ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

Maj Com LEANDRO **KUHN**

A organização de Guerra Eletrônica e Guerra Cibernética no Exército Brasileiro e nas Forças Armadas da Alemanha

Rio de Janeiro

2022

K96o Kuhn, Leandro

A organização de Guerra Eletrônica e Guerra Cibernética no Exército Brasileiro e nas Forças Armadas da Alemanha. / Leandro Kuhn.— 2022.
43 f. : il. ; 30 cm.

Orientação: Samuel Bombassaro Neto

Trabalho de Conclusão de Curso (Especialização em Ciências Militares)— Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2022.

Bibliografia: f. 42-43

1. Guerra Eletrônica 2. Guerra Cibernética 3. Exército Brasileiro 4. Forças Armadas da Alemanha. I. Título.

CDD 363.325

Maj Com LEANDRO **KUHN**

A organização de Guerra Eletrônica e Guerra Cibernética no Exército Brasileiro e nas Forças Armadas da Alemanha

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Orientador: Maj Com QEMA SAMUEL BOMBASSARO NETO

Rio de Janeiro

2022

Maj Com LEANDRO **KUHN**

A organização de Guerra Eletrônica e Guerra Cibernética no Exército Brasileiro e nas Forças Armadas da Alemanha

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Aprovado em ___ outubro de 2022

COMISSÃO AVALIADORA

_____

SAMUEL **BOMBASSARO** NETO – Maj Com QEMA – Presidente
Escola de Comando e Estado-Maior do Exército

_____

HERMES LEONARDO MORAIS **FAIOLO** SILVA **-** Maj Eng QEMA – Membro
Escola de Comando e Estado-Maior do Exército

_____

PAULO **COMUNALE** – Maj Int QEMA – Membro
Escola de Comando e Estado-Maior do Exército

AGRADECIMENTOS

Ao meu orientador, Maj SAMUEL BOMBASSARO NETO, por acompanhar todas as etapas de confecção do presente trabalho, estando sempre disposto a colaborar e intervir com orientações precisas sobre o assunto em estudo.

À minha família, por compreender o momento peculiar vivido, o qual exigiu dedicação à pesquisa em detrimento de horas de lazer, sempre estando ao meu lado e me apoiando.

À minha esposa e eterna companheira, pelo incentivo e dedicação à nossa família, cuidando como ninguém de nossa recém-chegada filha, Júlia, sem esmorecer frente às adversidades surgidas nessa nova rotina, deixando-me em confortável para seguir nos estudos. Amo-te.

A Deus que, com seus planos justos e perfeitos, traçou os caminhos e os iluminou para que eu pudesse estar vivendo este momento ímpar na carreira.

RESUMO

Os atuais conflitos mundiais têm sido marcados pela ascensão da guerra informacional. A Guerra Eletrônica (GE) e a Guerra Cibernética (G Ciber) atuam nesse ambiente, gerando conhecimento e capacidade de intervir decisivamente no combate. Nesse cenário, cresce a importância de se conhecer e analisar como essas capacidades estão organizadas no Exército Brasileiro (EB) e em outras potências militares, como a Alemanha. O EB criou o Sistema de Guerra Eletrônica do Exército (SIGELEx) e o Sistema de Guerra Cibernética do Exército (SGCEx) para gerenciar todos os elementos ligados à GE e G Ciber, respectivamente. A exploração tática do espectro eletromagnético e cibernético, em prol de uma Força Terrestre Componente, recai sobre o Batalhão de Guerra Eletrônica (BGE) e Batalhões de Comunicações e Guerra Eletrônica (BComGE), os quais possuem subunidades especializadas nessas atividades. Já a Alemanha, estruturou uma nova Força Singular, o Comando do Espaço Cibernético (Kdo CIR), apenas para atender às demandas do ciberespaço, com diversas organizações militares subordinadas. O estudo das capacidades do Kdo CIR elucidou o problema proposto por esta pesquisa, na medida que trouxe sugestões de aperfeiçoamento dos sistemas do EB.

Palavras-chave: Guerra Eletrônica, Guerra Cibernética, Exército Brasileiro, Forças Armadas da Alemanha.

RESUMEN

Los conflictos mundiales actuales han estado marcados por el auge de la guerra de la información. La Guerra Electrónica (GE) y Guerra Cibernética (G Ciber) operan en este entorno, generando conocimiento y la capacidad de intervenir decisivamente en el combate. En ese escenario, crece la importancia de conocer y analizar cómo se organizan esas capacidades en el Ejército Brasileño (EB) y en otras potencias militares, como Alemania. El EB creó el Sistema de Guerra Electrónica del Ejército (SIGELEx) y el Sistema de Guerra Cibernética del Ejército (SGCEx) para gestionar todos los elementos vinculados a GE y G Ciber, respectivamente. La exploración táctica del espectro electromagnético y cibernético, a favor de una Fuerza Terrestre Componente, recae en el Batallón de Guerra Electrónica (BGE) y en los Batallones de Comunicaciones y Guerra Electrónica (BComGE), que cuentan con subunidades especializadas en estas actividades. Alemania, por su parte, estructuró una nueva Fuerza Singular, el Comando del Ciberespacio (Kdo CIR), sólo para atender las demandas del ciberespacio, con varias organizaciones militares subordinadas. El estudio de las capacidades del Kdo CIR aclaró el problema propuesto por esta investigación, ya que trajo sugerencias para mejorar los sistemas EB.

Palabras Clave: Guerra Electrónica, Guerra Cibernética, Ejército Brasileño, Fuerzas Armadas Alemanas.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho aborda a estrutura da Guerra Eletrônica (GE) e da Guerra Cibernética (G Ciber) do Exército Brasileiro (EB) e das Forças Armadas Alemãs (*Bundeswehr*), buscando, ao final, apontar oportunidades de melhoria para a Força Terrestre brasileira.

Pode-se verificar que o século XXI impôs uma nova realidade aos exércitos mundiais, onde os conflitos armados estão cada vez mais dinâmicos e imprevisíveis, pois:

> envolvem não somente o combate entre oponentes armados e claramente definidos. O campo de batalha, outrora linear e previsível, agrega uma multiplicidade de atores, sistemas e ambientes operacionais, ora combinados em um cenário de combate de alta intensidade, ora presentes em ações descentralizadas ou não convencionais, de forma simultânea ou sucessiva, conjugando diversas operações militares (BRASIL, 2019).

Esse cenário requer uma adaptabilidade das Forças Armadas para fazer frente ao surgimento de um novo paradigma: a guerra da informação, onde a superioridade da informação possibilita uma vantagem competitiva no processo decisório. Para isso, as FA fazem uso de Operações de Informações, onde estão inclusas a Guerra Eletrônica e a Guerra Cibernética (BRASIL, 2019).

Segundo o Manual de Campanha - A Guerra Eletrônica na Força Terrestre, o apoio de GE à Força F Terrestre deve contribuir para a obtenção da capacidade militar terrestre superioridade de informação (2019). Para isso, cabe à GE:

> explorar as emissões do inimigo em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, suas intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os sistemas próprios (BRASIL, 2019).

Por definição, a atuação da GE dá-se em dois grandes campos: o das Comunicações (Com) e das Não Comunicações (N Com). O campo das Com abrange os sinais eletromagnéticos e equipamentos utilizados para o trânsito de informações - sejam analógicas ou digitais. Enquanto isso, o campo das N Com abrange os sinais eletromagnéticos e equipamentos utilizados na produção de informações por meio de sensoriamento (BRASIL, 2020).

Dentro de cada campo, ocorre a subdivisão nos seguintes ramos: as Medidas de Apoio de Guerra Eletrônica (MAGE), as Medidas de Ataque Eletrônico (MAE) e as

Medidas de Proteção Eletrônica (MPE). As MAGE são o ramo da GE, de natureza passiva (sem emissão de energia no espectro eletromagnético), que objetivam a obtenção e análise de dados, a partir das emissões eletromagnéticas de interesse, oriundas do oponente. As MAE caracterizam o ramo da GE, de natureza ativa (com emissão de energia no espectro eletromagnético), que visa a destruir, a neutralizar ou a degradar a capacidade de combate do oponente. Enquanto as MPE descrevem o ramo da GE, de natureza defensiva, que busca assegurar a utilização eficaz e segura das próprias emissões eletromagnéticas, a despeito da existência de ações ofensivas de GE empreendidas pelo oponente e/ou pelas forças amigas ou, ainda, de fontes de interferência não intencionais (BRASIL, 2020).

Seguindo a linha temática do trabalho, é necessária a introdução de alguns conceitos de Guerra Cibernética. Assim, pode-se definir G Ciber como:

> o uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C² ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar (BRASIL, 2017a).

O Sistema de Guerra Cibernética do Exército Brasileiro (SGCEx) possui as capacidades operativas de Proteção Cibernética, Ataque Cibernético e Exploração Cibernética. O Manual de Campanha EB70-MC-10.232 descreve cada uma dessas capacidades da seguinte forma:

Capacidade Operativa	**Descrição**
Proteção Cibernética (Prot)	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético (Atq)	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.

Exploração Cibernética (Expl)	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

TABELA 01 – Capacidades do SGCEx.
Fonte: BRASIL (2017a).

Em linha com a temática deste trabalho, pode-se verificar que uma possível integração ou ações conjuntas entre GE e G Ciber, tende a ser positivo e até fundamental para os exércitos modernos, uma vez que:

> a GE utiliza energia eletromagnética, dirigida a sistemas inimigos que utilizem o espectro eletromagnético, no sentido de o controlar ou atacar. A ideia de ataque ciber - eletrônico, que corresponde à sincronização de ataques no domínio cibernético em coordenação com a GE, corresponde a uma nova e aprimorada forma do desenvolvimento de ataques eletrônicos (FERNANDES, 2020).

Com isso, vários governos consideraram criar uma força exclusiva para cuidar dessas capacidades, como é o caso de China, Estados Unidos, Índia, Alemanha, França e Espanha (LAMBACH, 2019).

Na Alemanha foi criada uma força, de mesma hierarquia que Exército, Marinha e Aeronáutica, apenas para cuidar do aspecto informacional: o Kdo CIR - "*Kommando Cyber- und Informationsraum*" (Comando do Espaço Cibernético e de Informação). Este comando constitui-se como único responsável por garantir a superioridade nos domínios do Ciberespaço e das Informações (FERNANDES, 2020).

1.1 PROBLEMA

Os sistemas de GE e G Ciber requerem uma estrutura específica e, por vezes, complexa para seu funcionamento. O EB organiza seus meios de GE e G Ciber sob a perspectiva do Sistema de Guerra Eletrônica do Exército (SIGELEx) e do Sistema de Guerra Cibernética do Exército (SGCEx), respectivamente. Já a Alemanha, possui uma força Singular responsável por ambas as capacidades. Assim, da comparação

entre as estruturas dos dois países, quais oportunidades de melhoria podem ser levantadas para o EB nessas capacidades?

1.2 OBJETIVOS

1.2.1 Objetivo geral

Analisar a organização de Guerra Eletrônica e Guerra Cibernética nos exércitos do Brasil e da Alemanha, concluindo sobre possíveis contribuições da estrutura alemã para o EB.

1.2.2 Objetivos específicos

Para alcançar o Objetivo Geral, foram traçados os seguintes objetivos específicos:

a. Apresentar a organização da GE no EB.

b. Apresentar a organização da G Ciber no EB.

c. Apresentar a organização da GE e da G Ciber na Alemanha.

d. Identificar e propor oportunidades de melhoria que a estrutura alemã pode demonstrar ao EB.

1.3 DELIMITAÇÃO DO ESTUDO

O presente estudo estará limitado aos meios de GE e G Ciber do EB e do Kdo CIR na Alemanha. Ao final, este trabalho também buscará sugerir oportunidades de melhoria ao EB.

1.4 RELEVÂNCIA DO ESTUDO

Segundo Almeida, Machado e Sá (2019) o efeito dos ataques eletrônicos e cibernéticos pode ser equiparado ao efeito de um ataque cinético. Os autores, ainda, escrevem que:

> A inclusão do domínio cibernético na arte da guerra vem sendo amplamente discutida nas áreas de Ciência e Tecnologia, Defesa, Estratégia e Relações Internacionais. Por sua complexidade e peculiaridades, as ameaças cibernéticas têm feito com que pesquisadores e estrategistas revisitem os princípios da guerra erguidos ao longo do tempo com base nas literaturas de Sun Tzu, Nicolau Maquiavel, Carl von Clausewitz, Antoine-Henri Jomini, Basil Liddell Hart, dentre outros (ALMEIDA, MACHADO e SÁ, 2019).

Assim, pode-se perceber a relevância de qualquer estudo que busque entender ou aprimorar o funcionamento das capacidades de GE e G Ciber da Força Terrestre. O estudo dessas capacidades extrapola o meio militar, pois um uso de ataques eletrônicos e cibernéticos, pode afetar não somente meios militares, mas também civis. Os efeitos desses ataques, podem incluir a destruição física de estruturas do inimigo, chegando à manipulação da informação por ele gerada (FERNANDES, 2020).

Tem-se, ainda, que Alemanha, além de ser um importante membro da Organização do Tratado do Atlântico Norte (OTAN), vem se destacando por liderar, após o Caso Snowden projetos com ênfase na questão normativa do ciberespaço (REISDOERFER e ALCÂNTARA, 2020). Tal fato, enfatiza a importância da análise das estruturas de GE e G Ciber deste país, buscando-se apresentar contribuições com o aumento do poder de combate dessas capacidades, após comparação com o EB.

No meio acadêmico, verifica-se, por meio de pesquisa em indexadores como “Schoolar Google” e “Scielo”, a escassez de trabalhos com a temática GE e G Ciber de maneira integrada. Assim, o presente trabalho pode colaborar no preenchimento dessa lacuna de conhecimento.

2 METODOLOGIA

A metodologia que foi utilizada para desenvolver o trabalho está apresentada nesta seção, evidenciando-se os seguintes tópicos: tipo de pesquisa, universo e amostra, coleta de dados, tratamento de dados e limitações do método.

2.1 TIPO DE PESQUISA

Baseado no Manual de Elaboração de Projetos de Pesquisa na ECEME (BRASIL, 2012), pode-se classificar a metodologia a ser empregada na confecção deste trabalho científico como: qualitativa, explicativa, bibliográfica e documental. Qualitativa, pois privilegiará contemplar a subjetividade, a descoberta, e a análise de documentos para construir o entendimento da organização das estruturas de GE e G Ciber nos exércitos brasileiro e alemão. Explicativa, porque o autor buscará tornar o assunto inteligível, principalmente ao reproduzir termos mais técnicos e específicos. Bibliográfica porque terá sua fundamentação teórico-metodológica na investigação dos assuntos abordados e na criação do conhecimento, disponíveis em livros, manuais, artigos e redes eletrônicas de acesso livre ao público em geral. Documental porque se utilizará de material específicos do EB e das Forças Armadas Alemãs, não disponíveis para consultas públicas em geral, como relatórios e documentos de trabalho.

2.2 UNIVERSO E AMOSTRA

O universo do presente estudo são as doutrinas militares do Brasil e da Alemanha. As amostras que serão utilizadas são os manuais, cadernos de instrução, relatórios, instruções e artigos científicos que tratam de GE e G Ciber, publicados a partir do ano de 2010, por serem bastante recentes, e terem condições de retratar a situação atual.

.

2.3 COLETA DE DADOS

Os dados que comporão o presente trabalho de conclusão de curso serão coletados na literatura, realizando-se uma pesquisa bibliográfica e documental, em livros, manuais, revistas especializadas, jornais, artigos, internet, relatórios, monografias, teses e dissertações, sempre buscando os dados pertinentes ao assunto.

2.4 TRATAMENTO DOS DADOS

Segundo o Manual de Elaboração de Projetos de Pesquisa na ECEME (BRASIL, 2012), os métodos de tratamentos de dados que serão utilizados no presente estudo serão a análise de conteúdo e o comparativo, pois será realizado um estudo de textos e documentos, além de destacar as similaridades e diferenças nas estruturas de GE e G Ciber dos Exércitos do Brasil e Alemanha.

2.5 LIMITAÇÕES DO MÉTODO

Por fim, o pesquisador encontrou limitações na metodologia em questão, particularmente, quanto à profundidade na pesquisa sobre a Doutrina Militar da Alemanha, por se tratar de um tema com restrições de acesso. Todavia, a literatura disponível é suficiente para atingir o objetivo geral do trabalho.

3 A ORGANIZAÇÃO DE GUERRA ELETRÔNICA NO EXÉRCITO BRASILEIRO

No contexto da atual era informacional, com crescente e até indispensável uso do espectro eletromagnético por qualquer contendor em um campo de batalha, a GE se revela como uma ferramenta, seja em situações de guerra e não guerra, com os objetivos imediatos de tirar proveito do uso do espectro eletromagnético pelo oponente ou, ainda, de destruir, neutralizar ou reduzir-lhe a capacidade de combate, empregando meios eletrônicos especializados (BRASIL, 2020).

Nesse sentido, o Exército Brasileiro criou o Sistema de Guerra Eletrônica do Exército (SIGELEx), estrutura responsável pela gerência sistêmica da GE. Por meio dele, a GE se integra aos demais sistemas do EB. Além disso, segundo a perspectiva orgânica, o SIGELEx é o único sistema do EB que possui Organizações Militares (OM) e estruturas vocacionadas para as ações de GE (BRASIL, 2019).

Graficamente, pode-se visualizar a perspectiva orgânica da GE da seguinte forma:

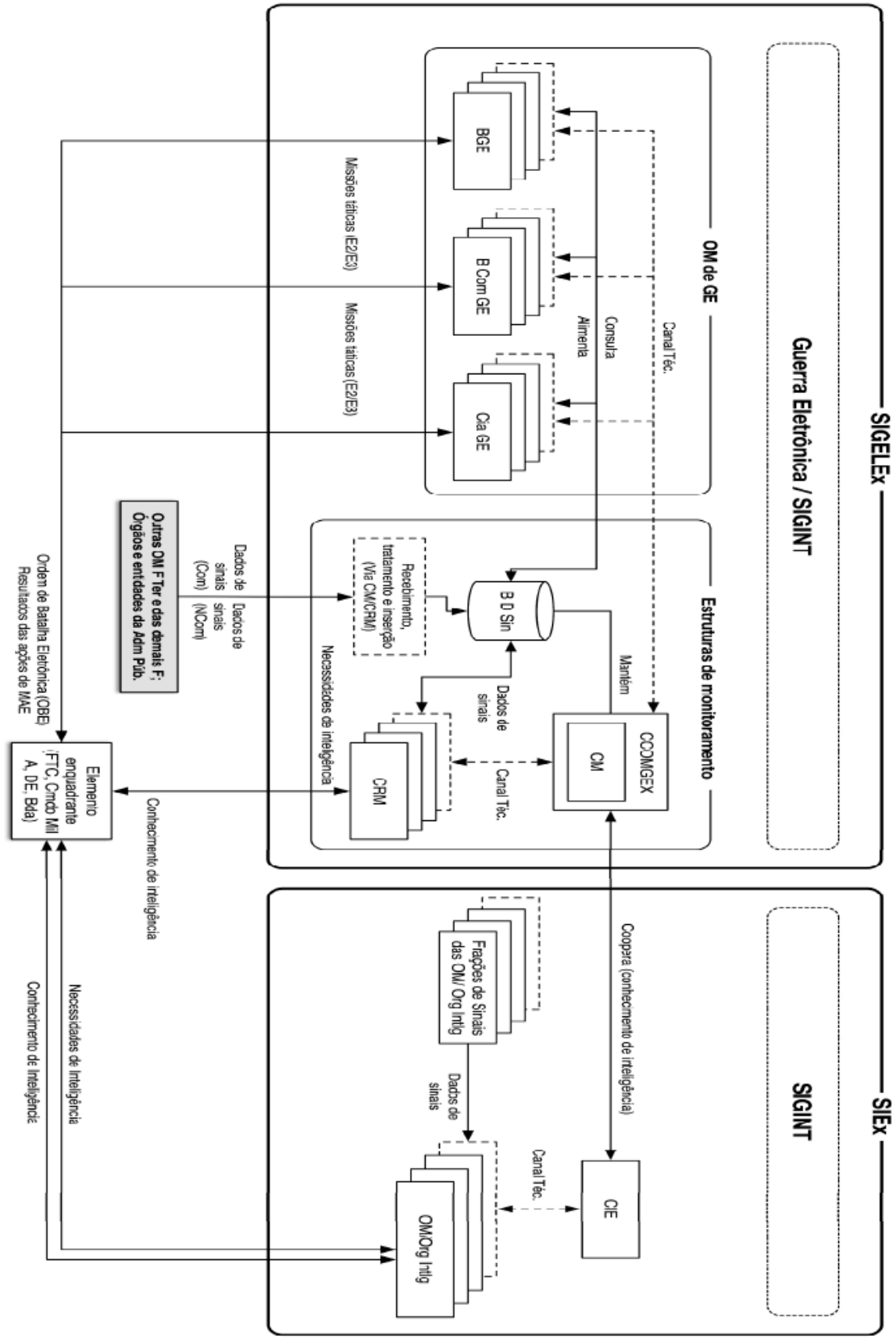

Figura 01: Perspectiva Orgânica da Guerra Eletrônica.

Fonte: BRASIL (2019).

Em uma operação, uma OM GE mobilia as seguintes instalações: Posto de Comando (PC), os Centros de Operações de Guerra Eletrônica (Principal e Avançado) e os Postos de Guerra Eletrônica (BRASIL, 2020).

O PC de uma OM de GE é a instalação de comando e controle (C^2) que reúne pessoal e material incumbidos das atividades de planejamento e condução das operações táticas de GE. Por sua vez, os Centros de Operações de Guerra Eletrônica (COGE) são instalações de C^2 desdobradas e operadas pelas subunidades e frações de GE, destinadas às atividades de coordenação e condução das ações de GE, executadas pelas frações respectivas (BRASIL, 2020).

Os COGE são divididos em COGE Principal e COGE Avançado. Caso o COGE se encontre justaposto ao PC da OM GE, este se denominará COGE Principal. Já os COGE Avançados, são aqueles desdobrados pelas frações de GE em suas áreas de responsabilidade (BRASIL, 2020).

A missão precípua do COGE Principal é realizar a análise final de GE, a partir dos relatórios e alarmes produzidos pelos COGE Avançados, produzindo e encaminhando Conhecimentos de Inteligência, relatórios e alarmes ao Comando do Escalão Enquadrante (BRASIL, 2020).

Por sua vez, os COGE Avançados:

> São responsáveis pela atribuição de missões táticas e ações específicas de MAGE e MAE aos postos de GE que lhe são afetos, bem como a análise dos dados e informações por eles gerados. Dessa forma, emitem relatórios e alertas em face dos alvos eletrônicos e das ameaças identificadas (BRASIL, 2020).

Na ponta da linha, temos os postos de GE, responsáveis pela instalação e operação dos equipamentos e sistemas de MAGE e MAE. Devem, ainda, possuir mobilidade e transportabilidade compatíveis com a força ou elemento apoiados (BRASIL, 2020).

À luz do Manual de Campanha EB70-MC-10.201 - A Guerra Eletrônica na Força Terrestre, temos que são OM de GE:

> a) os Batalhões de Guerra Eletrônica (BGE), em apoio a uma FTC, no amplo espectro das operações;
> b) os Batalhões de Comunicações e Guerra Eletrônica (B Com GE), subordinados aos Comandos Militares de Área (Cmdo Mil A); e

> c) as Companhias de Guerra Eletrônica (Cia GE), na dosagem de uma por Divisão de Exército (BRASIL, 2019).

Na perspectiva de que o assunto GE está em constante evolução e aprimoramento, o Comando de Operações Terrestres (COTER) aprovou, em dezembro de 2021, a Nota Doutrinária Nr 04/2021 - Sistema de Comando e Controle da Força Terrestre. Nesta, pode-se verificar o estabelecimento de uma a arquitetura do Sistema de Comando e Controle da Força Terrestre (SC^2FTer), atendendo à metodologia do Planejamento Baseado em Capacidades (PBC), (BRASIL, 2021), com impactos na estrutura organizacional de GE, cujos principais pontos, estão descritos nos próximos parágrafos.

No que tange ao emprego operacional do Corpo de Exército, cabe a uma grande unidade (GU), o Grupamento de Comunicações e Eletrônica (GCE), a responsabilidade por instalar, explorar, manter e proteger os sistemas de comunicações, de guerra eletrônica e de tecnologia da informação (BRASIL, 2021).

O GCE está organizado da seguinte forma, cuja visualização gráfica pode-se verificar na Figura 02:

> a. comando e estado-maior;
> b. 01 (uma) companhia de comando e apoio;
> c. 01 (um) batalhão de comando e controle;
> d. número variável de batalhões de comunicações/batalhões de comunicações e guerra eletrônica;
> e. 01 (um) batalhão de guerra eletrônica; e
> f. 01 (um) batalhão logístico de classe VII (BRASIL, 2021).

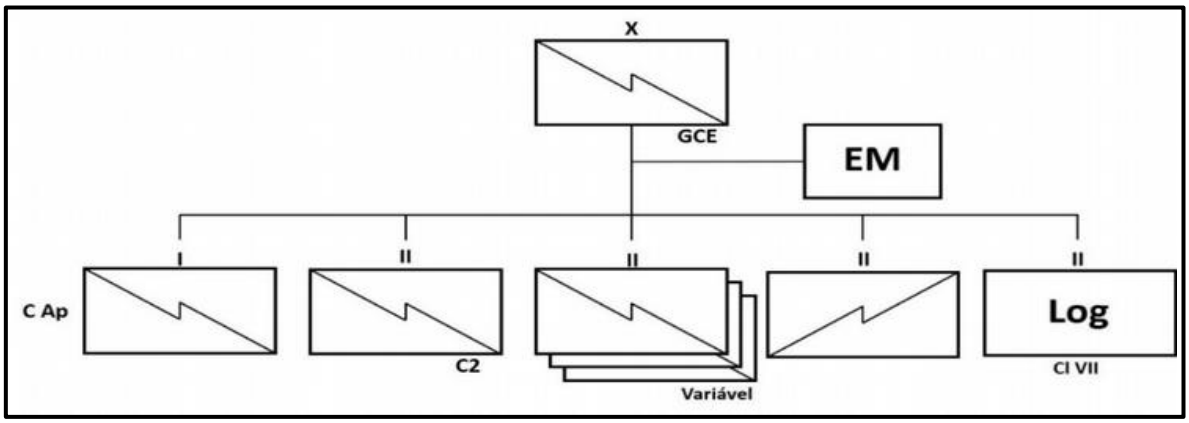

FIGURA 02 – Estrutura organizacional do GCE.
Fonte: BRASIL (2021).

O Batalhão de Comunicações e Guerra Eletrônica (B Com GE), como destacável mudança doutrinária, incorporou a Cia GE, antes diretamente subordinada às Divisões de Exército e que deixa de existir como OM independente. O B Com GE é um elemento de apoio de Com e GE podendo ser orgânico de uma Divisão de Exército (DE) ou de um GCE quando um corpo de exército for ativado. Em tempo de paz, o B Com GE estará subordinado a um Comando Militar de Área ou uma Divisão de Exército (BRASIL, 2021).

O B Com GE é constituído por 05 Subunidades (Figura 03), a saber:

a. comando e estado-maior;
b. 01 (uma) companhia de comando e apoio;
c. 01 (uma) companhia de comunicações;
d. 01 (uma) companhia de comunicações nodal;
e. 01 (uma) companhia de comando e controle; e
f. 01 (uma) companhia de guerra eletrônica (BRASIL, 2021).

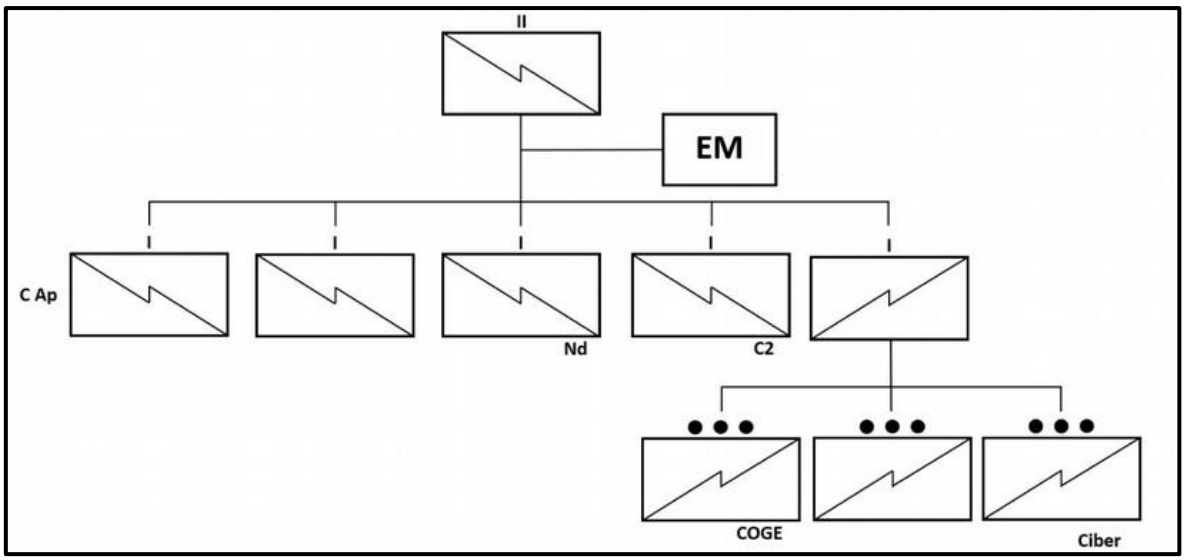

FIGURA 03 – Estrutura organizacional do B Com GE.
Fonte: BRASIL (2021).

Dentro da estrutura do GCE, no escopo da GE, tem-se ainda o Batalhão de Guerra Eletrônica (BGE). O BGE tem por missão apoiar em guerra eletrônica 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 (BRASIL, 2021).

Cabe ao BGE estabelecer o centro de operações de guerra eletrônica (COGE) em proveito do GCE. Para isso, o BGE conta com a seguinte constituição, também descrita na Figura 04:

a. comando e estado-maior;
b. 01 (uma) companhia de comando e apoio;
c. 02 (duas) companhias de guerra eletrônica; e
d. 01 (uma) companhia de guerra cibernética.

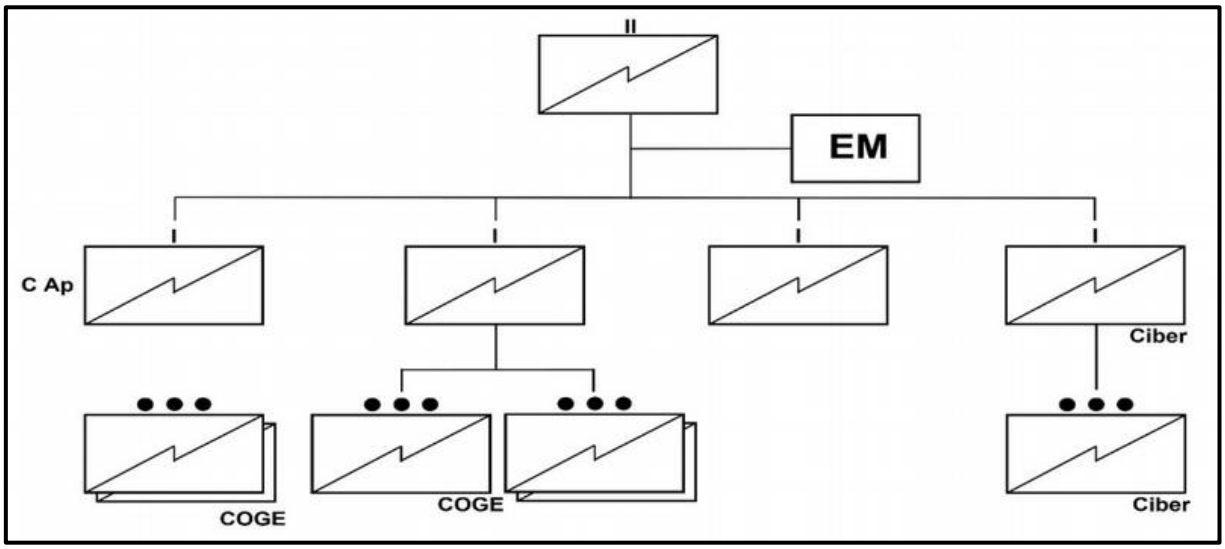

FIGURA 04 – Estrutura organizacional do BGE.
Fonte: BRASIL (2021).

Por fim, cabe salientar que na GE é totalmente válido o conceito de que todo militar é um meio de obtenção de dados em potencial (ESS – conceito do inglês "*Every Soldier is a Sensor"*), amplamente utilizado na Função de Combate Inteligência (BRASIL, 2015). Pode confirmar tal pressuposto na definição de manual que diz que:

> Qualquer escalão da F Ter dotado de meios eletrônicos de sensoriamento e de comunicações, pode, por intermédio das seções de inteligência, fornecer ao sistema de GE dados de sinais dos campos das Com e de NCom, eventualmente adquiridos e registrados, em suas atividades e operações, bem como outras informações de relevância acerca de possíveis atividades hostis sobre aqueles sistemas eletrônicos (BRASIL, 2015).

4 A ORGANIZAÇÃO DA GUERRA CIBERNÉTICA NO EXÉRCITO BRASILEIRO

A revolução tecnológica elevou o espaço cibernético a uma nova condição nos assuntos relacionados à defesa e segurança (BRASIL, 2017a). Após terra, mar, ar e espaço, a guerra entrou no quinto domínio: ciberespaço. Nesse sentido, os principais países do mundo estão a se preparar, de uma forma ou de outra, para aquilo que hoje já é uma realidade, ou seja, o quinto domínio da guerra (PASSOS, 2020).

No Brasil, em linha com a tendência mundial, o Exército Brasileiro tem acompanhado essa revolução tecnológica e seus impactos doutrinários. Com esse foco e de forma coerente com a Doutrina Militar de Defesa Cibernética, foi formulada a doutrina sobre Guerra Cibernética do Exército Brasileiro, de forma a contribuir para o desenvolvimento de capacidades nesse domínio (BRASIL, 2017a).

Assim, é de fundamental importância que a expressão militar do Poder Nacional esteja permanentemente preparada e capacitada para responder, de forma proativa, oportuna e adequada, a quaisquer cenários adversos à defesa nacional. Agravando ainda esse quadro, observa-se o aumento do risco de perpetração de ataques por estados, organizações e até mesmo pequenos grupos, com as mais diversas motivações (BRASIL, 2017aa).

Dentro desse cenário, segundo o Manual de Campanha EB70-MC-10.232, a defesa cibernética vem se estabelecendo como atividade importante no êxito das operações militares em todos os escalões de comando. Da mesma forma, a guerra cibernética, conduzida por componentes especializados das Forças Armadas (FA) nos níveis operacional e tático, busca contribuir para as ações mais amplas da defesa cibernética (2017a).

O setor cibernético foi formalmente estabelecido em 2008, com a aprovação da Estratégia Nacional de Defesa, e dividido em dois campos distintos: a segurança cibernética, a cargo da Presidência da República (PR), e a defesa cibernética, a cargo do Ministério da Defesa (MD), por meio das FA (BRASIL, 2017a).

De acordo com o Manual de Guerra Cibernética, no contexto do Ministério da Defesa, o nível de decisão determina as ações no espaço cibernético de cada setor, conforme discriminado abaixo e ilustrado na Figura 05:

> a) nível político - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a administração pública federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais;

> b) nível estratégico - Defesa Cibernética - a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das FA, interagindo com a Presidência da República e a APF; e
> c) níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das FA (2017a).

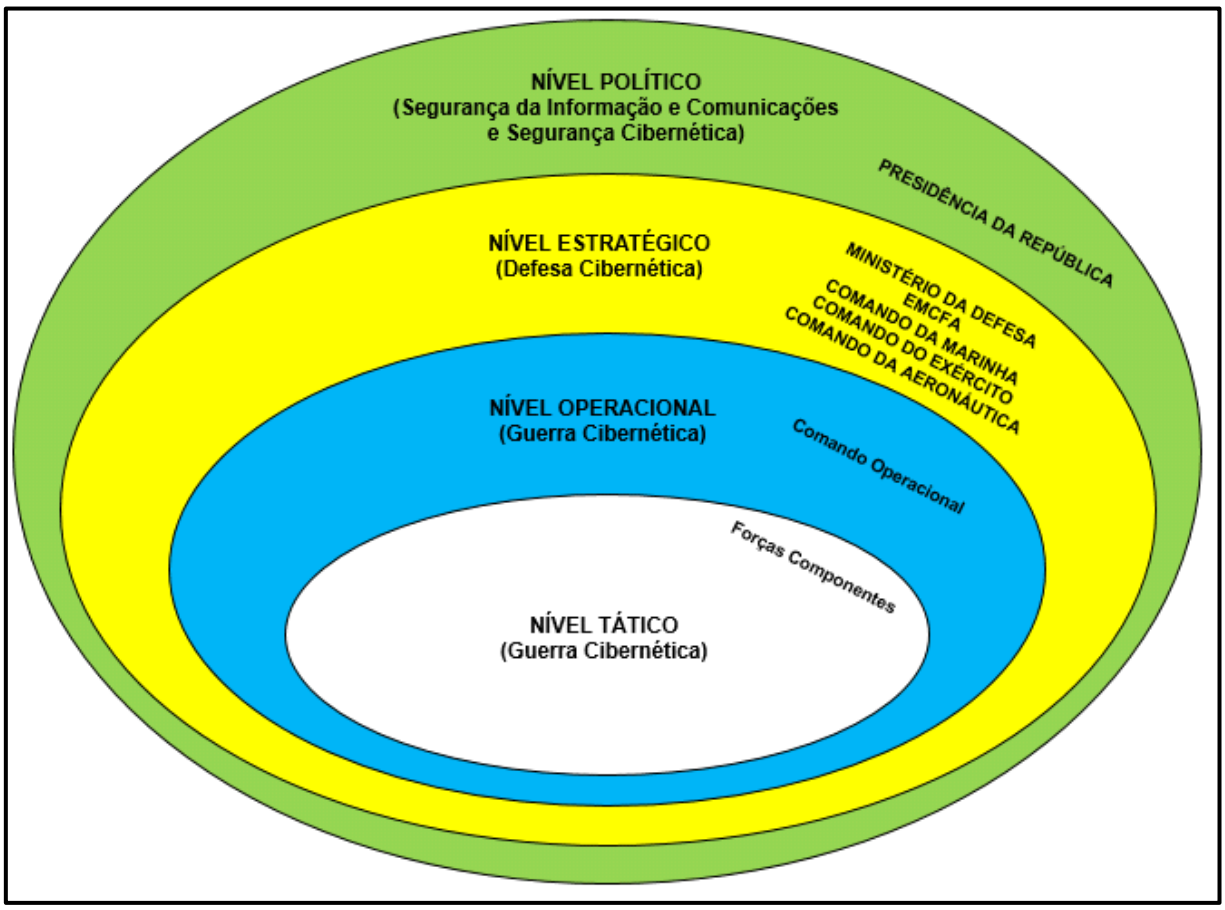

FIGURA 05 – Níveis de decisão.
Fonte: BRASIL (2017a).

No decorrer deste capítulo, foi dada ênfase apenas para a organização cibernética no nível tático, no qual se insere o Exército, sendo o assunto designado como Guerra Cibernética (BRASIL, 2017a).

Para detalhar e coordenar as estruturas e responsabilidades na Guerra Cibernética no âmbito EB, criou-se o Sistema de Guerra Cibernética do Exército (SGCEx), o qual é:

> um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de guerra cibernética, assegurando o seu uso efetivo pelo Exército Brasileiro, bem como impedindo ou dificultando a utilização do espaço cibernético pelo oponente.
>
> O SGCEx visa à proteção cibernética do Sistema de Comando e Controle do Exército, assegurando a capacidade de atuar em rede com

> segurança, bem como coordenar e integrar a proteção das infraestruturas críticas da informação sob responsabilidade do Exército (BRASIL,2017a).

O SGCEx está inserido no Sistema Militar de Defesa Cibernética (SMDC), conforme Figura 06:

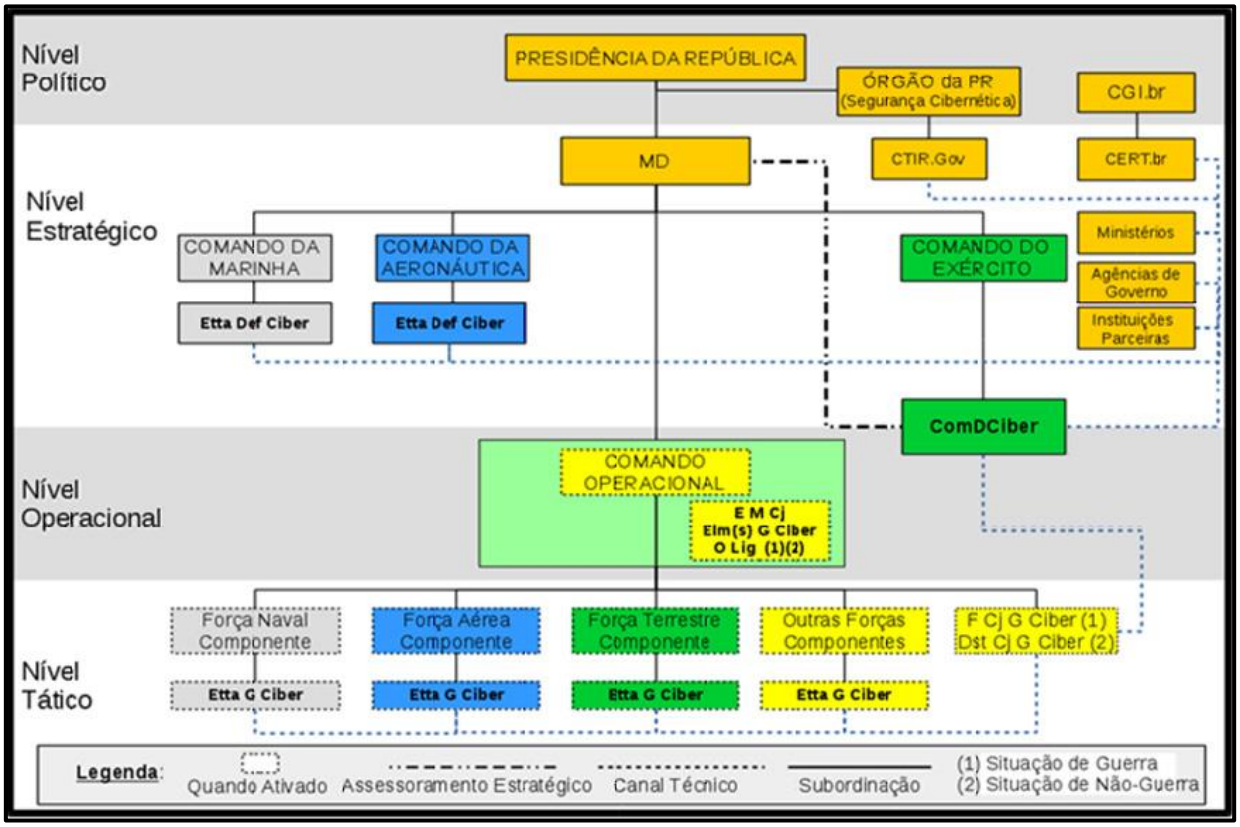

FIGURA 06 – Sistema Militar de Defesa Cibernética (SMDC).
Fonte: BRASIL (2017a).

Conforme visto na Figura 06, no nível tático, a Força Terrestre Componente (FTC), quando ativada, receberá o apoio de uma Estrutura de Guerra Cibernética (Etta de G Ciber). Essa estrutura engloba os elementos do Batalhão de Guerra Eletrônica, o Batalhão de Comunicações, o Batalhão de Comunicações e Guerra Eletrônica, o Batalhão de Inteligência Militar, a Companhia de Comando e Controle e as Companhias de Comunicações (BRASIL, 2017a).

Nesse contexto, destaca-se o Batalhão de Guerra Eletrônica, a única OM capaz de realizar as 03 atividades cibernéticas (Atq, Expl e Prot), como pode ser constatado na Tabela 02. Conforme já visto no Capítulo 3, além do apoio em GE, cabe ao Batalhão de Guerra Eletrônica apoiar em guerra cibernética uma FTC até o nível Corpo de Exército ou que enquadre mais de uma Divisão de Exército no amplo

espectro dos conflitos. Para tal, o BGE possui, de maneira orgânica, uma companhia de G Ciber (BRASIL, 2021).

A seguir, na Tabela 02, estão apresentadas as estruturas operativas de G Ciber, suas atividades cibernéticas e a respectiva discriminação de responsabilidades:

Estrutura	Atq	Expl	Prot	Responsabilidades
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.
Batalhão de Comunicações (B Com)			X	Realiza a 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 da FTC.
Batalhão de Comunicações e Guerra Eletrônica (B Com GE)		X	X	Realiza a proteção cibernética dos sistemas de informação da FTC apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção

				cibernética e de exploração cibernética da FTC, quando o BGE não estiver presente.
Batalhão de Inteligência Militar (BIM)		X	X	Realiza a exploração cibernética em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. Seu comandante será responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.
Companhia de Comando e Controle (Cia C2)			X	Realiza a proteção cibernética dos postos de comando da Força Terrestre Componente.
Companhia de Comunicações (Cia Com)			X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade.
OM integrantes da FTC			X	Realiza a proteção cibernética (somente preventiva) dos sistemas de informação da OM.

TABELA 02 – Estruturas operativas de G Ciber, suas atividades cibernéticas e responsabilidades.
Fonte: BRASIL (2017a).

Ainda, em operações, caso haja necessidade, o Manual EB70-MC-10.232 descreve que as atividades de G Ciber poderão ser complementadas pelas seguintes OM:

a) Comando de Defesa Cibernética (ComDCiber);
b) Centro de Defesa Cibernética (CDCiber);
c) Centro Integrado de Telemática do Exército (CITEx);
d) Centros de Telemática de Área (CTA) e Centros de Telemática (CT);
e) Centro de Desenvolvimento de Sistemas (CDS);
f) Centro de Inteligência do Exército (CIE); e
g) outras OM, conforme a situação (2017a).

5 A ORGANIZAÇÃO DA GUERRA ELETRÔNICA E DA GUERRA CIBERNÉTICA NA ALEMANHA

5.1 ESTRUTURA DAS FORÇAS ARMADAS DA ALEMANHA

Inicialmente, é importante conhecer a estrutura das Forças Armadas da Alemanha (*Bundeswehr*). No nível político, encontra-se o Ministério da Defesa Federal (*Bundesministerium der Verteitigung)*, sendo o departamento especializado em defesa militar e responsável por todos os assuntos da *Bundeswehr* dentro do Governo Federal. Atua como a mais alta autoridade de comando militar e autoridade suprema de serviço para a administração da *Bundeswehr* (ALEMANHA, 2022a).

No campo militar, a condução é realizada pelo Comandante Geral das Forças Armadas (*Generalinspekteur der Bundeswehr*), que é o único General de Quatro Estrelas em função na Alemanha. Diretamente subordinados, estão os comandos das 06 Forças Singulares Alemãs: Exército (*Heer*), Força Aérea (*Luftwaffe*), Marinha (*Marine*), Base de Apoio das Forças Armadas (*Streitkräftebasis*), Serviço de Saúde das Forças Armadas (*Sanitätsdienst*) e o Comando do Espaço Cibernético e da Informação (*Kommando Cyber- und Informationsraum*). Essa divisão encontra-se ilustrada na Figura 07 (ALEMANHA, 2019a).

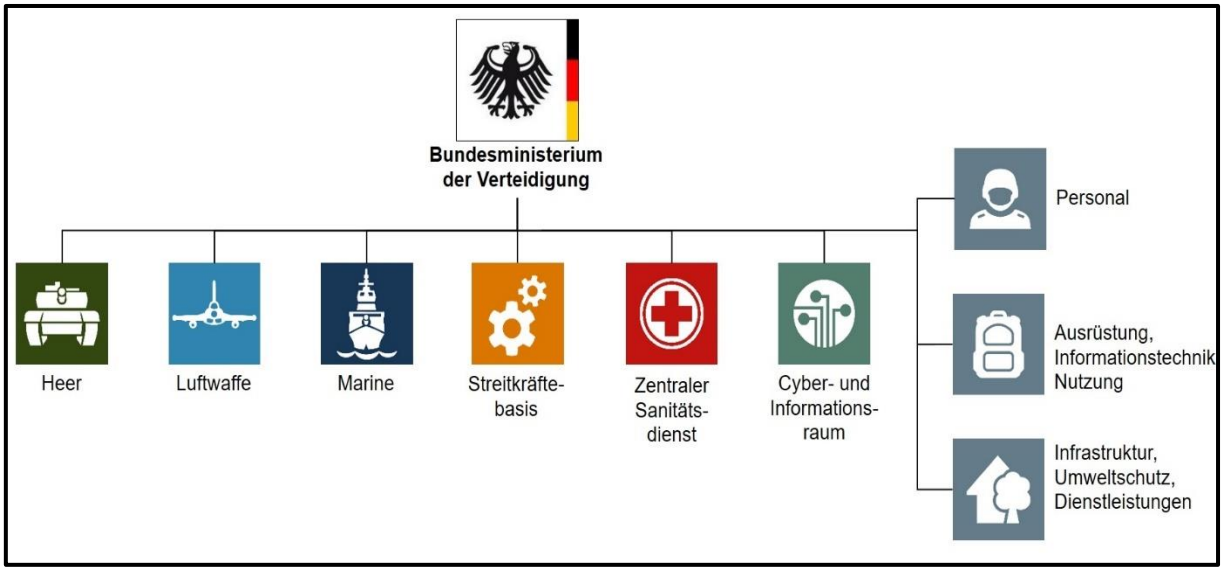

FIGURA 07 – Organização do Ministério de Defesa da Alemanha.
Fonte: ALEMANHA (2019a).

Na sua estrutura, o Ministério de Defesa Alemão (Figura 08) possui o Exército para atuar no espaço terrestre, a Força Aérea para atuar no espaço aéreo, a Marinha para atuar no espaço marítimo e, recentemente, criou o KdoCir para atuar na quarta dimensão dos combates, o espaço informacional ou ciberespaço.

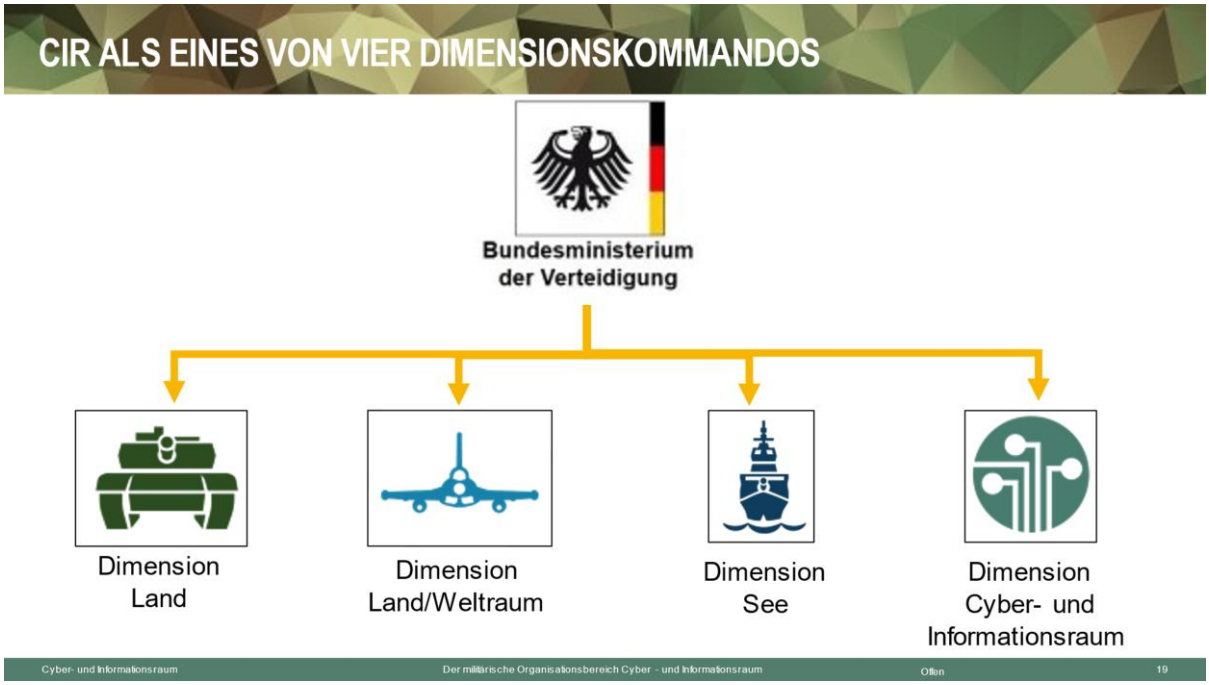

FIGURA 08 – Divisão do Ministério de Defesa Alemão nas 4 dimensões.
Fonte: ALEMANHA (2019a).

Devido à relevância do assunto ciberespaço, as Forças Armadas Alemãs modificaram suas estruturas para acomodar essa nova dimensão. Segundo Fernandes:

> A doutrina alemã acrescenta, ao domínio do ciberespaço, operações em dois outros domínios militares: (i) o ambiente eletromagnético; e (ii) o domínio militar informacional. Tudo em conjunto é designado o Espaço Informacional, sendo este espaço a área de operações do Kdo CIR (2020).

O Comando do Espaço Cibernético e da Informação (KdoCIR), foi criado em abril de 2017 e se tornou responsável por concentrar, numa estrutura conjunta, todas as capacidades relativas ao ambiente informacional, tais como Inteligência, Guerra Eletrônica, Comando e Controle, Comunicações, Tecnologia da Informação, Cibernética, Geoinformação e Operações Psicológicas. Dessa forma, foram reunidas nesse novo comando diversas estruturas que estavam espalhadas em outros comandos, além de terem sido criadas organizações militares (ALEMANHA, 2019a).

Internamente, o KdoCIR é organizado numa Divisão de Governança, responsável pelas ações voltadas aos níveis político e estratégico junto ao govemo e outros ministérios, e pela Divisão de Segurança da Informação, com a responsabilidade de atuar no nível operacional, além de coordenar e acompanhar as ações junto as demais Forças. Além disso, o Subcomandante tambem é o Chefe do Escritório de Segurança da Informação das Forças Armadas, sendo o responsável por coordenar as ações relativas à Segurança Cibernética e da Informação no campo militar interno junto à OTAN (ALEMANHA, 2019a).

Diretamente subordinados ao KdoCIR, estão: o Comando de Reconhecimento Estratégico (*Kommando Strategische Aufklärung* – KdoStratAufkl), Centro de Geoinformação (*Zentrum für Geoinformationswesen der Bundeswehr* – ZGeoBw) e o Comando de Tecnologia da Informação (*Kommando Informationstechnik der Bundeswehr* - KdoITBw), conforme ilustrado na Figura 09 (ALEMANHA, 2019a).

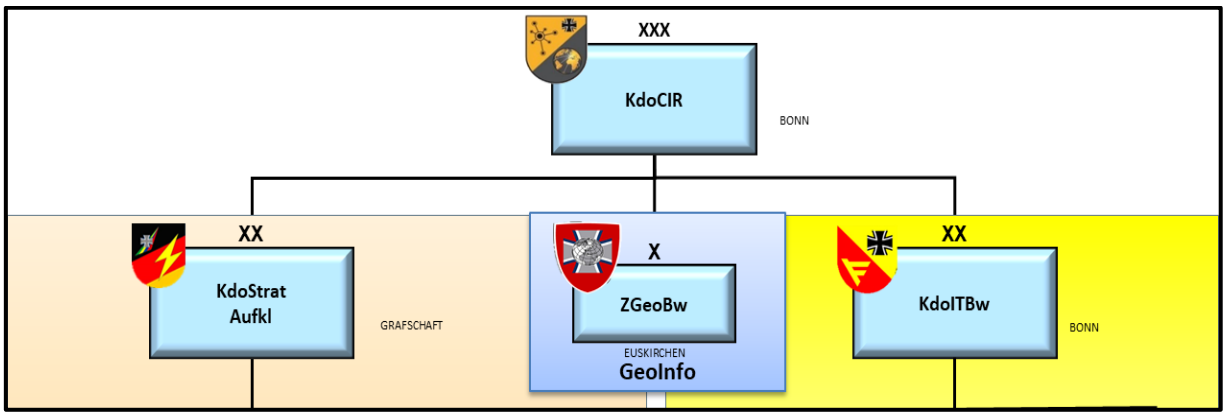

FIGURA 09 – Organização do KdoCIR.
Fonte: ALEMANHA (2019a).

Cabe ao Comando de Reconhecimento Estratégico obter e fornecer, aos decisores dos diversos escalões, informações úteis em tempo útil, seja para detecção precoce de crises ou para apoio às operações. A gama de tarefas e capacidades do *KdoStratAufkl* inclui a guerra eletrônica, o reconhecimento de imagens por satélite, o reconhecimento eletrônico e de comunicações, além de realizar a análise de objetos. As informações obtidas são processadas e dão origem a informações, notificações e relatórios, entre outros produtos. A proteção do pessoal localizado nas áreas operacionais da *Bundeswehr* também é objeto de trabalho do comando. Isto inclui, em particular, a proteção contra armadilhas, como os Dispositivos Explosivos

Improvisados (*Improvised Explosive Device* - IED), para a qual as competências nas áreas de reconhecimento de telecomunicações e capacidade de interferência com radiações eletromagnéticas são fundamentais (ALEMANHA, 2022b).

Já o Centro de Geoinformação da *Bundeswehr* garante o suporte de geoinformação para toda a gama de tarefas da *Bundeswehr*. O espaço, com seus geofatores, é registrado, analisado e disponibilizado para que todos os usuários possam, com precisão, se posicionar, navegar e agir nos alvos. Compete ao *ZGeoBw*, a execução das seguintes tarefas: produção e fornecimento de geoinformação, a implementação da consulta informações geográficas, e pesquisa geocientífica (ALEMANHA, 2022c).

O Comando de Tecnologia da Informação é o encarregado em prover toda a infraestrutura fisica e de serviços para as Forças Armadas da Alemanha. Inicialmente, todo o suporte de tecnologia de informação (TI) e comunicações é proporcionado por intermédio de uma empresa civil, a BWI, por meio de um contrato extremamente complexo e de elevado custo. Dessa forma, todos os equipamentos destinados a rotina administrativa das unidades é fornecido por essa empresa, assim como os serviços e o suporte técnico. O modo de atuação do *KdoITBw* é orientado a serviços e à disponibilidade destes e monitorada por um Centro de Operações de Rede (*Network Operations Centre - NOC*) (ALEMANHA, 2019a).

O segundo serviço disponibilizado é a conectividade de longo alcance, para as tropas no país e no exterior, por meio de enlaces satelitais e redes privadas virtuais (VPN), de forma a prover comunicações seguras e confiáveis. Da mesma forma, é disponibilizado o apoio de comunicações e TI a todas as instalações fixas e transportáveis das Forças Armadas, por meio de acesso de voz e dados a todos os postos de comando e sedes de unidades (ALEMANHA, 2019a).

Por fim, é disponibilizado todo o apoio e suporte de comunicações e TI às unidades militares móveis em exercícios e emprego real, no país e exterior. Nesse nivel, as tropas especializadas de comunicações são orgânicas das Forças Singulares, mas são capacitadas, apoiadas e tern o emprego coordenado pelo KdoITBw (ALEMANHA, 2019a).

5.2 A ORGANIZAÇÃO DA GUERRA ELETRÔNICA NA ALEMANHA

Conforme visto anteriormente, compete ao KdoStratAufkl, sob coordenação do KdoCIR, executar as tarefas de guerra eletrônica no âmbito da *Bundeswehr*. Para tal, o KdoStratAufkl conta com a seguinte organização, demonstrada na Figura 10:

a. Centro Conjunto de Análise de Imagens (ZabbAufkl – Zentrale Abbildende Aufklärung);

b. Centro de Comunicação Operacional da Bundeswehr (ZopKomBw - *Zentrum für Operative Kommunikation der Bw*);

c. Centro de Avaliação de Guerra Eletrônica (AuswZentr EloKa - *Auswertezentrale Elektronische Kampfführung*);

d. Batalhões de Guerra Eletrônica (EloKaBtl - *Bataillon Elektronischer Kampfführung*)

e. Centro de Reconhecimento de Inteligência do Sinal (ZU-StelleBwTAufkl - *Zentrale Untersuchungsstelle der Bw für Technische Aufklärung*);

f. Escola de Reconhecimento Estratégico da Bw (SchStratAufklBw - *Schule Strategische Aufklärung der Bw*);

g. Centro de Operações Cibernéticas (ZCO - *Zentrum für Cyber-Operationen*).

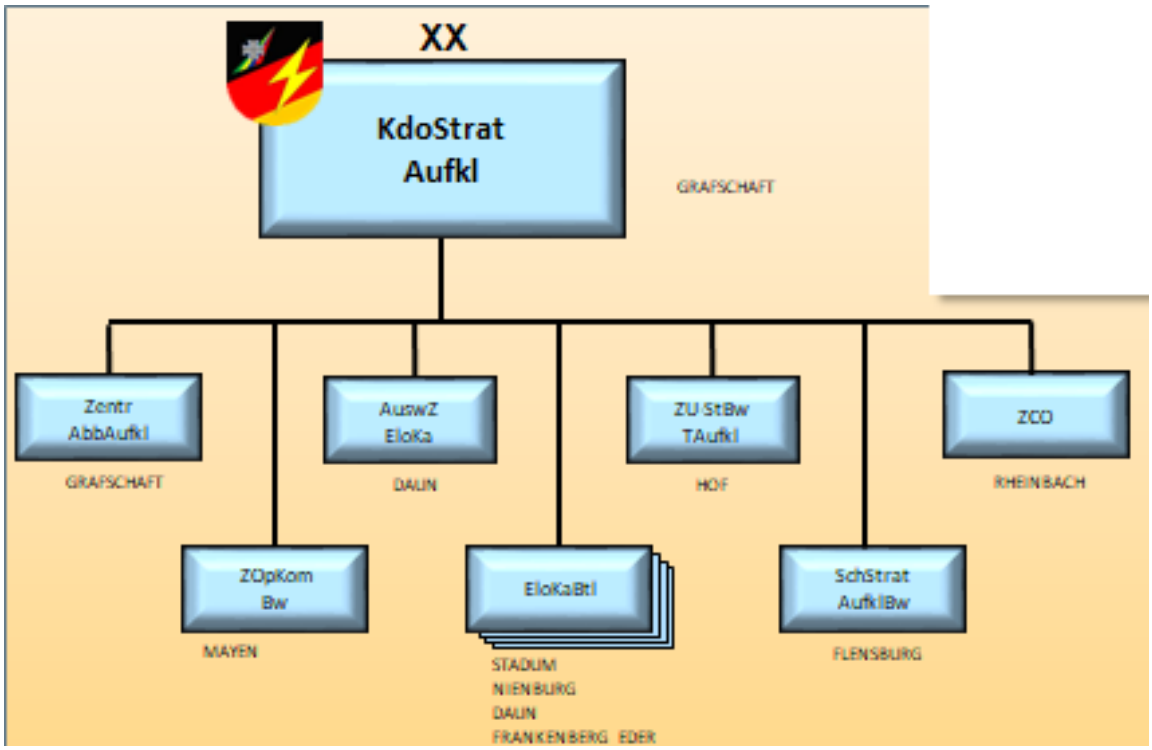

FIGURA 10 – Organização do KdoStratAufkl.
Fonte: ALEMANHA (2019a).

Os batalhões de guerra eletrônica são os elementos operacionais do KdoStratAufkl, totalizando 04 unidades, assim distribuídos:

a. 911º Batalhão de Guerra Eletrônica (*Bataillon Elektronischer Kampfführung 911)* – localizado na cidade de Stadum;

b. 912º Batalhão de Guerra Eletrônica *(Bataillon Elektronischer Kampfführung 912)* localizado na cidade de Neimburg;

c. 931º Batalhão de Guerra Eletrônica *(Bataillon Elektronischer Kampfführung 931)* localizado na cidade de Daun;

d. 932º Batalhão de Guerra Eletrônica (*Bataillon Elektronischer Kampfführung 932)* localizado na cidade de Frankenberg Eder (ALEMANHA, 2019a).

O 911º Batalhão de Guerra Eletrônica é uma unidade de reconhecimento de telecomunicações semi-móvel da *Bundeswehr*. O batalhão realiza duas atividades principais: o reconhecimento móvel terrestre e o reconhecimento de aquisição de sinais estacionários. Além de fornecer contingentes de guerra eletrônica, o seu centro de reconhecimento e direção investiga as emissões eletromagnéticas 24 horas por dia. Os resultados de reconhecimento assim obtidos dão uma importante contribuição como auxílio à tomada de decisão do comando militar e ajudam a avaliar a ameaça às forças da *Bundeswehr*. Para tal, a unidade conta com sítios de antenas, como da Figura 11. Eles também servem à liderança política para uma avaliação mais aprofundada da situação no reconhecimento e áreas de interesse, utlizando o princípio: saiba antes que os outros saibam (ALEMANHA, 2022b).

FIGURA 11 – Sítio de Antenas do EloKaBtl 911.
Fonte: ALEMANHA (2022b).

O 912º Batalhão de Guerra Eletrônica é considerado uma unidade altamente especializada e moderna, possuindo a tarefa de realizar a aquisição de informações de emissões eletromagnéticas, seja pelo tráfego de rádio ou emissões de radar. Com seus equipamentos, pode obter informações sobre as forças inimigas nas áreas operacionais da *Bundeswehr*. Entre os batalhões do Comando de Reconhecimento Estratégico, destaca-se pela cobertura das três dimensões, terrestre, aérea e marítima. O batalhão, ainda, processa as diversas informações individuais sobre forças militares, paramilitares e de atuação assimétrica nas áreas de atuação e áreas de interesse, visando obter conhecimento sobre suas intenções, movimentos de forças e distribuição de sistemas de armas e redes de comunicação (ALEMANHA, 2022b).

O batalhão é composto por quatro companhias operacionais e uma companhia suplementar, a qual é formada quase exclusivamente por reservistas e ativada em casos de necessidade. A 1ª Companhia, enquanto subunidade de avaliação, fornecimento e formação, tem a função de avaliar e dar continuidade ao tratamento da informação obtida junto das restantes companhias. Realiza o treinamento básico, bem como a reparação de veículos e equipamentos para o batalhão. A 2ª Companhia é a "unidade marítima" da unidade, contanto com embarcações e militares especializados neste tipo de missão. Essa subunidade (SU) realiza o reconhecimento

no mar para obter informações sobre a água, subaquáticas e terrestres junto à costa nas várias áreas operacionais (ALEMANHA, 2019a).

A 3ª Companhia do EloKaBtl 911 é a "SU aérea". Esta tem a função de fornecer à Força Aérea as informações de que necessita durante seus exercícios, operações e missões. Além disso, possui a capacidade de realizar reconhecimento por um sistema de reconhecimento aéreo. A 4ª Companhia, como "SU terrestre", tem a capacidade de reconhecimento móvel de transmissões de rádio direcionadas e emissões de radar com seus sistemas baseados em veículos blindados na plataforma *Transportpanzer Fuchs*, o qual pode ser visto na Figura 12 (ALEMANHA, 2019a).

FIGURA 12 – Viatura Blindada de transporte de pessoal - *Transportpanzer* FUCHS.
Fonte: ALEMANHA (2022b).

O 931º Batalhão de Guerra Eletrônica realiza uma variedade de tarefas em prol do Comando de Reconhecimento Estratégico. Elas podem ser resumidas sob as palavras-chave reconhecimento e proteção. Quando em operações no exterior, os especialistas em guerra eletrônica do Btl têm capacidade de proteger suas próprias tropas, por exemplo durante a execução de patrulhas, do acionamento remoto de armadilhas e minas (IED), suprimindo sinais de rádio inimigos usando um *Jammer*,

uma espécie de barreira eletromagnética. Tal sistema pode ser visto na Figura 13 (ALEMANHA, 2022b).

Além disso, podem registrar a comunicação inimiga, avaliar e relatar os resultados ao escalão superior. Os seus serviços de emergência, dão assim, uma contribuição decisiva para a criação de um quadro de consciência situacional, possibilitando o alerta antecipado de ameaças reconhecidas. Também, a partir da sua localização em Daun, o Btl utiliza a mais moderna tecnologia para o reconhecimento contínuo, a fim de identificar conflitos e ameaças mesmo antes de aparecerem nas notícias. Desta Maneira, o EloKaBtl 931 dá um importante contributo para a detecção precoce de crises em todo o mundo, para a monitorização de conflitos e para o apoio a soldados e parceiros em missões no exterior (ALEMANHA, 2022b).

FIGURA 13 – Sistema de bloqueio protegido construído em um veículo de transporte blindado Fuchs.
Fonte: ALEMANHA (2022).

Por fim, o 932º Batalhão de Guerra Eletrônica realiza as tarefas de telecomunicações e reconhecimento eletrônico, além de guerra eletrônica. O foco principal está, atualmente, em operações baseadas em terra e no fornecimento de forças rápidas. A Unidade é altamente especializada nas áreas de contramedidas eletrônicas e reconhecimento de redes celulares. Além disso, há um componente aéreo para combate eletrônico para suporte próximo. Com essas habilidades, o batalhão é capaz de apoiar, de forma sustentável, a operação de suas próprias forças,

por meio da coleta de informações e dificultar a operação do inimigo, por meio de contramedidas (ALEMANHA, 2022b).

Desde 1996, EloKaBtl 932 fornece regularmente soldados para destacamentos da Bundeswehr, além de ser um fornecedor regular de tropas para missões semelhantes da OTAN e da UE. A unidade é, atualmente, líder para a Força -Tarefa de Guerra Eletrônica como parte da Força -Tarefa Conjunta de Alta Prontidão da Força de Resposta da OTAN (Figura 14), no curso da qual uma prontidão de desdobramento mundial deve ser mantida dentro de alguns dias (ALEMANHA, 2022b).

FIGURA 14 – Tropa de GE do EloKaBtl 932 em operação no norte do Afeganistão.
Fonte: ALEMANHA (2022b).

5.3 A ORGANIZAÇÃO DA GUERRA CIBERNÉTICA NA ALEMANHA

Em relação especificamente ao setor cibernético, o KdoCIR dividiu as atribuições da seguinte forma: o KdoStratAufkl recebeu a responsabilidade pelas operações cibernéticas ofensivas (principal) e defensiva (segundário), enquanto ao KdoITBw, coube a responsabilidade pelas operações cibernéticas defensivas. O organograma desses dois comandos encontra-se discriminado na Figura 15 (ALEMANHA, 2019a).

O KdoStratAufkl estabeleceu um Centro de Operações Cibernéticas (*Zentrum für Cyber-Operationen* - ZCO), com a responsabilidade de realizar ataque e exploração cibernética. Já o KdoITBw, realiza a proteção das redes corporativas, por meio do Centro de Operações do Sistema de Tecnologias de Informação (*Betriebszentrum IT-System der Bundeswehr* - BtrbZ IT-SysBw) e a defesa cibernética dos sistemas de armas e redes operacionais e táticas, por meio do Centro de Defesa Cibernética (Zentrum für Cyber-Sicherheit der Bundeswehr – ZCSBw)(ALEMANHA, 2019a).

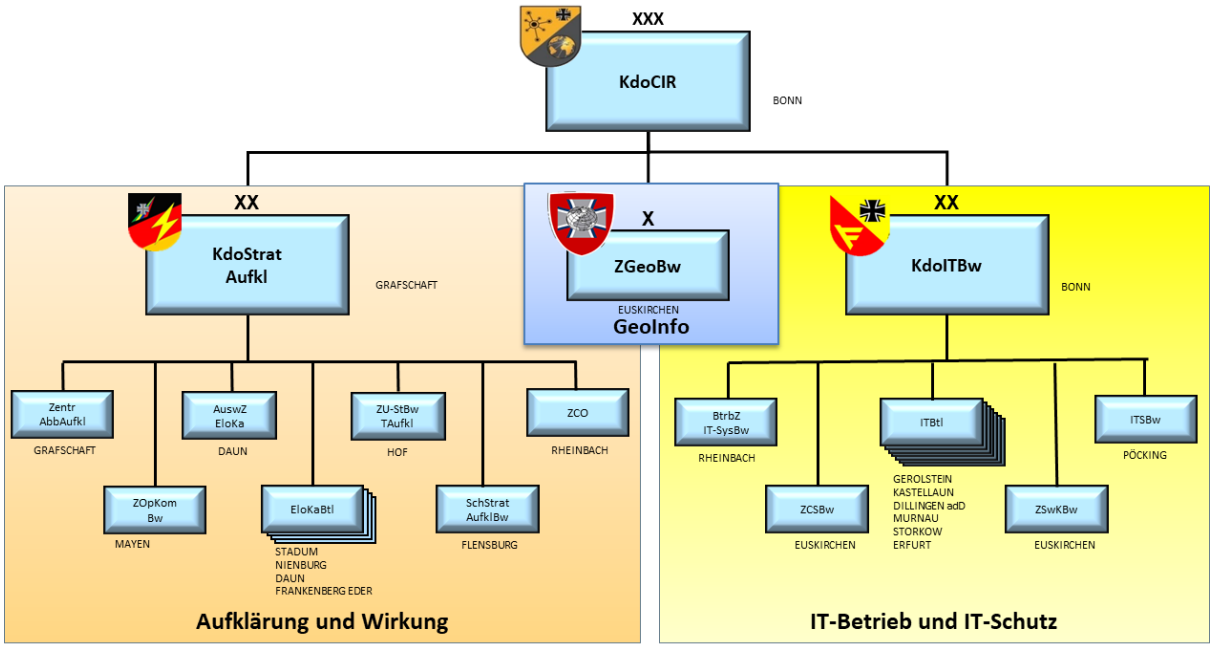

FIGURA 15 – Organograma do KdoCIR, KdoStratAufkl e KdoITBw.
Fonte: ALEMANHA (2019a).

No Centro de Operações Cibernéticas, estão agrupadas as capacidades específicas necessárias para a preparação e implementação de operações militares para reconhecimento e impacto. A missão central do ZCO é o planejamento, preparação, gerenciamento e implementação de operações para reconhecimento e impacto tanto no contexto da defesa nacional e aliada, quanto em desdobramentos obrigatórios da *Bundeswehr*. Além da responsabilidade pelas operações cibernéticas ofensivas e defensivas, as forças do ZCO podem apoiar as forças de segurança do KdoCIR no contexto de uma crise de Tecnologia da Informação) (ALEMANHA, 2019a).

Dentro do KdoITBw, merecem destaque o Centro de Operações do Sistema de Tecnologias de Informação (BtrbZ IT-SysBw) e Centro de Defesa Cibernética

(ZCSBw). A missão precípua do BtrbZ IT-SysBw é fornecer serviços de TI para a *Bundeswehr*, em particular para assegurar a capacidade central de comando e controle das forças armadas em operações em qualquer hora e em qualquer lugar do mundo. Com o seu *Network Operations Centre Basis Inland* (NOC B.I.), o *Betriebszentrum IT - System* é capaz de monitorar todo o sistema de TI das áreas operacionais e assegurar as aplicações e serviços necessários 24 horas por dia. Ali trabalham, entre outros, administradores de TI para infraestruturas e aplicativos de servidores complexos, especialistas em redes e TI, especialistas no controle de sistemas de comunicação por satélite e executivos para gerenciamento de serviços de tecnologia da informação (ALEMANHA, 2019b).

O Centro de Segurança Cibernética da *Bundeswehr* (ZCSBw) é a agência central responsável por garantir a proteção abrangente dos sistemas e serviços de tecnologia da informação da *Bundeswehr*. O centro fornece o conhecimento especializado para proteger o sistema de TI e as informações nele processadas. Com suas equipes de resposta a incidentes, o centro garante reações rápidas e flexíveis a ataques cibernéticos à *Bundesweh*, seja em seu território ou exterior, no cotidiano ou em operações. Trabalha com parceiros externos, nacionais e internacionais, bem como organizações multinacionais ou supranacionais como a OTAN e a União Europeia (ALEMANHA, 2019b).

O ZCSBw é chefiado por um coronel, sendo responsável pela produção e distribuição dos sistemas criptográficos, incluindo a certificação digital, auditorias de segurança, realização de testes de penetração de redes (PenTest), organização das equipes de tratamento dos incidentes de rede, com o acompanhamento 24/7, realização de análise forense, análise e gestão de riscos cibernéticos. Cabe destacar que o foco está na proteção dos sistemas de armas, aeronaves remotamente tripuladas e sistemas de comunicações militares, ficando a responsabilidade pela segurança de TI a cargo do Centro de Operações do Sistema de Tecnologias de Informação (BRASIL, 2017a).

Para cumprir suas missões, o ZCSBw é organizado em uma Central Administrativa e quatro divisões operacionais, conforme se segue:

a. Divisão de Proteção e Prevenção – cujas principais tarefas são produção e distribuição de material criptográfico; planejamento, observação e avaliação

de exercícios de defesa cibernética e avaliação de produtos de segurança de TI.

b. Divisão de Auditoria e Consulta – responsável pelas avaliações de vulnerabilidade técnicas, testes de penetração e auditorias de segurança de criptografia de unidades, projetos de armamento, locais de implantação, exercícios, incluindo sistemas especiais e de armas.

c. Divisão do Centro de Operações de Segurança Cibernética – suas tarefas precípuas englobam o monitoramento de rede 24 horas por dia, 7 dias por semana e resposta a incidentes; gerir o quadro situacional de segurança da informação (Info Sec); realizar apoio a investigações policiais e defesa cibernética avançada/responsiva.

d. Divisão da Autoridade de Acreditação de Segurança Militar Alemã – realiza a acreditação e recredenciamento de sistemas de TI de projetos de armamento, unidades, exercícios como qualificação para processamento de informações classificadas; além da consultoria para projetos de armamento em relação a acreditação, bem como a implementação de medidas de InfoSec apropriadas em todas as etapas do projeto e consultoria a projetos de armamento quanto ao uso de produtos de segurança aprovados (ALEMANHA, 2019b).

6 CONCLUSÃO

O presente trabalho teve o objetivo de analisar a organização de Guerra Eletrônica e Guerra Cibernética nos exércitos do Brasil e da Alemanha, concluindo sobre possíveis contribuições da estrutura alemã para o EB. Foi possível realizar o levantamento, a partir da metodologia de pesquisa bibliográfica e documental, de oportunidades de melhoria e confirmação de boas práticas.

Nas estruturas de GE pôde-se identificar as Cia GE como elementos-chave de exploração do espectro eletromagnético, tanto no EB quanto na *Bundeswehr.* No Brasil, um BGE e um B Com GE dispõem, respectivamente, de duas e uma Cia GE, para o cumprimento de suas missões. Os alemães possuem uma estrutura mais robusta em seus batalhões, apresentando, como no caso do EloKaBtl 912, quatro Cia GE, das quais, três estão vocacionadas à GE no mar, ar e terra. Essa organização, aliada aos elementos de cibernética, possibilitam a presença e capacidade de intervir em, pelo menos, quatro dos cinco domínios atuais da guerra.

Finalizada a análise, verificou que o EB e a *Bundeswehr* possuem diferenças nas suas estruturas de GE e de G Ciber. A composição dos seus batalhões de GE e de seus elementos de G Ciber, aliada à cadeia de comando de cada capacidade, aparecem como as principais dessemelhanças encontradas.

Assim, pode-se inferir como uma oportunidade de melhoria para o EB, a realização de estudos para o incremento do número de Cia GE no BGE, buscando, se possível, a capacidade de atuar em mais de uma dimensão simultaneamente.

Além disso, as Forças Armadas Alemães criaram, recentemente, o Kdo CIR, retirando as tropas especializadas em GE e G Ciber, entre outras, das forças singulares tradicionais (Marinha, Exército e Aeronáutica) e realocando nesse novo comando. Tal decisão buscou atender às crescentes demandas da dimensão informacional, criando uma força para trabalhar de forma centralizada em prol das demais.

Essa linha de ação parece ser uma tendência mundial, já adotada em outros países como forma de atuar no espaço informacional. Com isso, outra oportunidade de melhoria advinda da doutrina militar alemã, seria a realização de estudos para verificar a pertinência de criação de uma nova força singular no Brasil, responsável

pelo ciberespaço. Em que pese essa ação extrapolar o âmbito do EB, a sua implementação traria impactos significativos para a Força Terrestre, considerando-se pertinente a inclusão desta sugestão neste trabalho.

Outro ponto de relevância verificado no trabalho foi o protagonismo que a GE e G Ciber assumiram no atual cenário militar. O desconhecimento dessas capacidades pode fadar um exército ao insucesso. Além disso, a combinação de suas capacidades mostrou-se um possível fator multiplicador de poder.

O EB já tem demonstrado preocupação neste aspecto. Conforme visto no Capítulo 3, o BGE possui em sua composição duas companhias de GE e uma de G Ciber, enquanto um BComGE possui, na sua companhia de GE, dois pelotões de GE e um pelotão de G Ciber, permitindo à FTC ou Grandes Comandos Operativos apoiados usufruírem dessas capacidades desde o nível pelotão.

Essa integração pode ser vista como uma boa prática a ser mantida e desenvolvida até os mais altos escalões, tal qual a *Bundeswehr*. Os alemães seguem a mesma linha de pensamento ao compor um comando valor Grande Unidade para realizar ações de GE e G Ciber, o Comando de Reconhecimento Estratégico, que abarca unidades de GE, como os seus quatro EloKaBtl, com unidades de cibernética, como o ZCO.

A investigação comparativa realizada neste trabalho entre a organização de GE e G Ciber do EB e um dos líderes da OTAN, a Alemanha, revelou importantes aspectos de interesse para a doutrina militar terrestre, além de preencher parte da lacuna acadêmica nessa temática. A exploração do espaço informacional já extrapolou os níveis táticos militares, despontando como assunto a ser tratado nos mais altos níveis políticos e pela sociedade como um todo.

Ressalta-se que essa pesquisa teve limitações na obtenção de maiores informações, por se tratar de um assunto sensível e de difícil aprofundamento, principalmente no estudo de doutrina militar de outro país.

Sugere-se a realização de novos trabalhos, buscando aumentar o cabedal de conhecimento doutrinário e prático nas áreas de GE e G Ciber. A comparação com outras forças armadas pode ratificar ou retificar as conclusões e sugestões aqui apresentadas, até se chegar em insumos para a realização de experimentação

doutrinária das novas práticas ou estruturação orgânica, visando sua futura implementação. Tudo isso sempre buscando aumentar o poder de combate do EB na sua missão de defender a pátria brasileira.

REFERÊNCIAS

ALEMANHA. Bundesministerium der Verteitigung. **Struktur und Organisation**. 2022a. Disponível em <https://www.bmvg.de/de/ministerium/organisation>. Acesso em: 27 jul.2022.

ALEMANHA. Bundeswehr. Kommando Cyber- und Informationsraum. **Instruções do curso de Comandante de Unidade de Comunicações: Der militärische Organisationsbereiche - Cyber- und Informationsraum.** Bonn, 2019a.

ALEMANHA. Bundeswehr. **Kommando Strategische Aufklärung.** 2022b. Disponível em: <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung>. Acesso em: 28 jul.2022.

ALEMANHA. Bundeswehr. Kommando Cyber- und Informationsraum**. Instruções do curso de Comandante de Unidade de Comunicações: Das Kommando Informationstechnik der Bundeswehr.** Bonn**,** 2019b.

ALEMANHA. Bundeswehr. **Zentrum für Geoinformationswesen der Bundeswehr**. 2022c. Disponível em: <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/zentrum-fuer-geoinformationswesen-der-bundeswehr>. Acesso em: 28 jul.2022.

ALMEIDA, Nival Nunes; MACHADO, Raphael Carlos Santos; SÁ, Alan Oliveira de. O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo. **Naval War College Journal**, v. 25, n. 1, jun. 2019. ISSN e-2359-3075.

BRASIL. Exército. Comando de Operações Terrestres. **Nota Doutrinária Nr 04/2021 Sistema de Comando e Controle da Força Terrestre**. Brasília, 2021.

BRASIL. Exército. ECEME. **Elaboração de Projetos de Pesquisa na ECEME.** Rio de Janeiro, 2012.

BRASIL. Exército. Estado-Maior. **EB20-MC-10.207 Inteligência**. 1. Ed. Brasília, 2015.

BRASIL. Exército. Estado-Maior. **EB70-MC-10.201 A Guerra Eletrônica na Força Terrestre.** 1. ed. Brasília, DF, 2019.

BRASIL. Exército. Estado-Maior. **EB70-MC-10.232 Guerra Cibernética**. 1. ed. Brasília, DF. 2017a.

BRASIL. Exército. Estado-Maior. **EB70-MC-10.247 A Guerra Eletrônica nas Operações**. 1. Ed. Brasília, 2020.

BRASIL. Exército. Estado-Maior. **Relatório de Missão no Exterior**. Brasília, 2017b.

FERNANDES, João Daniel Gaioso. **Levantamento da estrutura orgânica de guerra eletrônica e de ciberdefesa para o nível tático no exército português.** Instituto Universitário Militar. Pedrouços, 2020.

LAMBACH, Daniel. The Territorialization of Cyberspace. **International Studies Review**, Oxford University Press. 2019.

PASSOS, Carlos Manuel Ferreira de. **A cibernética na defesa da integridade dos estados. As possibilidades portuguesas, no seio da OTAN, no domínio da ciberdefesa**. Dissertação (Mestrado Em Estudos da Paz e da Guerra nas Novas Relações Internacionais) - Universidade Autónoma de Lisboa, Lisboa, 2020.

REISDOERFER, Bruna Roh; ALCÂNTARA, Bruna Toso de. Alemanha como Líder na Determinação de Ameaças Cibernéticas na União Europeia? Neoclassical realist and conventional constructivist views. **Carta Internacional,** [S. l.], v. 15, n. 2, 2020. DOI: 10.21530/ci.v15n2.2020.1063.