ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

TC Com RODRIGO LUIZ VALIM

A interação entre a Guerra Eletrônica e a Guerra Cibernética no contexto do combate moderno do Século XXI: uma análise dos Exércitos do Brasil e dos Estados Unidos da América

Rio de Janeiro
2022

TC Com RODRIGO LUIZ VALIM

A interação entre a Guerra Eletrônica e a Guerra Cibernética no contexto do combate moderno do Século XXI: uma análise dos Exércitos do Brasil e dos Estados Unidos da América

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.

Orientador: Maj Com Samuel Bombassaro Neto

Rio de Janeiro
2022

V172i Valim, Rodrigo Luiz

A interação entre a Guerra Eletrônica e a Guerra Cibernética no contexto do combate moderno do Século XXI: uma análise dos Exércitos do Brasil e dos Estados Unidos da América./ Rodrigo Luiz Valim.—2022.
42 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. 39-40

1. Guerra Eletrônica. 2. Guerra Cibernética. 3. Interação. 4. Combate Moderno.. I. Título.

CDD 363.325

TC Com RODRIGO LUIZ VALIM

A interação entre a Guerra Eletrônica e a Guerra Cibernética no contexto do combate moderno do Século XXI: uma análise dos Exércitos do Brasil e dos Estados Unidos da América

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.

Aprovado em 24 de 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

À minha esposa que, com extrema paciência e dedicação a família, soube compreender os momentos abdicados em prol da execução deste trabalho.

AGRADECIMENTOS

Ao Major Samuel Bombassaro Neto pelo tratamento dispensado em todas as oportunidades, buscando entender as necessidades e as limitações de seu orientando, atuando com intenso profissionalismo durante todas as tarefas realizadas.

À minha família que, com todos os percalços advindos da rotina diária, foi capaz de entender a importância da dedicação ao trabalho

RESUMO

A Guerra Eletrônica e a Guerra Cibernética são capacidades que vem se tornando imprescindíveis para o combate moderno. Com o rápido avanço tecnológico presenciado na atual “Era da Informação”, verifica-se no cenário dos conflitos a atuação cada vez maior das comunicações de dados por meios centrados em redes informatizadas, no intuito de se obter a superioridade informacional ante a estratégia planejada. Ainda, a intensificação da globalização do sistema internacional permitiu a universalização da informação, inserindo a presença de atores estatais e não estatais, mídia e opinião pública como fatores de decisão no planejamento e condução das operações militares. Nesse sentido, seja no espectro eletromagnético, seja no espaço cibernético, existe a necessidade de uma análise pormenorizada da conjuntura que envolve o ambiente operacional, a fim de oferecer consciência situacional ampla, fidedigna e oportuna para os comandantes decidirem as melhores linhas de ações a serem adotadas, orientando seus esforços de forma a garantir os interesses nacionais com o menor dano colateral possível aos serviços essenciais para o desenvolvimento da população presente no local dos conflitos. Para tanto, o emprego de atuadores não cinéticos é de grande valia para as operações militares multidomínios e de amplo espectro, os quais podem atuar antes mesmo do emprego das armas cinéticas, proporcionando poder de combate a exércitos considerados mais fracos. Além disso, a interação da Guerra Eletrônica com a Guerra Cibernética otimiza as atividades desenvolvidas na dimensão informacional dos conflitos, causando maior impacto aos centros de gravidade pelo uso recorrente dos princípios da surpresa e concentração de forças na conquista dos objetivos planejados. Desse modo, essa pesquisa buscou analisar as capacidades de Guerra Eletrônica e de Guerra Cibernética, bem como a congruência de suas tarefas no contexto operativo do combate no Século XXI, considerando os modelos dos exércitos dos EUA e do Brasil, a fim de apresentar práticas e conceitos que possam servir de base para a inovação doutrinária do Exército Brasileiro, evitando a sobreposição ou interferência entre esses dois vetores. ataques não cinéticos ou para a mitigação de ações cibernéticas oponentes. Ainda, o trabalho foi concluído com as lições aprendidas da comparação da organização e formas de emprego da Guerra Eletrônica e da Guerra Cibernética nos EUA e no Brasil, atendendo aos objetivos específicos e geral do estudo proposto, finalizando com as práticas desenvolvidas por esses países, sendo algumas semelhantes e outras diferentes para a superação dos desafios atinentes a um mundo volátil, incerto, complexo e ambíguo. Por fim, foram destacadas uma série de práticas que podem ser aprofundadas em pesquisas futuras, visando a melhoria da doutrina nacional, implementando técnicas, táticas e procedimentos que facilitem a ação combinada da Guerra Eletrônica e da Guerra Cibernética nos conflitos.

PALAVRAS-CHAVE: Guerra Eletrônica, Guerra Cibernética, Interação, Combate Moderno

RESUMEN

La guerra electrónica y cibernética son capacidades que se han vuelto indispensables para el combate moderno. Con los rápidos avances tecnológicos presenciados en la actual "Era de la Información", se puede comprobar en el escenario del conflicto el creciente uso de las comunicaciones de datos a través de medios centrados en redes informáticas, con el fin de obtener una superioridad informativa ante la estrategia planificada. Además, la intensificación de la globalización en el sistema internacional ha permitido la universalización de la información, insertando la presencia de actores estatales y no estatales, de los medios de comunicación y de la opinión pública como factores de decisión en el planeamiento y conducción de las operaciones militares. En este sentido, ya sea en el espectro electromagnético o en el ciberespacio, es necesario un análisis detallado de la situación que rodea al entorno operacional con el fin de proporcionar un amplio conocimiento de la situación, fiable y oportuno para que los comandantes puedan decidir las mejores líneas de acción a adoptar, orientando sus esfuerzos a garantizar los intereses nacionales con los menores daños colaterales posibles a los servicios esenciales para el desarrollo de la población presente en el lugar de los conflictos. Para tanto, el uso de actuadores no cinéticos es de gran valor para las operaciones militares de amplio espectro y multidominio, que pueden actuar incluso antes del uso de armas cinéticas, proporcionando poder de combate a ejércitos considerados más débiles. Además, la interacción de la Guerra Electrónica con la Ciberguerra optimiza las actividades desarrolladas en la dimensión informativa de los conflictos, provocando un mayor impacto en los centros de gravedad mediante el uso recurrente de los principios de sorpresa y concentración de fuerzas en la consecución de los objetivos previstos. Así, esta investigación buscó analizar las capacidades de Guerra Electrónica y Cibernética, así como la congruencia de sus tareas en el contexto operativo del combate en el siglo XXI, considerando los modelos de los ejércitos de Estados Unidos y Brasil, para presentar prácticas y conceptos que puedan servir de base para la innovación doctrinal del Ejército brasileño, evitando la superposición o interferencia entre estos dos vectores. Aún así, el trabajo se concluyó con las lecciones aprendidas a partir de la comparación de la organización y las formas de empleo de la Guerra Electrónica y la Ciberguerra en los EE.UU. y Brasil, cumpliendo con los objetivos específicos y generales del estudio propuesto, terminando con las prácticas desarrolladas por estos países, algunas similares y otras diferentes para la superación de los desafíos relacionados con un mundo volátil, incierto, complejo y ambiguo. Finalmente, se destacaron una serie de prácticas en las que se puede profundizar en futuras investigaciones, destinadas a mejorar la doctrina nacional, implementando técnicas, tácticas y procedimientos que faciliten la acción combinada de la Guerra Electrónica y la Ciberguerra en los conflictos.

PALABRAS CLAVE: Guerra electrónica, ciberguerra, interacción, combate moderno

SUMÁRIO

1 **INTRODUÇÃO**

A Era da Informação tornou os ativos tecnológicos em ferramentas estratégicas para organizações e Estados-Nação, conferindo àqueles que os detém e deles se utilizam, efetiva e oportunamente, uma inquestionável vantagem no ambiente competitivo do sistema internacional e nos contenciosos interestatais. Visacro descreve uma visão geral da mudança da “Era Industrial” da humanidade, para a “Era da Informação”.

> A “revolução da informação” tornou antiquada e ineficaz a compreensão da guerra segundo a dinâmica das sociedades industriais. O fortalecimento da opinião pública, a onipresença dos órgãos de imprensa, a redução do controle estatal sobre as agências de notícias, o acesso irrestrito aos meios de comunicação de massa, a disseminação da informação digital em escala planetária, a globalização da informação e o alcance ilimitado das mídias sociais levaram a um achatamento dos níveis decisórios. Aquilo que até então fora claramente compartimentado, sobrepõem-se, agora, no tempo e no espaço. (VISACRO, 2018, p. 69)

Nessa conjuntura mundial, cada vez mais volátil, incerta, complexa e ambígua (VUCA), as mudanças são muito mais rápidas e influenciarão diretamente na tomada de decisão dos chefes e líderes. Tal afirmação pode ser observada no texto de Bennett e Lemoine, que retrata a magnitude desse ambiente.

> Mudanças voláteis são frequentes e causam instabilidade; mudanças incertas são aquelas sobre as quais os líderes não têm informação completa; mudanças complexas são confusas devido à interconectividade de variáveis, processos e informações; enquanto mudanças ambíguas dificultam a análise precisa de um determinado evento ou cenário, gerando a possibilidade de diferentes interpretações (BENNETT e LEMOINE, 2014)

Verifica-se que após a 2ª Guerra Mundial houve uma intensificação no processo de desenvolvimento tecnológico em todo o Mundo, muito pelo avanço da globalização, configurando um novo domínio para soberania do Estado, o qual pode ser denominado como espaço eletromagnético cibernético.

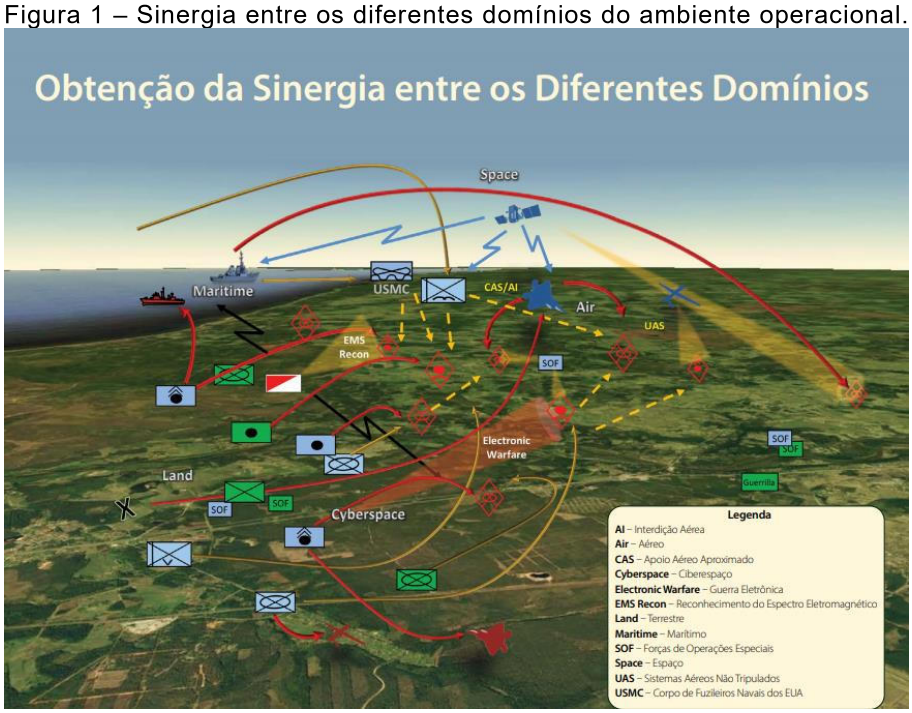
Nesse sentido, atores estatais e não estatais investem recursos para proteger seu acesso ao espectro eletromagnético e ao espaço cibernético, bem como para interromper ou negar o acesso a outras pessoas. O uso dessas capacidades tem o potencial de degradar o poder de combate das forças oponentes e a superar a inferioridade tecnológica dos armamentos, conforme

exemplifica o General de Exército (Gen Ex) David G. Perkins, do Exército dos EUA.

> Para se oporem à nossa rede de comunicações de última geração, eles podem violar, abalar ou negar nossas garantias, por meio de um grupo bem-organizado de hackers, que ataquem alvos deliberadamente selecionados com base em Inteligência e em conformidade com um plano de manobra mais amplo — executando todas essas ações fora da área de operações. (PERKINS, 2018, p. 5).

Sendo assim, os conflitos armados no Século (Sec) XXI não envolvem somente o combate entre oponentes armados e claramente definidos. O campo de batalha, que antes era linear e previsível, agrega agora uma multiplicidade de atores, sistemas e ambientes operacionais, combinados em um cenário de combate de alta intensidade, presentes em ações descentralizadas ou não convencionais, de forma simultânea ou sucessiva, conjugando diversas operações militares, ilustrados na figura 1, do General de Exército (Gen Ex) dos Estados Unidos da América (EUA) David G. Perkins.

Figura 1 – Sinergia entre os diferentes domínios do ambiente operacional.



Fonte: Gen Ex David G. Perkins, Exército dos EUA.

Além disso, a busca incessante pela superioridade das informações na Área de Operações concederá a liberdade de ação necessária para o sucesso da missão. Isso se deve pelo novo conceito de “Guerra Híbrida”, cujo cenário é a presença no campo de batalha de uma diversidade de atores e a combinação de várias tecnologias e táticas, caracterizando a tendência do combate

moderno. Mattis e Hoffman (2005) descrevem a Guerra Híbrida da seguinte forma:

> O conceito mais utilizado atualmente é aquele que definiram como uma nova forma de combater: a Guerra Híbrida. Em seu artigo publicado em 2005, *Future Warfare: The rise of Hybrid Wars*, os autores alertavam que a superioridade dos Estados Unidos criaria uma lógica que estimularia os outros atores estatais e não estatais a buscar uma capacidade ou algum tipo de combinação de tecnologias e táticas para obtenção de vantagens sobre o oponente, abandonando o modo tradicional de fazer guerra. (MATTIS E HOFFMAN, 2005)

Assim, as operações de amplo espectro e multidomínios, em um ambiente caracterizado por inúmeras ameaças, demandará dos comandantes, em todos os níveis e escalões, ampla flexibilidade de planejamento e emprego de meios cada vez mais complexos. Desse modo, empregada adequadamente e de forma combinada, a guerra eletrônica e a guerra cibernética se constituem como importantes fatores multiplicadores do poder de combate nos conflitos atuais.

Um exemplo é o ataque aéreo de Israel sobre a Síria, descrita pelos autores Richard A. Clark e Robert Knake, na obra "*Cyber War: the next threat to national security and what to do about it*". Ele menciona que o exército israelense, utilizando-se de técnicas operacionais norte-americanas, pode ter usado drones para sobrevoar as defesas antiaéreas sírias emitindo sinais com informações capazes de iludir os computadores que estavam interligados aos radares, impedindo que fossem detectados antes do ataque. Nesse caso, pode-se observar que há uma atividade no espaço eletromagnético com efeitos no espaço cibernético, elevando o grau de degradação das capacidades do oponente.

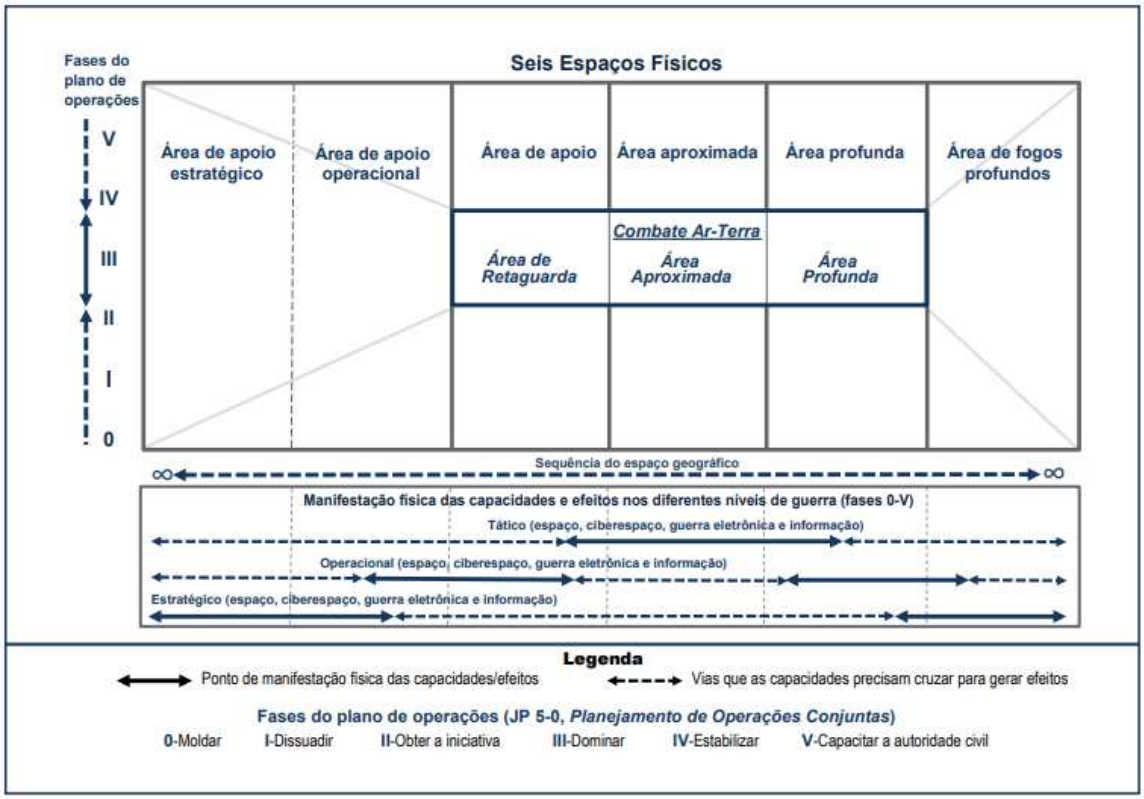
Observando o Manual do Ministério da Defesa (MD), A Guerra Eletrônica na Força Terrestre, 2019, observa-se que ao empregar capacidades de ciberespaço e espectro eletromagnético como um sistema integrado, atuando como um multiplicador do poder de combate, há melhores condições do comandante de alcançar os efeitos operacionais desejados. Esses sistemas fornecem pontos de presença significativos no campo de batalha e podem ser usados como plataformas para combates de precisão, agregando capacidades ofensivas e defensivas para o êxito das operações.

> Concomitante à evolução doutrinária e tecnológica da Força Terrestre, a guerra eletrônica tem se atualizado de forma contínua, atuando conjuntamente à guerra cibernética, adaptando-se aos novos rigores e exigências do combate moderno. (BRASIL, 2019)

Apesar de haver similitudes no emprego dessas capacidades operativas, existem pontos de sobreposição e até de lacunas doutrinárias que por vezes dificultam o planejamento das ações militares. Diante desse fato, diversas nações vêm desenvolvendo táticas, técnicas e procedimentos inovadores, a fim de garantir a eficiência operacional desejada.

Nos EUA, uma das formas de interação da GE e da G Ciber é a *Cyber Electromagnetic Activities* (CEMA), que conduz as operações no ciberespaço, em redes de informações, ataque eletrônico, exploração e proteção, inteligência e operações de informações, dentre outras atividades, visando se adequar aos desafios apresentados pelo combate moderno, conforme demonstrado na figura 2.

Figura 2 - Versão Preliminar da Estrutura do Campo de Batalha Comparada à do Combate Ar-Terra.



Fonte: Gen Ex David G. Perkins, Exército dos EUA.

Dessa forma, o presente trabalho busca analisar as formas de interação da GE e G Ciber no Brasil e nos EUA, considerando as peculiaridades de emprego dessas capacidades no combate moderno do Sec XXI, a fim de concluir sobre os possíveis benefícios para a Força Terrestre do Brasil.

1.1 PROBLEMA

As atividades de Guerra Eletrônica (GE) e Guerra Cibernética (G Ciber) são relativamente recentes no âmbito do Exército Brasileiro. O emprego dessas capacidades ocorre, por vezes, em ações isoladas e descentralizadas. Em outros momentos elas se confundem, como é o caso de ações em redes wifi, que podem empregar tanto meios de GE, como de G Ciber.

Nesse sentido, verificar a interação dessas duas capacidades nos EUA, país que possui uma bagagem no emprego operacional e doutrinária a mais tempo, comparando-a ao modelo adotado no Brasil, poderá servir de parâmetro para o aprofundamento doutrinário nacional.

Dessa forma, a pergunta a ser respondida é: em que medida o modelo norte-americano de organização e emprego da Guerra Eletrônica e Cibernética pode ser utilizado no Brasil, a fim de diminuir as lacunas de interação entre essas capacidades no âmbito do Exército Brasileiro?

1.2 OBJETIVOS

1.2.1 Objetivo geral

Segundo Lakatos e Marconi, 2017, toda pesquisa deve ter um objetivo determinado para saber o que se vai procurar e o que se pretende alcançar. Torna explícito o problema, aumentando o conhecimento sobre determinado assunto, podendo ser gerais ou específicos. Os objetivos podem definir a natureza do trabalho, o tipo de problema a ser selecionado e o material a coletar.

Assim, para que se pudesse responder o problema elencado para este estudo, segue-se o seguinte objetivo geral: Comparar as formas de interação da GE e G Ciber do Exército dos EUA com a forma de interação da GE e G Ciber do Exército Brasileiro (EB), considerando as peculiaridades de emprego dessas capacidades no combate moderno do Sec XXI, concluindo sobre os possíveis benefícios para a Força Terrestre do Brasil.

1.2.2 Objetivos específicos

Conforme conceito apresentado por Lakatos e Marconi, os objetivos específicos apresentam um caráter mais concreto sobre o tema de estudo. Têm função intermediária e instrumental, permitindo, de um lado, atingir o objetivo geral e, de outro, aplicá-lo a situações particulares. Desse modo, para atingir o objetivo geral elencado, foram estipulados os seguintes objetivos específicos:

a. Caracterizar o combate moderno;

b. Analisar a interação da GE e G Ciber no Brasil;

c. Analisar a interação da GE e G Ciber nos EUA; e

d. Comparar a interação da GE e G Ciber do EB com a do Exército dos EUA.

1.3 DELIMITAÇÃO DO ESTUDO

O presente estudo está limitado no espaço pela interação da GE e G Ciber no Brasil e nos EUA, considerando as exigências do combate moderno. Além disso, quanto a limitação do tempo, esse estudo buscará estudar a doutrina e capacidades operativas adotadas pelos Exércitos brasileiro e norte-americano a partir do final do Sec XX, a fim de se ter uma visão atualizada do combate moderno no Sec XXI.

1.4 RELEVÂNCIA DO ESTUDO

A Teoria Geopolítica da Incerteza ou da Turbulência previa uma desordem mundial, caracterizada pelo surgimento de novas ameaças, como a pirataria, o narcotráfico, o terrorismo, crimes ambientais (derramamento de petróleo), pesca ilegal e predatória, ataques cibernéticos e etc, que ocorreriam no mundo, contribuindo para os desafios a serem superados pelos Estados na defesa da soberania no Sec XXI.

> De acordo com a teoria da geopolítica contemporânea da Incerteza, após a decorrada da União Soviética das Repúblicas Soviéticas (URSS), em 1991, e o fim do conflito Leste-Oeste, período conhecido como Guerra Fria, em que os Estados Unidos da América e a URSS disputaram a hegemonia mundial, não haveria a esperada ordem mundial Norte-Sul, mas uma “desordem mundial” que poderá durar até 03 decadas. (MAFRA, 2007)

O termo ameaça pode ser definido de acordo com o Glossário das Forças Armadas:

> 1. É qualquer conjunção de atores, entidades ou forças com intenção e capacidade de, explorando deficiências e vulnerabilidades, realizar ação hostil contra o país e seus interesses nacionais, com possibilidades de causar danos ou comprometer a sociedade nacional (a população e seus valores materiais e culturais) e seu patrimônio (território, instalações, áreas

> sob jurisdição nacional e o conjunto das informações de seu interesse). Ameaças ao país e a seus interesses nacionais também podem ocorrer na forma de eventos não intencionais (naturais ou provocados pelo homem). 2. São atos ou tentativas potencialmente capazes de comprometer a preservação da ordem pública ou ameaçar a incolumidade das pessoas e do patrimônio. (BRASIL, 2015)

Outrossim, as guerras e conflitos armados da Era da Informação não estão mais restritos a teatros de operações bem delimitados e inimigos facilmente identificáveis e distinguíveis. Esses inimigos podem ser tanto Estados, quanto organizações não estatais, terroristas, organizações criminosas ou mesmo indivíduos isolados, não se limitando a dimensão física, como apontado por Visacro, 2018.

> Torna-se imperativo, portanto, reconhecer que o campo de batalha, na Era da Informação, não se restringe apenas à sua dimensão física, pois incorpora também uma dimensão humana e outra informacional. Na verdade, a disputa travada no âmbito dessas duas últimas dimensões tem se sobreposto, em importância, ao tradicional enfrentamento no domínio físico. (VISACRO, 2018, p. 115)

Diante desse cenário, ao final da pesquisa espera-se identificar capacidades, técnicas, táticas e procedimentos do exército norte-americano que possam servir de base para a inovação da doutrina nacional, no domínio da Guerra Cibernética e da Guerra Eletrônica, como forma de contribuir para a preparação do Exército na solução de problemas inéditos, face as ameaças do combate moderno desse Século.

2. REFERENCIAL TEÓRICO

2.1 Características do combate moderno

Muitos estudiosos da guerra vêm se aprofundando para descrever as características da guerra no Sec XXI. O cenário de incertezas dificulta ainda mais as previsões e tendências do mundo para as próximas décadas. Desse modo, o Comando de Doutrina e Preparação do Exército dos EUA (TRADOC) destaca as seguintes tendências globais:

> a. Acirramento de disputas geopolíticas entre estados antagônicos, assim como aquelas que envolvem atores não estatais;
> b. Competição por recursos naturais, especialmente, recursos hídricos;
> c. Mudanças climáticas;
> d. Alterações demográficas significativas;
> e. Urbanização incontida e ascendência das megacidades;
> f. Insatisfação com a globalização;
> g. Revitalização do nacionalismo;

h. Disparidades socioeconômicas persistentes;
i. Aumento da percepção dessas desigualdades;
j. Rápido desenvolvimento tecnológico;
k. Hiperconectividade digital; e
l. Surgimento de novos espaços contestados. (EUA, 2017)

Além disso, o crescimento acelerado de tecnologias e meios informacionais, que contribui para uma maior permeabilidade das fronteiras entre os Estados, resulta em um maior fluxo das informações entre as nações, muitas vezes em tempo real, o que reflete diretamente nos campos de batalha. A declaração de Charles K. Bartles, o General Valery Gerasimov, Chefe do Estado-Maior Geral russo, revela o seguinte entendimento sobre os conflitos no Sec XXI:

> No século XXI, vemos uma tendência ao obscurecimento da linha divisória entre os estados de guerra e de paz. O emprego de ações assimétricas foi amplamente difundido, possibilitando a neutralização das vantagens de um inimigo em conflitos armados. Entre tais ações estão o uso de forças de operações especiais e da oposição interna para criar uma frente em operação permanente em todo o território do Estado inimigo e ações, dispositivos e meios informacionais em contínuo aperfeiçoamento. (BARTLES, 2016)

Pode-se dizer, então, que o campo de batalha no combate moderno será cada vez mais dinâmico, devido o advento dessas novas tecnologias. Nesse viés, a guerra na Era da Informação coloca a dimensão humana e informacional em um elevado grau de importância, como mencionado por Visacro, 2018, em seu livro “A Guerra na Era da Informação”:

> Torna-se imperativo, portanto, reconhecer que o campo de batalha, na Era da Informação, não se restringe apenas à sua dimensão física, pois incorpora também uma dimensão humana e outra informacional. Na verdade, a disputa travada no âmbito dessas duas últimas dimensões tem se sobreposto, em importância, ao tradicional enfrentamento no domínio físico. (VISACRO, 2018, p. 115)

Uma outra tendência do combate moderno é atuar no ambiente operacional VUCA (Vulnerável, Incerto, Complexo e Ambíguo), com atores estatais e não-estatais capazes de interferir em todos os domínios, além do emprego de armamentos letais e não-letais, tropas regulares e irregulares, operações de guerra e não-guerra, dentre outros fatores que exigirão a adequação das estratégias militares. O Gen Ex David G. Perkins, Exército dos EUA faz a seguinte afirmação em relação ao ambiente operacional no futuro:

> O ambiente operacional será definido por um inimigo que desafiará nossa (Exército dos EUA) capacidade de manter a liberdade de manobra e superioridade nos domínios aéreo, cibernético, terrestre, marítimo e espacial e no espectro eletromagnético. (PERKINS, 2018)

Além disso, a guerra moderna e de múltiplos domínios amplia a ênfase nas operações de informações, que se inicia antes mesmo do emprego das armas. O trecho do documento do TRADOC a seguir evidencia essa característica:

> A batalha da informação será travada com ideias e narrativas bem trabalhadas, combinadas com atividades cibernéticas de alcance global, guerra eletrônica, operações de informação e ferramentas de guerra psicológica. Coerção através da dimensão cognitiva não é apenas possível, mas muitas vezes é o primeiro e decisivo recurso em um conflito, além de se manter como uma atividade permanente entre duas potências antagônicas. Empregar as operações de informação para vencer a guerra antes de travar a batalha tornar-se-á um imperativo e as forças terrestres precisarão contribuir para manipular a percepção na dimensão cognitiva como uma das atividades centrais das operações militares. (EUA, 2019)

Corroborando com esse argumento, a Diretriz do Comandante do Exército também ressalta as perspectivas futuras sobre os conflitos militares, cujas transformações continuarão sendo bastante significativas. O desenvolvimento de novas tecnologias apresentará novos desafios a serem superados pela Força Terrestre, como pode ser comprovado na citação abaixo:

> As transformações, por certo, continuarão a ser significativas. O desenvolvimento de tecnologias impactantes sofrerá nova aceleração, especialmente em meios militares para a defesa nacional. Novos métodos serão incorporados ao caráter da guerra. Temas inéditos ganharão relevância. Os desafios serão ainda mais diversos, exigindo flexibilidade e adaptação, para que o Exército esteja pronto a proteger os interesses maiores do Estado Brasileiro. O Processo de Transformação do Exército deve resultar em um efetivo aprimoramento da Força em seus diversos sistemas, possibilitando melhores condições para enfrentar os desafios do futuro, que, em sua essência, é incerto e difuso. (GOMES, 2022)

Ainda, reforçando a importância do ambiente informacional, verifica-se no artigo da *Military Review* do autor James Derleth, “Guerra de Nova Geração Russa - Dissuasão e vitória no nível tático”, 2021, o entendimento da concepção dos líderes militares russos para o combate moderno, o qual tem sido atestado nas ações recentes das operações da Rússia na Guerra da Ucrânia.

> Os líderes militares russos acreditam que os combates decisivos de um conflito estão na dimensão informacional e que as operações de informação nas fases iniciais são mais decisivas do que o combate convencional posterior. (DERLETH, 2021)

Desse modo, observa-se que o espaço cibernético e eletromagnético são cada vez mais relevantes no combate moderno, pois além de fornecer a possibilidade de forças mais fracas se sobreporem a exércitos mais bem

equipados e com maior poder de fogo, pode se tornar uma grande vantagem estratégica e operacional nos conflitos.

Como conclusão parcial, infere-se que o combate moderno está inserido no contexto de um mundo em transformações, cada vez mais conectado e com crescente evolução tecnológica, cujo cenário prospectivo pode ser representado pelo acrônimo VUCA. Nesse interim, atores estatais e não estatais são capazes de interferir nos conflitos, aumentando o valor do domínio informacional no ambiente operacional e por conseguinte das capacidades de GE e G Ciber no planejamento e condução das operações militares.

2.2 A GE e G Ciber no Exército brasileiro (EB)

A GE e a G Ciber atuam no espaço eletromagnético e cibernético, que integram o domínio informacional do combate. Sobre esse domínio, a Política Nacional de Defesa (PND) realiza uma prospecção no intuito de guiar a preparação e as estratégias pertinentes contra essas ameaças, sejam estatais ou não estatais, observada no trecho abaixo:

> Em relação a sistemas de informações, de gerenciamento e de comunicações, tornar-se-ão mais frequentes os acessos indesejados, inclusive com eventuais bloqueios do fluxo de informações de interesse nacional, capazes de expor ou paralisar atividades vitais para o funcionamento das instituições do País. No campo militar, esses acessos poderão afetar, ou mesmo inviabilizar, operações militares, em face da dificuldade ou da impossibilidade de se exercerem as ações de Comando, Controle e Inteligência. (BRASIL, 2012)

Complementando a PND, a Estratégia Nacional de Defesa (END) estabelece os mecanismos para que os objetivos elencados sejam alcançados, orientando os segmentos do Estado brasileiro quanto às medidas que devem ser implementadas. Cabe destacar a estratégia de possuir capacidade de projeção de poder, a qual poderá ser viabilizado por meio dos projetos estratégicos do Exército, dentre eles os vetores de transformação relacionados ao setor da GE e da G Ciber, conforme descrito a seguir:

> Dos sistemas indutores da transformação, alguns colaboram diretamente para a capacidade de dissuasão, em conjunto com as demais Forças Singulares. O Sistema Integrado de Monitoramento de Fronteira – SISFRON, o Sistema de Mísseis e Foguetes, o Sistema de Defesa Antiaérea, o Sistema de Defesa Cibernética e a Mecanização do Exército atuam por meio do incremento da mobilidade, da atividade de monitoramento e controle das fronteiras e da capacidade de atuar na

> negação de acesso indesejado a áreas ou a sistemas estratégicos de interesse da Defesa Nacional. (BRASIL, 2012)

Ainda, é importante mencionar algumas características visualizadas pelo EB sobre o ambiente operacional dos futuros conflitos, constante do Manual EB20-MF-10.101 Fundamentos do Exército Brasileiro, 1ª Edição, 2014:

> - Um ambiente no teatro de operações, redefinido por extensa rede de sensores e de fluxo de dados seguros, centrada no comandante, que proporcionam vantagens decisivas ao que melhor integrar, analisar, difundir e utilizar com oportunidade a informação relevante.
> - O incremento nas capacidades de atuar no espaço cibernético com liberdade de ação, de usar Sistemas Remotamente Pilotados (SRP) e de utilizar munições inteligentes. (BRASIL, 2014)

Por sua vez, a fim de mitigar as ameaças provenientes do combate moderno, o Estado Maior do Exército, Órgãos de Direção Setorial e Comandos Militares de Área constituíram uma equipe multidisciplinar para mapear as capacidades militares terrestres e operativas do Exército na atuação em um amplo espectro dos conflitos nas próximas décadas, materializado no Catálogo de Capacidades do Exército 2015-2035. Dentre elas, a Guerra Eletrônica e a Guerra Cibernética se enquadram nas seguintes capacidades:

> a. **CO16. Consciência Situacional** - ser capaz de proporcionar em todos os níveis de decisão, em tempo real, a compreensão, a interação do ambiente operacional e a percepção sobre a situação das tropas amigas e dos oponentes.
> b. **CO30. Segurança das informações e Comunicações** - ser capaz de fornecer proteção adequada, mantendo a integridade e a disponibilidade dos sistemas e das informações armazenadas, processadas ou transmitidas, por meio da implementação de medidas adequadas para viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações.
> c. **CO31. Guerra Eletrônica** - ser capaz de desempenhar atividades que visam a desenvolver e a assegurar o emprego eficiente das emissões eletromagnéticas próprias, ao mesmo tempo em que buscam impedir, dificultar ou tirar proveito das emissões inimigas, proporcionando a segurança, liberdade de ação e o êxito no espaço de batalha.
> d. **CO34. Inteligência** - ser capaz de proporcionar os conhecimentos necessários para apoiar os processos decisórios e para a proteção dos ativos da Força.
> e. **CO35 Exploração Cibernética** - ser capaz de conduzir 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.
> f. **CO36 Proteção Cibernética** - ser capaz 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.
> g. **CO37 Ataque Cibernético** - 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. (BRASIL, 2015)

Nesse sentido, o Comando de Operações Terrestres aprovou o Manual de Campanha EB70-MC-10.341, LISTA DE TAREFAS FUNCIONAIS, 2016, o qual aborda a solução de problemas militares por meio de seis funções de combate, Comando e Controle (C²), Movimento e Manobra, Inteligência, Fogos, Logística e Proteção, considerando as atividades e tarefas executadas pelos diversos sistemas e elementos operativos da Força Terrestre.

Assim como nas capacidades operativas, A GE e a G Ciber perpassam por essas diversas funções de combate. Abaixo estão algumas atividades das funções de combate que também estão relacionadas ao espaço eletromagnético e cibernético:

> a. **Comando e Controle** - Realizar a gestão do conhecimento e da informação.
> b. **Movimento e Manobra** - Executar manobra tática, apoio de fogo (não cinético) e apoio ao movimento e manobra.
> c. **Inteligência** - Produzir continuado conhecimento em apoio ao planejamento da Força, apoio a obtenção de consciência situacional, executar ações de aquisição de alvos, apoio a obtenção de superioridade de informações e apoio a busca de ameaças.
> d. **Fogos** - Executar fogos não cinéticos.
> e. **Proteção** - Adotar medidas de contrainteligência, aplicar medidas antiterroristas, realizar medidas de guerra eletrônica e de guerra cibernética. (BRASIL, 2016)

Tratando especificamente de GE, seu conceito é apresentado pelo Manual EB70-MC-10.247 A GUERRA ELETRÔNICA NAS OPERAÇÕES, 2020, o qual estabelece o seguinte:

> A GE é um conjunto de ações que visam a explorar as emissões do inimigo em toda a faixa do Espectro Eletromagnético (Ept Eltmg), 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, 2020)

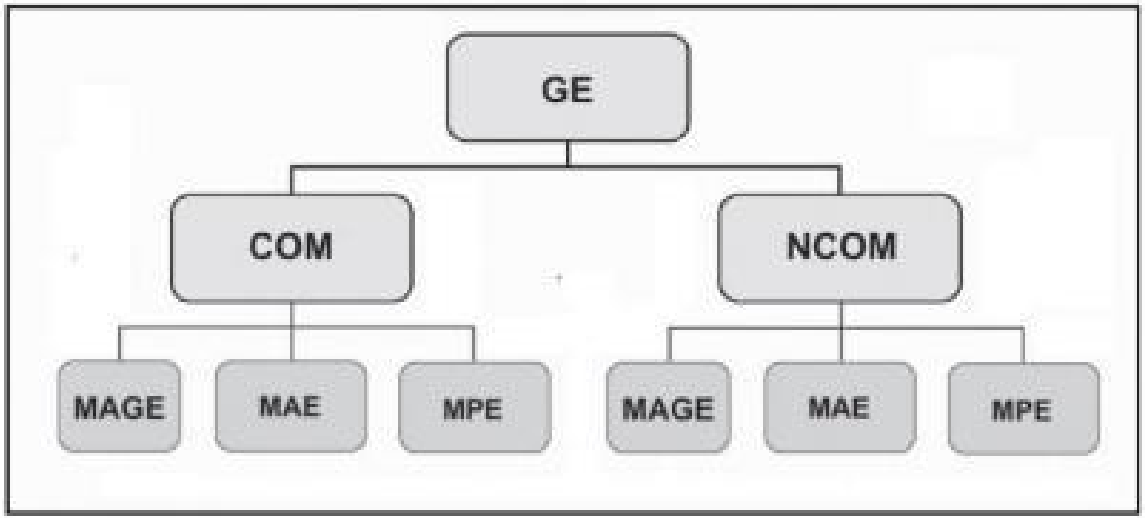
Nesse viés, as atividades de GE se desenvolvem em dois campos, o das Comunicações (Com) e o das Não Comunicações (N Com). O primeiro enquadra as emissões de sinais eletromagnéticos e equipamentos destinados a transmissão de informações, como o equipamento rádio tático, enquanto o segundo está voltado para a produção de informações, como o radar de vigilância terrestre (BRASIL, 2020). A Figura 3 ilustra alguns exemplos desses dois campos de atuação.

Figura 3 – Campo das Com (à esquerda) e Campo das N Com (à direita).

Fonte: Manual EB70-MC-10.247, 2020.

O Manual supramencionado também apresenta os ramos que integram cada campo de atuação da GE: As Medidas de Ataque Eletrônico (MAE), de natureza ativa, que degradar a capacidade de combate do oponente, as Medidas de Apoio de GE (MAGE), de natureza passiva, que objetivam a obtenção e análise de dados oriundas do oponente e as Medidas de Proteção Eletrônica (MPE), 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.

Figura 4 - Ramos de atuação da GE dentro de seus respectivos campos.



Fonte: Manual EB70-MC-10.247, 2020.

Na Força Terrestre, as Organizações vocacionadas para as atividades de GE são aquelas que integram o Sistema de Guerra Eletrônica do Exército (SIGELEx), composto pelo Grupamento de Comunicações e Eletrônica (GCE), pelo Batalhão de Guerra Eletrônica (BGE), Batalhão de Comunicações e Guerra

Eletrônica (B Com GE) e CM/CRM (Centro de Monitoramento e Centro Regional de Monitoramento). O apoio de GE pode ser identificado no Quadro a seguir:

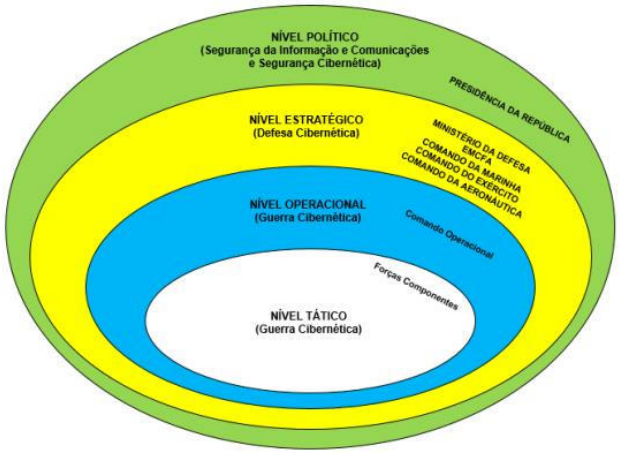
Quadro 1 Organizações e Respectivas Atividades de GE

Comando Operativo	OM GE		Atividades de GE		
			MAE	MAGE	MPE
Corpo de Exército / FTC	CCOMGEX / GCE	BGE	x	x	X
		B Com GE	x	x	x
		Centro de Monitoramento (CM)	-	x	x
Divisão de Exército	B Com GE		x	x	x
Brigada	Não possui OM GE orgânica		-	-	x
U/SU	Não possui OM GE orgânica		-	-	x

Fonte: EB70-MC-10.201 - Guerra Eletrônica na FT, 2019.

No que se refere a doutrina do EB sobre G Ciber, o Manual EB70-MC-10.232 Guerra Cibernética, 2017, atribui a essa capacidade como fator multiplicador do poder de combate, haja vista seu caráter eminentemente transversal. Para tanto, a G Ciber está dividida em dois campos distintos: a segurança cibernética, a cargo do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), e a defesa cibernética, a cargo do MD, conforme observado na Figura 5 a seguir.

Figura 5 Níveis de Decisão



Fonte: EB70-MC-10.232 Guerra Cibernética, 2017

Além disso, o Catálogo de Capacidades do Exército, 2015, ressalta essa capacidade e considera que o EB deve ser capaz de realizar ações de ataque, de

exploração e de proteção cibernética. Tal Catálogo orienta, como capacidades operativas de cibernética, o que se segue:

> - Conduzir busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados (Exploração Cibernética);
> - 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 (Proteção Cibernética); e
> - 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 (Ataque Cibernético). (BRASIL, 2015)

Para realizar as ações do nível tático mencionado, quando ativado, o EB dispõe de uma estrutura militar de defesa cibernética, conforme o quadro abaixo:

Quadro 2 Estruturas operativas de G Ciber, suas atividades cibernéticas e 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	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM.

Fonte: EB70-MC-10.232 Guerra Cibernética, 2017

Também, pode ser observado como atividades e tarefas correspondentes a G Ciber, dentre outras, as previstas no Manual EB70-MC-10.232 Guerra Cibernética, 2017:

> a. Consciência Situacional - Monitorar sistematicamente o espaço cibernético de interesse do EB no tocante à possibilidade de concretização de ameaça, de modo a estar em condições de decidir e aplicar as ações requeridas conforme as condições do espaço cibernético;
> b. Defesa Ativa - Detectar, identificar, avaliar e neutralizar vulnerabilidades nas redes de computadores e sistemas de informação em uso pelo EB, antes que elas sejam exploradas. Mediante ordem, desencadear ações ofensivas contra a fonte da ameaça, mesmo que localizada fora do espaço cibernético defendido
> c. Pronta Resposta - Reagir prontamente às ameaças identificadas, observando os diferentes níveis de alerta cibernético (grau de risco).
> d. Forense Digital - Coletar e examinar evidências digitais em redes e sistemas de informação de interesse do EB.
> e. Reconhecimento - Investigar em fontes abertas para obter informações sobre o alvo.
> f. Escaneamento (Scanning) - Encontrar falhas na proteção cibernética do alvo.
> g. Exploração da Vulnerabilidade - Realizar ações como: obter acesso, degradar uma aplicação ou negar acesso para outros usuários.
> h. Manutenção do acesso - Manipular software instalado no sistema alvo com objetivo de disponibilizar um backdoor para acesso futuro.
> i. Cobertura de rastros - Ocultar as ações realizadas no sistema alvo com objetivo de impedir ou dificultar que usuários e/ou administradores identifiquem as ações de um atacante.
> j. Inteligência Cibernética - Realizar ações de busca e de coleta de dados no espaço cibernético, para a produção do conhecimento de Inteligência. (BRASIL, 2017)

Assim, é cabível projetar que as capacidades operativas relacionadas a GE e G Ciber estarão cada vez mais presentes no ambiente operacional do combate moderno no Sec XXI, podendo agregar poder de combate a Força Terrestre face as ameaças do amplo espectro dos conflitos.

2.2.1 A interação entre GE e G Ciber no EB

Considerando as características do combate moderno e as tendências de maior velocidade das ações no campo de batalha, verifica-se a necessidade de se obter, mesmo que temporariamente, a superioridade de informação no teatro de operações, o que pode ser favorecida pelo emprego efetivo da interação entre a GE e da G Ciber. O Manual de Campanha EB20-MC-10.205 Comando e Controle, 2015, define superioridade de informação da seguinte forma:

> Superioridade de informação traduz-se por uma vantagem operativa derivada da habilidade de coletar, processar, disseminar, explorar e proteger um fluxo ininterrupto de informações aos comandantes em todos

> os níveis, ao mesmo em que se busca tirar proveito das informações do oponente ou negar-lhes essas habilidades. Isso significa possuir maior quantidade e melhor qualidade de informações do que o adversário sobre o ambiente operacional. Permite o controle da dimensão informacional (espectro eletromagnético, espaço cibernético e outros) por determinado tempo e lugar. (BRASIL, 2015)

Ademais, o emprego combinado de atuadores não cinéticos de GE e G Ciber são capazes de dissuadir ou até mesmo degradar a condição operativa dos exércitos, diminuindo o uso da força e os reflexos de uma ação mais intensa, principalmente na manutenção de uma opinião pública e internacional favorável. O Manual de EB70-MC-10.341 Lista de Tarefas Funcionais, 2016, corrobora com esse entendimento.

> ...os comandantes devem dar preferência às soluções que impliquem no menor emprego da força, resguardando as capacidades letais de sua tropa para as situações mais críticas. Capacidades não letais que possam dissuadir o oponente ou retirar-lhe a legitimidade das ações podem e devem ser exploradas, antes de optar-se pelo emprego de capacidades letais. (BRASIL, 2016)

Como observado, existem diversas atividades e tarefas que podem ser executadas pela GE ou pela G Ciber. Essa congruência pode levar a sobreposição das capacidades e até interferência na atuação desses meios, já que ambas podem fazer uso do espaço eletromagnético para realizarem suas atividades. É o caso das redes *wifi e bluetooth*, na qual podem ser utilizados para as ações dos dois atuadores.

Desse modo, mais importante do que atribuir a responsabilidade de atuação a um único meio, é criar condições durante o planejamento e condução das operações para o emprego combinado dos atuadores de GE e G Ciber, proporcionando maior poder de combate na obtenção do efeito esperado, conforme verificado no Manual EB70-MC-10.201 Guerra Eletrônica na Força Terrestre, 2019.

> Em qualquer nível de planejamento e condução das operações, deve haver constante integração entre a GE, a Inteligência de Sinais e a Guerra Cibernética, quer em situação de guerra ou de não guerra. (BRASIL, 2019)

Verifica-se, ainda, a interação da GE e G Ciber na estrutura organizacional do BGE e do B Com GE, considerando o nível tático e operacional do EB. Outra forma de combinação dessas capacidades é a possibilidade delas integrarem as células de funções de combate no Estado Maior das Divisões de Exército e na Força Terrestre Componente, no intuito de reunir as competências necessárias a

solução de qualquer problema militar que se apresente no cenário ao qual está inserido.

Segundo o Manual EB70-MC-10.341 Lista de Tarefas Funcionais, 2016, as funções de combate são: Comando e Controle, Movimento e Manobra, Inteligência, Fogos, Logística e Proteção, que serão evidenciadas a seguir.

2.2.2 GE e G Ciber na Função de Combate Comando e Controle

Segundo o Manual EB70-MC-10.341 Lista de Tarefas Funcionais, 2016, a função de combate Comando e Controle compreende as atividades que proporcionam o elo entre os escalões superiores e subordinados e as ferramentas necessárias para planejar, dirigir, coordenar e controlar os meios em operações militares.

Nesse viés, o processo decisório de um comandante está diretamente relacionado a essa função, no qual requer uma criteriosa seleção das informações para conseguir estabelecer uma consciência situacional mais próxima a realidade e favorecer o emprego adequado dos meios a sua disposição.

Dessa forma, a GE e G Ciber podem atuar na gestão do conhecimento para obter informações necessárias a construção do entendimento do ambiente operacional e da conjuntura interna e externa relacionada ao teatro de operações. O Manual EB20-MC-10.205 Comando e Controle, 2015, faz a seguinte consideração:

> O processo de tomada de decisão envolve a obtenção de dados, a conjugação de fatores intervenientes, a obtenção e a manutenção da consciência situacional, até a decisão propriamente dita.
> ...
> Para ter sucesso em operações terrestres, as atividades eletromagnéticas e cibernéticas devem ser integradas e sincronizadas em todos os escalões de comando e funções de combate. Os comandantes, apoiados por seus EM, integram as operações no ciberespaço e as operações no espectro eletromagnético (BRASIL, 2015)

O Manual de Campanha EB70-MC-10.255 Força Terrestre Componente determina que a chefia da Célula de Comando e Controle fica a cargo do E6 (Chefe da Seção de C2), no nível Divisão de Exército ou Força Terrestre Componente (FTC), ocasião em que se materializa a interação da GE e G Ciber, pois engloba elementos dessas duas atividades, como pode ser observado na figura abaixo.

Figura 6 Exemplo de Célula Funcional de Comando e Controle

Fonte: EB70-MC-10.255 Força Terrestre Componente

Dessa forma, a interação da GE com a G Ciber pode fornecer ao decisor informações sobre as capacidades do adversário, vulnerabilidades dos sistemas corporativos, impactos potenciais sobre a missão e sobre as forças amigas, os riscos associados com as ações realizadas no ciberespaço e no espectro eletromagnético, tudo a fim de proporcionar uma vantagem nos campos de batalha por meio da superioridade da informação.

2.2.3 GE e G Ciber na Função de Combate Movimento e Manobra

A função de combate Movimento e Manobra é definida como o conjunto de atividades, tarefas e sistemas inter-relacionados, empregados para deslocar forças, de modo a posicioná-las em situação de vantagem em relação às ameaças. (Brasil, 2016)

O emprego combinado da GE e G Ciber poderá apoiar o Movimento e Manobra agindo nos sistemas estratégicos e operacionais das tropas inimigas, causando a negação dos serviços que operam no espaço cibernético e eletromagnético ou até iludindo o oponente das reais intenções das forças amigas por meio de desinformação, ao mesmo tempo que busca proteger as infraestruturas necessárias a condução das operações.

Outra possibilidade é o levantamento da ordem de batalha do inimigo, explorada pelas ações de GE e G Ciber. Tal informação servirá para planejar o posicionamento mais eficaz das tropas, face as vulnerabilidades e fraquezas do oponente, o que corrobora com o Manual EB20-MC-10.203 Movimento e Manobra, 2015, que descreve a característica dessa função de combate:

> Caracteriza-se pela capacidade de deslocar ou dispor forças de forma a colocar o inimigo em desvantagem relativa e, assim, atingir os resultados que, de outra forma, seriam mais custosos em pessoal e material. Contribui para obter a superioridade, aproveitar o êxito alcançado e preservar a liberdade de ação, bem como para reduzir as próprias vulnerabilidades. Procura destruir a coesão inimiga por meio de variadas ações localizadas e inesperadas. (BRASIL, 2015)

2.2.4 GE e G Ciber na Função de Combate Inteligência

Conforme o Manual EB70-MC-10.341 Lista de Tarefas Funcionais, 2016, a função de combate Inteligência compreende o conjunto de atividades, tarefas e sistemas inter-relacionados empregados para assegurar compreensão sobre o ambiente operacional, as ameaças (atuais e potenciais), os oponentes, o terreno e as considerações civis.

Nesse sentido, o Manual EB20-MC-10.207 Inteligência esclarece o seguinte:

> No combate atual, a Inteligência não é empregada somente na mera descrição das forças militares oponentes e de suas capacidades de combate. Deve possibilitar, também, uma ampla compreensão dos agentes presentes no ambiente operacional: cultura, motivações, perspectivas, objetivos, aprovação popular e apoio que recebe ou pode receber. (BRASIL, 2015)

Dessa maneira, considerando os alvos selecionados pelos comandantes, a GE e G Ciber poderão realizar a coleta e busca de dados de potenciais ameaças ou adversários e a análise dos dados coletados no espaço cibernético e eletromagnético, no intuito de fornecer a compreensão mencionada.

2.2.5 GE e G Ciber na Função de Combate Fogos

A função de combate Fogos reúne as atividades, tarefas e sistemas inter-relacionados que permitem o emprego coletivo e coordenado de fogos cinéticos e

não cinéticos, orgânicos da Força ou conjuntos, integrados pelos processos de planejamento e coordenação de fogos. (BRASIL, 2016)

A GE e G Ciber estão enquadrados nos fogos não cinéticos e podem causar danos a equipamentos e estruturas físicas estratégicas por meio de emissão de energia direcionada (GE) ou alteração nos sistemas operados em redes que prejudiquem o seu funcionamento (G Ciber). O trecho abaixo do Manual EB20-MC10.206 Fogos apresenta a integração da GE e G Ciber na função de fogos.

> Nas operações conjuntas, as unidades devem possuir apoio de fogo adequado e preciso que forneça alcance operativo e mobilidade para a tropa e o comandante da Força. Para isso, os sistemas de fogos devem estar integrados, considerando os meios conjuntos e incorporando a defesa antiaérea e a capacidade de realizar ações eletrônicas e cibernéticas. (BRASIL, 2015)

Além disso, a exploração eletrônica e cibernética pode fornecer informações sobre alvos pretendidos, sejam eles cibernéticos ou não, contribuindo para a decisão de alvos compensadores para os fogos de artilharia, promovendo a economia de meios e a contenção de danos colaterais.

2.2.6 GE e G Ciber na Função de Combate Logística

O Manual EB70-MC-10.341 Lista de Tarefas Funcionais, 2016, define a função de combate Logística como o conjunto de atividades, tarefas e sistemas inter-relacionados para prover apoio e serviços, de modo a assegurar a liberdade de ação e proporcionar amplitude de alcance e de duração às operações. Engloba as Áreas Funcionais de apoio de material, apoio ao pessoal e apoio de saúde.

Para o apoio as tarefas da Logística, a GE e a G Ciber atuam para fornecer dados relacionados a possíveis ataques inimigos que possam impactar o suprimento e ressuprimento da tropa. Além disso, o fornecimento de equipamentos e a mobilização de pessoal são alguns exemplos da integração da capacidade cibernética e eletrônica à logística, viabilizando até mesmo o recrutamento de especialistas de instituições públicas e privadas, acadêmicas ou não, a fim de atuarem colaborativamente junto as forças amigas.

2.2.7 GE e G Ciber na Função de Combate Proteção

Conforme previsto no Manual EB70-MC-10.341 Lista de Tarefas Funcionais, 2016, a função de combate Proteção reúne o conjunto de atividades empregadas na preservação da força, permitindo que os comandantes disponham do máximo poder de combate para emprego. As tarefas permitem identificar, prevenir e mitigar ameaças às forças e aos meios vitais para as operações, de modo a preservar o poder de combate e a liberdade de ação. Permitem, também, preservar populações e infraestruturas críticas.

O Manual EB20-MC-10.208 Proteção descreve as formas de atuação da GE e da G Ciber em proveito dessa função de combate:

> A GE atuará em proveito da F Cmb Ptç executando medidas de proteção eletrônica (MPE) que garantirão o uso efetivo do espectro eletromagnético. As MPE se caracterizam pelo emprego de tecnologias disponíveis nos equipamentos de comunicações e procedimentos na exploração desses meios.
> A G Ciber atuará em proveito da F Cmb Ptç executando medidas de proteção cibernética (MPCiber) que garantirão o uso efetivo de redes de informação. As MPCiber se caracterizam pelo emprego de tecnologias nos hardwares, a utilização de aplicativos de segurança de rede e de procedimentos executados pelos respectivos operadores. (BRASIL, 2016)

Diante do exposto, observa-se que as atividades de GE e G Ciber podem auxiliar na seleção de alvos, dados e informações a serem protegidos, além de estabelecerem as medidas de proteção eletrônica e medidas de proteção cibernética a serem empregados em todos os escalões da força terrestre, incluindo a proteção de infraestruturas críticas nacionais.

Nesse sentido, a combinação das capacidades de GE e G Ciber é uma tática que potencializa os efeitos, seja na obtenção de uma consciência situacional mais precisa sobre o ambiente operacional, seja na conquista de um objetivo militar. Elas permitem que o decisor tenha um ciclo informacional mais ágil ao mesmo tempo que prejudica o do oponente.

Assim, conclui-se parcialmente que a atuação da GE e da G Ciber podem ser empregadas em conjunto para alcançar o efeito desejado em todas as funções de combate. Para tanto, esse emprego combinado das capacidades deve ser previsto e planejado dentro das Células ou Estados Maiores das Grandes Unidades ou Grandes Comandos, evitando a sobreposição de tarefas entre elas.

2.3 GE E G CIBER No Exército dos EUA

A doutrina norte-americana refere-se ao espaço cibernético como um dos cinco domínios da guerra e que utiliza uma parte do espectro eletromagnético para operações, como por exemplo, o uso da ferramenta Bluetooth, Wi-Fi ou transmissão por satélite, os quais apresentam a apresentam a convergência nos campos de atuação da GE e da G Ciber. Desse modo, a doutrina norte-americana estabelece que as operações eletromagnéticas e cibernéticas requerem uma gestão do espectro para prevenir e atenuar conflitos de frequências e interferência eletromagnética entre forças amigas durante as ações militares. (EUA, 2021)

Em uma análise do histórico recente das capacidades no domínio eletromagnético e cibernético das forças armadas dos EUA, verifica-se que em 2014 o Exército estabeleceu oficialmente a Arma de Cibernética, inaugurando o *Army Cyber Institute* e o *US Army Cyber Center of Excellence.* No ano de 2015, criou o curso de Operações do Ciberespaço para Líderes do Exército e o integrou ao ensino de nível intermediário. Em 2021, emitiu a última versão do manual de campanha *FM 3-12 Cyberspace And Electronic Warfare Operations*, que estabelece os fundamentos, capacidades e organização para o emprego de GE e G Ciber nas operações.

Cabe mencionar que os EUA são um dos principais países que entendem o espaço eletromagnético e cibernético como um único domínio, integrando as atividades de GE e de G Ciber em uma única célula (Cyber Electro Magnetic Activities - CEMA) do Estado Maior, subordinada diretamente ao Chefe do Estado Maior, conforme observa-se no Manual *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021, traduzido abaixo.

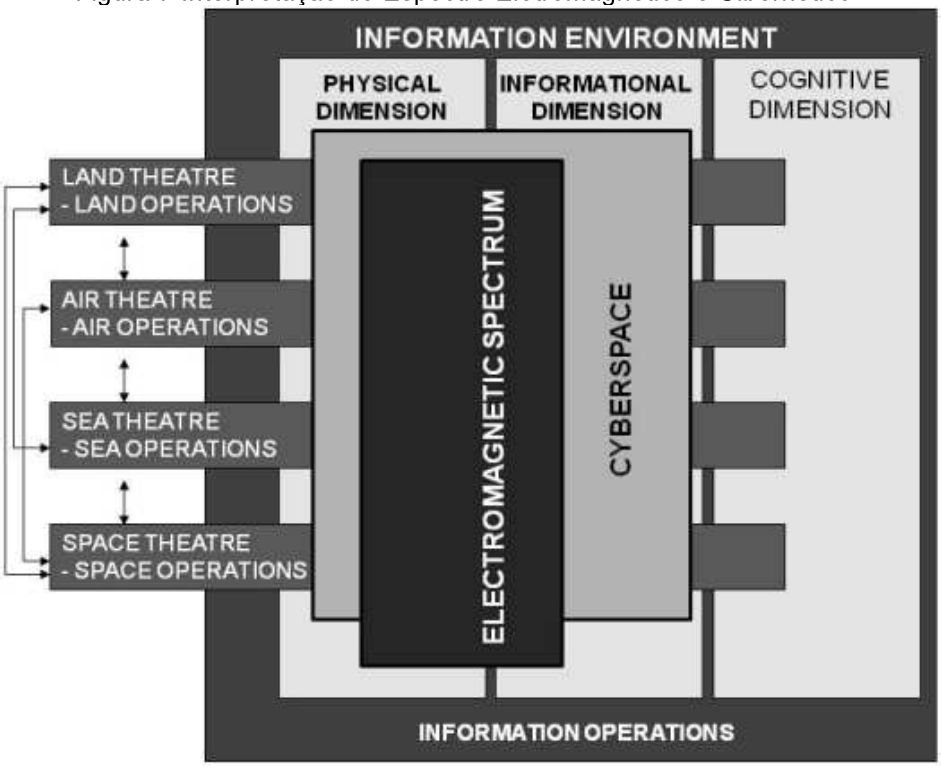
> As atividades eletromagnéticas cibernéticas (CEMA) é o processo de planejar, integrar e sincronizar operações de Guerra Eletrônica e Cibernética em apoio às operações terrestres combinadas. Por meio do CEMA, o Exército planeja, integra e sincroniza essas missões, apoia e habilita o sistema de comando da missão e fornece um recurso inter-relacionado para operações de informação e inteligência. (EUA, 2021, tradução do autor)

Conforme consta no Panfleto do Comando de Doutrina e Treinamento do Exército dos Estados Unidos (TRADOC) 525-8-6, 2018, as operações do ciberespaço e do espaço eletromagnético fornecem aos comandantes a

capacidade de conduzir manobras, simultâneas e vinculadas, através de vários domínios, além de enfrentar os futuros desafios do ambiente operacional.

Estudiosos norte-americanos enfatizam que com o incremento dos roteadores sem fio ou rádios táticos baseado em redes de computadores, o ciberespaço e o espectro eletromagnético agora formam um ambiente contínuo e coerente, formando um ambiente de informação específico fundamental às operações militares, igualmente importante aos domínios terrestre, aéreo, marítimo e espacial. A figura 6 ilustra esse ambiente.

Figura 7 Interpretação do Espectro Eletromagnético e Cibernético

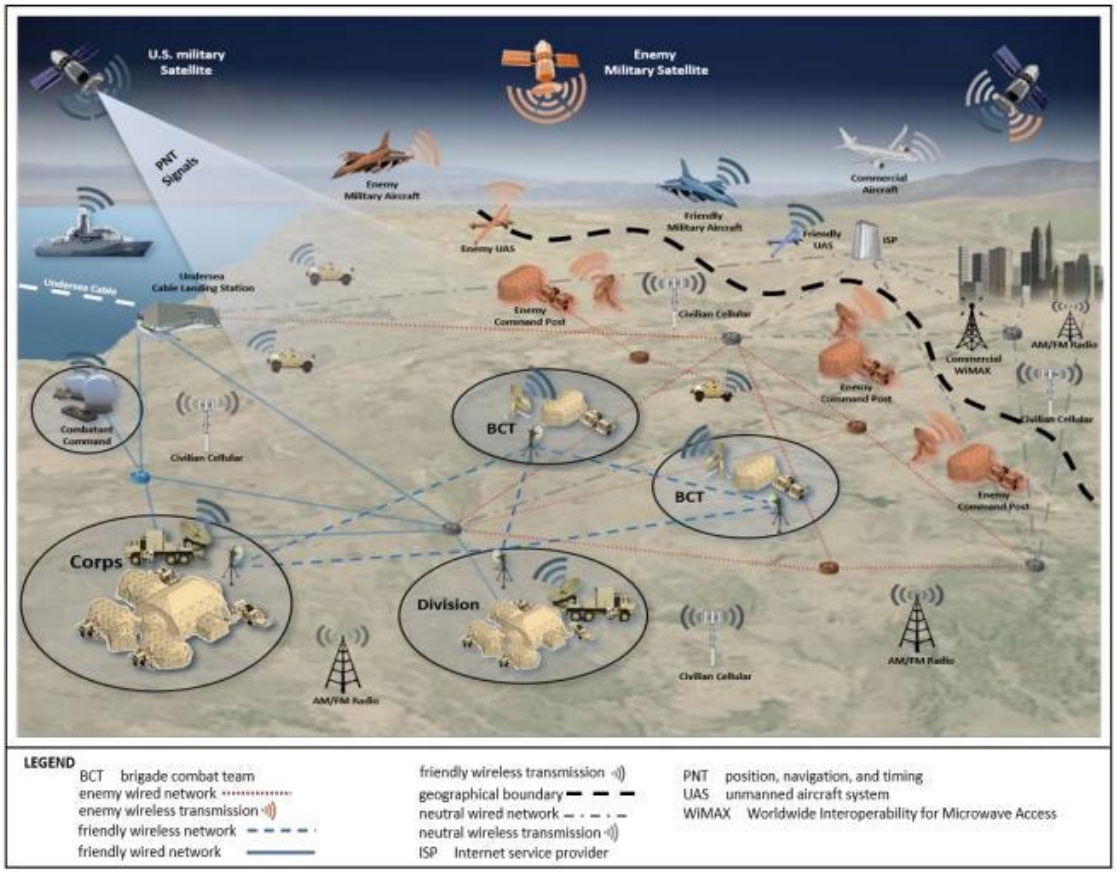


Fonte: Zsolt Haig, Faculdade de Ciências Militares e Formação de Oficiais

Ainda, o TRADOC 525-8-6 estabelece algumas premissas que norteiam as operações no ciberespaço: os conflitos serão mais complexos e terão maiores impactos em outros domínios, como sistemas políticos, econômicos, informacionais e culturais; as ações militares serão mais contestadas e congestionadas por uma quantidade crescente de rede de transmissões de dados; a comunicação será em sua maioria por redes sem fio, contribuindo para o aumento das vulnerabilidades.

Nesse sentido, o Manual *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021, demonstra na figura 7 o enquadramento do espectro eletromagnético e do ciberespaço em um ambiente operacional:

Figura 8 Visualização do ciberespaço e do espectro eletromagnético num ambiente operacional



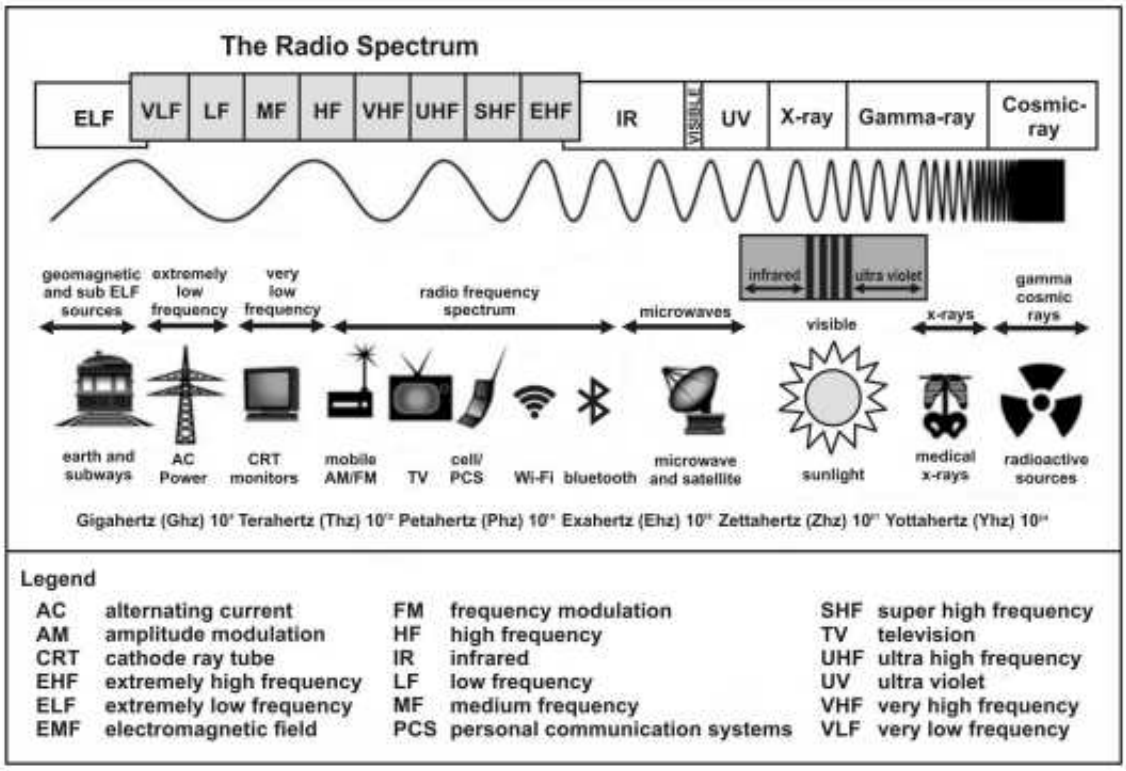
Fonte: Manual *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021

Tratando especificamente da GE, o Manual JP 3-13.1 Guerra Eletrônica, 2007, informa que as operações militares são executadas num ambiente de informação cada vez mais complexo devido a utilização do espectro eletromagnético em redes, tanto por organizações civis e militares, como por indivíduos de inteligência, de comunicações, de navegação, detecção, armazenamento e processamento de informação, assim como uma variedade de outros fins.

A capacidade de controlar o espectro eletromagnético é central para operações terrestres. Sendo a tecnologia da informação universalmente disponível, mais adversários confiam nas comunicações e redes de informática para tomar e implementar decisões. Os rádios continuam a ser a espinha dorsal dos militares tácticos de comando na missão. (EUA, 2018)

Além disso, a guerra eletrônica tem a função de utilizar a emissão de energia eletromagnética para controlar ou atacar pessoas, instalações ou equipamentos, com a intensão de degradar, neutralizar ou destruir a capacidade de combater, sendo considerado uma forma de apoio de fogos para interromper e aumentar o tempo de reação de tomada de decisão do inimigo. A figura abaixo exemplifica o espectro eletromagnético:

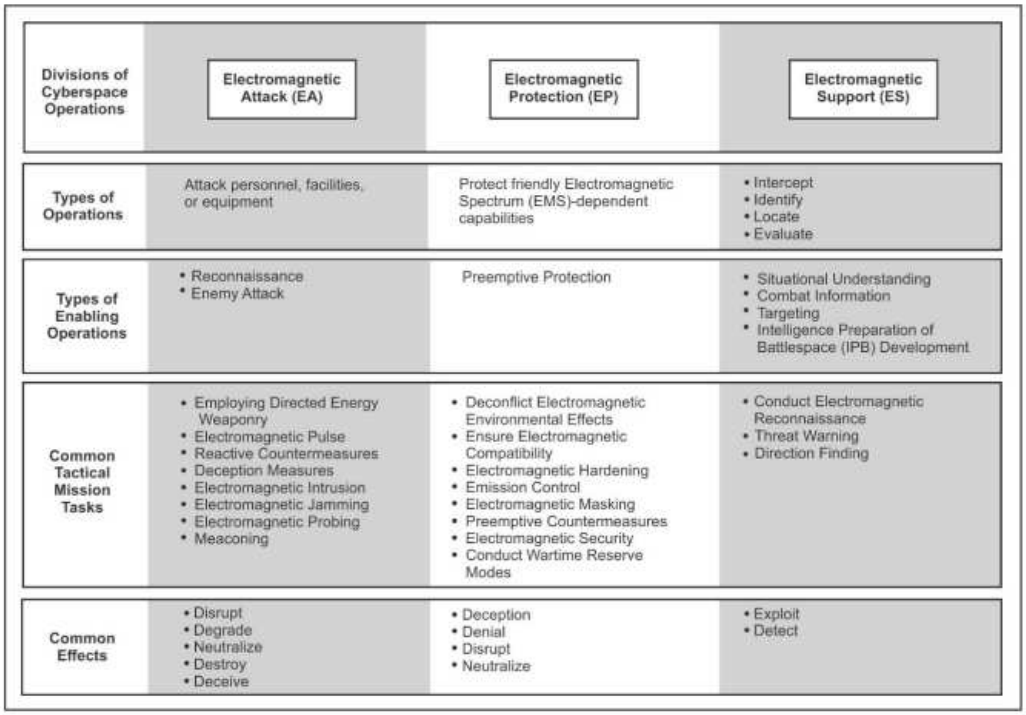
Figura 9 Espectro Eletromagnético



Fonte: *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021

Outro aspecto a considerar é o objetivo da GE, que segundo o Manual *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021, visa negar a vantagem do adversário no espaço eletromagnético, além de assegurar a liberdade de ação das próprias forças no ambiente informacional. As tarefas de GE podem apoiar as forças armadas na função de proteção, no desenvolvimento da consciência situacional e em ações contra comando e controle e demais meios de informação do inimigo. As capacidades de GE estão representadas na Fig 9 a seguir.

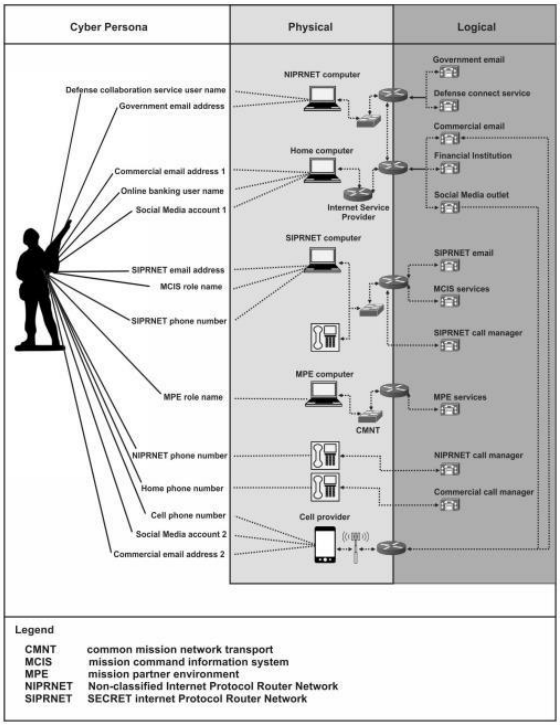
Figura 10 Capacidades de GE nos EUA



Fonte: *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021

Ao retratar as operações cibernéticas, pode-se dizer que as ações ocorrem em três camadas interdependentes do ciberespaço, a física, a lógica e a pessoal. Essa configuração está representada na Fig 10 abaixo.

Figura 11 Capacidades de GE nos EUA

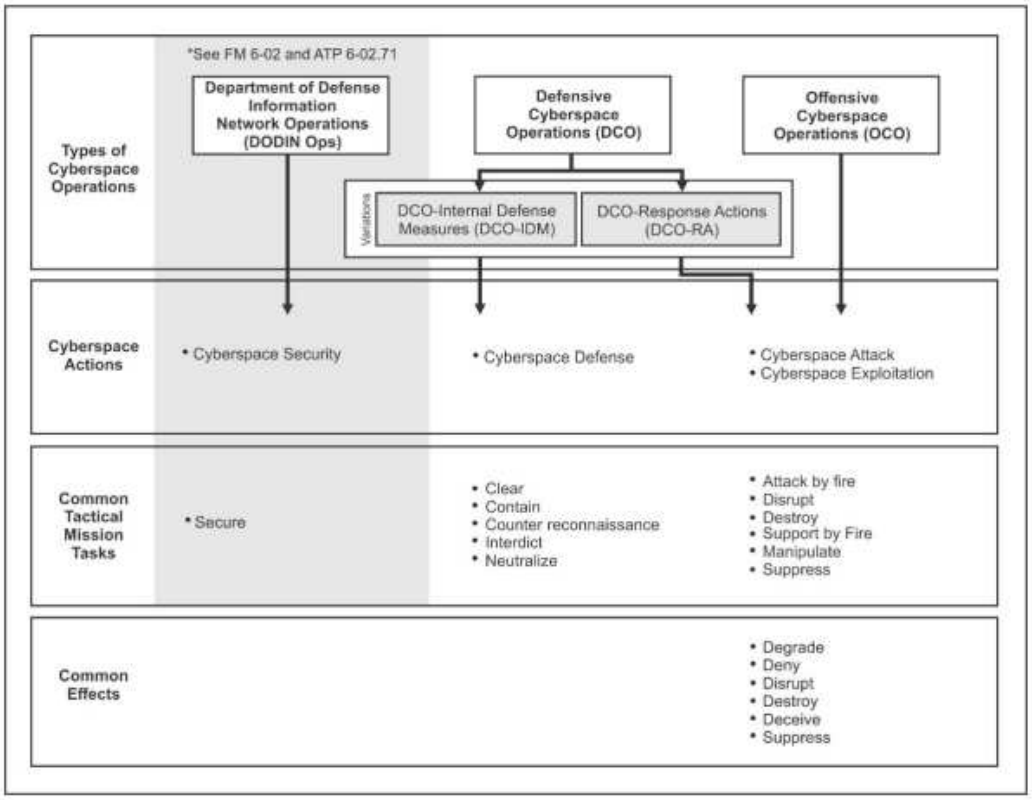


Fonte: *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021

Uma característica importante do ciberespaço, abordada na doutrina dos EUA, é que os sistemas de telecomunicações em rede operam usando o espectro eletromagnético e/ou conexão cabeada. Diferentes processos de gerenciamento de informações eletrônicas (coleta eletrônica de dados, processamento, armazenamento de dados, comunicação) estão acontecendo nesses sistemas. Sendo assim, a congruência das atividades de GE e G Ciber se tornam bem evidentes, justificando a concepção centralizada dessas capacidades.

Nesse sentido, os EUA estão organizados para operações cibernéticas, seja na área de segurança, ataque ou defesa cibernética, conforme a Fig 11 a seguir:

Figura 12 Operações no Espaço Cibernético



Fonte: *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021

A Convergência da GE e G Ciber nos EUA, como já mencionado, ocorre por meio do CEMA. Nessa Seção integram os oficiais de GE e de G Ciber, os técnicos em energia eletromagnética, o Sargento-Mor de GE e o gerente do espectro. Além do CEMA, outras organizações são responsáveis por atividades no espaço eletromagnético e cibernético:

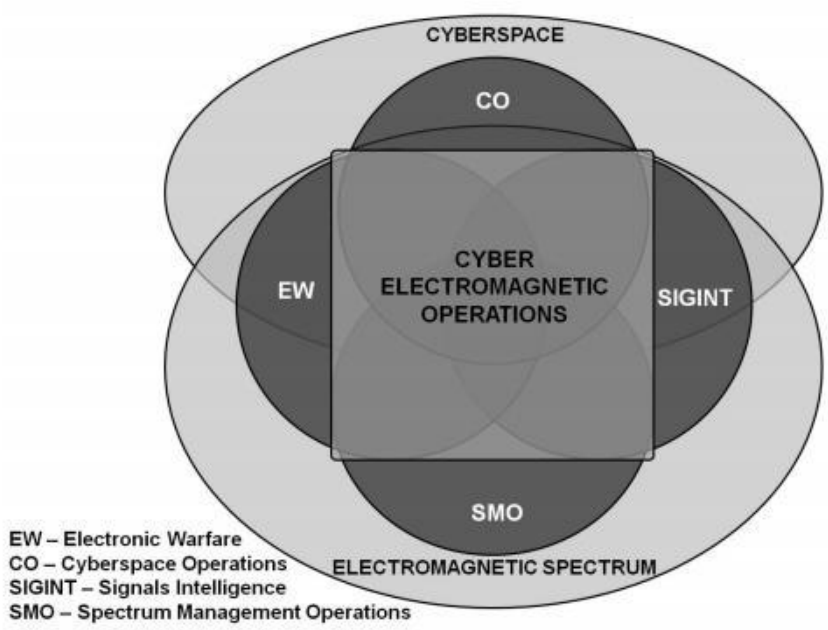
Quadro 3 Estrutura organizacional de GE e G Ciber

Atividade	Organização	Missão
G Ciber	ARMY CYBER COMMAND	Desenvolve e implementa capacidades do ciberespaço e a integra com a inteligência, fogos, espaço, operações psicológicas, comunicações estratégicas, assuntos públicos, operações técnicas especiais, guerra eletrônica e operações de informação para permitir aos comandantes do Exército uma vantagem na tomada de decisão durante a concorrência do conflito
	ARMY INFORMATION WARFARE OPERATIONS CENTER	Centro de coordenação, integração, sincronização de operações do ciberespaço, guerra eletromagnética, Informações, atendendo a requisitos de inteligência em apoio às diretivas nacionais, regionais e do Exército, para manter a consciência e compreensão da situação global e regional.
	ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND	A missão central da NETCOM engloba todos os aspectos de rede de transmissão, compartilhamento e armazenamento de dados do Exército.
	ARMY CYBER PROTECTION BRIGADE	Organiza, treina, equipa, orienta e implementa equipes de proteção cibernética para aumentar a capacidade de defesa das organizações em operações ou exercícios
	915TH CYBER WARFARE BATTALION	Batalhão expedicionário que inclui elementos de incluem elementos de atividades eletromagnéticas e cibernéticas, de operações de informação e inteligência.
	1ST INFORMATION OPERATIONS COMMAND	Fornecer informações e apoio a operações do ciberespaço ao Exército.
	780TH MILITARY INTELLIGENCE BRIGADE-CYBER	Conduz operações de ciberespaço para produzir efeitos emapoio ao Exército por meio da análise dos sinais eletromagnéticos e cibernéticos.
GE	ELECTROMAGNETIC WARFARE PLATOON (BRIGADE COMBAT TEAM)	Localizado na Companhia de Inteligência do Batalhão de Engenharia da Brigada, presta apoio em GE às operações dessa Grande Unidade.
	INTELLIGENCE, INFORMATION, CYBER, ELECTROMAGNETIC WARFARE, AND SPACE DETACHMENT (I2CEWS)	É uma unidade do tamanho de um batalhão atribuída a uma força-tarefa multidomínio e inclui uma seção melhorada do CEMA, para conduzir ataques de precisão e de longo alcance durante operações multidomínio

Fonte: *FM 3-12 Cyberspace And Electronic Warfare Operations*, 2021

Em uma interpretação mais ampla, as operações eletromagnéticas e cibernéticas do exército dos EUA são representadas pela Fig 12 abaixo:

Fig 13 Operações eletromagnéticas cibernéticas



Fonte: Zsolt Haig, Faculdade de Ciências Militares e Formação de Oficiais

Com isso, pode-se concluir, de forma parcial, que a interação de GE e G Ciber, ao ser coordenada por um órgão central permite a gestão das atividades desempenhadas no espectro eletromagnético e cibernético, viabilizando o emprego dessas capacidades em operações de segurança, defesa e ataque ao Exército norte-americano, além de conferir maior poder de combate em um ambiente de multidomínio cada vez mais complexo.

2.4 Comparação da interação da GE e G Ciber do EB com a do Exército dos EUA

Diante dos conceitos apresentados nos itens anteriores, dá-se que em relação a importância da GE e G Ciber na atualidade, ambos os países consideram o espaço eletromagnético e cibernético muito importantes para o combate moderno. No Brasil essa relevância está presente nos manuais de campanha e na Estratégia Nacional de Defesa, assim como nos EUA, o que representa um alinhamento na visão da conjuntura dos conflitos no Seculo XXI entre os dois países.

Em se tratando da interação dessas capacidades, verifica-se que ela não foi estruturada pelo EB de forma a considerá-los como um único domínio, diferentemente dos EUA, que em 2014 criou efetivamente a Arma de Cibernética e a Seção de Atividades Eletromagnéticas e Cibernéticas (CEMA), subordinada ao Chefe do Estado

Maior dos grandes comandos do Exército. Em tese, tal especificidade dos EUA demonstra uma gestão do espaço eletromagnético e cibernético de forma otimizada, evitando interferências entre as ações de GE e G Ciber.

Quanto a estrutura organizacional, pode-se aferir que possuem diferenças nos diversos níveis de atuação. Nos EUA a segurança e a defesa são realizadas por um organismo central do Estado, o Departamento de Defesa da Rede de Informações, enquanto no Brasil, a segurança cibernética é de responsabilidade do Gabinete de Segurança Institucional do Presidente da República e a defesa cibernética sob a responsabilidade do Comando de Defesa Cibernética, subordinado Ministério da Defesa, ensejando maior coordenação entres os órgãos dos níveis político e estratégico brasileiro.

No que tange a organização para o emprego no nível tático, percebe-se que os exércitos do Brasil e dos EUA diferem entre si, muito pelos escalões presentes em cada Força. No EB o maior escalão com capacidade de GE e G Ciber é o BGE, já nos EUA existem tropas valor Brigada, além de outras unidades vocacionadas para essas atividades, o que confere melhores condições de apoio na dimensão informacional do combate ao exército norte-americano.

Sobre a relação das atividades de GE e G Ciber com o trabalho de Estado Maior, observa-se uma abordagem semelhante entre os dois exércitos. No EB, o planejamento das capacidades de GE e G Ciber são realizadas na Célula de Comando e Controle, quando ativada para os trabalhos de Estado Maior de um Grande Comando (DE ou FTC), enquanto no exército norte-americano esse planejamento ocorre na CEMA, seção permanente do Estado Maior das Grandes Unidades, o que facilita a combinação das capacidades em prol do efeito desejado.

Dessa forma, conclui-se parcialmente, que os Exércitos do Brasil e dos EUA possuem soluções semelhantes para determinadas competências, mas também diferenças no modo de atuarem no domínio eletromagnético e cibernético. Verifica-se, também que ambos os países buscam efeitos semelhantes, seja nas tarefas de segurança, seja de defesa, a fim de disponibilizar ferramentas de apoio as operações militares frente a complexidade das ameaças nos conflitos desse Século.

3 METODOLOGIA

3.1 Tipo de pesquisa

A metodologia utilizada foi a pesquisa qualitativa, descritiva e documental. Para coleta de dados foram utilizadas, as seguintes fontes de busca, preferencialmente publicadas na última década:

- Artigos científicos;
- Manuais militares;
- Revistas de defesa nacionais e estrangeiras; e
- Sites especializados em artigos de defesa.

A pesquisa foi dividida em duas etapas:

- A primeira etapa foi destinada a reunir todo material bibliográfico e documental necessário ao embasamento teórico, como normas, conceitos, doutrinas, definições, perspectivas e demais estudos acerca da guerra eletrônica e cibernética no âmbito dos exércitos do Brasil e dos EUA, bem como considerações referentes a interação dessas capacidades nas operações militares.

- Na segunda etapa, o objetivo foi analisar a organização e o emprego da guerra eletrônica e da guerra cibernética nos Exércitos dos EUA e do Brasil, a fim de colher ensinamentos que pudessem agregar capacidade operacional a Força Terrestre brasileira.

Verifica-se que a referida pesquisa está com objetivos delimitados a analisar os processos associados a guerra eletrônica e cibernética nos EUA e no Basil, bem como analisar a possibilidade de interação dessas capacidades em operações militares do EB.

O trabalho teve prosseguimento com a elaboração do texto que abordou a questão objeto de estudo, bem como as conclusões pertinentes ao que foi proposto.

3.2 Universo e amostra

O universo do presente estudo foram as principais resoluções, manuais, doutrinas, trabalhos científicos e ações estratégicas dos EUA e do Brasil. Os dados das amostras que foram utilizados são, em sua maior parte, os vigentes a partir do ano de 2012, por serem considerados recentes e retratar a situação

atual da preparação dos Estados diante do surgimento de novas ameaças a soberania.

3.3 Coleta de dados

Conforme o Manual de Elaboração de Projetos de Pesquisa na ECEME (2017), a coleta de dados do presente trabalho de conclusão de curso se deu por meio da coleta na literatura, realizando-se uma pesquisa bibliográfica disponível, tais como livros, manuais, revistas especializadas, jornais, artigos, internet, monografias, teses e dissertações, sempre buscando os dados pertinentes ao assunto.

3.4 Tratamento dos dados

Conforme o Manual de Elaboração de Projetos de Pesquisa na ECEME (2017), o método de tratamento de dados utilizado no presente estudo foi a análise de conteúdo, no qual foram realizados estudos de textos para se obter a fundamentação teórica.

3.5 Limitações do método

A metodologia em questão possui limitações, particularmente, quanto à profundida do estudo a ser realizado, pois não contempla, dentre outros aspectos, o estudo de campo, com entrevistas de pessoas diretamente ligadas aos processos em estudo. Porém, devido ao fato de se tratar de um trabalho de término de curso, a ser realizado em aproximadamente seis meses, o método escolhido é adequado e possibilitou o alcance dos objetivos propostos no Projeto de Pesquisa.

4 RESULTADOS E DISCUSSÕES

O objeto dessa pesquisa científica foi verificar a interação entre a Guerra Eletrônica e a Guerra Cibernética no Exército Brasileiro, diante do cenário de combate moderno, tendo como referência o Exército dos EUA, um dos países mais avançados nesse quesito. Desse modo ficou constatado que o emprego dessas

capacidades é essencial para a manutenção da liberdade de ação para condução das operações militares no ambiente multidomínio, primordial nos conflitos atuais.

Ainda pôde-se averiguar que a percepção do Brasil e dos EUA em relação ao combate moderno e suas prospecções para o futuro, considerando a rápida evolução tecnológica e as transformações sociais que configuram o mundo VUCA, indicam um ambiente operacional com maior presença de atores não estatais, do auto valor estratégico da mídia e da opinião pública no planejamento e na condução das ações, demandando novas capacidades dos Exércitos, em prol de decisões mais eficazes para conquista dos objetivos.

Essa conjuntura também reforça como o emprego da GE e da G Ciber são importantes ferramentas para agregar poder de combate à Força Terrestre, principalmente no contexto dos combates modernos do Sec XXI, onde o domínio informacional é bastante relevante, proporcionando uma vantagem militar de superioridade de informação no momento e local decisivo para a consecução da estratégia elaborada.

Já em relação a interação propriamente dita entre a GE e a G Ciber, observa-se que essas atividades são por vezes desenvolvidas no mesmo domínio e destinadas ao mesmo efeito. Dessa forma, a coordenação do emprego combinado das ações no espectro eletromagnético e espaço cibernético viabiliza a otimização dos meios e evita a interferência e a sobreposição de tarefas, proporcionando um maior poder de combate à Força Terrestre.

Além disso, o planejamento centralizado em uma Seção de Atividades Eletromagnéticas e Cibernéticas, como é realizado no Exército dos EUA, pode ser uma solução para o emprego combinado das capacidades de GE e G Ciber. Contudo, deve ser analisado se essa seção consegue se integrar facilmente com as demais do Estado Maior, como a de Operações de Informações, Inteligência e Operações.

Como último aspecto a mencionar, no Brasil as capacidades de GE e G Ciber ocorrem por meio de curso de especialização. Nos EUA essas capacidades estão inseridas na formação do militar da Arma de Cibernética. Dessa maneira, o formato norte-americano indica a possibilidade do militar se aperfeiçoar constante e progressivamente ao longo da carreira, além de se dedicar especificamente a essa atividade, mitigando a probabilidade de desvio funcional desse recurso humano especializado.

5 CONCLUSÃO

Na visão de futuro para o Exército, definida em portaria do EME, a Força Terrestre deve ser capaz de se fazer presente, moderno, dotado de meios adequados e profissionais altamente preparados, composto por capacidades militares que superem os desafios do Século XXI e que possam respaldar as decisões soberanas do Brasil.

As prospecções do combate moderno, cuja evolução da tecnologia, principalmente na dimensão informacional, aliado a novos temas da agenda internacional, como o terrorismo, mudanças climáticas, crises econômicas globais, crises migratórias, crises energéticas e diversos outros que afligem a segurança do sistema internacional, demonstram a necessidade das forças armadas de atuarem em um ambiente de multidomínio.

Nesse sentido, as ações da GE e G Ciber nos campos de batalha remetem a importância dessas capacidades na ampliação do poder de combate. Atuar no espaço eletromagnético e cibernético é cada vez mais preponderante para assegurar os interesses nacionais frente as ameaças.

Ademais, o rápido avanço da tecnologia da informação, característico desse século, amplia a necessidade de consciência situacional fidedigna e oportuna aos decisores durante as operações, o que implica no emprego recorrente das atividades de GE e G Ciber nas operações militares, oferecendo ao EB uma força compatível com sua posição no cenário mundial.

Além disso, a intensificação da globalização, da transformação social e da inserção da opinião pública, das organizações internacionais, dos atores estatais e não estatais nos combates, limita a liberdade de ação das forças armadas. Tal conjuntura promove uma série de reflexos para o preparo e emprego do EB, sendo a GE e a G Ciber vetores de ampliação das capacidades operativas, a fim de superar esses desafios.

Desse modo, verifica-se que a interação entre as capacidades em estudo oferece a possibilidade do EB de maximizar o seu poder relativo de combate, impulsionando os esforços para a obtenção da superioridade informacional, na medida que emprega os meios sinérgica e objetivamente para alcançar todo o espectro do conflito (guerra e não guerra).

Assim, o desenvolvimento desse trabalho buscou apresentar as formas de interação dessas atividades, cuja atuação combinada configura-se como mais um fator multiplicador do poder para o sucesso das missões. Como objetivos específicos, procurou-se caracterizar o combate moderno, analisar a interação da GE e G Ciber no Brasil e nos EUA e realizar uma comparação dos dois modelos, a fim de identificar as soluções para os desafios e incertezas inerentes dos conflitos e as boas práticas que podem ser referência para inovação doutrinária do EB.

Em relação ao primeiro objetivo, verifica-se que as dimensões humana e informacional estarão cada vez mais evidentes no combate moderno, apesar da dimensão física ainda se manter com grande relevância. Com isso, obter a superioridade informacional se tornou tão importante quanto a superioridade aérea, terrestre, marítima ou espacial, sendo capaz de decidir a guerra e diminuir os danos colaterais de uma confrontação direta por meios cinéticos.

Ainda, no segundo objetivo, percebe-se que as atividades de GE e G Ciber podem interagir para alcançar objetivos comuns. Tal percepção pôde ser comprovada pelas tarefas desenvolvidas no âmbito das funções de combate Comando e Controle, Movimento e Manobra, Fogos, Inteligência, Logística e Proteção, bem como no emprego do nível tático do BGE ou dos B Com GE, demonstrando que o emprego combinado dessas capacidades é adequado, praticável e aceitável para se atingir o estado final desejado.

Desse modo, verificou-se que em Operações Ofensivas, a GE pode exercer ações de MAE com técnicas de despistamento, para emitir sinais eletromagnéticos para transmitir dados modificados que possam iludir os radares de defesa antiaérea inimigos, permitindo a aproximação de aeronaves destinadas a realizarem o ataque aéreo com segurança, como o utilizado nas ações iniciais da Rússia sobre as posições ucranianas no atual conflito entre esses países.

Nas Operações Defensivas, pode-se citar o *modus operandi* do CEMA nos EUA, que emprega a GE e G Ciber na obtenção de informações de inteligência sobre o inimigo desde as fases iniciais do planejamento. Nesse contexto, a MAGE pode realizar o levantamento da Ordem de Batalha Eletrônica (OBEI) enquanto a exploração cibernética permite explorar os sistemas de redes, a fim de identificar dados relevantes para a Seção de Inteligência. Assim, o cruzamento das informações na Célula de Atividades Cibernéticas e Eletromagnéticas colabora para uma análise

da situação do inimigo, contribuindo para consciência situacional do Teatro de Operações, imprescindível para a tomada de decisão dos líderes militares.

Em se tratando da comparação entre os Exércitos dos EUA e do Brasil, conclui-se que existem aspectos similares, mas também algumas diferenças. As semelhanças estão relacionadas principalmente a importância da interação da GE e G Ciber para o trabalho de Estado Maior, constituindo-se em uma ferramenta agregadora de poder de combate nas operações terrestres. Da mesma forma, vislumbram para esse século a tendência do emprego cada vez mais efetivo dessas capacidades no combate moderno, haja vista as características da “Era da Informação” identificadas no decorrer da pesquisa.

Ainda em relação as semelhanças, as capacidades operativas de GE e G Ciber, o EB e o exército dos EUA se equivalem, uma vez que a doutrina de emprego nos dois países e as ações no espaço eletromagnético e cibernético buscam causar efeitos afins nos campos de batalha, indicando que o EB tem se atentado para o domínio dessas atividades e condições para aperfeiçoá-las, visando superar os desafios inéditos e complexos dos conflitos.

Quanto as diferenças na comparação da interação da GE com a G Ciber no EB com a do Exército dos EUA, verificam-se algumas considerações que podem servir de referência para uma possível inovação da doutrina brasileira, como:

a. A Criação da Arma de Cibernética e do Curso de Operações do Ciberespaço para Líderes do Exército dos EUA (nível intermediário do ensino bélico – como o Curso de Aperfeiçoamento de Oficiais da Escola de Aperfeiçoamento de Oficiais do EB), permite o contínuo aprendizado do militar para as atividades no domínio eletromagnético e cibernético. Dessa forma, uma possível inovação para o EB seria a criação da Arma de Atividades Eletromagnéticas e Cibernéticas na formação dos oficiais de carreira, seja combatente, complementar ou até de formação específica, bem como seu aperfeiçoamento posterior, ampliando a especialização desses militares ao longo do serviço ativo;

b. A Seção Eletromagnética e Cibernética (CEMA) no Exército dos EUA reúne as atividades de GE e G Ciber em uma única seção, separadas da atividade de C2, permitindo um planejamento otimizado das operações, na dimensão informacional dos conflitos, no âmbito do trabalho de Estado Maior. No EB, todas essas atividades são desenvolvidas por uma única Seção ou Célula, coordenada pelo E6. Tal concepção da doutrina brasileira pode ser alterada, na intenção de facilitar a coordenação das

atividades dessas capacidades operativas, viabilizando uma análise mais detalhada das ações em cada nicho de atuação; e

c. Nos EUA existe uma integração de elementos técnicos, operacionais e de gestão do domínio eletromagnético e informacional na Seção Eletromagnética e Cibernética, possibilitando um eficiente assessoramento ao Cmt no processo decisório, bem como ao gestor desse domínio. No Brasil não há essa prática, podendo vir a ser uma oportunidade de melhoria utilizando-se das competências dos militares do quadro de engenheiros militares.

Nesse sentido, é possível constatar que o objetivo da presente pesquisa científica foi alcançado, já que foram apresentadas as formas de interação da GE com a G Ciber e a comparação dessa interação entre os exércitos dos EUA e do Brasil, trazendo à tona aspectos relevantes para uma possível inovação da doutrina militar terrestre, no intuito de ampliar as capacidades e o poder de combate da Força Terrestre no futuro.

Como sugestão para os próximos trabalhos relativos ao tema proposto, pode-se mencionar o aprofundamento da viabilidade de implementação do modelo norte-americano na doutrina nacional, utilizando-se de entrevistas direcionadas a militares especializados de GE e G Ciber do EB e que possuem experiência em operações reais no país e no exterior, além de pesquisadores de estabelecimentos de ensino, militar e civil, envolvidos nessa temática.

Por fim, considerando os estudos apresentados, seja de fontes primárias, manuais, artigos científicos, livros ou obras de estudiosos das áreas de defesa e segurança, é mister que a presença de novos atores nos conflitos, estatais e não estatais, aliado a rapidez do avanço tecnológico e o recrudescimento das disputas geopolíticas no mundo, indicam o uso cada vez maior de atuadores não cinéticos nos campos de batalha. Desse modo, a interação da GE e a G Ciber serão ainda mais relevantes na degradação do poder inimigo ou na manutenção das próprias forças, tornando-se decisivos nos futuros combates do Sec XXI.

REFERÊNCIA

ADAMY, David L. ***EW Against a New Generation of Threats***. *Artech House Power Electronic Warfare Library*, 2015.

BARTLES, Charles K.; **Para Entender Gerasimov**. Military Review, 2016.

BATISTA, Ana Laíse Ferreira Herculano. **Segurança Cibernética: Uma Abordagem Comparativa das Estruturas de Defesa Cibernética Norte-Americana e Brasileira**. ECEME, 2016.

BENNETT, N. e LEMOINE, G. J. **What a difference a word makes. Understanding threats to performance in a VUCA world**. Business Horizons, 2014.

BRASIL. Comandante do Exército. **PORTARIA Nº 1.985 Missão do Exército**. 2019.

BRASIL. Estado-Maior de Defesa. **MD 35-G-01: Glossário das Forças Armadas**. 5. ed. Brasília, 2015.

BRASIL. Exército. **C11-1 Emprego das Comunicações**. Estado Maior, 1997.

BRASIL. Exército. **Catálogo de Capacidades do Exército**. Estado Maior, 2015.

BRASIL. Exército. **Concepção Estratégica do Exército**. Estado Maior, 2019.

BRASIL. Exército. **EB20-MC-10.202 Operações Ofensivas e Defensivas**. Estado Maior, 2017.

BRASIL. Exército. **EB20-MC-10.203 Movimento e Manobra**. Estado Maior, 2015.

BRASIL. Exército. **EB20-MC-10.205 Comando e Controle**. Estado Maior, 2015.

BRASIL. Exército. **EB20-MC-10.206 Fogos**. Estado Maior, 2015.

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

BRASIL. Exército. **EB20-MC-10.208 Proteção**. Estado Maior, 2015.

BRASIL. Exército. **EB20-MC-10.213: Operações de Informação**. Estado Maior, 2014.

BRASIL. Exército. **EB20-MC-10.215 Operações de Dissimulação**. Estado Maior, 2014.

BRASIL. Exército. **EB20-MC-10.223 Operações**. Estado Maior, 2017.

BRASIL. Exército. **EB20-MC-10.225 Força Terrestre Componente**. Estado Maior, 2019.

BRASIL. Exército. **EB20-MF-03.106: Manual de Fudamentos Estratégia**. Estado-

Maior, 2020.

BRASIL. Exército. **EB20-MF-10.101 O Exército Brasileiro**. Estado Maior, 2014.

BRASIL. Exército. **EB20-MF-10.102 Doutrina Militar Terrestre**. Estado Maior, 2019.

BRASIL. Exército. **EB70-D-10.002 O Exército Brasileiro**. Comando de Operações Terrestres, 2014.

BRASIL. Exército. **EB70-MC.201 A Guerra Eletrônica na Força Terrestre**. Estado Maior, 2019.

BRASIL. Exército. **EB70-MC-10.232 Corpo de Exército**. Estado Maior, 2020.

BRASIL. Exército. **EB70-MC-10.232 Guerra Cibernética**. Estado Maior, 2017.

BRASIL. Exército. **EB70-MC-10.242 Operação de Garantia da Lei e da Ordem**. Estado Maior, 2018.

BRASIL. Exército. **EB70-MC-10.243 Divisão de Exército**. Estado Maior, 2020.

BRASIL. Exército. **EB70-MC-10.246 As Comunicações nas Operações**. Estado Maior, 2020.

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

BRASIL. Exército. **EB70-MC-10.248 Operações Interagências**. Estado Maior, 2020.

BRASIL. Exército. **EB70-MC-10.341 Lista de Tarefas Funcionais**. Estado Maior, 2016.

BRASIL. Exército. **Manual de Elaboração de Projetos de Pesquisa na ECEME**. ECEME, Rio de Janeiro, 2017.

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

BRASIL. **MD 35-G-01: Glossário das Forças Armadas**. 5. ed. Brasília, Ministério da Defesa, 2015.

BRASIL. MINISTÉRIO DA DEFESA. **Estratégia Nacional de Defesa.** Brasília, 2012.

BRASIL. MINISTÉRIO DA DEFESA. **Livro Branco de Defesa Nacional.** Brasília, 2020.

BRASIL. MINISTÉRIO DA DEFESA. **Política Nacional de Defesa.** Brasília, 2012.

CARNEIRO, Marcelino Haddad Aquino. **Os elementos de apoio ao combate Comunicações, Guerra Eletrônica e Guerra Cibernética na composição da Força**

Terrestre Componente: uma proposta de estrutura organizacional. ECEME, 2016.

CCOMGEX. **Defesa Cibernética: Capacidades do EB**. Disponível em: http://www.eceme.eb.mil.br/images/docs/PalestrasCEE/CAPACIDADES_DO_EB.pdf. Acessado em 02 de março de 2022.

CORRÊA, Marlos De Mendonça. **Espaço Cibernético: Análise de um cenário prospectivo e desdobramentos para as Capacidades do Exército Brasileiro**. ECEME, 2020.

DERLETH, James. **A Guerra de Nova Geração Russa: Dissuasão e vitória no nível tático**. Military Rewiew, 2021.

EUA. ***ATP 3-12.3: Electronic Warfare Techniques***. *Department of the Army*, 2019.

EUA. ***FM 3-12: Cyberspace and Electronic Warfare Operations***. *Department of the Army*, 2017.

EUA. ***FM 3-38: Cyber Eletromagnetic Activities***. *Department of the Army*, 2014.

EUA. ***JP 3-13.1: Electronic Warfare***. *Department of the Army*, 2017.

EUA. ***JP 6-01: Joint Electromagnetic Spectrum Management Operations***. Disponível em: https://irp.fas.org/doddir/dod/jp6_01.pdf. Acessado em 02 de março de 2022.

EUA. ***TRADOC Pamphlet 525-8-6: The U.S. Army Concept for Cyberspace and Eletronic Warefare Operations***. *Department of the Army*, 2018.

FLEMES, D. **Conceptualising Regional Power in International Relations : Lessons from the South African**. German Institute of Global and Area Studies (GIGA), v. 53, n. June, p. 1–60, 2007.

FONSECA, Hebert Cássio Guimarães. **O Brasil e os desafios da defesa do Atlântico Sul**. 2018.

GOMES, Marco Antônio Freire. **Diretriz do Comandante do Exército**. 2022.

GONÇALVES, Leandro Salenave. Sistemas de informação. Disponível em: http://www2.videolivraria.com.br/pdfs/6519.pdf. Acessado em 02 de março de 2022.

GREGORY, Valdecir. **Clausewitz nos conflitos atuais**. A Defesa Nacional**,** v. 103, n. 830, 2016.

HAIG, Zsolt. ***ELECTRONIC WARFARE IN CYBERSPACE. National University of Public Service***. *Budapest, Hungary*, 2015.
Institute for the advanced study of information warfare (IASIW). Disponível em: http://wgbis.ces.iisc.ernet.in/envis/doc97html/infocss610.html. Acessado em 02 de março de 2022.

LIMOEIRO, Christiano Zacconi. **A estrutura de emprego da subunidade de Guerra Eletrônica do Batalhão de Comunicações e Guerra Eletrônica em apoio às Funções de Combate**. ECEME, 2015.

MAFRA, Roberto Machado de Oliveira. **Teorias geopolíticas e cenários prospectivos**. Revista A Defesa Nacional, v. 93, n. 809, 2007.

MARCONI, Marina de Andrade e LAKATOS, Eva Maria. **Fundamentos de Metodologia Ciêntifica**. Ed. Atlas, 8ª ed.; 2017.

MATTIS, James N. e HOFFMAN, Frank. ***Future Warfare: The rise of Hybrid Wars***. *U.S. Naval Institute,* 2005.

MOUTINHO, João Marcos Drumond. **A Guerra Cibernética no Nível Operacional / Tático – 1º Batalhão de Guerra Eletrônica**. ECEME, 2015.

NASSER, R. M; MORAES, R. F. **O Brasil e a segurança no seu entorno estratégico América do Sul e Atlântico Sul.** Ipea, Brasília, 2014.

NETO, Samuel Bombassaro. **A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas**. ECEME, 2018.

PENA, Rodolfo R. Alves. **Era da Informação**. Disponível: https://mundoeducacao.bol.uol.com.br/geografia/era-informacao.htm. Acessado de 02 de março de 2022.

PERKINS, David G. **Combate em Múltiplos Domínios: Impulsionando a Mudança para Vencer no Futuro**. Military Review, 2018.

PINTO, Danielle Jacon Ayres e GRASSI, Jéssica Maria. **Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil**. Revista Brasileira de Estudos de Defesa, v. 7, 2020.

PORCHE III, Isaac R.; PAUL, Christopher; SERENA, Chad C.; CLARKE, Colin P.; JOHNSON, Erin-Elizabeth e HERRICK, Drew. **Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below**. RAND Corporation, Santa Monica, Calif, 2017.

SANT'ANNA, Renato Azevedo. **O ciclo OODA e o Mundo VUCA (Volátil, Incentro, Complexo, Ambíguo)**. Disponível em: https://medium.com/futuro-exponencial/o-ciclo-ooda-e-o-mundo-vuca-vol%C3%A1til-incerto-complexo-amb%C3%ADguo-def8da46b1d. Acessado em 02 de março de 2022.

SOUZA, Carlos Roberto Pinto de. **CCOMGEX: do SISFRON à Guerra Eletrônica, a arte de proteger o País**. DefesaNet: 25 de junho de 2014. Entrevista concedida à DefesaNet. Disponível em: http://www.defesanet.com.br/bid/noticia/15782/CCOMGEX--do-SISFRON-a-Guerra-Eletronica--a-arte-de-proteger-o-Pais/. Acessado em 02 de março de 2022.

SPRECKELSEN, Malte Von. ***Electronic Warfare – The forgotten discipline***. 2018. Disponível em: https://www.japcc.org/electronic-warfare-the-forgotten-discipline/. Acessado em 02 de março de 2022.

THEOHARY, Catherine A. ***Defense Primer: Information Operation***. *Congression Research Service*. IFI 0771, página 1, 2018.

THEOHARY, Catherine A.; e HOEHN, Johon R. ***Convergence of cyberspace operations and electronic warfare***. *Congressional Research Service*. IFI 1192, página 2, 2019.

TZU, Sun. **A arte da guerra**. Tradução de Sueli Barros Cassal. 1ª ed: L&PM editora, 2006.