ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM WEILLER DE ÁVILA CARDOSO

POSSIBILIDADES DO DESTACAMENTO DE GUERRA CIBERNÉTICA NA ATUAÇÃO TÁTICA EM OPERAÇÕES

Rio de Janeiro
2019

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM WEILLER DE ÁVILA CARDOSO

POSSIBILIDADES DO DESTACAMENTO DE GUERRA CIBERNÉTICA NA ATUAÇÃO TÁTICA EM OPERAÇÕES

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Operacional.

Rio de Janeiro
2019

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Com WEILLER DE ÁVILA CARDOSO**

Título: **POSSIBILIDADES DO DESTACAMENTO DE GUERRA CIBERNÉTICA NA ATUAÇÃO TÁTICA EM OPERAÇÕES**

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, com ênfase em Gestão Operacional, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **DARDANO DO NASCIMENTO MOTA - Maj** Cmt Curso e Presidente da Comissão	
_____ **AUGUSTO DA SILVA GUIMARÃES - Cap** 1º Membro e Orientador	
_____ **ROBSON KÖHLER DAMIÃO - Cap** 2º Membro	

_____
WEILLER DE ÁVILA CARDOSO – Cap
Aluno

POSSIBILIDADES DO DESTACAMENTO DE GUERRA CIBERNÉTICA NA ATUAÇÃO TÁTICA EM OPERAÇÕES

Weiller de Ávila Cardoso*
Augusto Silva Guimarães**

RESUMO

Este trabalho descreve as atuais capacidades operacionais em termos de recursos humanos, material e infraestrutura da Companhia de Guerra Cibernética, orgânica do 1º Batalhão de Guerra Eletrônica (1º BGE), sediado em Brasília-DF. O trabalho pretendeu verificar se a infraestrutura física, as ferramentas/materiais operacionais e o efetivo existente é compatível com as demandas operacionais da SU, bem como procurou apontar as possíveis causas da insuficiência de pessoal técnico especializado em Guerra Cibernética. Ainda, são identificados os fatores motivadores que levam à busca pelo Curso de Guerra Cibernética. Sob outro ponto de vista, foram propostas soluções visando o recrutamento de talentos e com o intuito de aumentar a atratividade da área de Cibernética. Além disso, também foram propostas soluções para o desafio da capacitação continuada e do reduzido efetivo operacional.

Palavras-chave: Guerra Cibernética. Capacitação Continuada. Recrutamento de Talentos. Companhia de Guerra Cibernética, Ataque Cibernético. Exploração Cibernética.

ABSTRACT

This paper describes the current operational capabilities in terms of human resources, material and infrastructure of the Cyber Warfare Company, organic of the 1st Electronic Warfare Battalion, based in Brasilia-DF. The work aimed to verify if the physical infrastructure, the operational tools/materials and the existing operational staff are compatible with the operational demands of the Company, as well as to point out the possible causes of the lack of human resources specialized in cyber warfare. Moreover, the motivating factors that lead to attend for the Cyber War Course are identified. From another point of view, solutions have been proposed to recruit talent and to increase the attractiveness of the cyber area. In addition, solutions have been proposed for the challenge of continued training and reduced operational staff.

Keywords: Cyber War. Continuing Training of Human Resources. Talent Recruitment. Warfare Cyber Company. Cyber-attack. Cyber Exploration.

* Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2010.

** Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2006. Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (AMAN) em 2015.

1 INTRODUÇÃO

O momento atual da sociedade, denominado “Era da Informação”, é marcado pela alta velocidade de comunicação e caracterizado pela ampla utilização de dispositivos eletrônicos conectados em rede, gerando alta dependência dos meios de Tecnologia da Informação. Nesse contexto, essa dependência está relacionada a uma série de vulnerabilidades que, em se tratando de um Estado, podem ser exploradas a fim de se obter informações confidenciais, realizar sabotagens ou até mesmo adquirir vantagem em um conflito armado, independentemente dos atores envolvidos (MENDONÇA, 2014).

O ciberespaço não possui fronteira física e suas características dificultam a identificação dos agentes. Isso potencializa e amplifica a extensão de um ataque cibernético na medida em que o ciberespaço é único e global (NUNES, 2015), podendo o efeito colateral de um ataque dessa natureza gerar intensos danos à população civil.

Assim, existe a possibilidade de igualar, nesse domínio operacional, Estados com poderios bélicos altamente assimétricos, até mesmo pelo fato de um ataque nesse domínio ter um custo relativamente baixo com alto grau de impacto militar (MENDONÇA, 2014).

A revolução tecnológica vivida no final do século XX e início do século XXI, caracterizada pela utilização de dispositivos computacionais cada vez menores interligados em rede, impulsionou os movimentos globalistas, alterou completamente as relações sociais e, de maneira geral, influenciou intensamente as culturas do globo. Assim um novo ambiente operacional, virtual e sem fronteiras, se formou, fomentando novas formas de combater e gerando novas necessidades de entender o combate (RUMSFELD, 2002). Nesse contexto, as Operações Militares se tornaram altamente complexas e passaram a exigir cada vez mais esforços conjuntos para que se tenha êxito (ALBERTS, 2006).

Ademais, tal complexidade do espaço cibernético também impõe uma série de problemáticas e limitações relacionadas ao direito internacional, tais como o problema da atribuição dos ataques (NUNES, 2015) e a reação estatal realizada com base nos princípios do Direito Internacional dos Conflitos Armados (DICA).

Nesse contexto, a finalidade desse trabalho é investigar se o Exército Brasileiro, atuando no nível tático através do Batalhão de Guerra Eletrônica (1º BGE), possui atualmente, em termos de material e recursos humanos, condições adequadas de cumprir suas missões regulamentares, mais especificamente, de Exploração e Ataque Cibernéticos. Ainda, pretende examinar as dificuldades e desafios encontrados.

1.1 PROBLEMA

A publicação do Decreto Legislativo nr 373, de 12 de setembro de 2013 atualizou e Estratégia Nacional de Defesa (END) e aprovou o Livro Branco de Defesa Nacional (BRASIL, 2013). Esses documentos associados à Política Cibernética de Defesa (PCD) são marcos do desenvolvimento da atuação cibernética como ferramenta de Estado e constituem as diretrizes pelas quais todo o Sistema de Defesa Cibernética é conduzido.

Quando da aprovação da Estratégia Nacional de Defesa em sua primeira versão (2008), o setor de Cibernética foi dividido em dois campos distintos: a Segurança Cibernética, a cargo da Presidência da República; e a Defesa Cibernética, a cargo do Ministério da Defesa através das Forças Armadas (BRASIL, 2013). Sendo assim, no tocante à Defesa Cibernética (Ministério da Defesa), pode-se dividir a atuação no Espaço Cibernético em 3 (três) níveis: operacional e tático, estratégico e político. Esse trabalho abordará de maneira mais intensa a atuação cibernética no Nível Operacional e Tático.

Desta feita, a Força Terrestre possui em seus quadros elementos operacionais capazes de atuarem no nível tático, dentro de uma Operação Militar, contribuindo para a obtenção de um efeito específico desejado. O quadro 1 mostra as responsabilidades relacionadas à Guerra Cibernética dos elementos envolvidos numa Operação:

QUADRO 1 – Estruturas Operativas De G Ciber, suas atividades cibernéticas e responsabilidades

Estrutura	Atq	Expl	Prot	Responsabilidades
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de

				informação da própria unidade. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.
Batalhão de Comunicações (BCom)			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
Outros integrantes da FTC			X	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM.

Fonte: BRASIL (2017)

Da análise do quadro supracitado são definidos os elementos responsáveis por realizar ataque, exploração e proteção cibernética. Apesar de todos os elementos citados estarem relacionados com a Guerra Cibernética em Operações, nesse trabalho o foco será dado ao Destacamento de Guerra Cibernética atuando em nível tático, ou seja, aos componentes da Companhia de Guerra Cibernética (Cia G Ciber), orgânica do 1º Batalhão de Guerra Eletrônica (1º BGE), sediado em Brasília-DF. Outrossim, é importante salientar que quando em Operações Interagências, é ativado o Destacamento Conjunto de Guerra Cibernética.

As missões do Destacamento G Ciber do 1º BGE podem ser entendidas como as mesmas de um Destacamento Conjunto de Guerra Cibernética por suas naturezas similares (JÚNIOR, 2016), como segue:

> a) identificar e analisar vulnerabilidades (conhecidas) nas redes de computadores e aplicações empregadas no Sistema de C2 desdobrado para a operação;
> b) recomendar ações para mitigar as vulnerabilidades identificadas;
> c) estudar as ameaças e entender seu impacto nas redes de C2 ou quaisquer outras estruturas/recursos computacionais das forças amigas;
> d) verificar a conformidade de Segurança da Informação e Comunicações no Sistema de C2 desdobrado para a operação;
> e) planejar e executar ações cibernéticas (proteção, exploração e ataque), no contexto da operação conjunta, com apoio dos órgãos de Defesa

> Cibernética das Forças Armadas em cumprimento às orientações e diretrizes emanadas do Comando Operacional;
> f) assessorar o(s) comandante(s) da(s) Força(s) Componente(s) nos pedidos de efeito desejado dirigidos ao escalão competente para obtê-los;
> g) colaborar com a execução das Op Info planejadas; e
> h) colaborar com o esforço de obtenção de dados para a produção de conhecimento de Inteligência, por intermédio da Fonte Cibernética, no contexto da operação conjunta, em cumprimento às orientações e diretrizes emanadas pelo EMCj.

Assim, tendo em vista as especificidades e a complexidade da capacitação de efetivos para o emprego em guerra cibernética, foi formulado o seguinte problema: a Companhia de Guerra Cibernética (Cia G Ciber), orgânica do 1º Batalhão de Guerra Eletrônica (1º BGE) possui condições adequadas, em termos de material e recursos humanos, de explorar e atacar em proveito de uma Força Terrestre Componente (FTC)?

1.2 OBJETIVOS

Para abordar as variáveis relacionadas ao problema acima referenciado, busca-se a consecução do Objetivo Geral desta pesquisa, nos termos de: analisar as situações de emprego tático de Destacamento de Guerra Cibernética no âmbito da Força Terrestre com base na Doutrina Militar, nas concepções de recursos humanos, materiais operacionais e instalações.

A fim de atingir o objetivo geral de estudo, foram estabelecidos os seguintes objetivos específicos, abaixo discriminados:

a) identificar se a Cia G Ciber/1º BGE possui recursos materiais compatíveis com a atividade tática que executa;

b) Analisar se o efetivo existente é compatível com a demanda operacional da SU; e apontar as possíveis causas relacionadas com a insuficiência de recursos humanos especializados em G Ciber na SU;

c) Examinar se seus recursos humanos estão efetivamente capacitados a realizar ações de Guerra Cibernética;

d) Identificar programas de capacitação técnica continuada passíveis de serem aplicados aos seus recursos humanos;

e) Identificar os fatores motivadores que levam à busca e realização do Curso de Guerra Cibernética no público interno da Força;

f) Apontar soluções para atração e recrutamento de talentos na área de cibernética.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

Nos últimos anos, a incidência de ataques cibernéticos tem aumentado veementemente e por conseguinte, existe uma forte preocupação de diversos países, como os Estados Unidos, Rússia e China (AVELAR, 2018), com as consequências desses ataques.

Dessa maneira torna-se tarefa primordial a preparação para o emprego do poderio militar como expressão nacional do poder nacional e, nesse contexto, a questão do recrutamento e descobrimento de novos talentos no âmbito do Exército Brasileiro, é fundamental. Além disso, dada a evolução das plataformas de Tecnologia da Informação (TI), bem como o irrefreável avanço tecnológico dos dias atuais, não basta apenas possuir uma massa de guerreiros especializados em Cibernética, é mister que haja capacitação continuada através de uma melhoria contínua nos processos de atualização do conhecimento dos militares que atuam nessa área.

Dessa forma, esse trabalho se justifica por promover a pesquisa de um tema extremamente relevante e atual para o Brasil no cenário geopolítico internacional e regional a que pertence. Ademais, a doutrina de Guerra Cibernética do Exército Brasileiro é relativamente recente e está em constante evolução e sendo assim, esse estudo pode contribuir para o aprimoramento da mesma pelo fato de pretender expor as dificuldades relacionadas com a capacitação técnica e recrutamento de talentos, além de identificar possíveis ausências de recursos materiais necessários ao desenvolvimento da atividade.

2 METODOLOGIA

Esta pesquisa científica é mista quanto à forma de abordagem e analítica quanto ao objetivo geral. Com o objetivo de compor o escopo de conhecimentos que permita o desenvolvimento do tema e a resolução dos problemas demarcados, contemplou uma pesquisa bibliográfica, entrevista com especialistas, questionários, argumentação e discussão dos resultados, que será dividida em 4 (quatro) etapas.

Na primeira será realizada uma revisão da literatura com o objetivo de apresentar os conceitos, as metodologias adotadas pela Força Terrestre no nível tático e as atualidades relacionadas à guerra cibernética.

Na segunda etapa será realizada uma pesquisa quantitativa através de questionários respondidos pelos integrantes da Cia G Ciber, orgânica do 1º Batalhão de Guerra Eletrônica.

A terceira etapa constará de uma pesquisa qualitativa através de entrevistas com militares atuantes e de comprovada experiência no ramo de ações cibernéticas.

Na quarta etapa, tendo por base os conceitos doutrinários observados e os dados qualitativos e quantitativos adquiridos através das entrevistas e questionários, serão analisadas as respostas e compiladas as informações visando atender aos objetivos propostos.

2.1 REVISÃO DA LITERATURA

A guerra cibernética é definida pelo manual MD-31-M-08 – Doutrina Militar de Defesa Cibernética nos seguintes termos:

> Guerra Cibernética - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC.

Ademais, LIBICKI (2009) entende que a guerra cibernética também pode ser considerada uma das categorias da Guerra da Informação e assim sendo, um ataque no ambiente operacional cibernético pode ter alto grau de dano e impacto a uma nação pelo fato do ciberespaço ser considerado um domínio operacional que permeia todos os outros (BRASIL, 2013).

A Companhia de Guerra Cibernética, concebida para atuar no nível operacional e tático através de destacamentos de G Ciber, tem doutrinariamente como foco a preparação do campo de batalha, num contexto de ambiente de crise ou conflito, apoiando uma ação militar. Sincroniza-se com a manobra dentro do contexto dos sistemas operacionais de uma Operação Militar. Além disso, a duração de sua atuação é limitada, normalmente com tempo moderado ou curto de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas (BRASIL, 2014).

2.2 COLETA DE DADOS

Na sequência do aprofundamento teórico a respeito do assunto, o delineamento dessa pesquisa contemplou a coleta de dados pelos seguintes meios: entrevista e questionário.

2.2.1 Entrevistas

Com a finalidade de ampliar o conhecimento teórico e identificar fatores e experiências relevantes, foram realizadas entrevistas com os seguintes especialistas:

Nome	**Justificativa**
DAVID DA SILVA POLVERARI – Maj EB	1) Instrutor de Defesa Cibernética na Escola de Comunicações do Exército Peruano; 2) Adjunto à Divisão de Exploração do CDCiber; 3) Instrutor de Introdução ao Desenvolvimento de Exploits para o Curso de Guerra Cibernética do EB.

PEDRO HENRIQUE DE OLIVEIRA SOUZA – Cap EB	1) Participação no Destacamento Conjunto Def Ciber Central, por ocasião dos Jogos Olímpicos de 2016; 2) Participação das Cyber Olimpíadas Militares das Américas em 2016; 3) Participação no Exercício Ibero-Americano de Defesa Cibernética.

QUADRO 2 – Quadro de Especialistas entrevistados.
Fonte: O autor.

2.2.2 Questionário

A amplitude da população foi estimada a partir do efetivo atual da Companhia de Guerra Cibernética do 1º Batalhão de Guerra Eletrônica (1º BGE), tendo em vista a natureza do objeto da pesquisa.

A amostra selecionada foi restrita ao público de oficiais, subtenentes e sargentos, já que são esses os únicos especialistas em Guerra Cibernética que efetivamente executam as atividades técnicas e são aptos a opinarem a respeito de efetivo, material e atuação tática de Guerra Cibernética em Operações Militares.

Nesse contexto, a população utilizada foi de 5 (cinco) militares. Buscando maior confiabilidade das induções realizadas, buscou-se uma amostra significativa, utilizando como parâmetros o nível de confiança igual a 90% e erro amostral de 10%. Nesse sentido, a amostra dimensionada como ideal foi de 5 ($n_{ideal} = 5$).

A distribuição dos questionários ocorreu de forma indireta (e-mail) para todos militares participantes, tendo obtido sucesso em toda a população selecionada, não inviabilizando nenhuma resposta por preenchimento incorreto ou incompleto.

Foi realizado um pré-teste com 3 oficiais que atendiam aos pré-requisitos para integrar a amostra proposta no estudo, com a finalidade de identificar possíveis falhas no instrumento de coleta de dados. Ao final do pré-teste não foram observados erros que justificassem alterações no questionário e, portanto, seguiram-se os demais de forma idêntica.

3. RESULTADOS E DISCUSSÃO

Como já dito, toda a discussão aqui realizada tem como base o atual efetivo técnico especializado em Guerra Cibernética da Cia G Ciber/1º BGE, ou seja, todos os militares questionados (total de 5 militares) são possuidores do Curso de Guerra Cibernética do Exército (Gráfico 1).

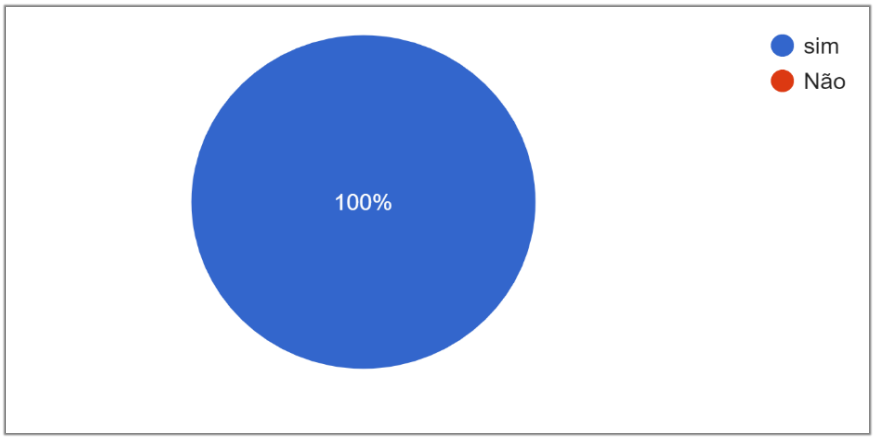

GRÁFICO 1 – Possuidores do Curso de Guerra Cibernética.
Fonte: O autor.

O gráfico 2 mostra a relação percentual de militares da Cia G Ciber que expressam a opinião de que a Cia G Ciber possui condições de realizar Ações Táticas de Guerra Cibernética, mais especificamente, Operações de Exploração e Ataque, em proveito de uma Força enquadrante. Como já citado na Revisão da Literatura, o foco das Operações da Cia G Ciber está na preparação do campo de batalha, apoiando uma ação militar e portanto, tendo uma duração bem limitada num curto espaço de tempo (BRASIL, 2014). Assim, da análise das entrevistas realizadas, foi constatado que tais Ações Táticas de Guerra Cibernética poderiam ocorrer atacando o Sistema de Comando e Controle do inimigo (vetor Ataque), bem como atuando em apoio à Inteligência Cibernética dentro do contexto das Operações de Informação (vetor Exploração).

Da análise do gráfico 2, pode-se entender que apesar de todo o efetivo ser capacitado a realizar Ações Táticas de Guerra Cibernética, 20% do efetivo expressa a opinião de que a Cia G Ciber não possui condições para tal. Foi levantado que uma dessas causas se deve ao fato da equipe ser bastante reduzida e na maior parte do seu tempo útil de trabalho, ser empregado em atividades não relacionadas ao setor cibernético.

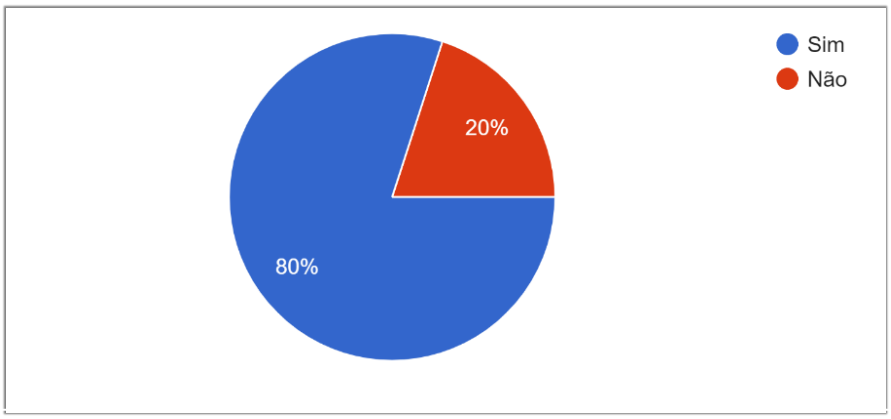

GRÁFICO 2 – Opinião da amostra acerca da Capacidade da Cia G Ciber realizar Ações Táticas Cibernéticas.
Fonte: O autor.

Sabe-se que a Cia G Ciber possui um efetivo relativamente pequeno. Nesse contexto, o gráfico 3 expressa a opinião da amostra em relação a se o efetivo atual da Cia está adequado à demanda das missões que recebe.

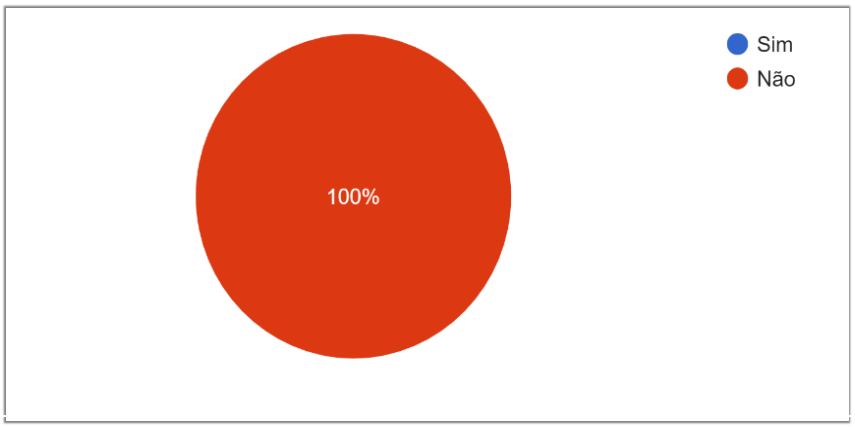

GRÁFICO 3 – Opinião da amostra acerca da adequação do efetivo da Cia G Ciber em relação à demanda das missões que recebe.
Fonte: O autor.

Analisando o gráfico 3, percebe-se, pela opinião unânime, que além do efetivo da Cia ser reduzido, está insuficiente à atual demanda das missões que recebe. Além disso, foi apontado que a maior dificuldade encontrada para o cumprimento das missões operacionais regulamentares da Cia G Ciber é a falta de efetivo técnico especializado, em detrimento da falta de material, como mostra o gráfico 4.

Em entrevista, o Maj Polverari, atual Instrutor de Defesa Cibernética na Escola de Comunicações do Exército Peruano e antigo Adjunto à Divisão de Exploração do Centro de Defesa Cibernética (CDCiber), defende como medida a ser realizada buscando atrair novos talentos para a área de cibernética, a necessidade de identificação de militares nas diversas escolas de formação que tenham grande

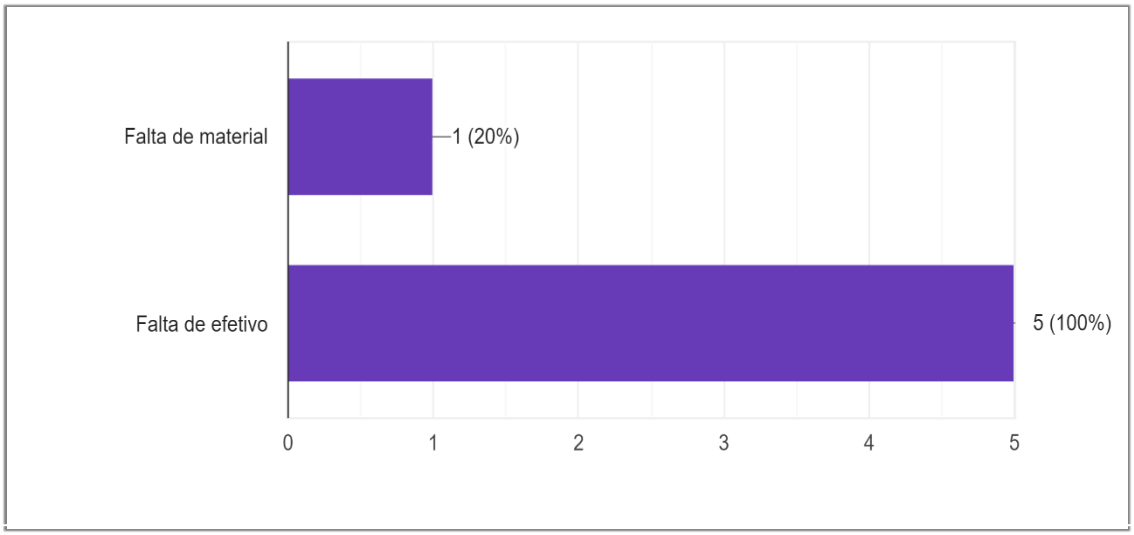

GRÁFICO 4 – Opinião da amostra acerca das dificuldades operacionais encontradas no cumprimento de suas missões.
Fonte: O autor

capacidade de abstração, resolução de problemas complexos, gosto por desafios técnicos, autodidatismo e outros atributos que não necessariamente são específicos da G Ciber, mas que compõe o perfil desejável do militar de G Ciber. Essa identificação nas escolas de formação proporcionaria um direcionamento para a área de cibernética já na escola de formação, o que poderia ser traduzido como aumento do efetivo especializado da Cia G Ciber, uma vez que o militar poderia ser designado ao término de seu curso de formação, na Cia G Ciber, por já possuir a especialidade, realizada durante o Curso de Formação de Oficiais.

Uma das principais causas levantadas da insuficiência de recursos humanos especializados na Cia G Ciber (gráfico 5) é a dificuldade relacionada com a problemática de Próprio Nacional Residencial (PNR). Isto é, o militar conclui o Curso de Guerra Cibernética com aproveitamento, é transferido e fica aguardando a liberação de PNR da cidade de Brasília-DF. Contudo, por vezes esse processo pode demorar anos, e em alguns casos a movimentação sequer chega a se concretizar. Outra causa levantada é o número reduzido de militares especializados em Guerra Cibernética no âmbito do Exército Brasileiro.

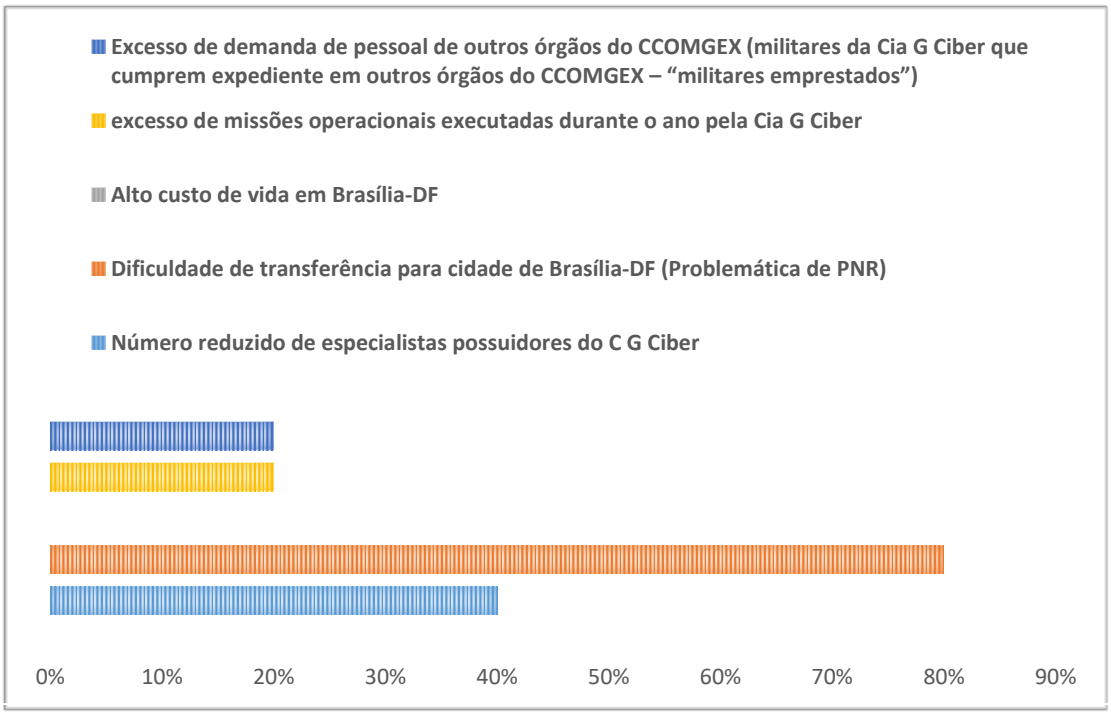

GRÁFICO 5 – Causas da insuficiência de recursos humanos especializados em Guerra Cibernética na Cia G Ciber.
Fonte: O autor

Além de conhecer as causas mais importantes relacionadas com a insuficiência de recursos humanos especializados, e para termos uma visão mais abrangente acerca dessa problemática, é mister saber também quais os motivos que levam os militares a se especializarem em Guerra Cibernética (gráfico 6).

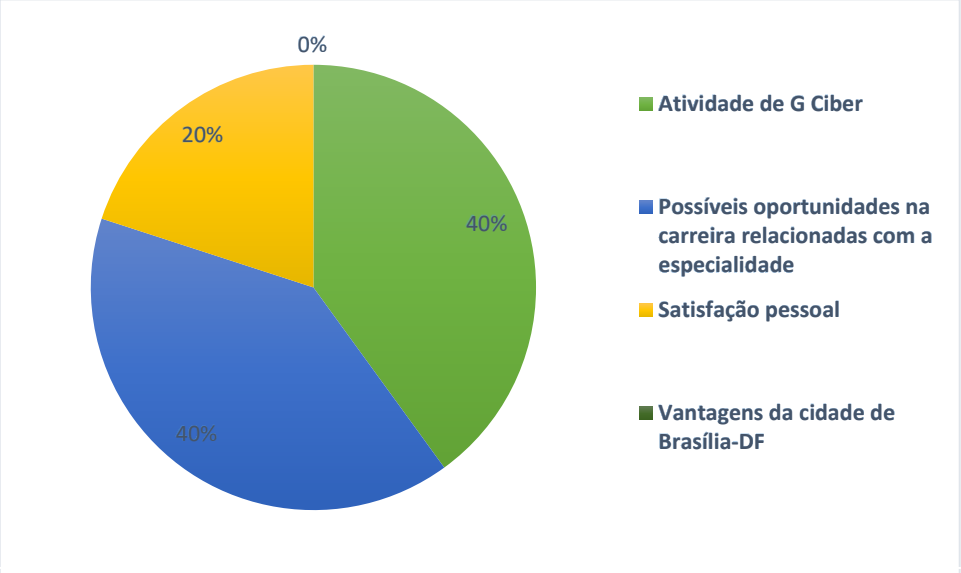

GRÁFICO 6 – Fatores motivadores para a busca do Curso de Guerra Cibernética.
Fonte: O autor

Dos dados extraídos do gráfico 6, pode-se entender que a afinidade com a atividade de Guerra Cibernética aliada às possíveis oportunidades na carreira são os principais fatores que motivaram os militares a realizarem o Curso de Guerra Cibernética.

Dentro desse contexto e tendo em conta que a atividade de guerra cibernética está em constante expansão, sendo norteada no Exército Brasileiro pelo catálogo de capacidades (BRASIL, 2015), é de fundamental importância que na área de cibernética haja o máximo de atratividade e que o recrutamento de talentos seja estimulado de maneira consistente e sistemática. Assim, deve-se também ser envidados esforços para garantir a efetiva identificação desses talentos. Sobre isso, o Maj Polverari, afirma em entrevista que que a melhor forma de identificar novos talentos na área de Cibernética é através de competições com desafios afetos à área, além da identificação de militares nas diversas escolas de formação que tenham grande capacidade de abstração, resolução de problemas complexos e gosto por desafios técnicos, além de outros atributos que não necessariamente são específicos da G Ciber, mas que compõem o perfil desejável do militar de G Ciber.

Dentro do escopo da atração de elementos civis da área de cibernética, o Cap Pedro Henrique, que participou das Cyber Olimpíadas Militares das Américas no ano de 2016, também defende, em entrevista, que haja competições promovidas pelo Exército Brasileiro com desafios que interessam à Instituição, no intuito de catalogar pessoas/equipes em um banco de dados. Ainda, afirma que a utilização de elementos civis deve se dar no sentido de prestação de serviços especializados, com objetivos bem definidos, não sendo o caso integrá-los à rotina militar.

Além da identificação e recrutamento de elementos para a área de cibernética, outra questão muito importante é a capacitação continuada dos recursos humanos especializados. Acerca desse tema, em entrevista, o Maj Polverari afirma que a melhor solução no nível Força Terrestre seria a instalação e operação de *“Cyber Ranges”* (simuladores) baseados em virtualização, para que os militares de G Ciber possam simular e treinar cenários para adestramento, além de realizar ensaios em um ambiente que simule aquele que encontrem em operações.

Já o Cap Pedro Henrique, em entrevista, entende que a melhor solução seria que Comando de Defesa Cibernética reunisse seus militares e talentos em uma estrutura que possibilitasse o treinamento e difusão desse conhecimento. Ainda, para

que essa implementação fosse efetiva, seria necessário que o militar permanecesse atuando na área de cibernética por pelo menos 4 ou 5 anos da carreira.

Além de recursos humanos especializados, também são necessárias boa estrutura física e de material para realização de atividade G Ciber. Sendo assim, o gráfico 7 apresenta a opinião da amostra sobre se a Cia G Ciber apresenta as ferramentas técnicas necessárias para realizar as Operações de Exploração e Ataque Cibernético.

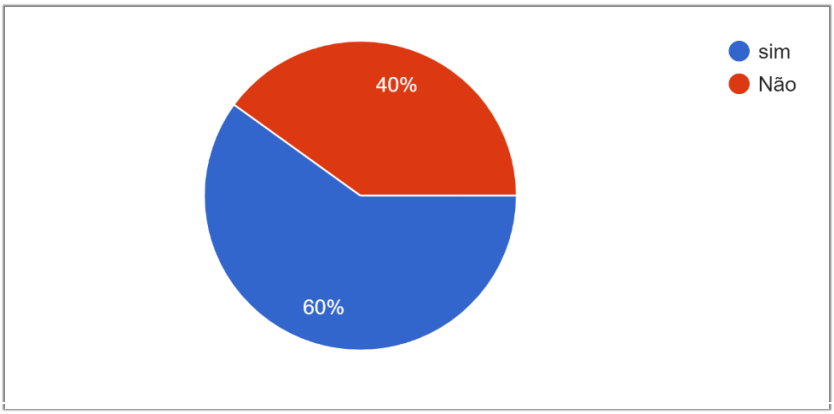

GRÁFICO 7 – Opinião da amostra acerca da posse de ferramentas necessárias para as Operações de Ataque e Exploração Cibernéticas.
Fonte: O autor

Foi levantado que a Cia G Ciber ainda está em fase de aquisição de softwares para realização de suas atividades e que nesse momento a SU está em fase de restruturação, não possuindo ainda todos os instrumentos necessários para atuação no ambiente cibernético.

Sobre a estrutura física da SU, o gráfico 8 mostra a opinião da amostra sobre se a estrutura física da SU se encontra condizente com as necessidades operacionais atuais.

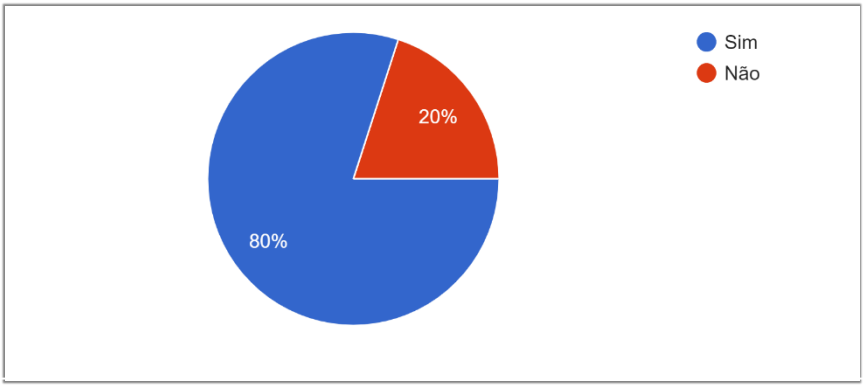

GRÁFICO 8 – Opinião da amostra acerca sobre adequabilidade da estrutura física mediante as necessidades operacionais atuais
Fonte: O autor

Da análise dos dados do gráfico 8 foi levantado que, como já mencionado, a SU está em processo de restruturação, tendo recebido a pouco tempo suas instalações reformadas.

4 CONSIDERAÇÕES FINAIS

Quanto às questões de estudo e objetivos propostos no início deste trabalho, conclui-se que a presente investigação atendeu ao pretendido, identificando e verificando as condições de operacionalidade da Cia G Ciber em termos de pessoal e material, além de examinar as dificuldades e propor algumas soluções relacionadas ao recrutamento de talentos e os desafios atinentes à capacitação continuada dos efetivos.

Pela compilação dos dados foi possível identificar que o efetivo técnico especializado da Cia G Ciber está inadequado para as demandas que recebe, e que o reduzido efetivo não emprega totalmente o tempo útil de trabalho em atividades especificas de cibernética, fato que pode gerar ineficiência operacional da SU.

Outra causa da problemática de efetivos especializados para a Cia G Ciber reside no fato da demora da liberação de Próprios Nacionais Residenciais (PNR) da cidade de Brasília-DF.

Por outro lado, as perspectivas na carreira e a afinidade com a atividade são os fatores que mais atraem os militares para a área de Cibernética. E dentro desse contexto, ações sistemáticas, como o fomento de competições contendo desafios cibernéticos (Capture The Flag – CTF, por exemplo) e divulgação nas escolas militares são consideradas as melhores soluções para o problema de recrutamento e identificação de talentos.

Para a questão do desafio da capacitação continuada dos efetivos especializados, concluiu-se que a melhor solução seria a permanência dos militares na área de cibernética de no mínimo 4 anos na atividade; e que há a necessidade de adestramento continuado nos simuladores de Guerra Cibernética.

Por fim, sob o aspecto de material operacional/instalações, conclui-se que a SU passou por uma recente restruturação física e que ainda está em processo de aquisição de softwares necessários à atuação efetiva em ambiente cibernético.

REFERÊNCIAS

ALBERTS, David S; HAYES, Richard E. **Understanding Command and Control.** CCRP, 2006.

AVELAR, JOSÉ RICARDO CABRAL. **A GUERRA CIBERNÉTICA E SEUS DESAFIOS PARA O BRASIL**. 2018. Trabalho de Conclusão de Curso (Programa de Pós-graduação lato sensu em Ciências Militares) - ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO, Rio de Janeiro, 2018

BRASIL. Ministério da Defesa. **Doutrina militar de Defesa Cibernética**. 1. ed. Brasília, DF, 2013.

BRASIL Ministério da Defesa. **MD31-M-07**: Doutrina Militar de Defesa Cibernética, 2014.

BRASIL. Exército. **EB20-C-07.001: Catálogo de Capacidades do Exército**. 1. ed. Brasília, DF, 2015.

BRASIL Ministério da Defesa. **EB70-MC-10.232**: Manual de Campanha - GUERRA CIBERNÉTICA, 2017.

JÚNIOR, Eliezer de Souza Batista. **Uso de Vírus desenvolvido no software Msfvenom contra Sistemas Operacionais Android com utilização de Mensagens Sms.** 2016. Trabalho de Conclusão de Curso (Pós-Graduação em Segurança da Informação) – CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA (CIGE), Brasília, 2016.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar.** RAND Corporation, 1 Ed. 2009. Estados Unidos da América

MENDONÇA, Cláudia da Silva. **GUERRA CIBENÉTICA: Desafios de uma Nova Fronteira**. 2014. Dissertação (Especialização em Gerência de Redes de Computadores e Tecnologia Internet) - Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2014.

NUNES, LUIZ ARTUR RODRIGUES. **GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL: Aplicabilidade do Jus ad Bellum e do Jus in Bello**. 2015. Trabalho de Conclusão de Curso (Altos Estudos de Política e Estratégia) - ESCOLA SUPERIOR DE GUERRA (ESG), Rio de Janeiro, 2015.

RUMSFELD, Donald H., **'Transforming the military"**, Foreign Affairs, vol. 81, n.° 3, May-June 2002

ANEXO A – SOLUÇÃO PRÁTICA

PROBLEMAS ENCONTRADOS	PROPOSTAS/SOLUÇÕES
Efetivo técnico especializado reduzido	1. Propor alteração de efetivo em QCP. Deve estar adequado às demandas operacionais e administrativas da SU; 1.1 Aumentar número de vagas no Curso de Guerra Cibernética; 2. Efetivo especializado deve se voltar totalmente para as atividades operacionais, não se envolvendo com atividades administrativas; 3. Aumentar nível de prioridade na liberação dos PNR's destinados aos militares especializados na área de cibernética;
Atração e recrutamento de talentos na área de cibernética	1. Fomentar desafios na área de cibernética em forma de competição para o público civil e militar; 2. Estimular eventos competitivos na área de cibernética dentro das Forças Armadas; 3. Intensificar a divulgação de relatórios e a capacidade tática cibernética do Exército Brasileiro para o pública civil e militar; 4. Realizar palestras nas escolas militares de formação com o intuito de divulgar a cibernética e atrair talentos;
Capacitação continuada de efetivos especializados	1. Determinar que o tempo mínimo de permanência de militares da área de cibernética seja de 4 anos contínuos na atividade; 2. Determinar a obrigatoriedade de utilização do simulador de Guerra Cibernética pelos efetivos especializados frequentemente.

QUADRO 3 – Problemas encontrados e suas possíveis soluções.
Fonte: O autor.