

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

Samuel Bombassaro Neto*

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

* Maj Com (AMAN/2003, EsAO/12). Realizou o curso Básico de Guerra Eletrônica para Oficiais no Centro de Instrução de Guerra Eletrônica em 2006 e o curso de Comandante de Batalhão de Comunicações na República Federal da Alemanha em 2014. Atualmente, é aluno da ECEME.

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.

Diante do cenário apresentado, o presente artigo se deparou com o seguinte problema – objeto de análise do tema desenvolvido –, o qual buscou responder, cientificamente, em que medida a Guerra Cibernética contribui para aumentar o poder de combate da Força Terrestre Componente em operações ofensivas.

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 Guerra Cibernética diante desse novo cenário, com o intuito de ser aproveitada para futuros aperfeiçoamentos da atividade.

Os fundamentos da Guerra Cibernética

Para o completo entendimento do emprego da G Ciber é necessária 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. Nos níveis tático e operacional, num dos quais se insere a FTC, a denominação dada é Guerra Cibernética; no nível estratégico, chama-se Defesa Cibernética; e no nível político, Segurança da Informação e Comunicações e Segurança Cibernética. Assim, tem-se o esclarecimento do vínculo com o tema do presente artigo, ao enquadrar o assunto no âmbito da Força Terrestre Componente.

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 Informacional¹, 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.

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.

Ainda assim, existem algumas limitações quanto ao emprego da G Ciber, haja vista a própria natureza técnica da atividade. A dificuldade de identificação da origem e atribuição de respon-

sabilidades por ataques cibernéticos é um dos exemplos mais característico dessas limitações, já que existem numerosos métodos que visam prejudicar o rastreamento de ações desse tipo.

Há também uma grande dificuldade na eficácia de ações cibernéticas defensivas. Tal situação decorre do fato de que os sistemas computacionais não permitem a completa eliminação de suas vulnerabilidades, existindo apenas um maior ou menor grau de segurança de acordo com as medidas defensivas adotadas; em suma, não é possível conceber qualquer sistema digital plenamente seguro.

Finalmente, a própria velocidade da evolução tecnológica dos meios cibernéticos é considerada uma limitação para o emprego da G Ciber. A rapidez da modernização dos sistemas exige que os recursos humanos que atuam no espaço cibernético estejam em constante atualização e treinamento; do mesmo modo, os meios de tecnologia da informação necessitam ser frequentemente substituídos, evitando a sua obsolescência e mantendo a sua eficácia.

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: Proteção Cibernética, Ataque Cibernético e Exploração Cibernética.

Na atividade de ataque cibernético, as tarefas ocorrem em sequência, sendo por essa característica conhecidas como as fases do ataque cibernético. Ainda, as ações demandadas 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.

Poder de combate

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 à 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.

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.

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 seus elementos que atuarão junto da Força Componente.

Nesse sentido, tem-se que a fase de geração de poder de combate de uma FTC, em que são agregadas tropas com capacidades diversas e complementares, é primordial para que se ob-

tenha êxito na missão atribuída, sendo que a G Ciber é capaz de contribuir sobremaneira para essa mesma etapa do processo.

A Força Terrestre Componente em operações ofensivas

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”.

O conceito 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.

Assim, tem-se que uma FTC pode participar de vários tipos de operações, dentre as quais destacam-se 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.

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.

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, dentre as quais a célula de Comando e Controle – que irá contribuir diretamente com o assessoramento no campo cibernético.

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, sendo 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.

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.

Salienta-se que a G Ciber pode contribuir com o poder de combate, já que cada operação 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 célula é o elo com a Força Conjunta de G Ciber, outra estrutura que é ativada quando da concepção da Força Terrestre Componente. Esta 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 empenhada, gerando aumento desse mesmo poder.

As estruturas que são adjudicadas para uma operação ofensiva, como um Batalhão de Comunicações ou uma Companhia de Guerra Eletrônica, possuem capacidades ímpares aptas a incrementar o poder de combate de uma tropa.

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. Do estudo, constatou-se que o melhor aproveitamento de frações cibernéticas ocorre com a centralização dos seus meios, gerando maior capacidade de atuar com as diversas demandas advindas dos escalões subordinados. Assim, infere-se que o emprego mais eficaz

dessas frações ocorre no nível Divisão de Exército ou da própria Força Terrestre Componente, integrando 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 atri-

buídas a uma FTC. A potencialização do poder de combate ocorre ao facilitar o atingimento de objetivos inerentes àquelas ações. Como exemplo: 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.

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 especializados em G Ciber constituem-se em relevantes aportes para a FTC 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. **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.

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

Notas

- 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.