ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Maj Com SAMUEL **BOMBASSARO** NETO

A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas

Rio de Janeiro

2018

Maj Com SAMUEL **BOMBASSARO** NETO

A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas.

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.

Orientador: Maj Com Glauber Juarez Sasaki Acácio

Rio de Janeiro
2018

Maj Com SAMUEL **BOMBASSARO** NETO

A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas.

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.

Aprovado em de de 2018.

COMISSÃO AVALIADORA

_____
Glauber Juarez Sasaki Acácio – Maj Com QEMA – Presidente
Escola de Comando e Estado-Maior do Exército

_____
Sidney Marinho Lima – TC QMB QEMA – Membro
Escola de Comando e Estado-Maior do Exército

_____
Anderson Luiz Alves Figueiredo – Maj Eng QEMA – Membro
Escola de Comando e Estado-Maior do Exército

À minha esposa que, com extrema sabedoria, soube compreender os momentos abdicados em prol da execução deste trabalho.

AGRADECIMENTOS

Ao Major Glauber Juarez Sasaki Acácio 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.

Todo cidadão, após ingressar em uma das Forças Armadas mediante incorporação, matrícula ou nomeação, prestará compromisso de honra, no qual afirmará a sua aceitação consciente das obrigações e dos deveres militares e manifestará a sua firme disposição de bem cumpri-los. [...] (Estatuto dos Militares).

RESUMO

A Guerra Cibernética, sendo uma vertente que busca o uso ofensivo e defensivo de informações e de sistemas de informações, é um dos temas de maior relevância no âmbito das Forças Armadas. Particularmente para o Exército Brasileiro o assunto é de especial importância, por ter sido atribuída ao mesmo a responsabilidade pelo setor cibernético na Estratégia Nacional de Defesa. Assim, é crescente o uso da Guerra Cibernética em operações diversas, principalmente ao envolver escalões elevados, como o nível de uma Força Terrestre Componente. É nesse ambiente que os atuadores cibernéticos desencadeiam ações que visam contribuir para o aumento do poder de combate da tropa. Inúmeros autores, além dos próprios documentos e manuais militares, são taxativos ao elencar benefícios advindos da utilização da Guerra Cibernética, conforme explorado no desenvolvimento da pesquisa. Ainda, as entrevistas concedidas por dois especialistas na área vieram a somar e ratificar pontos importantes do incremento proporcionado pelos meios e recursos humanos cibernéticos, especificamente em operações ofensivas, já que, doutrinariamente, as operações defensivas são atitudes temporárias e sempre devem visar a retomada da iniciativa. A Guerra Cibernética é capaz de auxiliar em praticamente todas as funções de combate, sendo empregada, por exemplo, para aquisição de dados, para ataques não cinéticos ou para a mitigação de ações cibernéticas oponentes. Desse modo, o trabalho, foi concluído com a confirmação das respostas às questões de estudo que foram formuladas, bem como aos objetivos específicos e geral do trabalho, finalizando com algumas recomendações de quais frações cibernéticas são mais aptas ao escalão em que se está trabalhando. Por fim, foi elaborada uma sugestão de se aprofundar as pesquisas visando a diferenciação dos cursos de Guerra Cibernética para oficiais e praças, haja vista que os mesmos, após formados, executarão funções também distintas.

Palavras-chave: Guerra Cibernética, Operações Ofensivas, Força Terrestre Componente, Poder de Combate.

ABSTRACT

The Cyber Warfare, being a branch that seeks the offensive and defensive use of information and information systems, is one of the most relevant topics within the scope of the Armed Forces. Particularly for the Brazilian Army, the issue is of particular importance, because it has been attributed to it the responsibility for the cyber sector in the National Defense Strategy. Thus, the use of Cyber Warfare in miscellaneous operations is increasing, especially when involving high levels, such as the level of a Component Ground Force. It is in this environment that the cybernetic actuators initiate actions that aim to contribute to the increase of the combat power of the troop. Numerous authors, in addition to the military documents and manuals themselves, are critical in listing benefits derived from the use of Cyber Warfare, as explored in the development of the research. Moreover, the interviews given by two experts in the field have added and ratified important points of the increase provided by cybernetic resources and human resources, specifically in offensive operations, since defensive operations are temporary attitudes and should always aim at resumption of work. initiative. Cyber Warfare is able to aid in virtually all combat functions, and is used, for example, for data acquisition, for non-kinetic attacks, or for mitigating opponents cybernetic actions. Thus, the work was concluded with the confirmation of the answers to the questions of study that were formulated, as well as the specific and general objectives of the work, ending with some recommendations of which fractions are more suitable to the stage in which one is working. Finally, a suggestion was made to deepen the research aiming at the differentiation of Cyber Warfare courses for officers and squares, since they, after being trained, will also perform different functions.

Keywords: Cyber Warfare, Offensive Operations, Ground Force Component, Combat Power.

SUMÁRIO

1 INTRODUÇÃO

A Guerra Cibernética (G Ciber) é definida como o uso ofensivo e defensivo de informações e de sistemas de informações que produzam efeitos nas capacidades de Comando e Controle (C2) do adversário, tais como exploração ou negação de dados (GUERRA CIBERNÉTICA, 2017). A revolução informacional, vivida desde meados da década de 70, elevou o domínio do campo virtual a uma nova condição, em especial quando relacionado aos assuntos de defesa e segurança. Assim, coube ao Exército Brasileiro (EB), da mesma forma, acompanhar essa evolução e traçar objetivos para desenvolver o seu setor cibernético.

O espaço cibernético é, hoje, uma valiosa fonte de informação em qualquer nível. Os ataques aos sistemas de tecnologia da informação e comunicações de um Estado soberano podem causar danos de grande vulto, como o ocorrido em outubro de 2017 aos Estados Unidos da América (EUA), por parte de *hackers* norte-coreanos (GAZETA DO POVO, 2017).

A Estratégia Nacional de Defesa (END), que teve a sua primeira versão confeccionada em 2008, é um documento governamental que busca operacionalizar os objetivos nacionais de defesa brasileiros, ou seja, tem por finalidade elencar as estratégias que devem nortear a sociedade como um todo na defesa do país (BRASIL, 2008). A revisão da END ocorre de quatro em quatro anos, sendo a sua última edição datada de 2016.

A END, desde a sua pioneira elaboração, definiu três setores tecnológicos essenciais para a defesa nacional: o espacial, o cibernético e o nuclear. Para cada um deles, o governo brasileiro atribuiu uma Força Armada responsável pelo seu desenvolvimento, sendo que o EB ficou incumbido do setor cibernético, deixando clara a importância que deve ser dada ao tema.

As ações no espaço cibernético possuem distintos níveis de atuação, desde o político até o tático, sendo este último o escalão no qual se enquadra a G Ciber, gerando, assim, impacto nas operações das Forças Terrestres Componentes (FTC). A FTC, por sua vez, é o elo de ligação entre o nível operacional e tático, constituindo um comando operativo coordenador das operações terrestres e elemento essencial no combate moderno.

Ainda, o combate terrestre, como missão precípua do EB e, por consequência, da FTC, pode ser conduzido por meio de ações ofensivas ou

defensivas. De acordo com o manual de Doutrina Militar Terrestre (BRASIL, 2014), as operações defensivas devem ser executadas até o momento em que se possa retomar a ofensiva, deixando claro que esta é a prioridade no emprego convencional da Força.

A FTC é o braço terrestre de um Comando Operacional, sendo responsável por assimilar os objetivos operacionais e, em última análise, cumprir a missão atribuída pelo escalão superior. E para desempenhar com sucesso essa atribuição, a FTC faz uso do poder de combate.

Segundo o Glossário das Forças Armadas (BRASIL, 2015), o poder de combate é a capacidade geral de que dispõe uma organização para desenvolver o combate, sendo que a sua medida é flexível e envolve inúmeros fatores, como moral, meios disponíveis e valor do comandante. Mensurar o poder de combate de uma força, a exemplo da FTC, só tem sentido se for comparada com outro elemento, como um oponente.

Portanto, o poder de combate de uma FTC pode ser medido de inúmeras maneiras, possuindo fatores nem sempre fixos – até em função da sua constituição variável. Porém, um desses fatores que influencia de modo determinante o êxito da missão atribuída à Força Terrestre Componente, por ser um componente que permeia transversalmente as diversas funções de combate, é a Guerra Cibernética.

1.1 PROBLEMA

O uso intenso da G Ciber, seja no âmbito internacional como no contexto brasileiro, suscita diversas questões que podem ser analisadas sob inúmeras óticas. Uma delas é que a relevância do cenário virtual cresce maneira progressiva, particularmente para as Forças Armadas e, sobretudo, para o EB, já que o mesmo é o responsável pelo setor dentro dos objetivos propostos pela END.

Também é sabido que a FTC é um escalão essencial para o desenvolvimento das operações terrestres, e que o mesmo é composto por elementos de G Ciber, os quais interferem em seu poder de combate.

Diante do cenário apresentado, a presente pesquisa se deparou com o seguinte problema – objeto de análise do tema a ser desenvolvido pelo trabalho –, a qual buscou responder, cientificamente:

Em que medida a Guerra Cibernética contribui para aumentar o poder de combate da Força Terrestre Componente em operações ofensivas?

1.2 OBJETIVOS

Os objetivos de uma pesquisa são parte crucial do trabalho, pois é da sua designação que será definido o caminho a ser trilhado para que a resposta ao problema seja atingida.

Segundo Neves (2007), os objetivos possuem diferentes níveis de profundidade, sendo divididos em objetivo geral e objetivos específicos. O mais comum é estabelecer um objetivo geral, mais amplo, e articulá-lo com objetivos específicos, que irão conduzir o trabalho à meta maior. Desse modo, o presente estudo apresenta os seus objetivos geral e específicos.

1.2.1 **Objetivo geral**

O objetivo geral é o foco do trabalho, estando ligado a uma visão ampla do tema. Por meio do seu atingimento, é pretendido determinar o produto final da pesquisa. Para que se pudesse responder o problema elencado para este estudo, segue-se o seguinte objetivo geral.

Apresentar a contribuição da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas (Op Of).

1.2.2 **Objetivos específicos**

Com o fito de delimitar e viabilizar a consecução do objetivo geral de estudo, foram elaborados os seguintes objetivos específicos:

a. Apresentar os fundamentos da Guerra Cibernética, identificando as suas tarefas, atividades e ações, em especial nas Operações Terrestres.

b. Identificar o conceito de poder de combate.

c. Apresentar a estrutura de uma FTC em operações ofensivas.

1.3 JUSTIFICATIVA

Esta seção busca, de forma resumida, discorrer sobre os principais tópicos que justificam a importância do presente estudo. Destarte, a relevância desta pesquisa está apoiada nos aspectos descritos a seguir.

A revolução tecnológica que elevou o espaço cibernético a uma condição ímpar quando relacionado a assuntos de defesa e segurança não passou

despercebida pelo Exército Brasileiro, que vem explorando capacidades nessa área. Desse modo, a presente pesquisa visa contribuir com o estudo das formas de emprego da G Ciber diante desse novo cenário, com o intuito de ser aproveitada para futuros aperfeiçoamentos da atividade.

O primeiro grande argumento é a diretriz traçada na própria END, que atribuiu a responsabilidade pelo desenvolvimento do setor cibernético, no âmbito da defesa, ao EB. Portanto, o ramo virtual, que já era uma das prioridades da Força, passou a ter ainda mais importância.

Em palestra proferida na Escola de Comando e Estado-Maior do Exército (ECEME) pelo Chefe do Estado-Maior do Exército (Ch EME), General de Exército Fernando, em 27 de fevereiro de 2018, o desenvolvimento da área cibernética foi apontado como uma das mais importantes frentes do EB na atualidade. Destaca-se que o EME é o Órgão de Direção Geral subordinado diretamente ao Comandante do Exército, responsável pela implementação das estratégias da Força nos diversos campos de atuação. Ainda, a posição em relação à cibernética foi ratificada pelo 2º Subchefe do EME, General de Brigada Tratz, contribuindo para a elevação da importância do assunto.

A experiência do autor da pesquisa como instrutor militar na área de cibernética do Centro Integrado de Guerra Eletrônica (CIGE) também justifica a escolha do tema. Tal base racional é sustentada por Neves (2007), ao afirmar que a história profissional pode corroborar com a propensão do assunto fixado pelo autor.

Por fim, o objetivo da pesquisa é tido como significativo para o país e para o Exército Brasileiro com base nos fatores acima considerados, os quais demostraram a importância do assunto e encontram suporte no crescente interesse da Força na temática ora elencada.

2 DESENVOLVIMENTO

Esta seção possui a finalidade de abordar os assuntos essenciais referentes ao tema em questão na presente pesquisa. Para tanto, o capítulo foi dividido em tópicos, que vão desde os fundamentos da Guerra Cibernética, com o detalhamento de sua atuação, até a definição do próprio conceito de poder de combate, bem como as particularidades de uma FTC atuando ofensivamente.

A intenção foi de que, para cada tópico, pudesse ser esmiuçado o que há de mais atual em cada vertente, ao mesmo tempo em que foi feita uma revisão dos principais conceitos doutrinários envolvidos. Essa sistemática permitiu a aquisição de uma visão abrangente sobre o campo cibernético, sobre poder de combate sob o ponto de vista do Exército e sobre a estrutura da FTC na ofensiva.

A parcela do capítulo correspondente à Guerra Cibernética apresenta um volume maior por se tratar do tema principal da pesquisa, constituindo a ideia central do trabalho. Além disso, é um dos assuntos de maior desconhecimento, em muito por se tratar de um campo ainda não completamente explorado no meio militar brasileiro, exigindo maior atenção por parte do estudo.

2.1 FUNDAMENTOS DA GUERRA CIBERNÉTICA

A primeira premissa para o completo entendimento do emprego da G Ciber é a definição de alguns conceitos, pois existe uma variada amplitude de termos e definições relacionadas ao assunto.

O Glossário das Forças Armadas define a Guerra Cibernética da seguinte maneira:

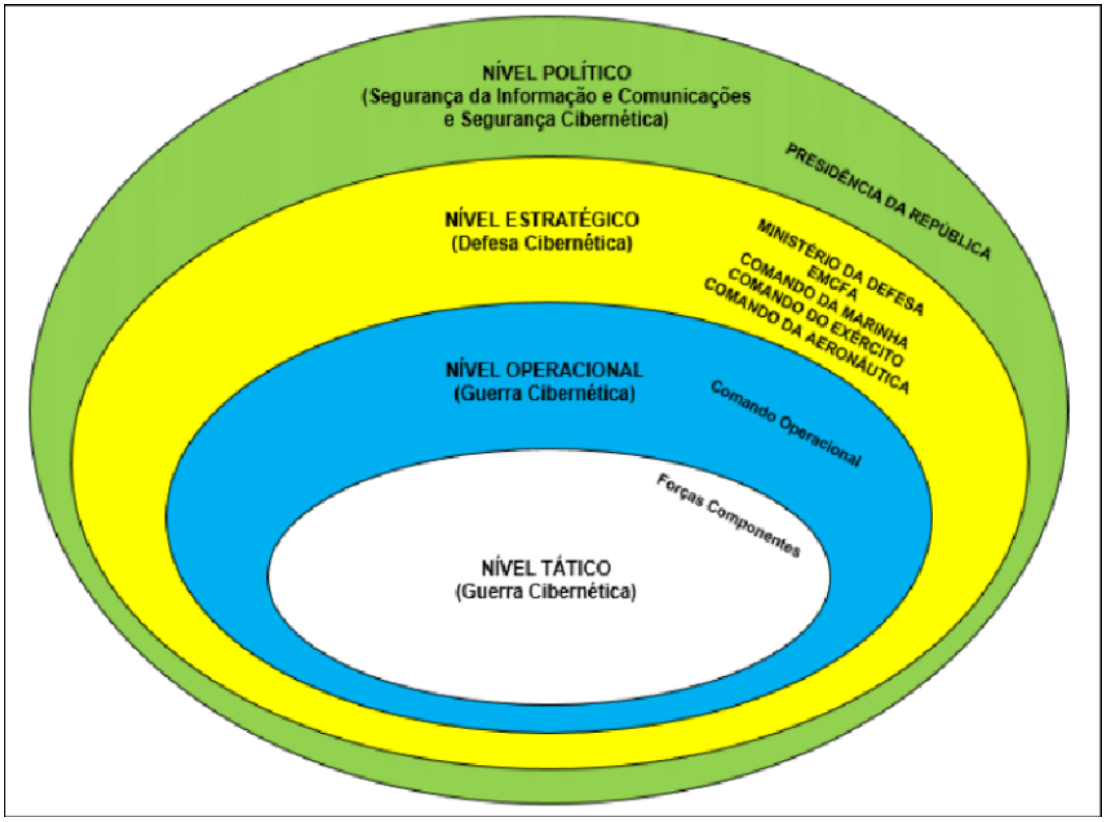
> Uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. (BRASIL, 2015)

O mesmo conceito é aplicado no manual do Ministério da Defesa Doutrina Militar de Defesa Cibernética, o qual cita, ainda, que a denominação Guerra

Cibernética “será utilizada quando o nível de decisão considerado for o operacional ou tático” (BRASIL, 2014).

A elucidação dos termos cibernéticos faz-se necessária porque existe um entendimento relativamente comum de que Segurança Cibernética, Defesa Cibernética e Guerra Cibernética atuam no mesmo campo, havendo somente uma variação de denominação. Porém, a nomenclatura determina, na realidade, em que nível decisório está ocorrendo a ação.

Assim, deve-se entender que as ações no Espaço Cibernético possuem denominações distintas de acordo com o seu nível de decisão, ou seja, conforme o seu grau de atuação. Tal distinção é importante porque define o seu espaço de ação e modifica o seu raio de ação, conforme figura a seguir, extraída do manual de Guerra Cibernética (2017).



Fonte: adaptado de Manual de Guerra Cibernética (BRASIL, 2017)

O esclarecimento acima possui vínculo com o tema da presente pesquisa ao enquadrar o assunto no âmbito da Força Terrestre Componente, força integrante o nível tático das esferas decisórias. Dessa forma, ao tratar de cibernética no escalão FTC, está sendo empregada a G Ciber.

Ainda relacionado aos conceitos da G Ciber, tem-se a importante definição do que vem a ser o Espaço Cibernético:

> Espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas. (BRASIL, 2017)

Esse é o ambiente no qual não somente a Força Terrestre Componente, mas grande parte das Forças Armadas, operam. A partir da Revolução Informacional[1], iniciada na década de 70, os sistemas passaram a adotar uma infraestrutura digital para os seus diversos fins, ultrapassando as barreiras militares. Os chamados ativos de informação – meios utilizados para o trânsito de informações virtuais, englobando dispositivos, locais, equipamentos e pessoas – tiveram a sua relevância aumentada, sendo inseridos nas mais diversas camadas. O conjunto de ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade é denominado infraestrutura crítica da informação (BRASIL, 2017). E é exatamente esse nível de destaque que fez do campo cibernético uma das mais compensadoras áreas de atuação.

As infraestruturas críticas estão presentes em inúmeros setores, e permeiam basicamente todos os sistemas militares. O nível tático, como o de operação de uma FTC, também é composto por sistemas virtuais, muitos dos quais dependem de infraestruturas cibernéticas para operar, contribuindo para que o ambiente virtual deva ser tratado como crucial.

Um exemplo prático da integração entre as operações militares e o campo cibernético é o próprio fluxo de dados que existe dentro do canal de comando das frações. Os dados que transitam por esses meios, muitas vezes fundamentais para o êxito das ações, devem ser norteados pelo conceito da Segurança da Informação e Comunicações (SIC), que são:

> [...] ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações.

[1] Também conhecida como Terceira Revolução Industrial, pode ser resumida na adoção sistemática e progressiva de tecnologias avançadas no sistema de produção industrial, tendo o seu início liderado pelos Estados Unidos da América.

> **2.3.14.1 Disponibilidade** – propriedade segundo a qual a informação deve ser acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade.
>
> **2.3.14.2 Integridade** – propriedade segundo a qual a informação não deve ser modificada ou destruída de maneira não autorizada ou acidental.
>
> **2.3.14.3 Confidencialidade** – propriedade segundo a qual a informação não deve estar disponível ou ser revelada a pessoa física, sistema, órgão ou entidade não autorizados ou não credenciados.
>
> **2.3.14.4 Autenticidade** – propriedade segundo a qual a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema, órgão ou entidade. (BRASIL, 2017)

Fica claro que os dados que transitam em um nível decisório tático, como o da FTC em operações, devem ser protegidos para que seja obtido sucesso na condução dessas operações militares, vinculando as ações oriundas das funções de combate, como manobra ou mobilidade, com as atividades da Guerra Cibernética.

Outro ponto de suma importância para que se possa integrar as ações cibernéticas às operações militares refere-se aos princípios de emprego da G Ciber, em número de quatro: princípio do efeito, princípio da dissimulação, princípio da rastreabilidade e princípio da adaptabilidade. Salienta-se que os princípios de guerra tradicionais são aplicados normalmente nas ações de G Ciber, assim como em atuações militares.

Segundo o manual de Guerra Cibernética (BRASIL, 2017), tem-se como definição do princípio do efeito que as ações cibernéticas devem produzir efeitos, ainda que não sejam cinéticos, de modo que se traduzam em vantagem estratégica, operacional ou tática que afetem o mundo real. Desse modo, os efeitos de uma atuação cibernética podem influenciar uma operação de diversas maneiras, seja no mundo virtual ou não.

O princípio da dissimulação define que todas as ações no mundo virtual devem ser compostas por medidas que busquem dificultar ou mascarar a

rastreabilidade, ou seja, mascarar a autoria e a origem dessas mesmas medidas, de modo que o oponente não identifique o cerne das ações.

Não menos importante é o princípio da rastreabilidade que, de modo oposto ao princípio da dissimulação, busca detectar a origem das ações contra sistemas virtuais amigos, por meio da exploração e análise de registros nos sistemas oponentes.

Finalmente, o princípio da adaptabilidade consiste “na capacidade da G Ciber de adaptar-se à característica de mutabilidade do espaço cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis” (BRASIL, 2017).

Tem-se, portanto, que os princípios da G Ciber são vetores fundamentais e balizadores de como devem ser empregadas as operações cibernéticas, de modo a contribuir para o sucesso da missão militar.

A G Ciber, ainda, possui características peculiares que lhe conferem um patamar diferenciado nas operações militares, sendo imprescindível para a compreensão do seu apoio nas operações militares. Dentre essas características, uma das mais relevantes é a do alcance global, qual seja o de não possuir limitações físicas de espaço e distância, podendo atuar em escala global e de modo simultâneo. O alcance global confunde-se com a vulnerabilidade das fronteiras geográficas – outra característica cibernética –: agentes podem atuar de qualquer lugar, gerando efeitos em qualquer local. Outra característica de importância é a dualidade, ou seja, uma mesma ferramenta de proteção cibernética pode, também, ser utilizada para um ataque cibernético.

Duas características da G Ciber possuem especial importância em ações militares: a percepção de que ações cibernéticas não são um fim em si mesmas, sendo uma ferramenta de apoio às operações; e a assimetria, cuja definição demonstra que as ações virtuais podem ser um ponto de ruptura e causar prejuízos tão grandes quanto aqueles causados por partes com maior poderio econômico.

Com o panorama da Guerra Cibernética desenhado, pode-se entender com maior clareza as possibilidades de suas ações, descritas abaixo:

> **2.6.1** São possibilidades da guerra cibernética:
> a) atuar no espaço cibernético, por meio de ações ofensivas, defensivas e exploratórias;

> b) cooperar na produção do conhecimento de inteligência por meio dos dados obtidos na fonte cibernética;
> c) atingir sistemas de informação de um oponente sem limitação de alcance físico e exposição de tropa;
> d) cooperar com a segurança cibernética, inclusive de órgãos externos ao Ministério da Defesa, mediante solicitação ou no contexto de uma operação;
> e) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da guerra cibernética;
> f) facilitar a obtenção da surpresa, com base na exploração das vulnerabilidades dos sistemas de informação do oponente;
> g) realizar ações contra oponentes com poder de combate superior; e
> h) realizar ações com custos significativamente menores do que aqueles envolvidos nas operações militares nos demais domínios. (BRASIL, 2017)

Verifica-se que o raio de atuação cibernético é imenso, e que as suas ações podem ser incluídas em inúmeras atividades, incluindo as operações militares. Desse modo, a atividade de G Ciber pode causar efeitos em vários escalões, particularmente no enquadramento da FTC – nível tático.

Existem, também, limitações quanto ao emprego da G Ciber, muito em função da própria natureza da atividade. Desse modo, essas restrições podem ser sintetizadas conforme abaixo.

> **2.7.1** São limitações da guerra cibernética:
> a) restrita capacidade de identificação da origem e atribuição de responsabilidades por ataques cibernéticos;
> b) restrita eficácia das ações cibernéticas defensivas, devido à existência de vulnerabilidades nos sistemas computacionais;
> c) restrita capacidade de gestão de pessoas, particularmente no que concerne à identificação, seleção, capacitação e retenção de talentos;
> d) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e
> e) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação. (BRASIL, 2017)

Entende-se por capacidade operativa, dentro do contexto da G Ciber, a “aptidão requerida a uma força ou organização militar, para que possa cumprir

determinada missão ou tarefa" (BRASIL, 2017). Dessa maneira, a guerra cibernética, na sua conjuntura militar, possui as seguintes capacidades operativas, descritas abaixo.

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Fonte: adaptado de Manual de Guerra Cibernética (BRASIL, 2017)

Prosseguindo no estudo aprofundado dos conceitos fundamentais do campo cibernético, verifica-se a sua interação com as funções de combate. Para melhor compreender como a G Ciber é capaz de agir dentro desses ramos, faz-se necessário entender o que é uma função de combate, descrita abaixo.

> FUNÇÃO DE COMBATE – Conjunto de atividades, tarefas e sistemas (pessoas, organizações, informações e processos) afins, integrados para uma finalidade comum, que orientam o preparo e o emprego dos meios no cumprimento de suas missões. Esta abordagem por funcionalidades proporciona uma ferramenta para os estados-maiores relacionarem, reunirem, integrarem e coordenarem as atividades, tarefas e sistemas sob sua responsabilidade, de modo a assegurar que todos os aspectos

> necessários à condução das operações tenham sido considerados no planejamento. (BRASIL, 2018)

As funções de combate são, portanto, um conceito relativamente moderno no Exército Brasileiro, que permitiram uma forma de abordagem diferenciada na solução de problemas, já que atuam por meio de tarefas. Isso significa que, dado um problema militar específico, o mesmo pode ser resolvido pela aplicação das diversas ações que compõem uma ou mais funções de combate.

A Força Terrestre, desse modo, emprega as funções de combate para executar as suas missões, sendo essas funções em número de seis: função de combate Comando e Controle (C2), Movimento e Manobra, Inteligência, Fogos, Logística e Proteção. Cada uma possui capacidades distintas, vocacionadas para a solução de determinadas situações de acordo com suas capacidades.

Verifica-se que, apesar de existirem diferentes funções de combate, todas são integradas e raramente atuam de modo isolado, fazendo com que as mesmas sejam permeadas, em algum nível, pela G Ciber.

Ao se fazer uma análise um pouco mais pormenorizada da atuação da G Ciber, o próprio manual de G Ciber identifica as atividades, tarefas e ações da Guerra Cibernética, conforme são apresentadas na tabela a seguir.

Atividade	Tarefa
Proteção Cibernética	**Gestão de Riscos** Gerenciar as relações entre ativos de informação, patrimônio digital, ameaças, vulnerabilidades, impactos, probabilidade de ocorrência de incidentes de segurança da informação e riscos. Estabelece o nível de alerta cibernético correspondente e executa o tratamento, a comunicação e a monitoração contínua desses riscos.
	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.
	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.
	Pronta Resposta Reagir prontamente às ameaças identificadas, observando os diferentes níveis de alerta cibernético (grau de risco).
	Forense Digital Coletar e examinar evidências digitais em redes e sistemas de informação de interesse do EB.
	Teste de Artefatos Cibernéticos Testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos.
	Conformidade de SIC Verificar a observância de aspectos legais, normativos e procedimentais de SIC no âmbito do SGCEx.
	Gestão de Incidentes de Redes Coordenar o tratamento de incidentes nas redes de interesse, acompanhar a solução e acionar procedimentos.
	Controle de Acesso Permitir que administradores e gerentes determinem o que os indivíduos podem acessar, de acordo com suas credenciais de segurança, após a autorização, a autenticação, o controle e a monitoração dessas atividades.
	Proteção das Comunicações Examinar os sistemas de comunicações internos, externos, públicos e privados; estruturas de rede; dispositivos; protocolos; acesso remoto e administração.
	Emprego de Criptografia Empregar técnicas, abordagens e tecnologias de criptografia.
	Implementação de controles de segurança Controlar atividades de pessoal e procedimentos de segurança, na utilização dos sistemas necessários às atividades na área cibernética.
	Segurança física Autorizar a entrada e estabelecer os procedimentos de segurança do ambiente operativo, a fim de proteger instalações, equipamentos, dados, mídias e pessoal contra ameaças físicas aos ativos de informação.
	Gestão da Continuidade da Missão e Recuperação de Desastres Preservar as atividades operativas por ocasião da ocorrência de interrupções ou de catástrofes.
Ataque Cibernético	**Reconhecimento** Investigar em fontes abertas para obter informações obre o alvo.
	Escaneamento (*Scanning*) Encontrar falhas na proteção cibernética do alvo.
	Exploração da Vulnerabilidade

	Realizar ações como: obter acesso, degradar uma aplicação ou negar acesso para outros usuários.
	Manutenção do acesso Manipular *software* instalado no sistema alvo com o objetivo de disponibilizar um *backdoor* para aceso futuro.
	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.
Exploração Cibernética	**Inteligência Cibernética** Realizar ações de busca e de coleta de dados no espaço cibernético, para produção de conhecimento de Inteligência.

Fonte: adaptado de Manual de Guerra Cibernética (BRASIL, 2017)

Na atividade de ataque cibernético, observa-se que as tarefas ocorrem em sequência, sendo por essa característica conhecidas como as fases do ataque cibernético. Ainda, as ações demandas em cada uma das tarefas são condutas técnicas, variando em grau de complexidade, e são detalhadas em manuais técnicos das atividades de G Ciber.

Destarte, constata-se que as capacidades operativas da G Ciber podem atuar de diferentes maneiras e em distintas vertentes da informação dentro das operações militares, de modo a colaborar com o êxito da missão.

2.2 PODER DE COMBATE

Para poder verificar se a guerra cibernética atua como elemento multiplicador do poder de combate, faz-se necessário compreender esse conceito. Esta subseção tem a citada finalidade, objetivando descrever, de maneira objetiva, o poder de combate no âmbito das operações militares.

O Glossário das Forças Armadas (2015) define como poder de combate “a capacidade global de uma organização para desenvolver o combate, a qual resulta da combinação de fatores mensuráveis e não mensuráveis que intervêm nas operações, considerando-se a tropa com seus meios, valor moral, nível de eficiência operacional atingido e o valor profissional do comandante. Sua avaliação é relativa, só tendo significação se comparada com o do oponente”.

Fica claro, na definição acima, que o poder de combate exige a análise de uma série de fatores não descritos, e que a sua medida só é possível quando comparada a de outra parte.

A Estratégia Nacional de Defesa brasileira (BRASIL, 2008) confere especial destaque ao poder de combate, ao citar o termo em várias oportunidades, particularmente ao referir-se às características doutrinárias do Exército Brasileiro, conforme a seguir.

> A modularidade confere a um elemento de combate a condição de, a partir de uma estrutura básica mínima, receber módulos que ampliem o seu poder de combate [...]
> A elasticidade, por sua vez, é a característica que, dispondo uma força de adequadas estruturas de comando e controle e de logística, lhe permite variar o poder de combate pelo acréscimo ou supressão de estruturas [...] (BRASIL, 2008)

Já o manual de Fundamentos – Doutrina Militar Terrestre (2014) procura particularizar e tornar mais tangível o conceito de poder de combate, incluindo a palavra “terrestre” ao final do termo. Assim, tem-se o poder de combate terrestre, o qual é composto por oito elementos essenciais: Liderança, Comando e Controle, Informações, Movimento e Manobra, Inteligência, Fogos, Logística e Proteção. Didaticamente, esses elementos estão representados na figura abaixo, retiradas do mesmo manual.

Fonte: adaptado de Fundamentos – Doutrina Militar Terrestre (2014)

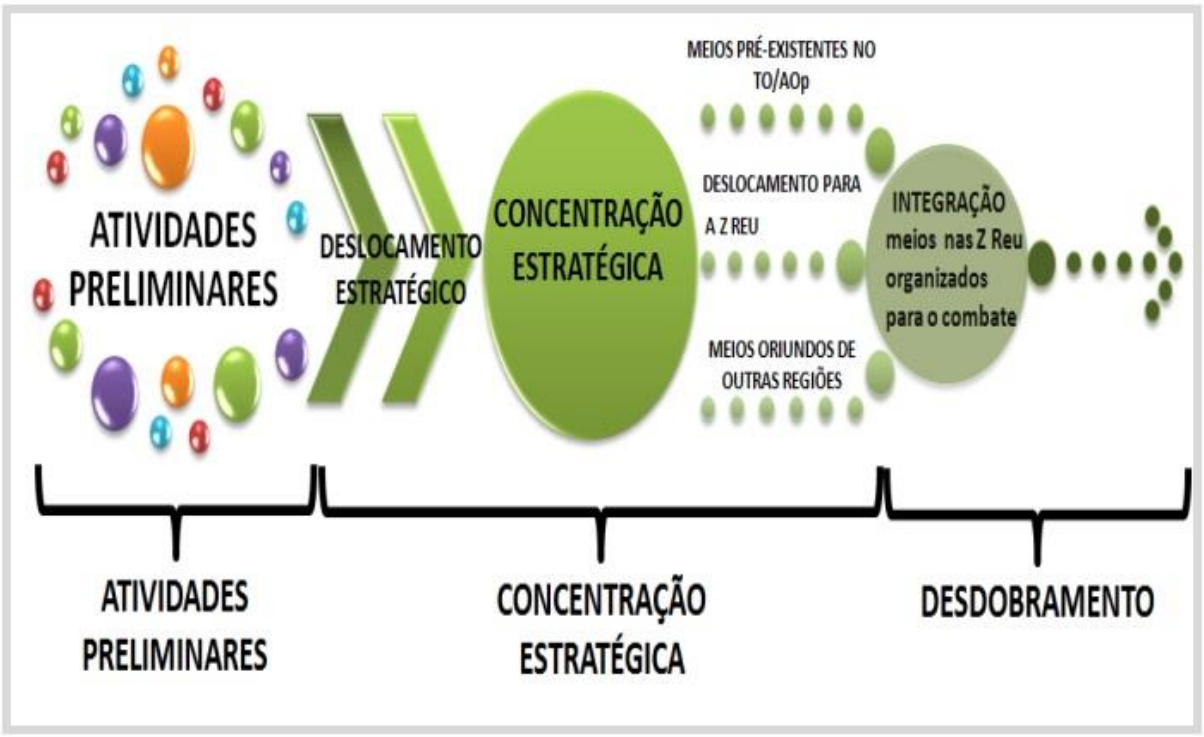
Das assertivas acima pode-se inferir que o poder de combate está presente em todos os escalões, sendo que os meios que compõem a estrutura que irá atuar em proveito da missão são fundamentais para definir o quão poderoso é esse poder de combater. Salienta-se que a força combativa é composta pelos elementos essenciais citados anteriormente, os quais possuem íntima ligação e podem ser influenciados pela guerra cibernética.

Ao entender os conceitos básicos de poder de combate, é promovido o estudo de como esse poder é gerado. No âmbito da Força Terrestre Componente (FTC), o manual EB20-MC-10.301 – A FTC nas Operações destaca que a geração do Poder de Combate possui como finalidade “permitir que as operações táticas previstas no Plano de Operações da FTC possam ser desencadeadas no prazo previsto” (BRASIL, 2014).

O manual também salienta que a FTC possui o desafio de ser composta – já que a mesma é flexível – por elementos que tenham a capacidade de cumprir a missão atribuída. Para tanto, após a definição da organização da Força Componente, esses elementos são deslocados estrategicamente para poder exercer a sua atuação de modo eficaz.

As etapas da geração do poder de combate da FTC, conforme o manual doutrinário citado acima, são três: a fase de Atividades Preliminares, a fase de

Concentração Estratégica e a fase de Desdobramento. Todas estão ilustradas na figura abaixo.



Fonte: adaptado de a FTC nas Operações (2014)

Na etapa de Atividades Preliminares, são executadas ações que permitem aos meios ou unidades que foram selecionados para comporem a FTC ficarem em condições de realizarem o seu deslocamento para o Teatro de Operações (TO) ou Área de Operações (A Op). É nessa fase que são definidos os elementos que serão empregados para que seja cumprida a missão, de modo a atingir-se o Estado Final Desejado.

Já na fase da Concentração Estratégica, os meios ou unidades são deslocados para o Teatro de Operações / Área de Operações, estando intimamente ligados à função de combate Movimento e Manobra, bem como a Logística.

Finalmente, na etapa do Desdobramento ocorre o “movimento dos elementos de emprego (pessoal e material, já devidamente integrados nas suas unidades) da área de concentração estratégica (ou aquartelamento, no caso das unidades que já se encontrem no interior do TO / A Op) até as suas Zonas de Reunião ou bases de combate. Consiste, ainda, na integração de novos meios aos elementos de emprego, sendo que ao final a FTC estará pronta para iniciar as operações” (BRASIL, 2014). Percebe-se que, nesse momento, é possível que poder de combate

seja agregado à FTC, a exemplo de frações de G Ciber que possam incorporar os elementos que atuarão junto da Força Componente.

Nesse sentido, tem-se que a fase de geração de poder de combate de uma FTC é primordial para que se obtenha êxito na missão atribuída, sendo que a G Ciber é capaz de gerar reflexos para essa mesma etapa do processo.

2.3 A FORÇA TERRESTRE COMPONENTE EM OPERAÇÕES OFENSIVAS

Esta subseção busca apresentar as características de uma Força Terrestre Componente atuando em operações ofensivas, desde os seus conceitos básicos para compreensão até a estrutura de guerra cibernética existente dentro dessa Força Singular.

Primeiramente, o Manual de Campanha Força Terrestre Componente (2014) traz como definição de FTC “o comando singular responsável pelo planejamento e execução das operações terrestres, no contexto de uma operação conjunta. Possui constituição e organização variáveis, enquadrando meios da Força Terrestre adjudicados ao Comando Operacional, bem como de outras Forças Singulares necessários à condução das suas operações”.

Assim sendo, fica lúcida a missão precípua da FTC, qual seja a de contribuir com o Comando Operacional para que os objetivos sejam atingidos e, em última instância, para que o combate terrestre seja vencido.

O conceito também define uma questão de importância crucial: a FTC não possui organização fixa, sendo que ela deve ser composta pelos meios que melhor atendam o cumprimento da missão atribuída. Isso explica a sua composição flexível, o que gera implicações na estrutura da Força Singular, inclusive na área da cibernética. Como exemplo, uma FTC pode enquadrar Grandes Comandos operativos (Divisões de Exército), Grandes Unidades (Brigadas) ou até mesmo unidades e subunidades independentes empregadas.

Ao passar para um maior detalhamento das possibilidades de uma Força Terrestre Componente, verifica-se dois pontos importantes: a atuação no Amplo Espectro e o foco no atingimento de um Estado Final Desejado.

As operações em Amplo Espectro “têm por característica a combinação (simultânea ou sucessiva) de diferentes atitudes: Ofensivas, Defensivas e de Cooperação e Coordenação com Agências, com máxima integração entre as forças e com outras agências, tudo isso aplicado em uma escala variável de violência”

(BRASIL, 2014). Portanto, torna-se nítido que a flexibilidade de uma FTC é fator preponderante para o sucesso de sua missão, haja vista a gama de ações a serem desencadeadas em prol dos diversos tipos de operações.

O Estado Final Desejado, conforme o Glossário do Termos e Expressões para uso no Exército, é definido conforme abaixo:

> Condições gerais a serem estabelecidas numa determinada área ou ambiente (ou sobre determinados grupos), cuja obtenção indicará que a missão recebida foi efetivamente cumprida, podendo-se passar, a partir daí, para a desmobilização total ou parcial dos meios empregados. É uma situação, política ou militar, favorável que deve ser alcançada quando a operação estiver finalizada. (BRASIL, 2018)

Desse modo, o Estado Final Desejado (EFD) é o conceito que guia a missão da fração que está executando uma determinada operação, em particular uma FTC. Para se chegar ao EFD, faz-se necessário o uso de uma metodologia cartesiana de estudo da missão recebida pelos elementos encarregados de executá-la, na qual são avaliados inúmeros itens de fundamental relevância para o êxito das ações, o que contribui para o balizamento do objetivo final.

Assim, tem-se que uma FTC pode participar de vários tipos de operações, dentre as quais destacam-se, para o presente trabalho, as Operações Ofensivas (Op Of). Esse tipo de operação é caracterizado, de acordo com o Manual de Campanha Operações Ofensivas e Defensivas, por uma “ação decisiva de emprego da força militar no campo de batalha, para impor a nossa vontade sobre o inimigo que se concentra para o combate de alta intensidade, representando o melhor caminho para se obter a vitória” (BRASIL, 2017). Nota-se que é o tipo de operação que deve ser privilegiada, pois sempre trará, de acordo com a doutrina, os melhores resultados para quem as tiver executando.

O manual acima citado, do Comando de Operações Terrestres, ainda traz as principais finalidades de uma Op Of:

> a) destruir forças inimigas;
> b) conquistar áreas ou pontos importantes do terreno que permitam a obtenção de vantagens para futuras operações;
> c) obter informações sobre o inimigo, particularmente sobre a situação e

> o poder de combate;
> d) adquirir ou comprovar dados referentes ao terreno e às condições meteorológicas;
> e) confundir e distrair a atenção do inimigo sobre o esforço principal, desviando-o para outras áreas;
> f) antecipar-se ao inimigo para obter a iniciativa, aproveitando qualquer oportunidade que se apresente, negando-lhe qualquer tipo de vantagem;
> g) fixar o inimigo, restringindo-lhe a liberdade de movimento e manobra, mediante diferentes esforços e apoio de fogo, com o objetivo de permitir concentrar o máximo poder de combate sobre ele no ponto selecionado;
> h) privar o inimigo de recursos essenciais com os quais sustente suas ações, realizando atividades e operações em profundidade; e
> i) desorganizar o inimigo mediante ataques sobre meios e/ou instalações essenciais para geração e emprego do seu poder de combate. (BRASIL, 2017)

Verifica-se que os objetivos das Op Of são extremamente variados e demandam uma ampla diversidade de ações, desde aquelas mais voltadas para um caráter bélico até as direcionadas para dissimulação. Dessa maneira, já é possível visualizar que a G Ciber pode contribuir com diferentes intensidades sobre esse tipo de operação, considerada prioritária sob a ótica doutrinária.

As Op Of são divididas em cinco tipos, sendo que o Ataque possui algumas formas de manobra específicas, conforme a tabela a seguir.

OPERAÇÕES OFENSIVAS	
TIPOS DE OPERAÇÕES	**FORMAS DE MANOBRA**
MARCHA PARA O COMBATE	-
RECONHECIMENTO EM FORÇA	-
ATAQUE	ENVOLVIMENTO
	DESBORDAMENTO
	PENETRAÇÃO
	INFILTRAÇÃO
	ATAQUE FRONTAL
APROVEITAMENTO DO ÊXITO	-
PERSEGUIÇÃO	-

Tab 3-1 – Formas de manobra das operações ofensivas

Fonte: adaptado de Operações Ofensivas e Defensivas (BRASIL, 2017)

Com o intuito de que sejam exploradas prováveis possibilidades de atuação da G Ciber, de modo a contribuir com o poder de combate da FTC, faz-se necessária a compreensão, ainda que superficial, de cada um dos tipos de Op Of.

A marcha para o combate é caracterizada por um “movimento tático na direção do inimigo, com a finalidade de obter ou restabelecer o contato com este e/ou assegurar vantagens que facilitem operações futuras” (BRASIL, 2017). Já o reconhecimento em força possui o objetivo de testar e revelar o dispositivo, bem como o valor do inimigo, além de tentar obter outras informações a seu respeito. Percebe-se que esses dois tipos de operação permitem o uso de frações cibernéticas para atuar de acordo com os seus objetivos, dados os produtos que cada uma pretende atingir ao final de missão.

Já o ataque é “o ato ou efeito de conduzir uma ação ofensiva contra o inimigo, tendo por finalidade a sua destruição ou neutralização. Pode ser de oportunidade ou coordenado. A diferença entre eles reside no tempo disponível ao comandante e seu estado-maior (EM) para o planejamento, para a coordenação e para a preparação antes da sua execução” (BRASIL, 2017). É um dos principais tipos de operação utilizados pela Força Terrestre, já que deve ser procurada e priorizada sempre que possível, considerando que um dos preceitos doutrinários atuais infere que a situação defensiva deve ser sempre observada como uma situação temporária.

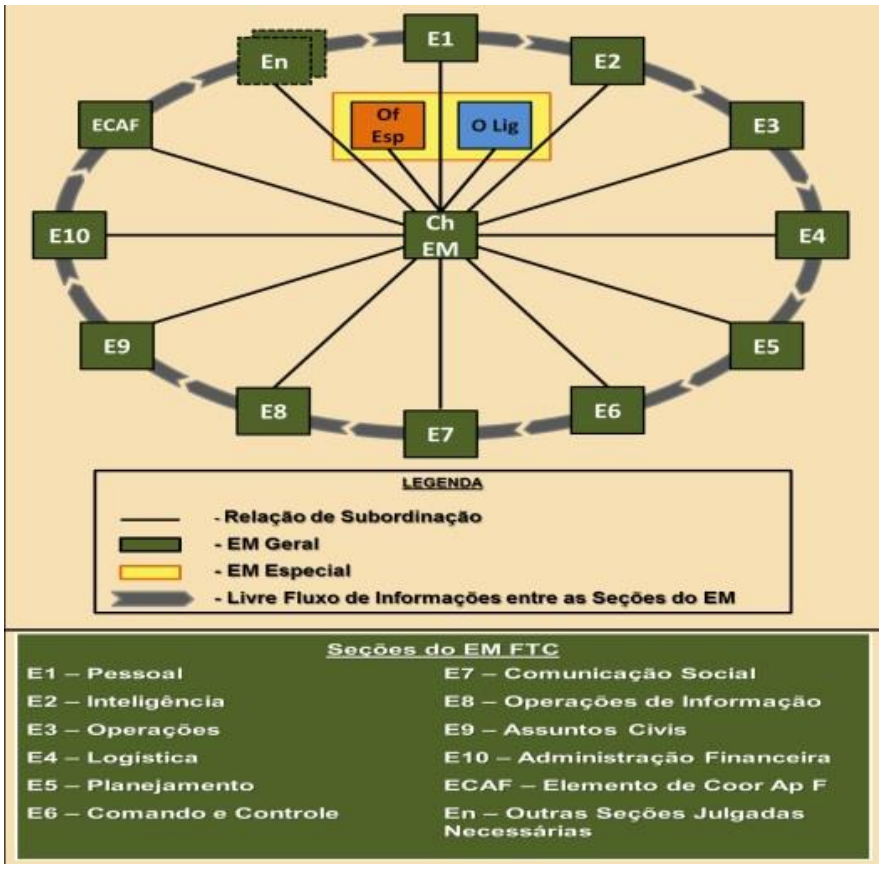
Os dois últimos tipos de Op Of são o aproveitamento do êxito e a perseguição. No aproveitamento do êxito, que “é a operação que se segue a um ataque exitoso e, normalmente, tem início quando a força inimiga se encontra em dificuldades para manter suas posições” (BRASIL, 2017), a principal característica é o avanço contínuo e rápido das forças amigas, tendo como objetivo a ampliação de vantagens obtidas em um ataque e a anulação da capacidade inimiga de reorganizar-se ou realizar um movimento retrógrado ordenado.

A perseguição “é a operação destinada a cercar e destruir uma força inimiga que está em processo de desengajamento do combate ou que tenta fugir. Ocorre, normalmente, logo em seguida ao aproveitamento do êxito e difere deste pela não previsibilidade de tempo e lugar de emprego, e por sua finalidade principal, que é a de completar a destruição da força inimiga” (BRASIL, 2017).

Tem-se, portanto, que as Operações Ofensivas, por serem ações que possuem prioridade e constituem-se das formas fundamentais de atuação de uma

Força Armada, necessita de um amplo poder de combate para o cumprimento de suas missões. Esse poder de combate pode ser aumentado, em várias situações, pelo emprego da Guerra Cibernética, que irá variar a constituição de seus elementos apoiadores na medida do Estado Final Desejado a ser atingido pela força, em especial pela Força Terrestre Componente.

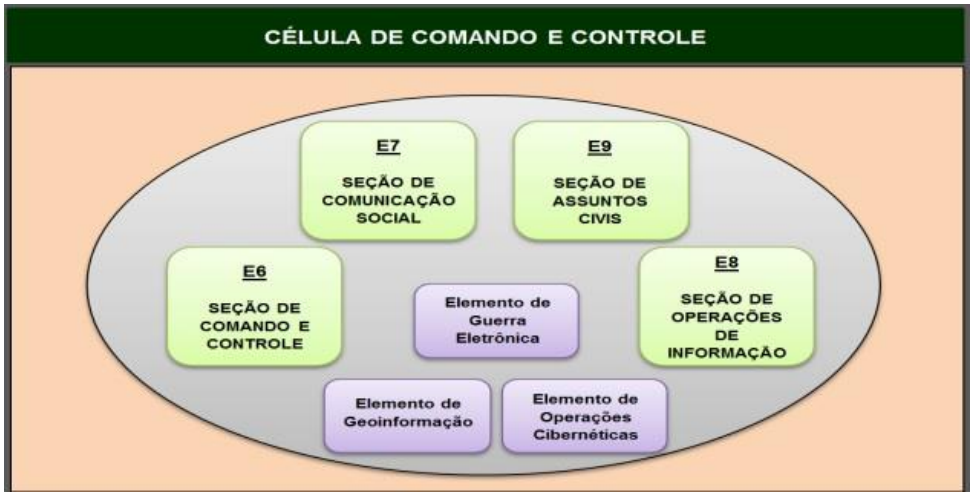
Para melhor entendimento do emprego da G Ciber dentro da FTC, faz-se necessário entender a organização da mesma. O comando da Força Terrestre Componente possui o seu Estado-Maior (EM) dividido em diversas seções afetas às áreas de interesse, conforme abaixo.



Fonte: adaptado de Força Terrestre Componente (BRASIL, 2014)

Verifica-se que as seções possuem assuntos diferenciados, e que irão auxiliar o comandante da Força Singular a escolher a melhor linha de ação durante a sua tomada de decisão.

Dentro da célula de Comando e Controle da FTC encontra-se o elemento que irá contribuir diretamente com o assessoramento no campo cibernético, conforme figura abaixo extraída do Manual da FTC (BRASIL, 2014).



Fonte: adaptado de Força Terrestre Componente (BRASIL, 2014)

Portanto, a FTC já faz uma previsão de elementos de Operações Cibernéticas em sua estrutura, inseridos dentro da célula de Comando e Controle da Força Singular. A alimentação desse elemento, com informações que possam ser pertinentes para o EM da FTC, será realizada pelas demais estruturas existentes na própria organização dos meios, quando disponíveis.

Destarte, quando for ativada a Estrutura Militar de Defesa, a FTC será apoiada por uma estrutura de G Ciber. Essa estrutura engloba elementos de vários meios e com capacidades diferenciadas, de acordo com a tabela abaixo.

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: adaptado de manual de Guerra Cibernética (BRASIL, 2017)

Tem-se, assim, que, como a estrutura da FTC é flexível e feita “sob medida” para a missão designada, os elementos cibernéticos que a compõem também variam de acordo com a demanda, podendo ser, por exemplo, um batalhão ou somente uma turma dessa mesma unidade.

Apura-se, também, que cada elemento possui capacidades operativas distintas, com destaque para o Batalhão de Guerra Eletrônica, capaz de desempenhar as três capacidades: ataque cibernético, proteção cibernética e exploração cibernética.

A G Ciber, no contexto da FTC, possui um emprego singular nas operações ofensivas. Segundo o Manual de G Ciber (2017), nesse tipo de operação crescem

de importância as ações de ataque e de exploração cibernética. Ainda, “em coordenação com os fogos e com a guerra eletrônica, deve-se elaborar uma lista de alvos cibernéticos (LIA Ciber) e uma lista priorizada de alvos cibernéticos (LIPA Ciber)”.

Um detalhe primordial é que as tarefas de ataque cibernético, como reconhecimento (investigação em fontes abertas para obter informações sobre o alvo), escaneamento (encontrar falhas na proteção cibernética do alvo) e exploração de vulnerabilidades, podem ser realizadas em apoio às operações da FTC, sendo integradas com as diferentes funções de combate.

Outra característica de ação cibernética de uma FTC em Op Of é a execução de tarefas ofensivas que procurem prejudicar o funcionamento de infraestruturas oponentes ou negar serviços do mesmo, dentro da sua zona de ação. Além disso, a exploração cibernética poderá atuar de modo a contribuir na produção de dados para a inteligência de fonte cibernética.

Por fim, as ações de proteção cibernética, desempenhada por todos os elementos cibernéticos previstos para atuarem dentro da FTC, possuem caráter permanente em todas as fases da operação, de modo a garantir o funcionamento eficaz dos sistemas de informação durante todo o período da missão.

3 METODOLOGIA

O presente capítulo tem por objetivo apresentar, com clareza e detalhamento, o itinerário a ser percorrido para se chegar à resposta do problema exposto na pesquisa, qual seja o de verificar em que medida a Guerra Cibernética contribui para aumentar o poder de combate da Força Terrestre Componente em operações ofensivas. Desse modo, serão explicitados os procedimentos a serem adotados nos levantamentos documentais e bibliográficos, bem como os instrumentos e técnicas para a análise dos dados, visando esclarecer os resultados que serão obtidos no presente estudo.

A pesquisa a ser realizada será de cunho qualitativo, já que a sua essência está nas respostas a serem obtidas na investigação com os instrumentos devidos, e não necessariamente em uma grande amostra, já que o prioritário é a análise dos dados coletados.

Portanto, de modo a facilitar a compreensão do assunto, esta seção está dividida nos seguintes tópicos: Delimitação da Pesquisa, Concepção Metodológica e Limitações do Método.

3.1 DELIMITAÇÃO DA PESQUISA

O tema ora descrito para a pesquisa, qual seja a Guerra Cibernética, é composto por inúmeras vertentes, tornando-o bastante abrangente. De forma a mitigar e otimizar o estudo, esta seção buscará delimitar o assunto, permitindo a confecção de uma referência para que seja estruturada uma base teórica que busque uma solução ao problema proposto.

Como critérios de inclusão, serão selecionadas fontes de pesquisa baseadas em publicações militares que abordem as temáticas de Doutrina de Guerra Cibernética, Doutrina de Operações Militares e manuais afetos ao tema, bem como periódicos militares, instruções provisórias, instruções gerais, instruções reguladoras, portarias normativas e diretrizes. Fora do escopo militar, serão buscados trabalhos acadêmicos, como artigos científicos e livros, relacionados ao emprego da G Ciber.

Já como estratégia para a busca em bases de dados eletrônicas, serão designados os seguintes termos de descrição para a pesquisa: “guerra cibernética,

defesa cibernética, meios de tecnologia da informação, cibernética nas operações", observando as particularidades de cada base de dados.

Ressalta-se que, como pressuposto de inclusão de dados na pesquisa, serão considerados válidos estudos no idioma português, inglês, espanhol e alemão, desde que publicados a partir de 2008 – esse marco temporal foi definido pela lógica das transformações implementadas no Exército Brasileiro após a elaboração da END. Da mesma maneira, serão excluídos trabalhos cujo foco central seja guerra eletrônica, estudos que abordem a guerra cibernética na área administrativa militar e estudos que abordem a guerra cibernética no nível operacional, estratégico ou político.

Outros fatores que colaboram para as delimitações de interesse da pesquisa estão afetas ao problema proposto. Desse modo, assuntos que estejam em outro nível diferente da Força Terrestre Componente, bem como assuntos que abordem operações que não sejam ofensivas, não serão considerados para a análise de dados.

3.2 CONCEPÇÃO METODOLÓGICA

A pesquisa do presente estudo possui caráter qualitativo descritivo. Pesquisa de abordagem qualitativa porque a sua essência está nas respostas que forem obtidas em investigação por meio dos instrumentos devidos, e não necessariamente em uma grande amostra, já que o que é prioritário são as análises dos dados coletados. Pesquisa de cunho descritivo porque o trabalho não está baseado em hipóteses de estudo, sendo o processo mais indicado para a exposição dos efeitos da G Ciber em uma FTC.

Assim, o estudo buscará, inicialmente, a busca e seleção de todos os conceitos que fazem parte do problema a ser solucionado para, então, executar uma análise pormenorizada dos dados coletados. Para tanto, faz-se necessário a revisão bibliográfica dos diversos manuais, regulamentos, decretos, periódicos e demais documentos que tratam sobre o assunto, dentro das limitações descritas na seção acima. A pesquisa será desenvolvida buscando apresentar os diversos fundamentos da G Ciber, particularizando as suas atividades, tarefas e ações nas operações exploradas pela F Ter. O poder de combate também será objeto de estudo, já que é parte crucial do problema, bem como a estruturação de uma FTC em Op Of,

procurando interligar os inúmeros conceitos com o assunto do estudo, objetivando uma resposta ao problema proposto.

Em um segundo momento, será aplicada uma entrevista com o Chefe da Divisão de Cibernética do Centro de Instrução de Guerra Eletrônica (CIGE), possuidor de notório conhecimento sobre o assunto objeto do estudo em tela. O objetivo é coletar opinião embasada das consequências para o poder de combate, em especial dos benefícios, advindos do emprego da Guerra Cibernética em operações ofensivas de uma Força Terrestre Componente. Desse modo, a qualidade do trabalho será elevada de maneira considerável, já que será composto pela visão de um especialista de alto nível no que se refere à formação de recursos humanos do campo cibernético do EB.

O instrumento a ser utilizado para a coleta dos dados do especialista do CIGE, descrito acima, será a entrevista. A escolha por esse recurso deve-se ao fato de que é o que melhor atende ao objetivo de se obter informações precisas sobre um determinado assunto, qual seja o da influência da G Ciber no poder de combate da FTC em operações de cunho ofensivo. A entrevista será do tipo padronizada ou estruturada, com perguntas previamente formuladas e que permitem ao pesquisador dar o sentido desejado à questão proposta ao entrevistado.

3.3 LIMITAÇÕES DO MÉTODO

Esta subseção tem por finalidade descrever, de forma sucinta, as possíveis limitações do método e como isso pode refletir no resultado da pesquisa.

A primeira dificuldade é a de que diversos aspectos doutrinários sobre a Guerra Cibernética dentro do EB ainda estão em pauta no comando do Exército. Por se tratar de um assunto relativamente recente, as discussões acerca do tema continuam ocorrendo. Prova de tal situação é o próprio manual de campanha de Guerra Cibernética, que teve a sua primeira versão publicada no ano de 2017. Destarte, há uma dificuldade na obtenção de grande volume de dados consistente, já testados e consagrados pela doutrina.

Além disso, existem poucos especialistas militares que atuam no campo virtual em tela na presente pesquisa. O CIGE, órgão gestor e formador dos recursos humanos para atuação cibernética, teve o seu primeiro curso de Guerra Cibernética concluído em 2012, formando os primeiros guerreiros cibernéticos do Exército Brasileiro no mesmo ano. Tal fato contribui para que haja uma variedade pequena

de opiniões acerca do assunto, limitando as possíveis ideias a serem exploradas na pesquisa.

Não obstante, salienta-se a importância escolha de um especialista para que seja entrevistado e que, teoricamente, travou contato com inúmeros militares formados pelo Centro de Instrução de Guerra Eletrônica durante anos, qual seja o Chefe da Divisão de Cibernética daquele Centro. Isso permitirá que, ainda que com limitações, seja obtida uma visão embasada sobre a influência da G Ciber no poder de combate da FTC.

4 RESULTADOS E DISCUSSÃO

A seguir, são apresentados e discutidos os resultados obtidos por meio das entrevistas estruturadas aplicadas durante a pesquisa. A finalidade precípua é comprovar ou refutar alguns dos tópicos explorados no desenvolvimento, de modo a contribuir para a solução do problema apresentado, qual seja o de mensurar os efeitos da Guerra Cibernética no poder de combate da Força Terrestre Componente em operações ofensivas.

As entrevistas foram executadas com dois militares de renomada experiência, como já abordado nos capítulos iniciais do trabalho. A condução da atividade foi de forma semiestruturada, como também já explicado anteriormente, com o intuito de direcionar para o objetivo proposto, por meio de perguntas previamente preparadas. Ainda assim, o entrevistado foi orientado a contribuir de maneira espontânea, se assim o desejasse, encontrando-se à vontade para expor mais pontos de vista pertinentes ao assunto. As transcrições das entrevistas encontram-se como apêndices à presente pesquisa, sendo que foram anexadas de maneira fidedigna, sem uma eventual correção de erros na expressão oral.

O primeiro entrevistado foi o Major de Comunicações Anderson Lellis Alves Moura. O Major Moura foi selecionado devido a sua experiência na área, tendo atuado como Chefe da Seção de Ensino de Guerra Cibernética e como Assessor do Supervisor do Projeto Força Cibernética no Centro de Instrução de Guerra Eletrônica (CIGE). Ressalta-se que o CIGE é o núcleo formador de recursos humanos para a área de cibernética dentro do Exército Brasileiro, ainda que a atual conjuntura esteja modificando essa perspectiva, já que a criação do Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber) está passando a cumprir esse papel. Em que pese a presente evolução, durante anos o CIGE foi – e continua sendo – o condutor da capacitação operacional do setor cibernético, gerenciando os talentos humanos da área.

O Major Moura atuou na função descrita durante quatro anos, tendo ampla experiência profissional relacionada ao setor cibernético: foi o responsável pela área de Tecnologia da Informação em todas as Organizações Militares em que trabalhou desde 2001, vindo a concluir o primeiro curso de Guerra Cibernética para oficiais, em 2012. A partir de então, dedicou-se ao aperfeiçoamento das técnicas

cibernéticas, particularmente nas atividades de proteção, exploração e ataque cibernético, incluindo a participação em eventos nacionais e internacionais.

O segundo entrevistado da pesquisa foi o Major de Comunicações Flávio Regueira Costa, o qual foi durante quatro anos instrutor do curso de Guerra Cibernética, desenvolvido no CIGE. O Major Regueira também possui vasto conhecimento do setor, tendo iniciado a sua formação durante a preparação da execução do primeiro curso de Guerra Cibernética (G Ciber). Nessa oportunidade, o referido militar trabalhou no desenvolvimento do Simulador de Operações Cibernéticas – ferramenta utilizada durante o curso de G Ciber – e no acompanhamento de proteção contra *malwares* nacional. O Major Regueira atuou, ainda, como membro de uma equipe multidisciplinar que representou o Exército Brasileiro em competições cibernéticas no Brasil e no exterior, obtendo resultados expressivos. Participou, ainda, ao trabalhar junto ao Comando de Defesa Cibernética, no planejamento e coordenação da Força Tarefa Conjunta Cibernética em operações no nível do Ministério da Defesa.

Desse modo, fica constatado o credenciamento que os entrevistados possuem em opinar sobre a atuação da G Ciber em vários contextos, particularmente como multiplicadora do poder de combate da Força Terrestre Componente. O cabedal de conhecimento e bagagem proveniente dos dois militares imprime confiabilidade nos resultados colhidos com as entrevistas, validando as ideias expostas no presente capítulo.

Inicialmente, cabe ressaltar o principal objetivo da Seção de Guerra Cibernética do CIGE, qual seja o de capacitar os recursos humanos na área de cibernética. Essa capacitação ocorre não somente no âmbito do Exército Brasileiro, mas também com militares da Marinha do Brasil e da Força Aérea Brasileira, abrangendo as três forças singulares do Estado brasileiro. Já é possível verificar a importância dos cursos de G Ciber ministrados, tendo em vista a amplitude dos mesmos, bem como a necessária preparação e conhecimento intelectual demandada pelos instrutores do Centro. Existe, ainda, um objetivo secundário de identificar e avaliar materiais relacionadas à cibernética e que sejam de interesse para as Forças Armadas, em particular para o EB.

Como forma de se obter um panorama sobre a atual situação dos recursos humanos formados na área de cibernética pelo Exército, foram realizadas perguntas iniciais relacionadas com a visão dos entrevistados sobre esses militares

mencionados. Uma das indagações foi sobre a diferença entre os cursos de G Ciber existentes para oficiais e praças, haja vista que as funções a serem desempenhadas pelos concludentes, nesses dois universos distintos, também serão diferenciadas. A análise de ambos os instrutores foi similar, concluindo que os cursos não são iguais, mas o caráter eminentemente técnico do conhecimento cibernético faz com que hajam diversos períodos e pontos em comum. Apesar disso, há uma maior carga horária programada para os oficiais em disciplinas de planejamento e gestão, direcionando o referido universo para os futuros cargos a serem ocupados.

Com relação à formação do guerreiro cibernético, a avaliação dos entrevistados foi de que, dado que o setor cibernético é relativamente novo no âmbito das Forças Armadas – no contexto da doutrina –, a capacitação do pessoal é um dos primeiros passos a serem desenvolvidos para o atingimento de um nível equilibrado. Assim, a formação inicial é condizente com o esperado, mas é necessário que haja uma continuidade de aquisição de conhecimento e também de prática na atividade, envolvendo a atuação de outros órgãos da Força Terrestre.

O curso de Guerra Cibernética, tanto para oficiais quanto para sargentos, consiste em aproximadamente quatro meses de ensino à distância e três meses de ensino presencial. Existem vários requisitos técnicos a serem cumpridos para que o militar ingresse na fase presencial no CIGE, o que permite uma avaliação continuada dos instruendos. A formação ainda é bastante dependente de conhecimento prévio adquirido individualmente, e que muitas vezes não faz parte das grades curriculares dos cursos de especialização militares. Além disso, o conhecimento cibernético, por ser demasiadamente técnico, exige prática periódica e constante, demandando esforço na política de pessoal para reter pessoal capacitado na área citada.

A despeito dos desafios citados, a formação do guerreiro cibernético, feita majoritariamente pelo CIGE, atende – de acordo com a visão dos entrevistados – os objetivos iniciais traçados pelo Exército no que tange aos recursos humanos da área. O curso possui um padrão rigoroso de cobrança cognitiva, ratificando o alto nível dos profissionais que se tornam especialistas cibernéticos.

O Sistema de Guerra Cibernética do Exército foi o tema de outro questionamento aos militares entrevistados. Com relação ao assunto, a conclusão foi de que ainda há o que se desenvolver, principalmente no campo material e de equipamentos. Existem alguns ativos que são considerados o estado da arte e que

cumprem a finalidade, mas a demanda é maior do que a necessidade. Já o ativo mais importante recaiu, mais uma vez, sobre o recurso humano: a excelente formação dada pelos cursos de especialização e do próprio sentimento de profissionalismo do militar confere alto grau de valor a este item, sendo unanimidade entre os entrevistados.

Uma das oportunidades de melhoria para o Sistema, o qual é composto por simuladores, equipamentos, instalações, tecnologias, recursos humanos, dentre outros ativos, é a aquisição de materiais que contribuam diretamente com o objetivo a ser atingido. Um dos entrevistados relatou que a pontual falta de integração em alguns setores faz com que se perca um pouco da sinergia necessária para que o sistema como um todo opere de maneira adequada. Uma das soluções para essa questão seria a definição de metas que sejam mais tangíveis e voltadas para a prática do guerreiro cibernético, o que impactaria em uma confluência de esforços para um mesmo objetivo, resultando em um provável ganho em aspectos relacionados ao material humano e equipamentos.

Ainda sobre o Sistema de Guerra Cibernética, foi explorado o Simulador de Operações Cibernéticas (SIMOC), adquirido recentemente pelo CIGE e utilizado nos cursos ministrados pelo Centro. Os majores Moura e Regueira destacaram a importância deste ativo, que foi desenvolvido com base nos melhores simuladores existentes da época (meados de 2013) e atendendo aos requisitos técnicos apresentados pelos instrutores de cibernética do CIGE, sendo um dos principais equipamentos que colaboram com a formação e preparação de integrantes do setor. As instalações do Sistema também estão em processo de aprimoramento, já que a mudança de sede do Comando de Defesa Cibernética e do Centro de Defesa Cibernética na cidade de Brasília visam aperfeiçoar os canais técnicos e unificar os diversos ramos afins, contribuindo para a integração do setor cibernético.

As entrevistas passaram, então, para uma fase mais tática de questionamentos. Primeiramente, foi solicitado para que os entrevistados numerassem, em sequência de prioridade, as frações que, em suas visões particulares, permitam o melhor aproveitamento do elemento de G Ciber atuando em prol do seu respectivo escalão quando da ativação da Estrutura Militar de Defesa por uma Força Terrestre Componente. A primeira prioridade foi unânime e o apontamento foi realizado para o Batalhão de Guerra Eletrônica (BGE), do qual o Exército Brasileiro, atualmente, dispõe de apenas um. Com pequenas variações, as

próximas opções inferiram que os escalões unidade (Batalhões de Comunicações e Batalhões de Comunicações e Guerra Eletrônica, além de Batalhões de Inteligência Militar) são os que teriam a extração do máximo aproveitamento das atividades de Guerra Cibernética. Destarte, tem-se claro pela ótica dos especialistas que os escalões Divisão de Exército e superiores possuem melhor capacidade de serem beneficiados pelos produtos oriundos das frações cibernéticas.

Em seguida, foi perguntado sobre as capacidades operativas que podem ser desenvolvidas por elementos ou frações de G Ciber que possam atuar em proveito de uma FTC, tais como elementos de um Batalhão de Guerra Eletrônica, de um Batalhão de Comunicações e Guerra Eletrônica, dentre outros, ou seja, daquelas tropas especializadas para tais funções. A resposta foi uníssona, confirmando as três capacidades que são levantadas pelo manual de Guerra Cibernética: a proteção, a exploração e o ataque cibernéticos.

Para consubstanciar a discussão dos resultados, cabe uma breve teoria sobre o que são essas três capacidades. A proteção cibernética pode ser feita por escalões que não são especializados, como uma Companhia de Comunicações de uma Brigada. Essa capacidade operativa consiste na condução de ações para “neutralizar ataques e exploração cibernética contra nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de G Ciber em face de uma situação de crise ou conflito, sendo de caráter permanente” (BRASIL, 2017). Portanto, é lógico que possa ser desenvolvida por organizações militares não necessariamente especialistas em cibernética.

Já o ataque cibernético é a condução de ações “para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente” (BRASIL, 2017). Nesse caso, fica patente a vocação técnica dessa capacidade, fazendo com que a mesma seja específica para tropas especializadas, como as que compõem as frações de Guerra Eletrônica.

Por fim, na exploração cibernética tem-se a condução de ações de “busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas” (BRASIL, 2017). Da mesma maneira que a

capacidade operativa do ataque cibernético, na exploração é exigido alto grau técnico, orientando-se para tropas especializadas.

Cada uma das três capacidades operativas citadas acima é composta por um conjunto de atividades, tarefas e ações já descritas no desenvolvimento do presente trabalho. Desse modo, cria-se uma espécie de molde do que uma tropa necessita em termos de doutrina, organização, material, educação, infraestrutura, meios, dentre outros aspectos, para que seja capaz de possuir tais capacidades. Esse é um dos motivos pelo qual nem todas as frações de guerra eletrônica ou de comunicações do Exército Brasileiro são capazes executar ações de exploração e ataque cibernético.

Ao serem questionados sobre que tipo de ação pode ser realizada, prioritariamente, pela G Ciber contra oponentes com poder de combate superior, ambos os entrevistados foram taxativos em afirmar que a capacidade operativa exploração cibernética é essencial. Essa forma de atuação é vital para que a consciência situacional do decisor esteja sempre atualizada, sendo que seus produtos irão beneficiar as demais capacidades cibernéticas – ataque e proteção.

Como potenciais alvos cibernéticos, capazes de compor uma Lista de Alvos Cibernéticos (LIA) em um contexto de operações ofensivas, os especialistas entrevistados elencaram alguns alvos específicos: infraestruturas críticas (particularmente as utilizadas para fins militares, o que pode variar de acordo com a conjuntura), sistemas de comando e controle do oponente, provedores de rede, bases de dados corporativos, operadores de telefonia celular e satelital, radares e sistemas de vigilância. Assim, tem-se uma priorização de objetivos que possuem importância mais alta no contexto da Guerra Cibernética.

Finalmente, como último questionamento, foi solicitado aos entrevistados para que apresentassem de que maneira a G Ciber poderia ser integrada às seis Funções de Combate existentes atualmente na doutrina militar terrestre, de modo a potencializar os efeitos das mesmas no combate. Um entrevistado apresentou várias considerações interessantes para o tema, conforme segue-se na transcrição abaixo:

Transcrição parcial de entrevista

Entrevistador:

De que maneira a G Ciber pode ser integrada às Funções de Combate (Movimento e Manobra, Inteligência, Fogos, Comando e Controle, Proteção e Logística), potencializando os efeitos dessas no combate?

Entrevistado:

Bem, do ponto de vista operacional, a G Ciber pode contribuir no Movimento e Manobra, estando integrada a Prontidão Operativa, pois está em condições de ser empregada desde o tempo de paz. Na Concentração Estratégica, as ações de exploração permitirão o conhecimento da Área de Concentração Estratégica. No Desdobramento, além do reconhecimento das áreas de destino, as ações de ataque podem dificultar o deslocamento tático até a Z Reu. Na Manobra Tática são utilizadas as ações de proteção, de exploração e de ataque com a finalidade de garantir a ação militar e a potencializar. No apoio de Fogo Orgânico as tropas que recebem Elm de G Ciber poderão utilizá-las no nível tático para possibilitar a obtenção de vantagens militares. Na Mobilidade e Contramobilidade as ações de proteção cibernética garantirá o nosso sistema de TIC e as de ataque cibernético dificultarão o deslocamento inimigo.

Na Função de combate Inteligência as ações de exploração cibernética possibilitam a produção continuada do conhecimento em apoio ao planejamento da força, o apoio à obtenção da consciência situacional e as atividades de IRVA (Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos), o apoio à obtenção da superioridade de informações e a busca de ameaças. Neste quesito é importante frisar que as ações de exploração cibernética são as que mais se integram à função de combate inteligência, tendo como principal vantagem a obtenção da informação sem riscos a integridade física dos militares e com um custo reduzido.

Na Função de Combate Fogos as ações de exploração cibernética estão integradas a atividade planejamento e coordenação de fogos, ao levantar alvos, estabelecer medidas de coordenação cibernéticas de apoio de fogo e na seleção dos alvos cibernéticos. Na execução dos fogos, entra as ações de ataque cibernético que são previstos na doutrina como fogos não cinéticos. Cabe a célula de FOGOS integrar todos os meios disponíveis e decidir o melhor momento de utilizar os fogos cibernéticos.

Na função de combate Comando e Controle as ações de proteção e exploração cibernéticas possibilitarão a condução do processo de planejamento e a

condução das operações, o correto funcionamento dos sistemas de TIC dos Postos de Comando e principalmente a gestão do conhecimento e da informação. As ações de ataque podem contribuir nas atividades de informar e influenciar, principalmente dentro das operações de informação.

Na função de combate Proteção a ações de proteção cibernética estão intimamente integradas as medidas de contrainteligência, a defesa química, biológica, radiológica e nuclear (DQBRN) quando se considera a proteção de infraestruturas críticas, as atividades de medidas de guerra cibernéticas previstas na Lista de Tarefas Funcionais (EB70-MC-10.341).

Por fim, na função de combate Logística, a G Ciber estará integrada nas atividades de mobilização de material e pessoal de interesse para o setor cibernético, uma vez que devido a complexidade do combate cibernético, existe uma necessidade da integração de esforços civis e militares em um conflito armado.

Fim da transcrição

O major Regueira ainda colaborou destacando um ponto vital no que tange à contribuição da G Ciber para o incremento do poder de combate de uma força militar. O entrevistado ressaltou a importância da centralização dos meios cibernéticos, dada a complexidade do espaço virtual e a necessidade de profissionais de diversas especialidades, bem como a experiência na área afim. A descentralização, para o entrevistado, diminui a capacidade de solução de problemas, em especial no nível Força Terrestre Componente. O comandante tático, ainda, deve ter conhecimento das capacidades cibernéticas para poder solicitar os efeitos desejados sobre o oponente, sem preocupar-se com o “como” atingir tais efeitos.

5 CONCLUSÃO

A Guerra Cibernética é, indubitavelmente, um dos novos domínios do campo de batalha, que tradicionalmente eram compostos pelos segmentos terrestre, marítimo e aéreo. A espaço virtual tornou-se, sem sombra de dúvida, imprescindível para as operações em qualquer nível ou escalão de atuação. Assim, torna-se imperioso que a Guerra Cibernética seja analisada sob uma ótica especializada e capaz de extrair todos as vantagens que o seu emprego possa garantir ao seu usuário.

O desenvolvimento do presente trabalho procurou atender alguns objetivos específicos. Ressalta-se que tais objetivos tinham como finalidade precípua o entendimento aprimorado da pesquisa como um todo, já que o desconhecimento dessas definições prejudicaria o restante da pesquisa. Ainda, a elaboração dos objetivos específicos fez-se necessária para delimitar e canalizar o estudo.

O primeiro objetivo específico foi o de apresentação dos fundamentos da Guerra Cibernética, identificando as suas tarefas, atividades e ações, em especial nas operações desenvolvidas no espaço terrestre. Calcado em manuais doutrinários, particularmente no manual de campanha de Guerra Cibernética, esses conceitos foram amplamente analisados no desenvolvimento, com exemplos e contextualizações. Salienta-se que a ideia de atuação por tarefas, que compõem as atividades e, em última instancia, constituem parte fundamental para gerar capacidade de uma força militar, é relativamente nova no Exército Brasileiro, fruto de aprimoramentos de estudos realizados e concretizados na década atual. Foram exploradas as três atividades da Guerra Cibernética – proteção, exploração e ataque cibernético –, enfatizando as tarefas atinentes à cada uma delas, como gestão de riscos, defesa ativa, escaneamento e manutenção do acesso. Conclui-se, assim, que o primeiro objetivo específico foi atingido com sucesso.

Já o segundo objetivo era o de identificar o conceito de poder de combate. Considerando que o problema a ser respondido pelo trabalho foi o da contribuição da Guerra Cibernética para o aumento do poder de combate da Força Terrestre Componente, no contexto de operações ofensivas, era de primordial importância o entendimento do conceito supracitado. E assim o poder de combate foi analisado, amparado em manuais doutrinários do Exército Brasileiro, bem como do Ministério da Defesa, datados de pelo menos cinco anos atrás. Foram explorados os oitos

elementos que fazem parte da geração desse poder de combate terrestre: Liderança, Comando e Controle, Informações, Movimento e Manobra, Inteligência, Fogos, Logística e Proteção. Fica nítido que, dados esses elementos, a G Ciber pode contribuir na potencialização das capacidades de vários desses elementos, notadamente Fogos, Comando e Controle, Inteligência e Informações. Infere-se, dessa maneira, que o objetivo de compreender o que é o poder de combate foi alcançado.

O último objetivo específico traçado esteve relacionado com a estrutura de uma Força Terrestre Componente em operações ofensivas. Dessa premissa podem ser extraídas duas ramificações: o entendimento de uma FTC, de maneira geral, e a compreensão das operações ofensivas das quais a mesma pode fazer parte. Durante o desenvolvimento, ambos os tópicos foram abordados, igualmente amparados por bibliografias recentes da doutrina militar do Brasil.

Existem inúmeros conceitos que envolvem uma FTC: o Estado Final Desejado, o modo como é gerado o poder de combate, ou seja, a composição dos meios da força que irá atuar, bem como a estrutura das seções de um Estado-Maior de uma FTC. Esses são alguns dos exemplos de assuntos que foram abordados no segundo capítulo, o qual procurou explorá-los para fornecer uma noção do funcionamento da organização, contribuindo para a compreensão de como as tropas procedem nesse contexto.

No tocante às operações ofensivas, foi feita uma análise pormenorizada dos tipos existentes, aspecto vital para a compreensão de como atuam as tropas em cada situação. Salienta-se que esse conhecimento permitiu a observância posterior de como a G Ciber pode contribuir com o poder de combate, já que cada operação ofensiva possui finalidades distintas, gerando reflexos também diferenciados quando apoiados por elementos ou meios cibernéticos.

Foi verificado, particularmente na FTC, que a célula de Comando e Controle dessa força singular possui elementos de G Ciber em sua composição. Essa fração é o elo de ligação entre uma outra estrutura cibernética que é ativada quando da concepção da Força Terrestre Componente. Tal estrutura pode variar, podendo ser um Batalhão de Guerra Eletrônica, um Batalhão de Comunicações, um Batalhão de Comunicações e Guerra Eletrônica, um Batalhão de Inteligência Militar, uma Companhia de Comando e Controle ou uma Companhia de Comunicações. Assim,

cada uma dessas tropas possui capacidades cibernéticas específicas, englobando ataque, proteção e exploração no campo cibernético.

Desse modo, é possível realizar uma relação entre o que a estrutura cibernética, que é composta “sob medida” para a missão a ser cumprida pela FTC, pode oferecer ao comando enquadrante e os seus efeitos sobre os meios disponíveis, como organizações militares que atuarão como elementos de combate ou serão empregadas em primeiro escalão. Essa relação modifica o poder de combate da força emprenhada, gerando aumento desse mesmo poder.

A finalidade dos objetivos específicos é, além da fundamentação de conceitos importantes – conforme já havia sido destacado –, percorrer o caminho natural até o atingimento do objetivo geral. Novamente, ressalta-se que essa meta é a principal responsável por vislumbrar a resposta ao problema proposto, ou seja, determinar o produto final do presente trabalho.

O objetivo geral foi constituído pela apresentação da contribuição da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas. Isso significa que, ao alcançar esse objetivo, a pesquisa atingiu o intuito de demonstrar qual é tal benefício trazido pela cibernética.

Os meios para atingir-se o objetivo geral já foram especificados, tratando-se dos objetivos específicos, bem como das posteriores entrevistas e seus respectivos resultados, apresentados em capítulo oportuno. O desenvolvimento do trabalho possuiu foco na revisão da literatura e estado da arte sobre o assunto; já as entrevistas realizadas buscaram uma visão mais prática e atual a respeito da cibernética na Força, particularmente no Exército Brasileiro.

As entrevistas – instrumentos de grande valia para o presente trabalho – puderam ampliar a visão trazida pela teoria dos manuais e legislações que regem o assunto, tanto no âmbito militar quanto no âmbito civil. Ainda, pôde-se ratificar alguns dos tópicos verificados durante o desenvolvimento, corroborando com a afirmação de que a Guerra Cibernética gera reflexos no poder de combate e na estrutura da FTC em Op Of.

Na apresentação dos resultados foi verificado que a embasada opinião de ambos os colaboradores da pesquisa foi uníssona ao certificar que a Guerra Cibernética é uma forte contribuinte do poder de combate da FTC. As estruturas que são adjudicadas para uma ação desse tipo, como um Batalhão de Comunicações ou

uma Companhia de Guerra Eletrônica, possuem capacidades ímpares aptas a incrementar grande parte dos elementos de uma tropa.

É possível, portanto, inferir que o objetivo geral foi atingido, já que a Guerra Cibernética foi explorada em sua porção teórica e mais abrangente dentro do desenvolvimento, e a sua parcela prática e atual foi estudada por meio das entrevistas concedidas por especialistas da área. Assim, pode-se concluir que a Guerra Cibernética, dada a sua dimensão e a sua capacidade de ampliar capacidades já existentes na estrutura de uma Força Terrestre Componente em operações ofensivas, contribui decisivamente para a multiplicação do poder de combate.

Dessa maneira, algumas práticas podem ser visualizadas como adequadas na utilização da G Ciber em uma FTC. As entrevistas realizadas comprovaram o melhor aproveitamento de frações cibernéticas em unidades especializadas, tendo em vista a centralização dos meios e a maior capacidade de atuar com diversas demandas advindas dos escalões subordinados. Assim, de acordo com os resultados apresentados, o emprego mais benéfico dessas frações é no nível Divisão de Exército ou da própria Força Terrestre Componente, fazendo parte de organizações especializadas, tais quais o Batalhão de Guerra Eletrônica, o Batalhão de Comunicações e Guerra Eletrônica e o Batalhão de Comunicações.

Existem, ainda, outras organizações militares que possuem capacidades cibernéticas, obviamente em escala reduzida, como a Companhia de Comando e Controle e a Companhia de Comunicações. Salienta-se que as próprias frações integrantes da FTC, ainda que não possuam elementos específicos de G Ciber, podem realizar medidas preventivas de proteção cibernética, consideradas mais simples, contribuindo com o poder de combate do escalão considerado.

Ficou explícita a contribuição da G Ciber nas diversas operações ofensivas que podem ser atribuídas a uma FTC. A potencialização do poder de combate ocorre ao facilitar, por exemplo, o atingimento de objetivos inerentes àquelas ações. Em uma marcha para o combate, que tem por objetivo a obtenção ou restabelecimento do contato com o inimigo, é fundamental a obtenção de informações sobre o oponente, de modo a evitar a surpresa e canalizar esforços. Já no reconhecimento em força, que tem por finalidade revelar e testar o dispositivo e valor do inimigo, além de obter outros dados, faz-se vital a presença de G Ciber

como forma de simplificar esses procedimentos, adquirindo informações que não seriam obtidas somente pelo contato da tropa.

Uma sugestão a ser apresentada, oriunda das respostas dadas nas entrevistas do presente estudo, é a pesquisa de uma forma de diferenciação dos cursos de Guerra Cibernética para praças e oficiais, ministrados pelo CIGE. Como visto no capítulo Resultados e Discussões, essa melhoria é necessária para tornar distinta a formação de ambos os universos, haja vista que as funções exercidas são diferentes após a conclusão da especialização, permitindo um melhor aproveitamento dos recursos humanos cibernéticos.

Por fim, a Guerra Cibernética surge como um elemento capaz de incrementar sobremaneira o poder de combate de um determinado escalão, produzindo efeitos que contribuem de forma significativa para o acréscimo de novas capacidades para a Força Terrestre Componente. Desse modo, tanto os meios quanto os recursos humanos cibernéticos constituem-se em um dos mais elevados aportes existentes em uma FTC para desenvolver ações ofensivas no combate moderno.

REFERÊNCIAS

BRASIL. Exército. Estado-Maior. **Doutrina Militar Terrestre**. 1. ed. Brasília, DF. 2014a.

_____. Exército. Estado-Maior. **Força Terrestre Componente**. 1. ed. Brasília, DF. 2014.

_____. Exército. Estado-Maior. **Força Terrestre Componente nas Operações**. 1. ed. Brasília, DF. 2014.

_____. Exército. Estado-Maior. **Glossário de Termos e Expressões para Uso no Exército**. 5. ed. Brasília, DF. 2018.

_____. Exército. Estado-Maior. **Guerra Cibernética**. 1. ed. Brasília, DF. 2017.

_____. Exército. Estado-Maior. **Lista de Tarefas Funcionais**. 1. ed. Brasília, DF. 2016.

_____. Exército. Estado-Maior. **Operações**. 5. ed. Brasília, DF. 2017.

_____. Exército. Estado-Maior. **Operações Ofensivas e Defensivas**. 1. ed. Brasília, DF. 2017.

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

_____. Ministério da Defesa. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas**. 3. ed. Brasília, DF. 2008.

DEPARTAMENTO DE PESQUISA E PÓS-GRADUAÇÃO - ECEME. **Elaboração de Projetos de Pesquisa na ECEME**. – Rio de Janeiro, 2012.

ESCOLA DE COMUNICAÇÕES. **O Comunicante Revista Científica Volume 7 Nr 2**. Brasília, DF. 2017.

ESCOLA DE COMUNICAÇÕES. **O Comunicante Revista Científica Volume 7 Nr 3**. Brasília, DF. 2017.

GAZETA DO POVO. **Falha grave em segurança do Wi-Fi deixa redes à mercê de ataques.** Disponível em: <http://www.gazetadopovo.com.br/economia/nova-economia/falha-grave-em-seguranca-do-wi-fi-deixa-redes-a-merce-de-ataques-39gs7cb1o64n6> Acesso em: 17 de outubro de 2017.

GAZETA DO POVO. **Hackers norte-coreanos roubaram táticas de guerra dos EUA e da Coreia do Sul**. Disponível em: <http://www.gazetadopovo.com.br/mundo/hackers-norte-coreanos-roubaram-taticas-de-guerra-dos-eua-e-da-coreia-do-sul-d4jcdi77i3tr0lwviz1aen8lz> Acesso em: 11 de outubro de 2017.

NEVES, Eduardo Borba; DOMINGUES, Clayton Amaral. **Manual de Metodologia da Pesquisa Científica.** Rio de Janeiro: EB/CEP, 2007.

APÊNDICE - ENTREVISTA

Esta entrevista estruturada tem por finalidade colher subsídios sobre a atuação da Guerra Cibernética no âmbito de uma Força Terrestre Componente, sendo aquela considerada um elemento multiplicador do poder de combate.

Atualmente, desenvolvo, junto à Escola de Comando e Estado-Maior do Exército (ECEME), Trabalho de Conclusão de Curso cujo título é: “A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente”.

Com este instrumento de pesquisa, procuro responder o seguinte problema: “Em que medida a Guerra Cibernética contribui para aumentar o poder de combate da Força Terrestre Componente em operações ofensivas?”.

A experiência e a opinião do senhor são fundamentais para a validação desta pesquisa, motivo pelo qual solicito que esta entrevista seja respondida com a maior precisão possível, para que a mesma tenha validade.

Os dados colhidos por meio desta entrevista auxiliarão no levantamento das eventuais consequências para o poder de combate, em especial no que tange aos efeitos benéficos advindos do emprego da Guerra Cibernética em operações ofensivas de uma Força Terrestre Componente.

Desde já agradeço a atenção dispensada e a inestimável colaboração.

Qualquer dúvida, favor entrar em contato pelo e-mail: bombassaro.samuel@eb.mil.br.

1. Por favor, preencha os campos abaixo com os seus dados pessoais, de modo a identificá-lo.

Nome completo: _____

Posto: _____

2. Qual a função desempenhada pelo Sr no Centro de Instrução de Guerra Eletrônica (CIGE)?

3. Por quanto tempo / em que período o Sr desempenhou essa função?

4. O Sr poderia comentar a sua experiência profissional relacionada ao setor cibernético?

5. Qual(is) o(s) principal(ais) objetivo(s) da Seção / Divisão de G Ciber do CIGE?

6. Existe alguma diferença entre o curso de G Ciber para oficiais e para sargentos, haja vista serem universos distintos e que desempenharão funções também diferenciadas após a conclusão do mesmo?

7. Qual a sua análise sobre a formação do guerreiro cibernético do Exército Brasileiro?

8. Como o Sr avalia o Sistema de Guerra Cibernética do Exército, considerando os meios materiais (simuladores, equipamentos, instalações, tecnologias, etc.) existentes atualmente?

9. Enumere, em sequência de prioridade, as frações abaixo que permitam o melhor aproveitamento do elemento de G Ciber, atuando em prol do seu respectivo escalão quando da ativação da Estrutura Militar de Defesa por uma FTC.
( ) B Com
( ) B Com GE
( ) Cia C2
( ) Cia Com
( ) BIM
( ) BGE
( ) OM da FTC

10. Que tipo de capacidade operativa pode ser desenvolvida por elementos ou frações de G Ciber que atuam em proveito de uma FTC (exemplo: elementos do BGE, B Com GE, Cia C2, etc.)?

11. Que tipo de ações podem ser realizadas, prioritariamente, pela G Ciber contra oponentes com poder de combate superior?

12. O Sr poderia dar exemplos de possíveis alvos cibernéticos, que comporiam a Lista de Alvos Cibernéticos (LIA), no contexto de uma Op militar ofensiva?

13. De que maneira a G Ciber pode ser integrada às Funções de Combate (Movimento e Manobra, Inteligência, Fogos, Comando e Controle, Proteção e Logística), potencializando os efeitos dessas no combate?

14. O Sr possui mais alguma ideia ou ponto para destacar, no que tange à contribuição da G Ciber para o incremento do poder de combate de uma força militar?