação da coesão e unidade nacionais;
>
> V. Contribuir para a estabilidade regional e para a paz e a segurança internacionais;
>
> VI. Contribuir para o incremento da projeção do Brasil no concerto das nações e sua inserção em processos decisórios internacionais;
>
> VII. Promover a autonomia produtiva e tecnológica na área de defesa; e
>
> VIII. Ampliar o envolvimento da sociedade brasileira nos assuntos de Defesa Nacional. (Ministério da Defesa, 2018)

Os oito OND citados possuem, ainda que em diferentes graus, algum ponto de contacto com o setor cibernético, setor este definido como estratégico na END. Ao interpretar a PND e desenvolver procedimentos para a sua operacionalização, o aludido documento traçou Estratégias de Defesa (ED) e Ações Estratégicas de Defesa (AED), no intuito de indicar o caminho a ser trilhado.

Várias ED e AED estão alinhadas com a edificação da capacidade cibernética, já que para se atingir determinados OND deve-se, impositivamente, perpassar pelo desenvolvimento de vetores cibernéticos. Tal orientação “vertical”, ou seja, que parte do documento produzido em nível superior e perpassa os demais de nível inferior, é percebida em toda a END, particularmente para o setor cibernético.

A assertiva anterior é determinada pela própria END, a qual enuncia que

> […] o Brasil orienta suas iniciativas na área de defesa no seu nível mais amplo, segundo as Estratégias de Defesa – ED, diretamente alinhadas aos Objetivos Nacionais de Defesa estabelecidos na Política Nacional de Defesa. Complementarmente, a cada Estratégia de Defesa são incorporadas Ações Estratégicas de Defesa – AED, que visam orientar as medidas que deverão ser implementadas no sentido da consecução dos Objetivos Nacionais de Defesa. (Ministério da Defesa, 2018, p. 59)

Um dos exemplos presentes na END é a Ação Estratégica de Defesa de número nove, a qual busca o desenvolvimento das capacidades de monitorar e controlar o espaço cibernético; tal AED faz parte da ED de número 2 – fortalecimento da capacidade de dissuasão, que por sua vez integra o rol de estratégias definidas para a conquista do OND I - Garantir a soberania, o patrimônio nacional e a integridade territorial (Ministério da Defesa, 2018, p. 59).

Por meio de uma análise pormenorizada da END, tem-se que a mesma é repleta de iniciativas que perseguem obstinadamente o aperfeiçoamento do setor cibernético, considerado de importância vital para os assuntos de defesa do país. A mesma ideia é compartilhada no Livro Branco de Defesa Nacional (LBDN), documento que complementa a PND e END e oferece ainda mais transparência na temática da Defesa Nacional para a sociedade.

De acordo com o LBDN, “compete ao Exército a responsabilidade pelo Setor Estratégico Cibernético, o que envolve uma série de medidas pontuais, de articulação e equipamento, para permitir a consolidação do setor. A capacidade de preservar a integridade de estruturas estratégicas que podem ser alvo de ataques cibernéticos em diferentes modalidades é de fundamental importância para o País” (Ministério da Defesa, 2020a, p. 200).

Isto posto, é de interesse crucial do presente estudo que o entendimento dos principais pontos da END, bem como das suas primordiais relações com eventuais documentos que possuem ligação com o setor cibernético (como a PND e o LBDN), sejam clarificadas, motivo pelo qual a sua definição e articulação consta da base concetual da investigação.

2.1.2. Ambiente Operacional

Urge compreender, de modo sucinto, o significado de ambiente operacional para o EB, sendo "[…] o conjunto de condições e circunstâncias que afetam os Domínios terrestre, marítimo, aéreo, espacial, cibernético e eletromagnético, onde uma Força emprega suas capacidades, a fim de cumprir determinada missão. Os Domínios são compostos pelas dimensões física, humana e informacional" (Exército Brasileiro, 2023a, p. 4–1).

Visacro (2018) acrescenta que o ambiente operacional da atualidade é complexo e extremamente dinâmico, exigindo mais da capacidade de planeamento, de decisão e de atuação. Fatores como a comunicação em alta velocidade, terrorismo, guerra híbrida e a própria Guerra Cibernética definem esse ambiente, implicando em um amoldamento constante para que se consiga compreender, antecipar e fazer frente aos desafios modernos.

Nota-se que uma das principais mudanças a ocorrer em torno do ambiente operacional é a convergência das novas tecnologias (TRADOC, 2019). Essa transformação faz com que o uso de meios tecnológicos seja não somente potenciado, mas tenha os seus efeitos maximizados por meio da sincronização (Exército Brasileiro, 2023a), implicando em adaptação da postura face ao apresentado.

E é exatamente neste atual ambiente operacional que o EB deve realizar as suas ações, voltadas para uma nova forma de se conduzir a guerra, adequando-se através de uma FTer orientada por meio de novas capacidades e suas respetivas tecnologias associadas, incluindo a aptidão para atuar no espaço cibernético (Exército Brasileiro, 2023a).

2.1.3. Guerra Cibernética

À esteira da PND e END foi publicado, em 2013, o Livro Branco de Defesa Nacional (LBDN), que tem sua última versão datada de 2020 e definiu medidas mais concretas para a implantação efetiva do setor cibernético, como melhorar a capacitação dos recursos humanos, realizar as atualizações doutrinárias necessárias e ser capaz de fazer frente às ameaças virtuais (Ministério da Defesa, 2020a, p. 72).

Com a criação e ativação do Núcleo do Centro de Defesa Cibernética (NuCDCiber), em 2010, prosseguia-se a estruturação do setor cibernético. Dois anos mais tarde, o mesmo órgão foi transformado no Centro de Defesa Cibernética (CDCiber) e passou a atuar de forma conjunta, tendo como responsabilidade tratar os diversos temas de interesse na área cibernética, como gestão de pessoal, capacitação, estruturação do setor e seu emprego (Carneiro, 2012, p. 72).

O ponto considerado de inflexão foi a criação, em 2014, do Comando de Defesa Cibernética (COMDCIBER), "fruto do crescimento de importância do tema no cenário mundial e a necessidade de colocar o país em condições de obter liberdade de ação no espaço cibernético em um prazo razoável" (Avelar, 2018, p. 52). O COMDCIBER é, hoje, aglutinador dos níveis operacional e estratégico no que tange à cibernética nas FFAA, sendo um comando conjunto permanentemente ativado e possuidor, em sua estrutura, do CDCiber como tropa operativa.

No Brasil, o Sistema Militar de Defesa Cibernética (SMDC) foi criado de modo oficial em 2020, pelo Ministério da Defesa, e consiste em "um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses" (Ministério da Defesa, 2020b).

Cumpre ressaltar que, conforme definido em portaria, o órgão central do sistema é o COMDCIBER, classificado como um comando operacional conjunto e permanentemente ativado, o qual possui, também, capacidade interagências – atuação colaborativa com representantes de órgãos da administração pública federal, de infraestruturas críticas e de outros órgãos, instituições e empresas, públicos ou privados, de interesse da Defesa (Ministério da Defesa, 2020b).

A relevância do entendimento do conceito do SMDC decorre justamente da sua composição que, além de possuir o órgão central já mencionado, engloba as estruturas de Defesa Cibernética / Guerra Cibernética das Forças Singulares[4]. Significa dizer que o SMDC é, logo, formado pelos elementos táticos de cada ramo das FFAA.

Outrossim, a estrutura do nível tático deve procurar concretizar uma série de finalidades estabelecidas pela Política Cibernética de Defesa (PCD), tais como

> […] assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional; adequar as estruturas de Ciência, Tecnologia e Inovação das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do setor cibernético; cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em

[4] Designação genérica de uma das Forças Armadas: Marinha, Exército e Aeronáutica (EB, 2018).

> consequência, a capacidade dissuasória do setor cibernético [...]. (Ministério da Defesa, 2012)

Precisamente as estruturas de Guerra Cibernética do ramo do Exército são o foco de análise do estudo. São elas que devem gerir e empregar as capacidades presentes no nível tático, colaborando com os diversos outros sistemas (por exemplo, com o sistema de Inteligência de Defesa - SINDE) e atingindo os objetivos definidos pela PCD.

A temática relacionada ao campo da cibernética é frequentemente composta por diversos termos similares, porém com significados distintos. De modo a definir o conceito estruturante para o presente estudo, é imperioso que se conceitue a Guerra Cibernética, expressão recorrente na análise do estudo de caso em tela.

Para tanto, faz-se necessário diferenciar os níveis de decisão que envolvem a cibernética no Brasil. O documento mais atual que fundamenta o assunto, o manual MD 31-M-07 Doutrina Militar de Defesa Cibernética (2023), define que

> Depois do estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa (END), em 2008, três campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR); a Defesa Cibernética, a cargo do Ministério da Defesa (MD); e a Guerra Cibernética, a cargo dos Comandos Operacionais[5] ativados e de suas Forças Componentes[6]. (Ministério da Defesa, 2023, p. 4)

A Figura 1 a seguir evidencia a divisão estabelecida pelo MD:

[5] Comando conjunto ou singular organizado de acordo com a Diretriz para o Estabelecimento da Estrutura Militar de Defesa (Ministério da Defesa, 2015, p. 65).
[6] Conjunto de unidades e organizações de uma mesma força armada que integra uma força conjunta. Pode ser Força Naval Componente (FNC), Força Terrestre Componente (FTC) ou Força Aérea Componente (FAC) (Ministério da Defesa, 2015, p. 120).

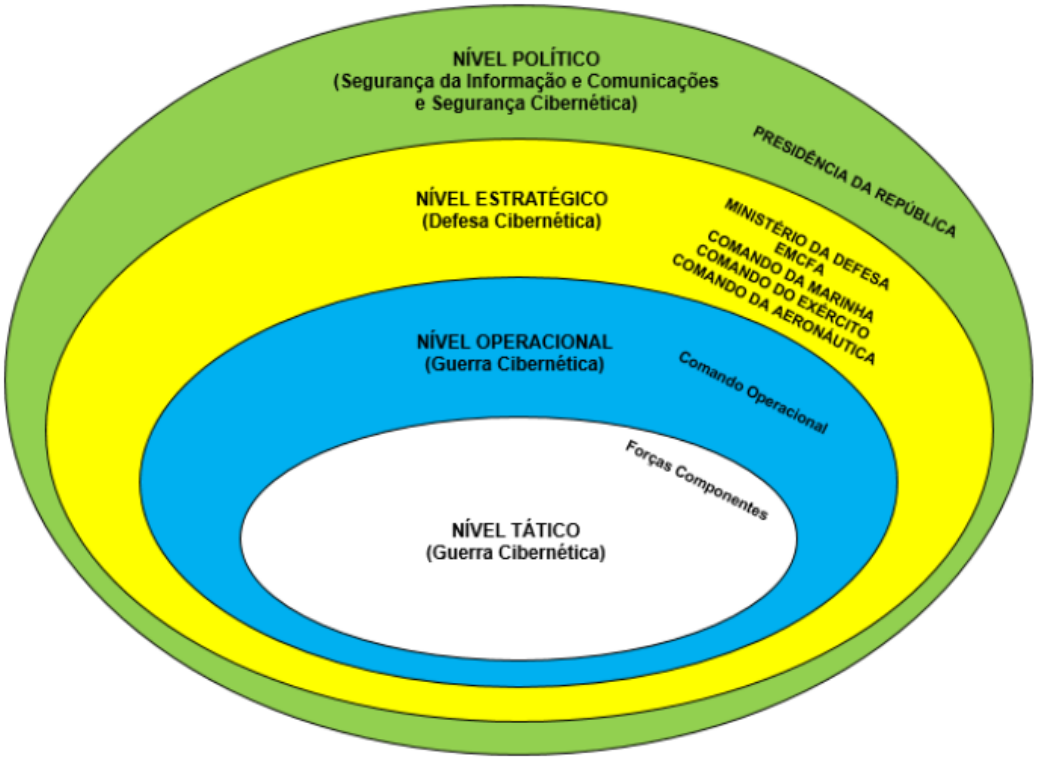

Figura 1 – Níveis de decisão das ações cibernéticas

Fonte: adaptado de MD 31-M-07 Doutrina Militar de Defesa Cibernética (2023)

Seguindo o alinhamento natural existente na hierarquização das instituições e dos documentos, o EB adota a mesma segmentação identificada acima, executando as ações que são desencadeadas no nível tático, isto é, nas Forças Componentes – incluindo a FTer.

Desse modo, conclui-se que o EB, como elemento atuador do nível tático – compondo a Força Terrestre Componente (FTC) e / ou as demais Forças Componentes –, realiza exclusivamente a Guerra Cibernética.

E o que vem a ser Guerra Cibernética, no contexto ora abordado? "Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar" (Ministério da Defesa, 2015, p. 134).

A mesma ideia central da definição citada é corroborada pelo manual de campanha de Guerra Cibernética do EB (2017c) e pelo Glossário de Termos e Expressões para uso no Exército (2018). Tem-se, portanto, delimitada como Guerra Cibernética toda a utilização da capacidade cibernética empregada pelo Exército Brasileiro – já que o mesmo situa-se no nível tático ou desdobra-se em uma FTC em operações no mesmo nível.

2.1.4. Capacidades Militares Terrestres e Capacidades Operativas

Para melhor perceção de como a Guerra Cibernética atua no nível tático, é fundamental que sejam apresentados os conceitos e definições relacionados com as Capacidades Militares Terrestres (CMT).

Alinhado com a END e a Doutrina da maioria das Forças Armadas dos países ocidentais, o Exército Brasileiro adota a geração de forças por meio do Planejamento Baseado em Capacidades (PBC). Dessa forma, o desenvolvimento de capacidades baseia-se em uma permanente análise da conjuntura e em cenários prospetivos, com o objetivo de identificar tanto as ameaças concretas quanto as ameaças potenciais ao Estado Brasileiro (Exército Brasileiro, 2015).

Figura 2 – Relação Capacidades x Níveis

Fonte: adaptado de EB20-C-07.001 Catálogo de Capacidades do Exército (Exército Brasileiro, 2015, p. 5)

Ainda que as CMT sejam apresentadas como integrantes do nível operacional, faz-se necessário o seu entendimento, já que as mesmas são aglutinadoras das capacidades presentes no nível tático. Destarte, uma CMT é "constituída por um grupo de capacidades operativas com ligações funcionais, reunidas para que os seus desenvolvimentos potencializem as aptidões de uma força para cumprir determinada tarefa dentro de uma missão estabelecida" (Exército Brasileiro, 2015, p. 7).

Já a "aptidão requerida a uma força ou organização militar, para que possa obter um efeito estratégico, operacional ou tático" é uma Capacidade Operativa (CO), a qual "é obtida a partir de um conjunto de sete fatores determinantes, inter-relacionados e indissociáveis: Doutrina, Organização (e/ou processos), Adestramento, Material, Educação, Pessoal e Infraestrutura - que formam o acrônimo DOAMEPI" (Exército Brasileiro, 2015, p. 7).

Figura 3 – Fatores determinantes das capacidades

Fonte: EB20-MF-10.102 Doutrina Militar Terrestre (Exército Brasileiro, 2022a, p. 3–3)

Salienta-se, para fins de assimilação mais adequada do objeto da investigação, que o fator Organização é materializado por meio da estrutura que compreende a organização estudada, atinente aos elementos de emprego da FTer (Exército Brasileiro, 2022, p. 3–3).

Com essas premissas estabelecidas, o EB buscou mapear as suas capacidades militares terrestres e operativas, "levando-se em consideração as áreas estratégicas do território nacional, o entorno estratégico e outras áreas de interesse" (Exército Brasileiro, 2015, p. 5). Foi desse modo que surgiu o Catálogo de Capacidades do Exército, documento definidor das principais aptidões existentes na FTer.

O Catálogo de Capacidades do Exército estabeleceu, à época, nove CMT, sendo que uma delas é a CMT Cibernética. Por definição, esta CMT se traduz na capacidade de realizar "ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para superar os Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC3) do oponente e defender os próprios. Abrange, essencialmente, as ações de ataque, exploração e proteção cibernética" (Exército Brasileiro, 2015, p. 18).

Finalmente, e a fim de consolidar o entendimento a respeito da capacidade cibernética, a CMT Cibernética é dividida em três CO basilares: CO Proteção Cibernética, CO Exploração Cibernética e CO Ataque Cibernético.

A CO Proteção Cibernética é entendida como a capacidade de conduzir ações para garantir o funcionamento dos nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética para

neutralizar ataques e exploração cibernética em nossos meios, sendo uma atividade de caráter permanente (Exército Brasileiro, 2015, p. 19).

Por sua vez, a CO Exploração Cibernética consiste na condução de "ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas" (Exército Brasileiro, 2015, p. 18).

Já a CO Ataque Cibernético possui como definição "ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente, contribuindo para o sucesso das operações" (Exército Brasileiro, 2015, p. 19).

Os conceitos explicitados acima são vitais para o estudo, já que serviram de base para uma identificação, de maneira mais adequada, da forma como as estruturas de Guerra Cibernética do nível tático atuam em proveito das operações militares – nomeadamente no atingimento dos OE2 e OE3, e se é possível que as mesmas sejam aperfeiçoadas para um melhor desempenho.

3. Metodologia e método

A metodologia utilizada no estudo seguiu as orientações de Santos e Lima (2019), bem como as normas de Execução Permanentes (NEP) de Investigação (INV) do Instituto Universitário Militar (IUM), particularmente as que tratam sobre a elaboração dos trabalhos de investigação (NEP/INV - 001, 2020) e de estruturação, regras de citação e referenciação de trabalhos escritos do IUM (NEP/INV - 003, 2020).

3.1. Metodologia

A investigação considerou os elementos essenciais previstos por Santos e Lima (2019): as posições filosóficas, o raciocínio, as estratégias de investigação e o desenho da pesquisa.

Quanto à filosofia, e com base na documentação da referência, o trabalho adotou o conceito epistemológico interpretativo, já que a principal ação do investigador foi a de compreender os efeitos da capacidade cibernética para as operações militares.

Alinhado com a filosofia traçada para o estudo, o raciocínio conduzido foi o dedutivo, que parte do geral para o particular, caracterizando-se como o mais adequado para o tema, pois o intento foi chegar a um modo de potenciar a forma como a capacidade cibernética atua em operações militares.

Relativamente à estratégia, foi utilizado o método qualitativo, por ser esta a estratégia que supõe que a relação entre a realidade e a subjetividade não pode ser quantificada estatisticamente, enquadrando-se na situação dos dados obtidos da análise documental e das entrevistas relacionadas com a Guerra Cibernética no EB (Santos & Lima, 2019, pp. 25–32).

Por fim, o problema explicitado conduziu ao caminho lógico do desenho de pesquisa como um estudo de caso, considerando que a análise possui como ponto fulcral o atual estágio estrutural da Guerra Cibernética no EB; tem-se, assim, o desenho que melhor se compatibiliza com a situação de estudo e permite uma aplicação complementada pelas entrevistas e pela análise documental – indicadas, por sua vez, como técnica de recolha de dados.

3.2. Modelo de análise

Dado o objeto a ser investigado, e considerando-se o estado da arte abordado, foi elaborado o modelo de análise descrito no Apêndice A. O objetivo deste modelo é criar uma estrutura mental fundamentada na organização dos objetivos, das questões, dos

conceitos, das dimensões, assim como dos indicadores e das técnicas de coleta de dados escolhidas para a condução e progresso do estudo.

3.3. Método

Adotou-se fundamentalmente uma abordagem qualitativa com o uso de instrumentos variados na obtenção das informações necessárias ao estudo, destacando-se a análise de documentos (com foco nas fontes primárias como legislação e publicações doutrinárias) e as entrevistas, com o fito de obter uma visão completa do objeto de estudo.

3.3.1. Participantes e procedimentos

As entrevistas realizadas foram direcionadas aos comandantes dos Batalhões de Comunicações e Guerra Eletrónica (BComGE) e ao comandante do 1º Batalhão de Guerra Eletrónica (BGE), todas OM presentes no nível tático do EB. Tais estruturas são, atualmente, as que detêm as capacidades de proteção, exploração e ataque cibernético, sendo precisamente o motivo pelo qual foram selecionadas para o trabalho.

Outrossim, as cinco entrevistas com os respetivos comandantes seguiram o guião de entrevista semiestruturada constante do Apêndice B, por se tratar da forma adequada para o aprofundamento do tema ao permitir dados abertos e que estejam alinhados com a lógica de raciocínio delineada pelo investigador. Os entrevistados encontram-se caracterizados conforme o Quadro 1 a seguir.

Quadro 1 - Lista de entrevistados

Código	Posto e Nome	Função
E1	Tenente-Coronel Alfredo Ferrão de Oliveira Junior	Comandante do 1º Batalhão de Comunicações e Guerra Eletrónica de Selva (1º BComGESl)
E2	Tenente-Coronel Marcelo Vieira Xavier	Comandante do 2º Batalhão de Comunicações e Guerra Eletrónica de Selva (2º BComGESl)
E3	Coronel Alexandre da Fonseca Nepomuceno de Souza	Comandante do 3º Batalhão de Comunicações e Guerra Eletrónica (3º BComGE)
E4	Tenente-Coronel Paulo Fernando de Barros	Comandante do 9º Batalhão de Comunicações e Guerra Eletrónica (9º BComGE)
E5	Tenente-Coronel Fabrício Ávila Guimarães	Comandante do 1º Batalhão de Guerra Eletrónica (1º BGE)

3.3.2. Instrumentos de recolha de dados

Com o intuito de recolha das informações necessárias ao estudo, optou-se pela utilização de duas técnicas principais: a análise documental e as entrevistas semiestruturadas.

A análise de documentos aplicou-se fundamentalmente no atingimento do OE1, já que a organização da Guerra Cibernética no EB está registada em manuais e portarias já publicadas pela FTer e de carácter ostensivo. Foi também utilizada, ainda que em menor

intensidade, na consecução dos OE2 e OE3, pois as respostas às QD de tais objetivos (atuação e contributos da cibernética para as operações militares) encontram-se documentadas, vindo a complementar as entrevistas realizadas.

Os principais documentos pesquisados podem ser categorizados, de modo sumário, em documentação de nível mais abrangente, nomeadamente aquelas elaboradas pelo Ministério da Defesa e pelo Estado-Maior do Exército, além da PND e END; outra que realiza uma abordagem tática da Guerra Cibernética e das operações militares, com destaque para os manuais do Exército Brasileiro; e finalmente a documentação normativa para execução do trabalho.

3.3.3. Técnica de tratamento de dados

Conforme o preconizado por Guerra (2006), a análise das entrevistas foi conduzida usando a tipologia temática ou categorial, desdobrando as respostas dos entrevistados em segmentos de registo e unidades de registo. Essa metodologia qualitativa visou extrair informações relevantes relacionadas ao tema em questão.

4. Organização da Guerra Cibernética do Exército Brasileiro

O EB possui, em sua estrutura organizacional, variadas OM que possuem algum tipo de capacidade cibernética. Importa, portanto, compreender a distribuição e a articulação de tais elementos para que se identifique de maneira fidedigna o que existe em termos de Guerra Cibernética na FTer brasileira.

A organização, um dos fatores determinantes na geração de capacidades do acrónimo DOAMEPI visto anteriormente, é "expressa por intermédio da estrutura organizacional dos elementos de emprego da FTer" (Exército Brasileiro, 2022a, p. 3–3), e é assim considerada no presente capítulo para identificar como está organizada a Guerra Cibernética no âmbito do EB.

4.1. Organizações Militares: distribuição, subordinação e organização

Em tempo de paz, a FTer é organizada para executar as suas missões operacionais através dos Comandos Militares de Área (CMilA), os quais estão sob a autoridade direta do Comandante do Exército, representando o nível mais elevado de coordenação das OM (Exército Brasileiro, 2014a).

Os CMilA possuem sob sua responsabilidade "o preparo, o planejamento e o emprego operacional da FTer, desdobrada na área sob sua jurisdição" (Exército Brasileiro, 2014a, p. 6–7). Assim, o território brasileiro encontra-se dividido, sob a ótica do EB, em oito comandos militares de área, conforme a Figura 4:

Figura 4 – Comandos Militares de Área do Exército Brasileiro

Fonte: adaptado de EB20-MF-10.101 O Exército Brasileiro (2014a)

A FTer "possui como estruturas organizacionais os grandes comandos operativos[7] e as organizações militares de valor unidade e subunidade. Essas estruturas constituem os escalões da FTer" (Exército Brasileiro, 2022a, p. 4–3). Os CMilA, portanto, aglutinam os elementos que são empregues durante as operações militares, incluindo aqueles que possuem capacidades cibernéticas. No caso em concreto do EB, tais capacidades usualmente estão vinculadas às Divisões de Exército (DE) e às Brigadas, por incluir em suas estruturas OM especializadas em Guerra Cibernética. Não obstante, ainda há a existência do mais alto escalão da FTer, o Corpo de Exército, que possui constituição e organização variáveis e normalmente é empregue como FTC nas operações (Exército Brasileiro, 2020).

De acordo com o manual de Guerra Cibernética do EB (2017c), existem quatro estruturas principais que possuem capacidade cibernética na FTer, seja ela Ataque, Proteção ou Exploração Cibernética: o Batalhão de Guerra Eletrónica (BGE), o Batalhão de Comunicações (BCom), o Batalhão de Comunicações e Guerra Eletrónica (BComGE) e

[7] "Denominação genérica de qualquer comando da FTer privativo de oficial-general" (Exército Brasileiro, 2022a, p. 4–4).

a Companhia de Comunicações (CiaCom). Destaca-se que as aludidas OM existem tanto na doutrina quanto de facto na estrutura do EB, e estão distribuídas de acordo com a necessidade da FTer (Exército Brasileiro, 2019a).

O BGE é a "unidade […] organizada e adestrada para prover os elementos de apoio ao combate de Guerra Eletrónica e Guerra Cibernética […]" (Exército Brasileiro, 2022b, p. 1–2) e tem "por missão apoiar em guerra eletrónica e guerra cibernética uma FTC até o nível Corpo de Exército ou que enquadre mais de uma Divisão de Exército no amplo espectro dos conflitos" (Exército Brasileiro, 2021, p. 20).

A fração responsável pela capacidade de Guerra Cibernética do BGE é a sua Companhia de Guerra Cibernética, conforme destaque em vermelho na Figura 5 a seguir.

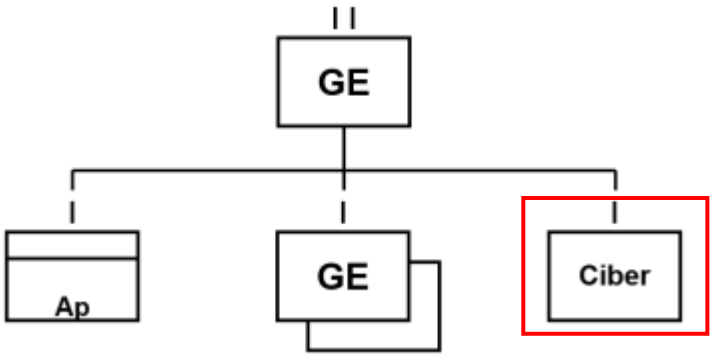

Figura 5 – Organigrama do Batalhão de Guerra Eletrónica

Fonte: adaptado de EB70-MC-10.315 Batalhão de Guerra Eletrónica (2022b)

O BComGE, por sua vez, é a "unidade responsável por instalar, explorar, manter e proteger os sistemas de comunicações, de guerra eletrónica e de tecnologia da informação em apoio ao preparo e emprego operativo do grande comando enquadrante" (Exército Brasileiro, 2021, p. 19). Ressalta-se que o BComGE é orgânico de uma DE, ou de uma estrutura específica quando da ativação de um Corpo de Exército, sendo que em tempo de paz a sua subordinação é a uma DE ou ao CMilA (Exército Brasileiro, 2021, p. 19).

A fração de Guerra Cibernética de um BComGE é constituída pelo seu pelotão de Guerra Cibernética, que compõe a Companhia de Guerra Eletrónica do batalhão, de acordo com o realçado na cor vermelha na Figura 6.

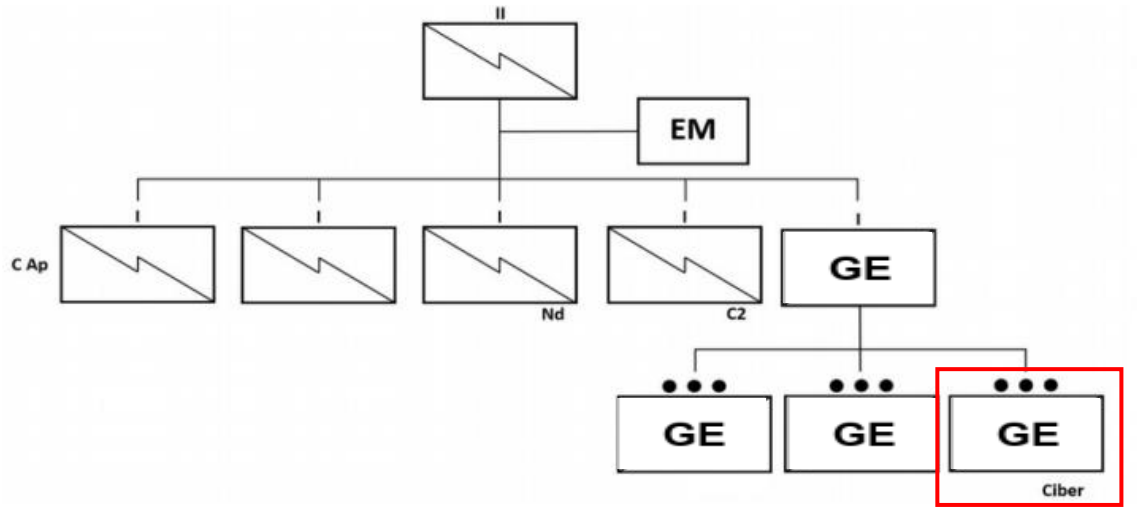

Figura 6 – Organigrama do Batalhão de Comunicações e Guerra Eletrónica

Fonte: adaptado de Nota Doutrinária Nr 04/2021 Sistema de Comando e Controle da Força Terrestre (2021)

O BCom possui uma estrutura bastante similar ao BComGE, sendo que a principal diferença é a não existência da Companhia de Guerra Eletrónica – o que limita as suas capacidades operativas de Guerra Cibernética. A subordinação e o valor de um BCom são exatamente os mesmos de um BComGE (Exército Brasileiro, 2021).

Finalmente, a CiaCom é uma "subunidade de comunicações independente responsável por instalar, explorar, manter e proteger os sistemas de comunicações e de tecnologia da informação em apoio ao preparo e emprego operativo da grande unidade enquadrante" (Exército Brasileiro, 2021, p. 21). Ou seja, a sua subordinação é a uma brigada do EB, e o seu valor equivale a uma companhia, sendo que as CO cibernéticas são exercidas por uma fração inferior a um pelotão (normalmente uma secção ou uma turma).

Importa também compreender o funcionamento e a organização do Grupamento de Comunicações e Eletrónica (GCE), "grande unidade de comunicações responsável por instalar, explorar, manter e proteger os sistemas de comunicações, de guerra eletrónica e de tecnologia da informação em apoio ao emprego operacional do Corpo de Exército" (Exército Brasileiro, 2021, p. 18). O GCE é equivalente a uma brigada e, por conseguinte, o mais alto escalão que opera com meios cibernéticos no nível tático, haja vista ser o elemento de apoio a um Corpo de Exército quando este for ativado.

A constituição de um GCE é variável e depende da missão a ser desempenhada, mas possui sempre em sua composição um BGE, além de uma quantidade flexível de BCom e BComGE (Exército Brasileiro, 2021). Assim, possui capacidades variadas de Guerra Cibernética capazes de multiplicar o potencial de combate da FTC.

Um GCE é mobilizado

> […] quando o Corpo de Exército for ativado, tendo sua estrutura organizacional oriunda do Comando de Comunicações e Guerra Eletrónica do Exército (CCOMGEx) acrescidas por um número variável de batalhões de comunicações e guerra eletrónica, em função da missão, da constituição do Corpo de Exército e da área de operações. (Exército Brasileiro, 2021, p. 18)

Considerada a organização das OM que possuem capacidade de Guerra Cibernética no EB – no que tange à doutrina militar terrestre –, faz-se necessário perceber a distribuição de tais elementos em território brasileiro, de modo a obter uma perspetiva real de como está articulada a capacidade cibernética da FTer.

Para tanto, deve-se observar o que prescreve a Concepção Estratégica do Exército (2019a), documento de mais alto nível, assinado pelo comandante do EB e que "constitui-se em um embasamento conceitual, decorrente de estudos, análises e avaliações, que indica como o Exército deve ser empregado para cumprir sua missão e, por via de consequência, organizado, articulado e preparado" (Exército Brasileiro, 2019a, p. 7). A Figura 7 a seguir, extraída do aludido documento, mostra a distribuição de todas as brigadas do EB em território nacional, alocadas pelos respetivos CMilA.

Figura 7 – Brigadas por Comando Militar de Área

Fonte: adaptado de Concepção Estratégica do Exército Brasileiro (2019a)

Conforme já visto, cada brigada possui em sua composição orgânica uma CiaCom, a qual possui capacidades cibernéticas – ainda que com limitações, de acordo com o que será visto em capítulo posterior. As brigadas estão agrupadas em seis DE, sendo que cada divisão possui em sua estrutura um BCom ou um BComGE. Por fim, o CCOMGEx contém, em sua composição, o único BGE existente no EB, tudo de acordo com o previsto na Concepção Estratégica do Exército (2019).

Dessa forma, a Figura 8 abaixo demonstra, de modo gráfico, a articulação dos elementos da FTer que possuem capacidade cibernética, ou seja, os BCom, BComGE e o BGE – excetuando-se as CiaCom que não foram representadas geograficamente por se tratar de OM subordinadas às brigadas já localizadas em figura anterior.

Figura 8 – Localização das OM com capacidades cibernéticas

Fonte: adaptado de EB20-MF-10.101 O Exército Brasileiro (2014a)

4.2. Síntese conclusiva e resposta à QD1

Face ao exposto, e em resposta à QD1 "Como está organizada a Guerra Cibernética no EB?", verifica-se que a organização das capacidades cibernéticas da FTer está

articulada no território brasileiro de modo a atender as prioridades da Força em todos os escalões, desde a brigada até o Corpo de Exército.

Assim, no tocante à subordinação, conclui-se que as OM possuidoras de condições de realizar atividades cibernéticas estão vinculadas: (i) ao Corpo de Exército quando ativado – no nível mais alto –, (ii) ao CMilA ou às DE, (iii) e finalmente às brigadas, caracterizando a presença da Guerra Cibernética a partir do módulo básico de emprego em operações militares (uma brigada).

Quanto ao indicador valor, a Guerra Cibernética apresenta-se, em sua organização, por meio de elementos de valor batalhão e companhia, quais sejam o BGE, os BCom ou BComGE e as CiaCom. Ressalta-se que todas as frações citadas existem como tropa constituída do EB.

Por fim, o Quadro 2 a seguir sintetiza as conclusões acima, materializando a resposta à QD1.

Quadro 2 – Organização da Guerra Cibernética no EB

Organização Militar	Subordinação	Valor
1º Batalhão de Guerra Eletrônica (1º BGE)	Corpo de Exército (através do CCOMGEx / GCE)	Batalhão
1º Batalhão de Comunicações e Guerra Eletrônica de Selva (1º BComGESl)	Comando Militar da Amazônia	
2º Batalhão de Comunicações e Guerra Eletrônica de Selva (2º BComGESl)	Comando Militar do Norte	
3º Batalhão de Comunicações e Guerra Eletrônica (3º BComGE)	Comando Militar do Sul	
9º Batalhão de Comunicações e Guerra Eletrônica (9º BComGE)	Comando Militar do Oeste	
1º Batalhão de Comunicações (1º BCom)	3ª Divisão de Exército (3ª DE)	
4º Batalhão de Comunicações (4º BCom)	Comando Militar do Nordeste	
5º Batalhão de Comunicações (4º BCom)	5ª Divisão de Exército (5ª DE)	
6º Batalhão de Comunicações (4º BCom)	6ª Divisão de Exército (6ª DE)	
Batalhão de Comunicações Escola	1ª Divisão de Exército (1ª DE)	
Companhias de Comunicações	Brigadas	Companhia

5. Atuação da Guerra Cibernética para a condução das operações militares

Para além da organização da Guerra Cibernética do EB, e de maneira a identificar e eventualmente selecionar os principais contributos dessa área para a potenciação da capacidade cibernética, é imperativo que se entenda a atuação de suas estruturas.

O intuito do presente capítulo é precisamente examinar a atuação dos elementos apontados anteriormente, reconhecendo de que modo os mesmos desempenham o seu papel nas operações militares, bem como compreender como os programas e projetos militares relacionados com a Guerra Cibernética colaboram com a sua evolução.

Outrossim, as entrevistas realizadas buscaram confirmar os dados encontrados na análise documental, confrontá-los com a realidade e concluir se a atuação da Guerra Cibernética do EB atende aos quesitos de adequabilidade (a estrutura existente está em conformidade com os objetivos propostos?) e de praticabilidade (a estrutura existente tem condições de executar o que é proposto pelos objetivos?).

5.1. Capacidades Operativas de Guerra Cibernética

Conforme verificado nos conceitos estruturantes deste trabalho, as CO de Guerra Cibernética são três (Proteção, Exploração e Ataque Cibernético), sendo que cada uma das OM que compõem a estrutura de Guerra Cibernética do EB possui diferentes CO, como será visto a seguir.

O 1º BGE é a OM que tem como missão, exclusivamente no que tange à cibernética, apoiar em guerra cibernética uma "FTC até o nível Corpo de Exército ou que enquadre mais de uma Divisão de Exército […]" (Exército Brasileiro, 2021, p. 20). Também é o único elemento no nível tático possuidor das CO Proteção, Exploração e Ataque Cibernético, pois contempla em sua organização uma companhia de Guerra Cibernética (Exército Brasileiro, 2022b; Kuhn, 2022).

De acordo com Guimarães (entrevista por videoconferência, 15 de janeiro de 2024), atual comandante do 1º BGE, há conformidade da missão proposta ao batalhão com aquilo que prevê a doutrina, pois a sua tropa apoia "em cibernética o Corpo de Exército". Além disso, há clara definição da área de atuação – qual seja todo o território nacional, a depender da operação que está sendo apoiada –, o que permite inferir que existe adequabilidade na atuação do 1º BGE.

Guimarães (*op. cit.*) ainda relata que há tempo suficiente para a preparação e para o emprego do efetivo especializado do batalhão em operações. A companhia de Guerra Cibernética é a fração responsável pela aplicação da capacidade cibernética, e a mesma

existe de fato, sendo possuidora das três CO cibernéticas (estando de acordo com o prescrito pela doutrina). Também há material especializado disponível para o atingimento dos objetivos do 1º BGE, confirmando que o emprego do batalhão é praticável, em virtude dos meios e capacidades existentes.

Os 1º BComGESl e 2º BComGESl são as duas unidades que possuem capacidades de Guerra Cibernética e que atuam preponderantemente em ambiente de selva. Tal ambiente possui características especiais e engloba, em particular, "a selva amazônica, tendo como área de abrangência a Amazônia brasileira e o seu entorno sul americano" (Exército Brasileiro, 2023c, p. 2–1).

Os BComGE são subordinados, conforme já analisado, às DE ou aos CMilA, podendo ainda constituírem elementos de um GCE (quando ativado). Desse modo, tais batalhões oferecem aos seus respetivos comandos somente duas CO cibernéticas: Proteção e Exploração Cibernética, pois possuem apenas um pelotão de Guerra Cibernética em sua organização (Exército Brasileiro, 2017c).

Os BComGE que atuam na região de selva do Brasil possuem nítida definição de área para operar – basicamente as responsabilidades são divididas entre a Amazônia Ocidental e Oriental –, tendo a sua missão em capacidade cibernética compatível com a OM, o que demonstra que há adequabilidade de ambos no cumprimento das respetivas missões (Xavier e Junior, entrevistas por videoconferência, 16 e 17 de fevereiro de 2024).

No tocante à praticabilidade, há somente uma diferença entre as duas OM: de acordo com Junior (*op. cit.*), o 1º BComGESl possui um "efetivo considerado insuficiente" para atender as necessidades atinentes à capacidade cibernética impostas ao batalhão, o que limita a organização em algumas ações, nomeadamente de exploração cibernética. Ainda em relação ao 1º e 2º BComGESl, o material disponível atende às exigências, há suficiência de tempo no preparo e emprego para as operações e as CO Proteção e Exploração Cibernética estão presentes, caracterizando o atingimento da praticabilidade.

Da mesma forma, o 3º BComGE é um batalhão que também possui as CO Proteção e Exploração Cibernética como contribuições oriundas do seu pelotão de Guerra Cibernética orgânico. Na prática, ainda está a desenvolver a exploração cibernética, haja vista ter sido o último BCom a ser transformado em BComGE pelo EB.

Desse modo, ainda que possua em sua atribuição, pela doutrina, a necessidade de realizar ações de exploração cibernética, esta é uma das capacidades que possuem limitações pelo batalhão. Segundo Nepomuceno (entrevista por *email*, 02 de fevereiro de

2024), a adequabilidade é parcialmente atingida, pois a área geográfica condiz com o que se espera da OM, ainda que haja uma limitação da missão doutrinária. Já a praticabilidade é prejudicada em razão da incompatibilidade da fração de Guerra Cibernética com a missão atribuída ao batalhão (há menor efetivo especializado), não obstante haver a previsão de distribuição de pessoal habilitado por parte do EB.

Responsável pela geração da capacidade cibernética no flanco oeste brasileiro, o 9º BComGE é o batalhão que mais cedo iniciou o processo de transformação, ao agregar capacidades de Guerra Eletrónica e Guerra Cibernética desde a sua origem, possuindo as CO Proteção e Exploração Cibernética. A OM foi uma das primeiras a serem contempladas pelos programas e projetos estratégicos do EB para a área de cibernética (Barros, entrevista por *email*, 05 de fevereiro de 2024).

O 9º BComGE atende aos quesitos de adaptabilidade e praticabilidade, possuindo farto material especializado, efetivo especializado compatível com a missão, área de atuação estabelecida e frações de Guerra Cibernética prontas para serem empregues (Barros, *op. cit.*).

Finalmente, os BCom são as OM que possuem a capacidade de realizar "proteção cibernética dos sistemas de informação do grande comando apoiado. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética [...]" (Exército Brasileiro, 2017c, p. 3–3). Não possui em sua organização uma companhia ou pelotão de Guerra Cibernética, somente frações específicas para a execução de medidas protetivas, o que limita o leque de CO cibernéticas. A mesma CO Proteção Cibernética está presente no BCom Escola, um batalhão de comunicações com a mesma constituição dos demais, porém com a responsabilidade extra de apoiar atividades de ensino do EB (Exército Brasileiro, 2019a).

As CiaCom, por sua vez, são o menor escalão do nível tático com alguma CO Cibernética, nomeadamente a Proteção. São elas que realizam a proteção cibernética das grandes unidades, em particular dos sistemas de informação da grande unidade (brigada) à qual é subordinada (Exército Brasileiro, 2017c).

Portanto, cada um dos comandantes das estruturas exploradas anteriormente, alicerçado pelo assessoramento de seu estado-maior, coordena, planeia e conduz ações no espaço cibernético, sejam essas ações de proteção, exploração ou ataque cibernético (Exército Brasileiro, 2023b).

Tem-se, assim, a definição de como cada estrutura estudada no capítulo anterior trabalha em função da Guerra Cibernética, e quais são as CO cibernéticas de cada uma delas.

5.2. Programas e projetos relacionados à Guerra Cibernética

Nomeadamente a partir da elaboração da END, o EB passou a investir com maior ênfase no campo cibernético, de modo a aperfeiçoar as capacidades já existentes e gerar novas – atendendo a demanda brasileira no setor (Ministério da Defesa, 2018).

A primeira iniciativa no que tange a qualquer projeto relacionado com a capacidade cibernética nas FFAA e no EB ocorreu em 2011, quando da criação do Projeto Estratégico do Exército Defesa Cibernética. Como projeto, o mesmo teve uma evolução natural até que passou ao nível de programa (ou seja, abrangendo vários projetos afetos), sendo denominado Programa Estratégico do Exército (PEE) Defesa Cibernética (Estado-Maior do Exército, 2023). Atualmente, o programa é a vertente mais relevante ao se considerar o ramo Exército, haja vista o EB ser o impulsionador do setor cibernético para a Defesa Nacional, de acordo com a END.

O PEE Defesa Cibernética está atualmente composto por cinco projetos fundamentais, visando estabelecer a capacidade cibernética no Exército e cooperar com os demais ramos, além do MD. Esses projetos são atualmente gerenciados por OM relacionadas ao setor, como o Instituto Militar de Engenharia, o Comando de Comunicações e Guerra Eletrónica do Exército, o Centro de Desenvolvimento de Sistemas do Exército, o Centro Integrado de Telemática do Exército, o Centro de Inteligência do Exército e o próprio Centro de Defesa Cibernética. O programa atende às demandas de capacidade, bem como promove o aprimoramento destas para mais de cinquenta OM específicas da área, além de proporcionar defesa para as redes operacionais e estratégicas dos envolvidos (Estado-Maior do Exército, 2023).

Verifica-se que o programa atende diversas áreas do ramo pela diversificação dos seus projetos: cada um dos projetos está voltado para o atendimento de uma necessidade específica. Alguns apresentam maior pertinência ao trabalho ora em tela. De acordo com o Estado-Maior do Exército (2023), iniciativas como o desenvolvimento de sistemas de segurança da informação, programas de deteção de intrusão, hardware para a criação de laboratórios e simuladores de Defesa e Guerra Cibernética, bem como o apoio ao desenvolvimento de software nacional, incluindo antivírus, seminários e programas de

treinamento especializado, representam algumas das medidas implementadas no escopo do programa.

O projeto Força Cibernética, integrante de vulto e um dos principais impulsionadores do programa, tem como objetivo estabelecer estruturas dedicadas à capacitação, preparo e emprego operacional em atividades de segurança, defesa e guerra cibernética. Essas estruturas visam assegurar à Força Terrestre a capacidade de operar de maneira segura e integrada à rede do sistema militar de comando e controle do Ministério da Defesa (Estado-Maior do Exército, 2023). Um dos produtos de destaque do projeto, no vetor Preparo, é o desenvolvimento de um simulador de ações cibernéticas, denominado SACI (acrônimo). Desse modo, a atuação se dá em variados campos, conforme a Figura 9 abaixo:

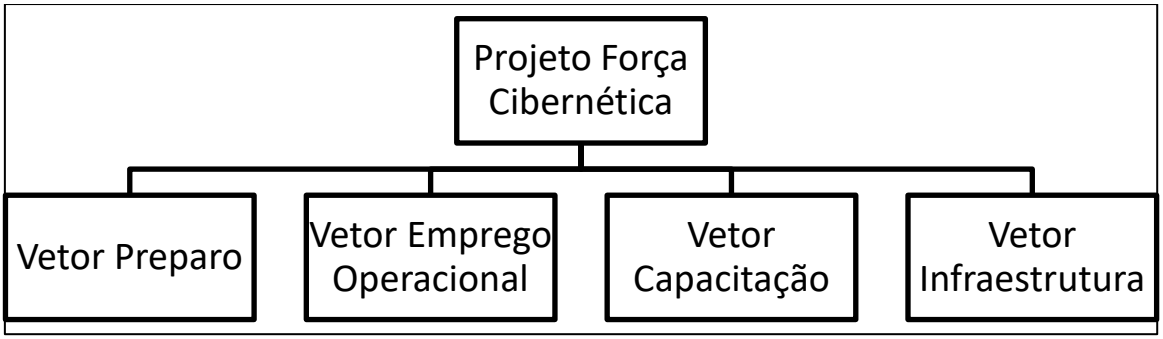

Figura 9 – Estrutura analítica do projeto Força Cibernética

Fonte: adaptado de Estado-Maior do Exército (2023)

Além do Força Cibernética, os demais projetos enquadrados no PEE Defesa Cibernética são: (i) Escudo Cibernético, voltado para a proteção dos ativos de informação e dos sistemas; (ii) Centro de Defesa Cibernética, que abrange as ações atinentes à estruturação do CDCiber; (iii) Apoio Tecnológico, com o fito de desenvolver os sistemas e estruturas de apoio ao setor cibernético; e (iv) Pesquisa Cibernética, destinado à capacitação de recursos humanos.

Nesse contexto, o PEE Defesa Cibernética pode ser visto como um dos mais relevantes propulsores das capacidades cibernéticas do EB, pois permite a identificação de lacunas existentes e oferece um significativo aporte de recursos para a evolução da Guerra Cibernética, contribuindo para a atuação do EB nas operações militares.

5.3. Síntese conclusiva e resposta à QD2

Daquilo que precede, tem-se que a estrutura de Guerra Cibernética do EB pode atuar mediante o emprego das três CO cibernéticas, utilizando-se das suas variadas OM

especializadas. Os manuais doutrinários que tratam sobre o assunto são explícitos ao classificar os tipos de batalhões e as suas capacidades.

As entrevistas com os comandantes do BGE e dos BComGE brasileiros permitiu uma visão mais aclarada sobre os quesitos da adequabilidade e da praticabilidade do emprego de tais capacidades em operações militares.

Em relação ao primeiro quesito, ficou nítido que o mesmo é atingido pela grande maioria, já que 100% das áreas geográficas estão delimitadas e 80% das missões dos batalhões estão de acordo com a doutrina – salvo uma única exceção com pequenas limitações (3º BComGE).

Pode-se inferir, ainda, que a praticabilidade também é alcançada, haja vista a maior parte de os resultados demonstrar que há pessoal, material e tempo compatíveis para que a missão da OM seja cumprida, de acordo com os entrevistados, ainda que existam óbices principalmente no tocante ao pessoal.

Sendo assim, tem-se consubstanciada a real forma de atuação das OM de Guerra Cibernética do EB, bem como a resposta à QD2 "De que forma a Guerra Cibernética do EB atua em proveito das operações militares?", no Quadro 3 a seguir.

Quadro 3 – Capacidades cibernéticas das OM do EB

Organização Militar	Capacidade cibernética
1º Batalhão de Guerra Eletrônica (1º BGE)	Proteção, Exploração e Ataque
1º Batalhão de Comunicações e Guerra Eletrônica de Selva (1º BComGESl)	Proteção e Exploração*
2º Batalhão de Comunicações e Guerra Eletrônica de Selva (2º BComGESl)	Proteção e Exploração
3º Batalhão de Comunicações e Guerra Eletrônica (3º BComGE)	Proteção e Exploração*****
9º Batalhão de Comunicações e Guerra Eletrônica (9º BComGE)	Proteção e Exploração
1º Batalhão de Comunicações (1º BCom)	Proteção
4º Batalhão de Comunicações (4º BCom)	
5º Batalhão de Comunicações (4º BCom)	
6º Batalhão de Comunicações (4º BCom)	
Batalhão de Comunicações Escola	
Companhias de Comunicações	
***com limitações**	

6. Impacto da capacidade cibernética para as operações militares

A Guerra Cibernética é uma das capacidades que pode impactar as operações militares de diferentes maneiras, multiplicando o poder de combate da força que possui tal aptidão (Neto, 2018).

Assim, para se obter uma visão holística de quais são esses impactos e como eles afetam as operações militares, torna-se imperioso a análise das aludidas operações no âmbito do EB, bem como a verificação dos eventuais contributos da Guerra Cibernética na condução das ações militares.

Destarte, a realização das entrevistas do presente estudo buscou cristalizar um último quesito, ao combinar os contributos analisados com a eventualidade das despesas e riscos atribuídos à Guerra Cibernética, materializando-se na aceitabilidade (os benefícios que o emprego da estrutura oferece compensam os custos e os riscos atrelados?).

6.1. Operações militares do Exército Brasileiro

A definição do EB para uma operação militar é "o conjunto de ações realizadas com forças e meios militares, coordenadas em tempo, espaço e finalidade, de acordo com o estabelecido em uma diretriz, plano ou ordem para o cumprimento de uma atividade, tarefa, missão ou atribuição" (Exército Brasileiro, 2017a, p. 2–1).

As atividades militares ocorrem em diferentes tipos de situações de conflito, que abrangem desde a prevenção de ameaças até a resolução de confrontos armados, incluindo o manejo de crises, dependendo do grau de envolvimento. Isso significa que as operações podem acontecer tanto em cenários de guerra como em cenário considerados de não guerra (Exército Brasileiro, 2017b).

Outrossim, o EB estabelece que na situação de guerra o instrumento militar é utilizado em sua plenitude; já na situação de não guerra o mesmo instrumento é utilizado de modo restrito, não sendo o poder preponderante nas ações (Exército Brasileiro, 2017a). Tal entendimento é necessário para se compreender as operações militares básicas executadas pela FTer, seja em contexto de guerra ou de não guerra, e de que modo a Guerra Cibernética contribui com cada uma delas.

Isto posto, tem-se que as operações podem ser consideradas básicas quando, "por si mesmas, podem atingir os objetivos determinados por uma autoridade militar ou civil, em situação de guerra ou em situação de não guerra". São elas: (i) em situação de guerra, operações ofensivas e defensivas, (ii) e em situação de não guerra, as operações de cooperação e coordenação com agências (OCCA) (Exército Brasileiro, 2017b).

As operações ofensivas são aquelas que possuem espírito agressivo com predominância da manobra, do movimento e da iniciativa, visando atingir o inimigo com potencial de combate superior para sua neutralização ou destruição. Por sua vez, as operações defensivas tem por objetivo manter a posse de uma região ou território, ou negá-lo ao oponente, bem como garantir a integridade de algum meio específico (Exército Brasileiro, 2017b).

Na esfera da situação de não guerra, temos as OCCA como "operações executadas por elementos do EB em apoio aos órgãos ou instituições (governamentais ou não, militares ou civis, públicos ou privados, nacionais ou internacionais), definidos genericamente como agências" (Exército Brasileiro, 2017b, p. 3–14). O intuito é a máxima coordenação dos esforços para o atingimento de um objetivo comum entre os envolvidos na operação.

Ressalta-se que

> [...] o conceito operativo do Exército é definido pela forma de atuação da Força Terrestre no amplo espectro dos conflitos, tendo como premissa maior a combinação, simultânea ou sucessiva, de operações ofensivas, defensivas e de cooperação e coordenação com agências, ocorrendo em situação de guerra e de não guerra. A situação determinará a preponderância de uma operação sobre outras. (Exército Brasileiro, 2017b, p. 2–16)

A figura a seguir ilustra o que é a condução das operações no amplo espectro, conforme citado anteriormente.

Figura 10 – Conceito Operativo do Exército – amplo espectro (exemplos de situações)

Fonte: adaptado de (Exército Brasileiro, 2017b)

Portanto, tem-se identificado o leque de operações nas quais a Guerra Cibernética pode atuar, com os diferentes propósitos e atores envolvidos, exigindo elevado grau de flexibilidade da capacidade cibernética do EB.

6.2. Principais contributos da capacidade cibernética do Exército Brasileiro nas operações militares

Doutrinariamente, as capacidades cibernéticas contribuem de modos distintos para cada tipo de operação militar (defensiva, ofensiva ou OCCA), haja vista os objetivos também díspares entre cada uma delas.

Nas operações ofensivas, dado o foco na ação decisiva de emprego da força para impor a nossa vontade sobre a do oponente e – por muitas vezes – destruir ou neutralizar o mesmo, as atitudes são de alta intensidade e buscam a concentração do potencial de combate (Exército Brasileiro, 2017a). Nessas situações, possuem importância vital as ações de exploração e ataque cibernético, nomeadamente aquelas que exigem coordenação com os fogos e a guerra eletrônica (Exército Brasileiro, 2017c).

De modo geral, os ataques cibernéticos irão visar a negação de serviços ou o prejuízo do funcionamento das infraestruturas críticas e dos sistemas do adversário; já a exploração cibernética busca a identificação de vulnerabilidades nos inúmeros sistemas e dispositivos

oponentes, contribuindo com o planeamento das ações ofensivas, bem como com a recolha de dados de informação (Exército Brasileiro, 2017c).

Por sua vez, as operações defensivas privilegiam as ações de proteção cibernética, ainda que as demais capacidades possam ser utilizadas – desde que não comprometam dados essenciais da operação, como posição, endereços lógicos ou intenções (Neto, 2018). O âmago da Guerra Cibernética nesse tipo de operação é preservar o fluxo de informação, a celeridade na tomada de decisão e difusão de ordens e a coordenação dos meios empregues (Exército Brasileiro, 2017c).

Como já visto, as OCCA são operações que possuem grande variedade de modalidades, já que o instrumento militar não é o preponderante e os objetivos são diversos. Uma das principais características é a presença das agências, o que pode condicionar a utilização das CO cibernéticas da força que está sendo empregada (Ministério da Defesa, 2017).

Outrossim, "a necessidade de coordenação entre as agências define a estrutura de capacidades cibernéticas a ser organizada para o cumprimento da missão [...] e na composição dessa estrutura estão presentes elementos de ligação interagências e elementos civis especialistas, para operação assistida e assessoria" (Exército Brasileiro, 2017c, p. 5–4). Verifica-se claramente que tal constituição é flexível, para atender aos propósitos da operação; porém, de maneira genérica, é dada ênfase maior a ações de proteção e de exploração cibernéticas" (Exército Brasileiro, 2017c, p. 5–4). É comum o uso da Guerra Cibernética como forma de potenciar as demais ações e como ferramenta de apoio para outros tipos de atitude, como a atuação de operações de informação[8] (Kuhn, 2022).

Para que se possa apurar se os contributos anteriormente expostos são efetivamente válidos, ou seja, se os benefícios almejados compensam os eventuais riscos e / ou despesas, fez-se uso das entrevistas realizadas com os comandantes de cada uma das estruturas de Guerra Cibernética do EB.

Assim, verifica-se como principais riscos atinentes ao emprego das capacidades cibernéticas: (i) a possível exposição da tropa que está a operar e (ii) a proteção limitada de estruturas ou sistemas a serem mantidos em segurança. Salientado por 60% dos entrevistados, o custo do material e soluções digitais para emprego da capacidade

[8] "Atuação metodologicamente integrada de capacidades relacionadas à informação, em conjunto com outros vetores, para informar e influenciar grupos e indivíduos, bem como afetar o ciclo decisório de oponentes, ao mesmo tempo protegendo o nosso" (Exército Brasileiro, 2014b, p. 3–1).

cibernética foi considerado reduzido, corroborando positivamente com o quesito da aceitabilidade.

Já os principais contributos apontados pelos entrevistados foram a capacidade de proteção dos sistemas de tecnologia da informação utilizados pelo escalão apoiado e a identificação das vulnerabilidades do oponente. No caso em concreto do 1º BGE, por possuir a CO Ataque Cibernético, também foi apresentado o contributo da neutralização dos sistemas digitalizados do adversário.

6.3. Síntese conclusiva e resposta à QD3

Face ao exposto, e em resposta à QD3 "Quais os contributos da capacidade cibernética do Exército Brasileiro na condução das operações militares?", constata-se que, primeiramente, o emprego da Guerra Cibernética é um dos multiplicadores do potencial de combate – condição esta apresentada por 100% dos entrevistados com relação ao quesito aceitabilidade; tal quesito foi avaliado por meio da análise documental e das entrevistas, sendo considerado atingido pelo trabalho.

De modo geral, os contributos variam de acordo com as operações militares e, como é óbvio, com as estruturas empregues. O capítulo ora em tela buscou consolidar as vantagens da utilização da Guerra Cibernética presentes na doutrina com aquelas apontadas como mais importantes nas entrevistas, sendo que o Quadro 5 a seguir sintetiza o evidenciado:

Quadro 4 – Contributos por OM do EB

Organização Militar	Principais contributos
1º Batalhão de Guerra Eletrônica (1º BGE)	- Negação de serviços do adversário - Interrupção/neutralização dos sistemas de informação do oponente - Identificação de vulnerabilidades do oponente - Preservar fluxo de informação, ciclo decisório e coordenação dos meios - Proteção dos sistemas de TIC
1º Batalhão de Comunicações e Guerra Eletrônica de Selva (1º BComGESl)	- Identificação de vulnerabilidades do oponente* - Preservar fluxo de informação, ciclo decisório e coordenação dos meios - Proteção dos sistemas de TIC
2º Batalhão de Comunicações e Guerra Eletrônica de Selva (2º BComGESl)	- Identificação de vulnerabilidades do oponente - Preservar fluxo de informação, ciclo decisório e coordenação dos meios - Proteção dos sistemas de TIC
3º Batalhão de Comunicações e Guerra Eletrônica (3º BComGE)	- Identificação de vulnerabilidades do oponente* - Preservar fluxo de informação, ciclo decisório e coordenação dos meios - Proteção dos sistemas de TIC
9º Batalhão de Comunicações e Guerra Eletrônica (9º BComGE)	- Identificação de vulnerabilidades do oponente - Preservar fluxo de informação, ciclo decisório e coordenação dos meios

	- Proteção dos sistemas de TIC
1º Batalhão de Comunicações (1º BCom)	- Preservar fluxo de informação, ciclo decisório e coordenação dos meios - Proteção dos sistemas de TIC
4º Batalhão de Comunicações (4º BCom)	
5º Batalhão de Comunicações (5º BCom)	
6º Batalhão de Comunicações (6º BCom)	
Batalhão de Comunicações Escola	
Companhias de Comunicações	
***com limitações**	

7. Perspetiva de evolução da capacidade cibernética do Exército Brasileiro

No presente capítulo, foi verificada uma perspetiva de evolução e consequente desenvolvimento das capacidades relacionadas com a Guerra Cibernética no EB, advindas dos dados anteriormente analisados.

7.1. Potenciação da capacidade cibernética na condução das operações militares

Como parte do processo evolutivo inerente a qualquer força armada, o EB busca estar em sintonia e alinhado com o ambiente operacional vivenciado na atualidade. O planeamento estratégico da Força Terrestre é um dos orientadores de tal processo, que apresenta simultaneamente o direcionamento necessário e os objetivos estratégicos que conduzem a transformação pleiteada no sentido de adequar-se à era do conhecimento (Exército Brasileiro, 2019b).

Assim sendo, o Objetivo Estratégico do Exército (OEE) de número quatro, presente no Plano Estratégico do Exército (PEEx), é designado como "Atuar no espaço cibernético com liberdade de ação" (Exército Brasileiro, 2019b, p. 19). O OEE 4 prevê inúmeras ações estratégicas e atividades para atingir o estado final proposto, como implantar novos órgãos com capacidades cibernéticas no nível tático e adequar estruturas de preparo, emprego e ensino que envolvam a capacidade cibernética. Ou seja, o EB já pensa na evolução do aludido setor e o coloca como uma de suas prioridades.

Nesse ínterim, o Quadro 5 do capítulo 6 consubstanciou as OM com capacidade cibernética e os seus respetivos contributos mais relevantes, aliando a doutrina existente com o exposto pelos seus comandantes. Significa que as vantagens apresentadas não são somente aquelas previstas em manuais institucionais, mas sim as que possuem maior significância na condução das operações militares e também estão orientadas conforme os ditames doutrinários.

Portanto, os contributos identificados são aqueles que efetivamente colaboram com os comandantes e, por conseguinte, com as suas OM na execução de ações de Guerra Cibernética. Nota-se que, dentre os benefícios anunciados, a proteção de sistemas de TIC e a identificação de vulnerabilidades merecem destaque, haja vista terem sido citados pela totalidade dos entrevistados – ou seja, pelas OM que possuem pelo menos as CO Proteção e Exploração Cibernética. Os BCom e as CiaCom, como OM que não possuem a CO Exploração Cibernética, contribuem na forma de proteção de sistemas de TIC, corroborando com tal contributo.

No que diz respeito à CO Ataque Cibernético, Guimarães (*op. cit.*) enfatiza que o fato de que os BComGE já possuem uma estrutura mínima de Guerra Cibernética, nomeadamente no que tange à proteção e exploração, facilita a adição, quando em operações, dos módulos ofensivos de cibernética do 1º BGE, o que traduz o conceito de modularidade: "característica de uma força que lhe confere a condição de, a partir de uma estrutura básica mínima, receber módulos que ampliem seu poder de combate ou lhe agreguem capacidades" (Exército Brasileiro, 2022a, p. 4–2).

Dessa forma, tendo como contributos mais expressivos a proteção dos sistemas e a identificação de vulnerabilidades, além de considerar que a CO Ataque Cibernético é adicionada pelo BGE conforme a necessidade e especificidade de cada operação, tem-se que a transformação dos BCom para BComGE se vislumbra como uma alternativa possível para a evolução da Guerra Cibernética no EB. A solução permite agregar, a baixo custo e envolvendo os projetos estratégicos estudados, capacidades cibernéticas mínimas às OM que ainda não as possuem, ao mesmo tempo em que se utiliza da modularidade para complementar eventuais competências ausentes.

7.2. Síntese conclusiva e resposta à QC

Em vista do analisado, e em resposta à QC "Em que medida o EB pode potenciar a sua capacidade cibernética na condução das operações militares?", tem-se como primeiro ponto a seleção dos contributos considerados mais significativos de acordo com a doutrina e com os entrevistados.

Nesse sentido, o principal contributo que abrange a CO Proteção Cibernética é a proteção dos sistemas de TIC; já para a CO Exploração Cibernética, designa-se a identificação de vulnerabilidades do oponente; e para a CO Ataque Cibernético, exclusiva do 1º BGE, apresenta-se a negação de serviços do adversário.

Em segundo lugar, como medidas de potenciação para a Guerra Cibernética das estruturas definidas de cada CO Cibernética, tem-se a manutenção das CO através do PEE Defesa Cibernética naquelas OM em que as capacidades estão a funcionar de modo pleno. A incompatibilidade da fração de Guerra Cibernética existente tanto no 1º BComGESl quanto no 3º BComGE, principalmente em falta de efetivo especializado, demanda uma medida particular de incremento da CO Exploração Cibernética para esses casos – nomeadamente quanto aos tópicos de formação de pessoal e adestramento da tropa.

Finalmente, e com o fito de acrescer a CO Exploração Cibernética aos BCom, consonante com a aceitabilidade da potenciação advinda da referida capacidade, propõe-se

a transformação gradual dos batalhões mencionados em BComGE. Desse modo, o Quadro 5 exibe a relação entre OM, contributos selecionados e as formas de potenciação verificadas.

Quadro 5 – Potenciação da capacidade cibernética do EB

Organização Militar	Contributos selecionados	Medidas para potenciação
1º Batalhão de Guerra Eletrônica (1º BGE)	- Negação de serviços do adversário - Identificação de vulnerabilidades do oponente - Proteção dos sistemas de TIC	Manutenção das CO através do PEE Defesa Cibernética
1º Batalhão de Comunicações e Guerra Eletrônica de Selva (1º BComGESl)	- Identificação de vulnerabilidades do oponente* - Proteção dos sistemas de TIC	- Incremento da CO Exploração Cibernética - Manutenção da CO Proteção Cibernética através do PEE Defesa Cibernética
2º Batalhão de Comunicações e Guerra Eletrônica de Selva (2º BComGESl)	- Identificação de vulnerabilidades do oponente - Proteção dos sistemas de TIC	Manutenção das CO através do PEE Defesa Cibernética
3º Batalhão de Comunicações e Guerra Eletrônica (3º BComGE)	- Identificação de vulnerabilidades do oponente* - Proteção dos sistemas de TIC	- Incremento da CO Exploração Cibernética - Manutenção da CO Proteção Cibernética através do PEE Defesa Cibernética
9º Batalhão de Comunicações e Guerra Eletrônica (9º BComGE)	- Identificação de vulnerabilidades do oponente - Proteção dos sistemas de TIC	Manutenção das CO através do PEE Defesa Cibernética
1º Batalhão de Comunicações (1º BCom)	- Identificação de vulnerabilidades do oponente - Proteção dos sistemas de TIC	- Transformação em BComGE para obtenção da CO Exploração Cibernética - Manutenção da CO Proteção Cibernética através do PEE Defesa Cibernética
4º Batalhão de Comunicações (4º BCom)		
5º Batalhão de Comunicações (5º BCom)		
6º Batalhão de Comunicações (6º BCom)		
Batalhão de Comunicações Escola		
Companhias de Comunicações	- Proteção dos sistemas de TIC	- Manutenção da CO Proteção Cibernética através do PEE Defesa Cibernética
***com limitações**		

8. Conclusões

Desde 2008, o campo cibernético tem ganhado importância para a Defesa Nacional do Brasil, sendo a END o marco da transformação e do desenvolvimento do setor nas forças militares brasileiras.

Além disso, o ambiente operacional atual, englobando as condições que influenciam seus domínios de atuação, é vital para o EB. Este ambiente é complexo e dinâmico, exigindo maior capacidade de planeamento e adaptação diante de inúmeros desafios, como a guerra cibernética. A convergência de novas tecnologias destaca a importância da sincronização dos meios para maximizar seus efeitos. Diante dessas mudanças, o EB deve ajustar sua postura e conduzir suas operações de forma apropriada, integrando novas capacidades, incluindo a atuação no espaço cibernético. Desse modo, a evolução de tal setor, nomeadamente ao nível tático – cerne da presente investigação – torna-se de imprescindível.

Na esfera metodológica, este TII incidiu na análise e interpretação de dados provenientes de documentos e entrevistas semiestruturadas. O propósito foi aprofundar as variáveis de organização, adequação, praticabilidade e aceitabilidade, combinando o conhecimento dos entrevistados com a doutrina militar atual e a estrutura de Guerra Cibernética do Exército Brasileiro. Considerando tais variáveis, é relevante destacar os principais resultados alcançados e suas contribuições para o conhecimento, em relação a cada uma delas.

No que concerne à organização, observa-se que a disposição das capacidades cibernéticas da FTer no Brasil está planeada para atender às necessidades do EB desde o escalão brigada, passando pelas DE ou CMilA até o Corpo de Exército, evidenciando a presença da Guerra Cibernética desde o nível básico de emprego em operações militares. Em relação ao indicador valor, a Guerra Cibernética é organizada por elementos de valor batalhão e companhia, como o BGE, os BComGE, (incluindo os BComGESl), os BCom e as CiaCom.

No que diz respeito à adequabilidade e praticabilidade, percebeu-se que ambas foram atingidas. A doutrina militar terrestre detalha as CO cibernéticas disponíveis para cada elemento, o que foi corroborado através das entrevistas com os respetivos comandantes de OM. Com apenas o constrangimento na utilização da CO Exploração Cibernética por parte do 3º BCom e do 1º BComGESl, os militares entrevistados consideraram a adequação e

viabilidade do emprego das capacidades cibernéticas como possíveis, demonstrando a forma de atuação da Guerra Cibernética em proveito de operações militares.

Já no que tange à aceitabilidade há unanimidade, tanto doutrinária quanto em relação aos entrevistados, de que a Guerra Cibernética é multiplicadora do potencial de combate. Já os riscos e custos advindos do seu emprego podem não ser admissíveis na opinião de somente um dos comandantes – com a ponderação que tal questão deve ser levada ao escalão superior para deliberação. Infere-se, portanto, que os ganhos auferidos pelas ações cibernéticas superam os óbices.

Destarte, foram selecionados os contributos a seguir, elencados como mais expressivos de acordo com o estudo: negação de serviços do adversário, identificação de vulnerabilidades do oponente e proteção dos sistemas de TIC. Ainda, tais contributos podem ser potenciados por medidas de acordo com a OM que os emprega, nomeadamente com as propostas de medidas doravante citadas: (i) a manutenção das CO cibernéticas através do PEE Defesa Cibernética, (ii) o incremento da CO Exploração Cibernética nas estruturas em que as mesmas estão limitadas e (iii) a transformação dos BCom em BComGE.

Relativamente a esta última medida, é de vital importância que a transformação das OM que ainda não possuem a CO Exploração Cibernética esteja oficializada em documento institucional, nomeadamente o PEEx. Dessa maneira, atribui-se responsabilidade e aporte de recursos – por meio dos programas e projetos estratégicos do EB – a cada um dos processos.

Ademais, a transformação dos BCom restantes em BComGE vai ao encontro do conceito de modularidade, que permite a existência de um conjunto mínimo de CO Cibernéticas que serão complementadas, em caso de necessidade, pelo 1º BGE quando em operações militares. Além disso, o incremento da capacidade ampliará o potencial de combate da própria OM e, por conseguinte, do escalão enquadrante.

No tocante às limitações da investigação, destaca-se que não foram considerados os pontos de vista dos comandantes dos BCom e das CiaCom, estando estes militares fora do escopo das entrevistas – haja vista essas OM possuírem apenas a CO Proteção Cibernética. Tal restrição não prejudicou o estudo, pois as aludidas OM possuem capacidades cibernéticas abrangidas também pelos BComGE. Contudo, em trabalhos futuros, a inclusão desse universo, bem como de comandantes de unidades de manobra, pode trazer reflexões que contribuam para o aperfeiçoamento da Guerra Cibernética.

Identificaram-se, ainda, oportunidades de estudos futuros que podem ser explorados, sobretudo em relação a aspetos não aprofundados da temática em apreço. O investimento no adestramento e na formação de recursos humanos especializados em Guerra Cibernética é uma delas, já que foi um dos pontos apresentados como adverso durante o trabalho.

Outra oportunidade é a utilização do TII como fonte de propostas, lições aprendidas e eventualmente aproveitamento de modelos propostos para a capacidade cibernética existente ou em desenvolvimento nas nações amigas, nomeadamente em Portugal. A integração entre países de língua portuguesa na realização de exercícios combinados e troca de experiências pode ser um facilitador significativo.

Por fim, é inegável o valor atribuído à Guerra Cibernética na atualidade, nomeadamente ao se considerar o ambiente operacional atual. A evolução das capacidades no domínio cibernético é impositiva para que qualquer Força tenha condições de ampliar o seu potencial de combate e atuar com êxito nos conflitos modernos.

Referências bibliográficas

Avelar, J. R. C. (2018). *A Guerra Cibernética e seus desafios para o Brasil*. TCC. Escola de Comando e Estado-Maior do Exército, Rio de Janeiro.

Carneiro, J. M. E. (2012). *A Guerra Cibernética: Uma proposta de elementos para formulação doutrinária no Exército Brasileiro*. Tese de Mestrado em Ciências Militares. Escola de Comando e Estado-Maior do Exército, Rio de Janeiro.

Clarke, R. A. (2010). *Cyber War: The Next Threat to National Security and What To Do About It*. Nova Iorque: HarperCollins.

CRFB. (1988). *Constituição da República Federativa do Brasil*. Diário Oficial da União, 05/10/1988. Brasília: Congresso Nacional.

Estado-Maior do Exército. (2023). *Escritório de Projetos do Exército [página online]*. Retirado de http://www.epex.eb.mil.br/index.php/defesa-cibernetica.

Exército Brasileiro. (2014a). *EB20-MF-10.101 O Exército Brasileiro*. Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2014b). *EB70-MC-10.213 Operações de Informação*. Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2015). *EB20-C-07.001 Catálogo de Capacidades do Exército 2015-2035*. Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2017a). *EB70-MC-10.202 Operações Ofensivas e Defensivas*. Brasília: Comando de Operações Terrestres.

Exército Brasileiro. (2017b). *EB70-MC-10.223 Operações*. Brasília: Comando de Operações Terrestres.

Exército Brasileiro. (2017c). *EB70-MC-10.232 Guerra Cibernética*. Brasília: Comando de Operações Terrestres.

Exército Brasileiro. (2018). *EB20-MF-03.109 Glossário de Termos e Expressões para uso no Exército* (5ª Edição). Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2019a). *Concepção Estratégica do Exército*. Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2019b). *EB10-P-01.007 Plano Estratégico do Exército*. Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2020). *EB70-MC-10-244 Corpo de Exército*. Brasília: Comando de Operações Terrestres.

Exército Brasileiro. (2021). *Nota Doutrinária Nr 04/2021 Sistema de Comando e Controle da Força Terrestre*. Brasília: Comando de Operações Terrestres.

Exército Brasileiro. (2022a). *EB20-MF-10.102 Doutrina Militar Terrestre*. Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2022b). *EB70-MC-10-315 Batalhão de Guerra Eletrônica*. Brasília: Comando de Operações Terrestres.

Exército Brasileiro. (2023a). *EB20-MF-07.101 Conceito Operacional do Exército Brasileiro Operações de Convergência 2040*. Brasília: Estado-Maior do Exército.

Exército Brasileiro. (2023b). *EB70-MC-10.205 Comando e Controle*. Brasília: Comando de Operações Terrestres.

Exército Brasileiro. (2023c). *EB70-MC-10.210 Operações na Selva*. Brasília: Comando de Operações Terrestres.

Guerra, I. (2006). *Pesquisa Qualitativa e Análise de Conteúdo. Sentidos e formas de uso*.

Kuhn, L. (2022). *A organização de Guerra Eletrônica e Guerra Cibernética no Exército Brasileiro e nas Forças Armadas da Alemanha*. TCC. Escola de Comando e Estado-Maior do Exército, Rio de Janeiro.

Ministério da Defesa. (2012). *Política Cibernética de Defesa*.

Ministério da Defesa. (2015). *MD35-G-01 Glossário das Forças Armadas*. Brasília: Ministério da Defesa.

Ministério da Defesa. (2017). *MD33-M-12 Operações Interagências*. Brasília: Ministério da Defesa.

Ministério da Defesa. (2018). *Política Nacional de Defesa. Estratégia Nacional de Defesa*. Brasília: Gráfica do Senado Federal. Retirado de https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/copy_of_pnd_e_end_2016.pdf

Ministério da Defesa. (2020a). *Livro Branco de Defesa Nacional*. Brasília: Gráfica do Senado Federal. Retirado de https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/livro_branco/Versaodolivroemportugues2020.pdf

Ministério da Defesa. (2020b). *Sistema Militar de Defesa Cibernética (SMDC)*. Brasília: Ministério da Defesa.

Ministério da Defesa. (2023). *MD31-M-07 Doutrina Militar de Defesa Cibernética*. Brasília: Ministério da Defesa.

NEP/INV - 001. (2020). *Procedimentos relativos à elaboração de trabalhos de investigação realizados no âmbito de cursos que não atribuem grau académico*. Lisboa: Instituto Universitário Militar.

NEP/INV - 003. (2020). *Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no Instituto Universitário Militar*. Lisboa: Instituto Universitário Militar.

Neto, S. B. (2018). *A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas*. TCC. Escola de Comando e Estado-Maior do Exército, Rio de Janeiro.

Santos, L. A. B. dos, & Lima, J. M. M. do V. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.a ed., revista e atualizada). Cadernos do IUM, 8.

TRADOC. (2019). *TRADOC Pamphlet 525-92 The Operational Environment and the Changing Character of Warfare*. Fort Eustis, Virginia: Training and Doctrine Command.

Visacro, A. (2018). *A guerra na era da informação*. São Paulo: Contexto.

Apêndice A — Modelo de análise

Título	Perspetiva de evolução da capacidade cibernética do Exército Brasileiro ao nível tático		
Sinopse	Ao longo das últimas décadas, os avanços tecnológicos permitiram uma maior integração da sociedade numa comunidade em rede, com elevada capacidade de partilha de informação e de ligação entre as pessoas a um nível sem precedentes na história humana. A instituição militar acompanhou esta evolução na sociedade, permitindo-lhe agilizar processos, partilhar informação e estabelecer uma capacidade de Comando e Controlo mais presente. No entanto, esta integração ao nível da rede traz consigo também novas ameaças, identificando-se o ciberespaço como um domínio equiparado aos tradicionais domínios operacionais (marítimo, terrestre e aéreo). Ao nível do Exército Brasileiro, a capacidade cibernética encontra-se materializada pela estrutura de Guerra Cibernética existente nos vários níveis, como os Batalhões de Comunicações e Guerra Eletrónica e o Batalhão de Guerra Eletrónica. Com este trabalho, pretende-se analisar evolução da capacidade cibernética ao nível do Exército e a sua adequabilidade face ao atual ambiente operacional.		
Domínio da Investigação	Domínio	Ciências Militares	
	Área	AI 2 – Operações Militares	
	Subárea	2.8 – Guerra Cibernética	
Objeto da Investigação	A capacidade cibernética do Exército Brasileiro.		
Delimitação	Domínios	Espaço	Exército Brasileiro
		Conteúdo	Organização da capacidade cibernética ao nível tático
		Tempo	De dezembro de 2008 (publicação da Estratégia Nacional de Defesa) aos dias atuais
Metodologia de Investigação	Metodologia de raciocínio		Dedutivo
	Estratégia de Investigação		Qualitativa
	Desenho de Pesquisa		Estudo de Caso
Problema de Investigação	Objetivo Geral (OG)		Selecionar contributos para potenciar a capacidade cibernética do EB na condução das operações militares.
	Questão Central (QC)		Em que medida o EB pode potenciar a sua capacidade cibernética na condução das operações militares?

	Objetivos Específicos	Questões Derivadas	Conceitos	Dimensões	Variáveis	Indicadores	Observação
Problema de Investigação	**OE1:** Analisar a organização da Guerra Cibernética do Exército Brasileiro.	**QD1:** Como está organizada a Guerra Cibernética no Exército Brasileiro?	Ambiente Operacional Capacidade Militar Terrestre Capacidade Operativa Guerra Cibernética	Capacidade cibernética do EB	Organização	Subordinação Valor	**Técnicas de recolha de dados:** - Análise documental
	OE2: Examinar a atuação da Guerra Cibernética do Exército Brasileiro para a condução das operações militares.	**QD2:** De que forma a Guerra Cibernética do Exército Brasileiro atua em proveito das operações militares?		Operações Militares do EB	Adequabilidade Praticabilidade	Missão Área atribuída Pessoal Material Tempo	- Análise documental - Entrevistas semiestruturadas
	OE3: Analisar o impacto da capacidade cibernética na condução das operações militares do Exército Brasileiro.	**QD3:** Quais os contributos da capacidade cibernética do Exército Brasileiro na condução das operações militares?		Exército Brasileiro	Aceitabilidade	Riscos Custos Efeitos	

Apêndice B — Guião da Entrevista

Exmo. Senhor,

Como auditor do Curso de Estado-Maior Conjunto (CEMC) 2023/2024, a decorrer no Instituto Universitário Militar (IUM), encontro-me a desenvolver o Trabalho de Investigação Individual que possui como tema **"Perspetiva de evolução da capacidade cibernética do Exército Brasileiro ao nível tático"**.

O estudo possui como objetivo geral selecionar contributos para potenciar a capacidade cibernética do Exército Brasileiro na condução das operações militares, incidindo em três áreas principais: (i) analisar a organização da Guerra Cibernética do Exército Brasileiro (EB), (ii) examinar a atuação da Guerra Cibernética do EB para a condução das operações militares, (iii) e analisar o impacto da capacidade cibernética na condução das operações militares do EB.

Neste contexto e reconhecendo o seu conhecimento e experiência sobre o assunto em tela, venho respeitosamente solicitar a valorosa colaboração na execução de uma entrevista semiestruturada, com o fito de enriquecer as informações referentes ao estudo em curso, bem como obter uma compreensão mais abrangente de determinados aspetos sob escrutínio na investigação em foco.

Agradeço antecipadamente pela disponibilidade e colaboração.

Respeitosamente,

TCor EXE BRA Comunicações, Samuel Bombassaro Neto

1. IDENTIFICAÇÃO DO ENTREVISTADO

Nome:	
Posto:	
Função:	
Data:	

2. ENTREVISTA

GUIÃO
Parte I – Atuação da Guerra Cibernética nas operações militares (categorias Adequabilidade e Praticabilidade)
01. Que aspeto da missão da Organização Militar (OM) que o senhor comanda está relacionado com o emprego da capacidade cibernética? R.:
02. Qual a área geográfica atribuída para o cumprimento da missão de sua OM? R.:
03. Que fração / frações da OM são responsáveis pelas ações de Guerra Cibernética? Qual o efetivo aproximado das respetivas frações? O efetivo é compatível com a missão atribuída, no tocante à Guerra Cibernética? R.:
04. Quais Capacidades Operativas de Guerra Cibernética (Proteção, Exploração e Ataque Cibernético) a OM tem condições de executar? R.:
05. Há material especializado e em quantidade adequada para o emprego da Guerra Cibernética? R.:
06. Usualmente, a OM dispõe de tempo adequado para a preparação e emprego da capacidade cibernética em operações militares? R.:
07. Considerando as respostas aos itens 01 a 06, o senhor julga que a OM está apta a cumprir a sua missão de modo eficiente? Que aspetos o senhor considera que podem ser melhorados? R.:
08. Considerando as respostas aos itens 01 a 06, o senhor julga que a OM possui os meios e as capacidades necessárias ao emprego da Guerra Cibernética no cumprimento de sua missão? Que aspetos o senhor considera que podem ser aperfeiçoados ou desenvolvidos (por exemplo, acréscimo de novas Capacidades Operativas)? R.:
Parte II – Contributos da Guerra Cibernética para as operações militares (categoria Aceitabilidade)
09. Quais são os principais riscos relacionados com o emprego da Guerra Cibernética da OM em operações militares? R.:
10. Quais as principais despesas, custos e / ou consumos (relacionados ao material, ao pessoal ou ao aspeto financeiro) que envolvem o emprego da capacidade cibernética da OM? R.:
11. Quais os efeitos mais significativos atingidos com o emprego das capacidades cibernéticas de sua OM nas operações militares? R.:
12. Considerando as respostas aos itens 09 a 11, o senhor julga que os benefícios do emprego da Guerra Cibernética em sua OM superam os custos e riscos assumidos? R.:
Parte III – Considerações gerais sobre a Guerra Cibernética nas operações militares
13. O senhor possui outras informações / sugestões que julgue relevantes para a presente pesquisa? R:

Apêndice C — Matriz das entrevistas

Questões / Categorias	1. Que aspeto da missão da Organização Militar (OM) que o senhor comanda está relacionado com o emprego da capacidade cibernética?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
Adequabilidade	E1	"A realização de proteção e também de exploração cibernética."	1.1 Conformidade da missão doutrinária em relação à capacidade cibernética
	E2	"O Batalhão possuiu (…) uma turma de proteção cibernética e (…) uma turma de exploração cibernética, para executar ações de proteção e exploração, esta com algumas limitações."	1.1 Conformidade da missão doutrinária em relação à capacidade cibernética
	E3	"(…) apoiar a 6ª Divisão de Exército em guerra cibernética (…) possuindo atualmente a capacidade de proteção cibernética."	1.2 Limitação da missão doutrinária em relação à capacidade cibernética
	E4	"(…) proteção e exploração cibernética em apoio ao C Mil A (…)"	1.1 Conformidade da missão doutrinária em relação à capacidade cibernética
	E5	"Apoiar em cibernética o Corpo de Exército."	1.1 Conformidade da missão doutrinária em relação à capacidade cibernética
	2. Qual a área geográfica atribuída para o cumprimento da missão de sua OM?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E1	"Amazônia Ocidental brasileira."	2.1 Definição da área de atuação
	E2	"Estado do Pará, Amapá, Maranhão e norte de Tocantins, dentro da área de responsabilidade do Comando Militar do Norte."	
	E3	"(…) área de operações atinente à 6ª Divisão de Exército."	
	E4	"(…) área de atuação, em tempo de paz ou não, do Comando Militar do Oeste."	
	E5	"Todo o teatro de operações. Em situação de normalidade, qualquer ponto do território nacional."	
Praticabilidade	3. Que fração / frações da OM são responsáveis pelas ações de Guerra Cibernética? Qual o efetivo aproximado das respetivas frações? O efetivo é compatível com a missão atribuída, no tocante à Guerra Cibernética?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E1	"(…) possui uma turma de Guerra Cibernética, com efetivo considerado insuficiente (…)"	3.1 Existência da fração de Guerra Cibernética

Praticabilidade			3.2 Incompatibilidade da fração existente com a missão doutrinária
	E2	"(…) turma de Proteção Cibernética com dois militares e turma de Exploração Cibernética com um militar. Atualmente, o 2º BComGESl está em fase de implantação e para essa etapa o efetivo é compatível."	3.1 Existência da fração de Guerra Cibernética 3.3 Compatibilidade da fração existente com a missão doutrinária
	E3	"(…) possui frações de Guerra Cibernética, conseguindo atuar com algumas limitações."	3.1 Existência da fração de Guerra Cibernética 3.2 Incompatibilidade da fração existente com a missão doutrinária
	E4	"(…) dentro da companhia de Guerra Eletrônica, possui um pelotão reduzido de Guerra Cibernética, capaz de executar as ações de proteção e exploração (…)"	3.1 Existência da fração de Guerra Cibernética 3.3 Compatibilidade da fração existente com a missão doutrinária
	E5	"Uma companhia de Guerra Cibernética, tendo o efetivo considerado compatível para a missão."	3.1 Existência da fração de Guerra Cibernética 3.3 Compatibilidade da fração existente com a missão doutrinária
	4. Quais Capacidades Operativas de Guerra Cibernética (Proteção, Exploração e Ataque Cibernético) a OM tem condições de executar?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E1	"(…) capacidade de realizar proteção e exploração cibernética."	4.2 Proteção e exploração cibernética
	E2	"(…) condições de executar proteção e exploração cibernética (…)"	4.2 Proteção e exploração cibernética
	E3	"(…) hoje, temos a capacidade de atuar com proteção cibernética em prol do escalão superior (…)"	4.1 Proteção cibernética
	E4	"(…) a proteção cibernética, bem como a exploração, são duas capacidades presentes no batalhão (…)"	4.2 Proteção e exploração cibernética
	E5	"O BGE possui todas as CO relacionadas à Guerra Cibernética."	4.3 Proteção, exploração e ataque cibernético
	5. Há material especializado e em quantidade adequada para o emprego da Guerra Cibernética?		
	Entrevistado	Unidade de Contexto	Unidade de Registo

Praticabilidade	E1	"Sim, o batalhão é provisionado de maneira satisfatória para o cumprimento da missão, em termos de material para a Guerra Cibernética."	5.1 Existência de material especializado 5.2 Quantidade de material especializado suficiente
	E2	"Sim. Existe material específico e em número adequado (…)"	
	E3	"Para a realização das atividades de proteção, há material suficiente."	
	E4	"Os programas estratégicos tendem a priorizar a área do Comando Militar do Oeste, ou pelo menos vários deles assim o fazem, e isso reflete na quantidade necessário e adequada de material para o 9º BComGE."	
	E5	"Sim."	
	6. Usualmente, a OM dispõe de tempo adequado para a preparação e emprego da capacidade cibernética em operações militares?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E1	"Sim."	6.1 Suficiência de tempo
	E2		
	E3		
	E4		
	E5		
Adequabilidade	7. Considerando as respostas aos itens 01 a 06, o senhor julga que a OM está apta a cumprir a sua missão de modo eficiente? Que aspetos o senhor considera que podem ser melhorados?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E1	"Ainda há algum ajuste necessário para se empregar a exploração cibernética em sua plenitude, mas a missão é compatível."	7.1 Objetivos propostos à OM são adequados
	E2	"Sim, julgo que o 2º BComGESl consegue cumprir a missão que lhe foi atribuída. As melhorias que podem ser feitas são afetas ao campo técnico de emprego da Guerra Cibernética, tais como (…) o desenvolvimento de ambientes virtualizados para treinamento de modo a manter os operadores cibernéticos em constante treinamento."	
	E3	"Ainda que a missão esteja de acordo com a doutrina, existem algumas poucas lacunas principalmente na capacidade de exploração cibernética (…)"	
	E4	"Conseguimos acionar as frações para atuar com as CO proteção e exploração cibernética cada vez com mais conhecimento (…)"	
	E5	"O batalhão está apto a cumprir sua missão. Existem algumas especificidades a serem melhoradas, e uma delas é a mobilidade que deve estar de acordo com a tropa apoiada, o que eventualmente acaba por ser um obstáculo a ser transposto, mas que não afeta o atingimento do objetivo."	
Praticabilidade	8. Considerando as respostas aos itens 01 a 06, o senhor julga que a OM possui os meios e as capacidades necessárias ao emprego da Guerra Cibernética no cumprimento de sua missão? Que aspetos o senhor considera que podem ser aperfeiçoados ou desenvolvidos (por exemplo, acréscimo de novas Capacidades Operativas)?		
	Entrevistado	Unidade de Contexto	Unidade de Registo

Praticabilidade	E1	"Há grande necessidade de efetivo especializado para alcançar alguns objetivos em tarefas específicas (…)"	8.2 Objetivos propostos à OM não são totalmente praticáveis ou atingíveis
	E2	"Sim, possuo. Aspetos a serem desenvolvidos poderia ser o fornecimento de mais meios de proteção cibernética e a priorização dos militares servindo na OM para realizarem os cursos de especialização."	8.1 Objetivos propostos à OM são praticáveis ou atingíveis
	E3	"Como disse, há carência na capacidade de exploração cibernética, a qual ainda não estamos em condições de empregar."	8.2 Objetivos propostos à OM não são totalmente praticáveis ou atingíveis
	E4	"Os meios que temos nos permite cumprir a nossa finalidade por meio das CO de cibernética."	8.1 Objetivos propostos à OM são praticáveis ou atingíveis
	E5	"Consegue-se cumprir a missão com os meios existentes, por meio da modularidade oferecida pelos BComGE. Assim, a integração ocorre de forma natural e não há necessidade de acréscimo de capacidades."	8.1 Objetivos propostos à OM são praticáveis ou atingíveis
Aceitabilidade	9. Quais são os principais riscos relacionados com o emprego da Guerra Cibernética da OM em operações militares?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E1	"Exposição institucional e a dificuldade de fazer a proteção de infraestruturas críticas."	9.1 Exposição da tropa 9.2 Proteção limitada de determinadas estruturas ou sistemas
	E2	"Os sistemas táticos apresentam características diferentes que, por vezes, impõem maiores esforços para a proteção. (…) A exploração deve ser realizada de maneira a não exteriorizar o emprego da tropa para essa atividade."	9.1 Exposição da tropa 9.2 Proteção limitada de determinadas estruturas ou sistemas
	E3	"No tocante à proteção, alguns sistemas e estruturas carecem de conhecimento muito especializado para uma segurança eficaz."	9.2 Proteção limitada de determinadas estruturas ou sistemas
	E4	"A exploração, se não for bem conduzida, pode denunciar a tropa que está realizando as ações cibernéticas (...)"	9.1 Exposição da tropa
	E5	"(…) reduzida capacidade de autodefesa da tropa empregada; reduzida capacidade de reposição de material e de pessoal; reduzida capacidade de apoio logístico aos seus elementos, quando desdobrados fora da área do posto de comando do escalão enquadrante; e restrita eficácia das ações cibernéticas defensivas."	9.2 Proteção limitada de determinadas estruturas ou sistemas 9.3 Autodefesa deficiente 9.4 Apoio logístico deficiente
	10. Quais as principais despesas, custos e / ou consumos (relacionados ao material, ao pessoal ou ao aspeto financeiro) que envolvem o emprego da capacidade cibernética da OM?		
	Entrevistado	Unidade de Contexto	Unidade de Registo

Aceitabilidade	E1	"(…) os principais gastos são com manutenção tecnológica atualizada, software e meios de anonimização. (…) são custos compatíveis com a capacidade orçamentária do escalão enquadrante (…)"	10.2 Custo reduzido de material e soluções digitais
	E2	"Os equipamentos possuem razoável valor agregado, para que a atividade de exploração e ataque possa ser realizada existem etapas que envolvem custos elevados, de forma a mitigar os riscos."	10.3 Alto custo de material e soluções digitais
	E3	"Existem gastos relativamente equilibrados com o material para realização da proteção cibernética."	10.2 Custo reduzido de material e soluções digitais
	E4	"Os custos para o emprego da tropa especializada existem, mas são mais voltados para a área de apoio logístico. As despesas relacionadas aos equipamentos são consideráveis, mas menos custosas quando comparadas ao emprego de blindados, artilharia ou Guerra Eletrônica, por exemplo."	10.2 Custo reduzido de material e soluções digitais
	E5	"(…) manutenção / reposição de suprimento de várias classes; custos com deslocamento de pessoal para as áreas de operações, uma vez que a OM se faz presente em todos os CMilA."	10.1 Despesas com atividades de suporte
	11. Quais os efeitos mais significativos atingidos com o emprego das capacidades cibernéticas de sua OM nas operações militares?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E1	"Segurança do ambiente cibernético nas operações."	11.1 Proteção dos sistemas de tecnologia da informação
	E2	"A proteção do sistema de comando e controle tático do Comando Militar do Norte contra ataques à rede de dados."	11.1 Proteção dos sistemas de tecnologia da informação
	E3	"O principal efeito é a proteção que é gerada pelo batalhão aos sistemas de C2 usados pela Divisão."	11.1 Proteção dos sistemas de tecnologia da informação
	E4	"Além da proteção das redes (…) a capacidade de exploração permite revelar os pontos fracos da força inimiga (…)"	11.1 Proteção dos sistemas de tecnologia da informação 11.2 Identificação de vulnerabilidades do oponente
	E5	"Efeitos táticos no teatro de operações, tanto de proteção quanto de exploração. (…) proteção do espaço cibernético em que operamos (…) A exploração cibernética oferece um ganho muito significativo, já que contribui com a identificação de vulnerabilidades dos sistemas do oponente. (…) tais vulnerabilidades são aproveitadas para ações de ataque cibernético (…)"	11.1 Proteção dos sistemas de tecnologia da informação 11.2 Identificação de vulnerabilidades do oponente 11.3 Neutralização dos sistemas de tecnologia da informação oponentes
	12. Considerando as respostas aos itens 09 a 11, o senhor julga que os benefícios do emprego da Guerra Cibernética em sua OM superam os custos e riscos assumidos?		
	Entrevistado	Unidade de Contexto	Unidade de Registo

Aceitabilidade	E1	"Sim."	12.1 Emprego da Guerra Cibernética é aceitável 12.2 Guerra Cibernética multiplica o potencial de combate
	E2	"Sim. (…) na exploração, há de se consultar o escalão demandante para uma melhor avaliação."	12.3 Emprego da Guerra Cibernética pode não ser aceitável 12.2 Guerra Cibernética multiplica o potencial de combate
	E3	"Sim."	12.1 Emprego da Guerra Cibernética é aceitável 12.2 Guerra Cibernética multiplica o potencial de combate
	E4		
	E5		
Experiência	13. O senhor possui outras informações / sugestões que julgue relevantes para a presente pesquisa?		
	Entrevistado	Unidade de Contexto	Unidade de Registo
	E2	"Sugiro a criação de um servidor com acesso remoto para que os operadores cibernéticos possam manter o treinamento tanto em proteção, quanto em exploração e ataque. Esse servidor possibilitará acesso a treinamento e a execução de competições entre os BComGESl."	13.1 Adestramento
	E3	"Formação do guerreiro cibernético não é de um dia para o outro." "[…] a ativação ou transformação dos batalhões em BComGE colabora com o desenvolvimento da capacidade cibernética do Exército […]"	13.2 Formação 13.3 Transformação
	E5	"A efetividade da cibernética nas operações depende do trabalho em tempo de paz, no preparo e capacitação do pessoal e nos levantamentos de informações no espaço cibernético." "Acho importante a criação ou transformação do BComGE, porque inclui pelo menos uma parcela da capacidade de Guerra Cibernética nos BCom. Poderia ser estendido a todos os BCom, dentro do Plano Estratégico do Exército […]" "[…] ao cumprirmos missões junto aos BComGE, já temos o trabalho bastante adiantado, o que vai ao encontro ao conceito da modularidade."	13.1 Adestramento 13.2 Formação 13.3 Transformação 13.4 Modularidade

Apêndice D — Agrupamento das Unidades de Registo

Questão	Categoria	Unidade de Registo	E1	E2	E3	E4	E5	Resultado (%)
1	Adequabilidade	1.1 Conformidade da missão doutrinária em relação à capacidade cibernética	X	X		X	X	80%
		1.2 Limitação da missão doutrinária em relação à capacidade cibernética			X			20%
2	Adequabilidade	2.1 Definição da área de atuação	X	X	X	X	X	100%
3	Praticabilidade	3.1 Existência da fração de Guerra Cibernética	X	X	X	X	X	100%
		3.2 Incompatibilidade da fração existente com a missão doutrinária	X		X			40%
		3.3 Compatibilidade da fração existente com a missão doutrinária		X		X	X	60%
4	Praticabilidade	4.1 Proteção cibernética			X			20%
		4.2 Proteção e exploração cibernética	X	X		X		60%
		4.3 Proteção, exploração e ataque cibernético					X	20%
5	Praticabilidade	5.1 Existência de material especializado	X	X	X	X	X	100%
		5.2 Quantidade de material especializado suficiente	X	X	X	X	X	100%
6	Praticabilidade	6.1 Suficiência de tempo	X	X	X	X	X	100%
7	Adequabilidade	7.1 Objetivos propostos à OM são adequados	X	X	X	X	X	100%
8	Praticabilidade	8.1 Objetivos propostos à OM são praticáveis ou atingíveis		X		X	X	60%
		8.2 Objetivos propostos à OM não são totalmente praticáveis ou atingíveis	X		X			40%
9	Aceitabilidade	9.1 Exposição da tropa	X	X		X		60%
		9.2 Proteção limitada de determinadas estruturas ou sistemas	X	X	X		X	80%
		9.3 Autodefesa deficiente					X	20%
		9.4 Apoio logístico deficiente					X	20%
10	Aceitabilidade	10.1 Despesas com atividades de suporte					X	20%

		10.2 Custo reduzido de material e soluções digitais	X		X	X		60%
		10.3 Alto custo de material e soluções digitais		X				20%
11	Aceitabilidade	11.1 Proteção dos sistemas de tecnologia da informação	X	X	X	X	X	100%
		11.2 Identificação de vulnerabilidades do oponente				X	X	40%
		11.3 Neutralização dos sistemas de tecnologia da informação oponentes					X	20%
12	Aceitabilidade	12.1 Emprego da Guerra Cibernética é aceitável	X		X	X	X	80%
		12.2 Guerra Cibernética multiplica o potencial de combate	X	X	X	X	X	100%
		12.3 Emprego da Guerra Cibernética pode não ser aceitável		X				20%
13	Experiência	13.1 Adestramento		X			X	40%
		13.2 Formação			X		X	40%
		13.3 Transformação			X		X	40%
		13.4 Modularidade					X	20%