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

Maj Com **ROBSON** KOHLER DAMIÃO

A cibernética na formação do oficial da arma de Comunicações na AMAN

Rio de Janeiro
2022

Maj Com **ROBSON** KOHLER DAMIÃO

A cibernética na formação do oficial da arma de Comunicações na AMAN

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

Orientador: Ten Cel NORBERTO VILAS BÔAS HENNEMANN

Rio de Janeiro
2022

D158g Damião, Robson Kohler

Guerra Cibernética na formação do oficial da arma de Comunicações na AMAN./ Robson Kohler Damião.

64 f. : il. ; 30 cm

Orientação: Norberto Vilas Bôas Hennemann

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

Bibliografia: f. 57-58

.

1. GUERRA CIBERNÉTICA. 2. DEFESA CIBERNÉTICA. 3. MULTIDOMÍNIO. 4. PROTEÇÃO CIBERNÉTICA. I. Título.

CDD 003.5

Maj Com **ROBSON** KOHLER DAMIÃO

A cibernética na formação do oficial da arma de Comunicações na AMAN

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

Aprovado em ___ de outubro de 2022.

COMISSÃO AVALIADORA

_____
NORBERTO VILAS BÔAS HENNEMANN – TC Inf - Presidente
Escola de Comando e Estado-Maior do Exército

_____
MARLOS DE MENDONÇA CORRÊA – TC QEM - Membro
Escola de Comando e Estado-Maior do Exército

_____
PAULO CESAR DOS SANTOS FARIA – TC Med - Membro
Escola de Comando e Estado-Maior do Exército

AGRADECIMENTOS

A Deus pela graça da vida e bençãos concedidas, fundamentais na continuidade deste trabalho.

À minha esposa e filhas que colaboraram dando suporte e entendendo minha ausência em determinados momentos.

Aos militares que responderam os questionários e os oficiais do Centro de Defesa Cibernética e do CIGE que colaboraram com suas experiências e conhecimento na área.

Aos militares da ECEME, companheiros e instrutores, que ajudaram, direta ou indiretamente, com a minha pesquisa, colaborando para que fosse alcançado o melhor resultado possível em prol do Exército Brasileiro.

“To truly make America safe, we must make cyber security a major priority.” (Donald Trump)

RESUMO

Na atualidade, o domínio do espectro da guerra cibernética já se constitui em ponto essencial para um país ter dissuasão e projetar maior poder de combate no campo de batalha, tanto nos ataques, como na exploração e na proteção. Dentro desta realidade, o ensino desta matéria nos bancos escolares da Academia Militar das Agulhas Negras, particularmente dos oficiais da Arma de Comunicações, torna-se um vetor fundamental na persecução das capacidades cibernéticas do Exército Brasileiro. O oficial de Comunicações será o militar responsável, após a formação, por integrar as Organizações Militares de Comunicações, sendo estas integrantes das Grandes Unidades que conduzem os planejamentos das operações no ambiente cibernético. Nesse sentido, é necessário a avaliação constante do nível de capacitação que os oficiais formados na Academia Militar das Agulhas Negras estão atingindo e em qual medida esse ensino está sendo eficaz frente às necessidades operativas das Grandes Unidades. Outrossim, é relevante saber quais são as capacidades operativas do espectro cibernético, as atividades e as tarefas que integram todo esse domínio, preservando desta forma os ativos, as informações e os meios civis e militares essenciais para o combate moderno.

Palavras-chave: Guerra Cibernética, Proteção Cibernética, Segurança cibernética.

ABSTRACT

Currently, the domain of the spectrum of cyber warfare is already an essential point for a country to have deterrence and project greater combat power on the battlefield, both in attacks, exploration and protection. In this reality, the teaching of this subject in the Academia Militar das Agulhas Negras, particularly to the officers of the Signal Corps, becomes a fundamental vector in the pursuit of the cyber capabilities of the Brazilian Army. This officer will be the military responsible, after his formation, for integrating the Military Communications Organizations, which are members of the Large Units that conduct the planning of operations in the cybernetic environment. In this sense, it is necessary to constantly assess the level of training are reaching and to what extent this teaching is being effective in the face of the operative needs of the Large Units. Furthermore, it is important to know what the operational capabilities of the cybernetic spectrum are, the activities and tasks that comprise this entire domain, thus preserving the assets, information and civilian and military assets essential for modern combat.

Keywords: Cyber War, Cyber Protection, Cyber Security.

LISTA DE ABREVIATURAS

AMAN	Academia Militar das Agulhas Negras
B Com	Batalhão de Comunicações
B Com GE	Batalhão de Comunicações e Guerra Eletrônica
C2	Comando e Controle
CC² FTC	Centro de Comando e Controle da Força Terrestre Componente
CC² MD	Centro de Comando e Controle do Ministério da Defesa
C Cj	Comando Conjunto
CCOMGEx	Centro de Comunicações e Guerra Eletrônica do Exército
CDCIBER	Centro de Defesa Cibernética
CDS	Centro de Desenvolvimento de Sistemas
Cia C2	Companhia de Comando e Controle
Cia Com	Companhia de Comunicações
CIE	Centro de Inteligência do Exército
CIGE	Centro de Instruções de Guerra Eletrônica
CITEx	Centro Integrado de Telemática do Exército
Cmdo	Comando
Cmt	Comandante
CMT	Capacidade Militar Terrestre
ComDCIBER	Comando de Defesa Cibernética
CTA	Centros de Telemática de Área
CT	Centros de Telemática
G Ciber	Guerra Cibernética
EB	Exército Brasileiro
EM	Estado-Maior
EMCFA	Estado-Maior Conjunto das Forças Armadas
EME	Estado-Maior do Exército
EPEx	Escritório de Projetos do Exército
F Cte	Força Componente
FTC	Força Terrestre Componente
FTP	Serviço de Transferência de Arquivo
IA	Inteligência Artificial
IME	Instituto Militar de Engenharia

OCCA	Operações de Cooperação e Coordenação com Agências
PBC	Planejamento Baseado em Capacidades
PC	Posto de Comando
PIM	Programa de Instrução Militar
PND	Política Nacional de Defesa
PR	Presidência da República
ROD	Rede Operacional de Defesa
RPC	República Popular da China
SC²EX	Sistema de Comando e Controle do Exército
SC²FTER	Sistema de Comando e Controle da Força Terrestre
SC²FTC	Sistema de Comando e Controle da Força Terrestre Componente
SGCEx	Sistema de Guerra Cibernética do Exército
SIC	Segurança da Informação e Comunicações
SIMOC	Simulador Nacional de Operações Cibernéticas
SINDE	Sistema de Inteligência de Defesa
SISCOMIS	Sistema de Comunicações por Satélite
SMDC	Sistema Militar de Defesa Cibernética
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações

LISTA DE APÊNDICES

Apêndice 1 – Questionário aos Cmt/S3 OM Comunicações.....59
Apêndice 2 – Questionário aos Of Subalternos OM Comunicações..... 63

LISTA DE FIGURAS

Figura 1 – Níveis Político, Estratégico, Operacional e Tático de decisão.....22
Figura 2 – Ranking nacional de poder cibenético..... 25
Figura 3 – SGCEx.....31
Figura 4 – Capacidades.....39

LISTA DE GRÁFICOS

Gráfico 1 – Conhecimento acerca do manual.....41
Gráfico 2 – Tarefa Defesa Ativa e Pronta Resposta.....42
Gráfico 3 – Tarefa Forense Digital e Teste de Artefatos Cibernéticos..... 42
Gráfico 4 – Controle de Acesso, Emprego de Criptografia e Segurança Física..... 43
Gráfico 5 – Gestão de Riscos..... 44
Gráfico 6 – Instalar e Gerenciar um Sistema.....44
Gráfico 7 – Conhecimento do manual..... 48
Gráfico 8 – Tarefa Defesa Ativa e Pronta Resposta..... 49
Gráfico 9 – Tarefa Forense Digital e Teste de Artefatos Cibernéticos..... 49
Gráfico 10 – Controle de Acesso, Emprego de Criptografia e Segurança Física..... 50
Gráfico 11 – Gestão de Riscos..... 51
Gráfico 12 – Instalação e gerenciamento de um sistema..... 51

LISTA DE QUADROS

Quadro 1 – Conceitos de cibernética..... 23
Quadro 2 – Capacidades Operativas do SGCEx..... 32
Quadro 3 – Atividades e tarefas de proteção cibernética..... 35
Quadro 4 – Graus de responsabilidade..... 37

SUMÁRIO

1. INTRODUÇÃO 14
1.1 PROBLEMA 21
1.2 OBJETIVOS 17
1.2.1 Objetivo geral 17
1.2.2 Objetivos específicos 17
1.3 QUESTÕES DE ESTUDO 17
1.4 DELIMITAÇÕES DO ESTUDO 18
1.5 RELEVÂNCIA DO ESTUDO 18
1.6 METODOLOGIA 19
1.6.1 Tipo da pesquisa 19
1.6.2 Delimitação da pesquisa 19
1.6.3 Coleta de dados 19
1.6.4 Tratamento dos dados 20
1.6.5 Delimitações do método 20
2 OS PRINCIPAIS CONCEITOS E A EVOLUÇÃO DA CIBERNETICA 21
2.1 OS PRINCIPAIS CONCEITOS 21
2.2 A EVOLUÇÃO DA CIBERNÉTICA NO MUNDO 23
2.3 A EVOLUÇÃO DA CIBERNÉTICA NO BRASIL 26
2.4 AS AMEAÇAS DO ESPAÇO CIBERNÉTICO 27
3. A ESTRUTURA BRASILEIRA DE GUERRA CIBERNÉTICA 29
3.1 O SISTEMA MILITAR DE DEFESA CIBERNÉTICA 30
3.2 DOUTRINA DE GUERRA CIBERNÉTICA 30
3.2.1 Capacidades do SGCEx 32
3.2.2 Proteção Cibernética 34
3.2.3 O Emprego das Capacidades Operativas pelas OM 36
4. A CIBERNÉTICA COMO CAPACIDADE OPERATIVA DAS OM 39
5. A FORMAÇÃO DO OFICIAL DE COMUNICAÇÕES DA AMAN 47
6. CONCLUSÃO 54
REFERÊNCIAS 57

1. INTRODUÇÃO

O conhecimento na área de cibernética na formação do oficial de Comunicações do Exército Brasileiro se faz cada vez mais necessário frente à evolução constante e exponencial das ameaças desse setor. O espaço cibernético ocupa atualmente uma nova dimensão de possibilidades nos campos de batalha, com peculiaridades que podem decidir os rumos de uma guerra.

Os desafios para os oficiais de Comunicações neste setor são de primordial importância para o andamento das operações, principalmente na questão de proteção das informações. A invenção dos computadores, assim como o advindo desses em redes, tem oferecido ao mundo globalizado um constante crescimento na propagação e difusão de informações. Fruto disso, o mundo tem vivenciado mudanças de Eras, como da Informação e do Conhecimento, e se torna cada vez mais dependente da tecnologia em rede, elevando as preocupações de todos com a segurança dessas informações.

As ações cibernéticas de ataque seguem nesta mesma esteira, crescendo constantemente e de forma exponencial nos últimos anos. Frequentemente somos noticiados de invasões de sites, roubo de dados, sequestro de informações, entre outros, levando diversos países a considerar o setor cibernético como crítico para a sobrevivência do Estado, inclusive colocando-o como um novo ambiente operacional. “São inúmeros os países que consideram o ‘ambiente cibernético’ com uma nova dimensão do combate, assim como o mar, a terra, o ar e o espaço sideral” (PINHEIRO, 2008, p.10).

A definição desse novo domínio pode ser explicada por meio da conceituação de “Multi-Domain Battle”, para isso usaremos o conceito do Gen. David G. Perkins (2017), do Exército Norte-Americano, que define o termo como a guerra sendo realizada em diversas dimensões, incluindo, por exemplo, o espectro eletrônico e o cibernético. A evolução natural do poder de combate de cada país transcende, dessa forma, os conhecidos vetores ar, mar e terra, tornando uma complexidade ainda maior da guerra.

A Estratégia Nacional de Defesa (END), em 2008, visualizando esse e outros setores, definiu três importantes vetores para a Defesa Nacional: o cibernético, o nuclear e o espacial, destacando o Exército Brasileiro para o

primeiro, a Marinha do Brasil para o segundo e a Força Aérea Brasileira para o terceiro.

O Setor Cibernético envolve grande parte dos aspectos da vida cotidiana atual, uma vez que atua por meio de redes de computadores e de comunicações, com o uso de modernos meios tecnológicos destinados ao trânsito de informações. Assim, seja nas necessidades individuais, seja nas corporativas e de Estado, a Cibernética se configura por um complexo sistema imaterial que implica na necessidade do desenvolvimento de capacidades para se contrapor às ameaças externas e proteger nossos ativos.

O Brasil, por intermédio do Exército Brasileiro, tem reconhecido a importância do setor cibernético como atuador importante nos conflitos atuais e evoluindo sua organização e doutrina para permitir gerar as capacidades necessárias às novas ameaças, como explica o EB70-MC-10.232 - Manual de Campanha Guerra Cibernética:

> Na atual conjuntura mundial, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de modo a capacitá-la a responder oportuna e adequadamente, com proatividade, antecipando-se em face dos possíveis cenários adversos à defesa nacional. (BRASIL, 2017, p. 1-1)

A União Internacional de Telecomunicações (UIT), agência da ONU especializada no assunto, divulgou em 2021 o ranking de quase 200 países sobre a governança de cibernética e o Brasil subiu para a 18ª posição, melhorando mais de 50 posições, em 3º lugarna América, atrás, apenas, dos EUA e do Canadá.

Ademais, a proteção cibernética é constantemente desafiada, mesmo no âmbito das redes internas do Exército Brasileiro, como ocorrido em 2020: “No fim da tarde do último domingo (10), um perfil no Twitter (@DigitalSp4c3) retaliou o Exército Brasileiro e o governo federal com a exposição de supostos dados de 200 mil militares.” (TECMUNDO, 2020). Sendo assim, é vital que a proteção cibernética ocorra de forma constante e atualizada, tudo para mitigar os riscos atuais desse complexo espectro multidimensional.

As Organizações Militares (OM) do Exército Brasileiro estão todas interligadas em redes e conectadas por via da internet e da EBNET (rede

corporativa do Exército), exigindo que a necessidade da proteção cibernética ocorra deste este nível. Os primeiros elos desta corrente são as Unidades e Subunidades de Comunicações do Exército Brasileiro, responsáveis por gerenciar as informações táticas das GU em operações.

O espaço cibernético tem sido empregado largamente nos conflitos da atualidade como um dos principais meios pelos quais os Estados em disputa buscam obter vantagem sobre seu oponente. Em um ambiente de crecente evolução do espaço cibernético, o Exército Brasileiro vem priorizando a segurança das informações, especialmente no tocante àquelas que transitarão nos sistemas de comando e controle da Força Terrestre, em caso de um conflito envolvendo o Brasil.

Nesse sentido, o início da capacitação em cibernética dos oficiais de Comunicações se faz necessária já nos bancos escolares da AMAN, continuando o aperfeiçoamento pelos cursos de especialização disponíveis no âmbito do Exército Brasileiro. Estes oficiais serão os responsáveis técnicos das OM de Comunicações que conduzirão, no escalão Grande Unidade (GU), as ações que envolvem o domínio cibernético, particularmente à proteção cibernética.

1.1. PROBLEMA

As diversas ameaças do setor cibernético têm exigido, principalmente na última década, uma nova organização e evolução doutrinária da organização do Exército Brasileiro, das capacidades atinentes à Defesa Nacional e um constante monitoramento de nossas infraestruturas lógicas, desde o nível OM.

Cabe salientar que as OM da arma de Comunicações (Com) são as responsáveis pela instalação, exploração e proteção das informações que circulam entre os diversos escalões da Força Terrestre (F Ter), cabendo, dessa forma, a preocupação e geração de capacidades atinentes ao setor cibernético.

O presente trabalho de conclusão de curso será desenvolvido em torno do seguinte problema: os conhecimentos sobre Guerra Cibernética adquiridos pelo Aspirante a Oficial (Asp Of) de Comunicações da Academia Militar das Agulhas Negras (AMAN) são suficientes para fazer frente às atuais e futuras ameaças deste setor?

1.2. OBJETIVOS

1.2.1. Objetivo geral

Estabelecer se a capacidade desenvolvida pelo Asp Of de Com, egresso da AMAN, tem sido suficiente para proteger os ativos e as informações que circulam entre os elementos da F Ter, particularmente atinentes ao setor cibernético.

1.2.2. Objetivos específicos

Com a finalidade de alcançar o objetivo deste trabalho num desenvolvimento lógico, coerente e progressivo, foram levantados os seguintes objetivos específicos:

a) apresentar a evolução da Guerra Cibernética no mundo e no Brasil e os principais conceitos que envolvem o setor.

b) apresentar a estruturação da Guerra Cibernética no Exército Brasileiro.

d) apresentar as necessidades atinentes ao setor cibernético das OM de Com e GU.

e) analisar as principais capacidades e dificuldades dos Asp Of Com da AMAN neste setor.

1.3. QUESTÕES DE ESTUDO

Alinhado com os objetivos específicos esse trabalho abordará os seguintes questionamentos:

a) como a Gerra Cibernética evoluiu no mundo e no Brasil?

b) como o Brasil e o Exército Brasileiro tem se estruturado no setor?

c) quais são as necessidades operacionais de Guerra Cibernética das OM de Com em apoio às GU?

d) quais são as capacidades e dificuldades que o Asp Of Com da AMAN possui ao se formar?

1.4. DELIMITAÇÃO DO ESTUDO

O presente estudo estará limitado ao emprego da Guerra Cibernética pelas OM de Com no âmbito das GU, no nível tático, particularmente as Companhias de Comunicações e os Batalhões de Comunicações.

Está limitação de estudo busca focar as necessidades operacionais dos menores escalões da F Ter no setor cibernético, verificando se os oficiais formados na AMAN (sem curso de especialização de cibernética) tem as capacidades dpara suprir tais demandas.

Não é objeto de estudo neste trabalho a correlação da conclusão deste trabalho com a carga horária total do Curso de Comunicações da AMAN. A substituição ou não desta matéria, em detrimento de outro assunto, não cabe neste trabalho, mas somente avaliar se a capacitação está sendo suficiente ou insuficiente para que o Asp Of possua, ao final do curso da AMAN, possua capacidades de cibernética necessárias para desempenhar suas missões na tropa.

1.5. RELEVÂNCIA DO ESTUDO

Este trabalho busca contribuir para a evolução dos conceitos doutrinários do setor de cibernética do Exército Brasileiro, reforçando a necessidade de constante atualização e análise dos conceitos de proteção cibernética e, consequente, geração das capacidades operativas para fazer frente às ameaças do setor. Esta constância se dá frente às frequentes novas ameaças que surgem dentro de um mundo cada vez mais volátil.

A formação correta e direcionada do Oficial de Comunicações na AMAN nesta área irá mitigar tais ameaças, por meio do recrudescimento da proteção cibernética das GU. A quantidade de carga horária e quais conceitos e instruções serão ministrados fazem parte da relevância do estudo para melhor dimensionar a formação dos recursos humanos.

Assim, esta pesquisa está de acordo com a Política Nacional de Defesa (PND), de 2020, particularmente nas Ações Estratégicas de Defesa (AED), relacionada à AED-11: “Incrementar as capacidades de defender e explorar o espaço cibernético” (BRASIL, 2020, p. 32).

1.6 METODOLOGIA

1.6.1 Tipo de pesquisa

Com a finalidade de elucidar o problema objeto deste trabalho, buscou-se classificar esta pesquisa conforme as categorias mais comuns. No que diz respeito à natureza, a pesquisa será classificada como aplicada, pois o conhecimento tem a finalidade de avaliar se a carga horária sobre cibernética ao Asp Of AMAN de Comunicações é suficiente para gerar a capacidade necessária para o ambiente cibernético.

Esta pesquisa será envidada de forma documental, com base na pesquisa, principalmente no que tange as publicações doutrinárias sobre o assunto.

1.6.2 Delimitação da pesquisa

Nas pesquisas na em bancos de dados diversos, de fontes abertas, foram pesquisados os termos “guerra cibernética, *cyberwarfare*, *cyber*, defesa cibernética, cibernética e meios de TI, domínio cibernético, *multidomainbattle*”, sempre realizando a análise da fonte, observando as peculiaridades de cada dado e dando preferência para informações contidas na doutrina militar.

1.6.3 Coleta de dados

Os dados serão obtidos por meio de pesquisas documentais e bibliográficas conforme os critérios de inclusão e exclusão abaixo citados. E por meio de questionários para os oficiais egressos da AMAN, de Comunicações, e seus Cmt ou S3 das diversas Organizações Militares (OM).

a) critérios de inclusão

- Estudos publicados em português, alemão, espanhol ou inglês, relacionados ao setor cibernético;
- DMT em vigor;
- PND, END; e
- Estudos qualitativos sobre Guerra Cibernética.

b) critérios de exclusão

- Publicações em outros idiomas diferentes dos citados; e
- Aspectos doutrinários em formulação e que não estejam em vigor.

1.6.4 Tratamento de dados

Aplicar-se-á a técnica da análise de conteúdo nos dados obtidos pela pesquisa documental e bibliográfica. Após a coleta dos dados e seleção dos conceitos a serem abordados, será realizado a análise sumária dos dados a serem utilizados.

A pesquisa permitirá as conclusões iniciais sobre o assunto, respondendo as questões de estudo propostas. Após, os dois questionários propostos irão fornecer dados concretos para que as ideias sejam confirmadas ou refutadas de forma parcial ou total, permitindo uma conclusão final. Esta conclusão será o objetivo geral proposto e a solução do problema objeto da pesquisa.

1.6.5 Limitações do método

O método está limitado pela volatilidade do assunto e falta de conceituação padronizada do tema, gerando uma percepção particular do objeto. Assim, fica limitado pela percepção pessoal e daqueles que responderam os questionários.

2. OS PRINCIPAIS CONCEITOS E A EVOLUÇÃO DA CIBERNETICA

O surgimento do domínio cibernético remonta à invenção dos computadores e a criação do ambiente em redes. A intenção de ligar essas máquinas em redes foi idealizada nos Estados Unidos da América para fins de defesa do Estado. As posteriores evoluções desse setor formaram o que conhecemos hoje de internet e é deste princípio que abordaremos os aspectos relacionados a cibernética.

A internet passou a ser usada em larga escala, a partir do final da década de 1990, nas mais variadas áreas, lazer, negócios, investimentos, transações financeiras, entre outras formavam um mundo de novas possibilidades. Com o advindo das redes sociais e a possibilidade de compartilhamento cada vez maior de informações, o mundo virtual começou também a apresentar ações com o intuito de se obter vantagem sobre outros, de forma criminosa, chamando a atenção de todos para a necessidade de proteção dos dados individuais e coletivos.

Essas ações criminosas caracterizam-se por atuar nesse novo domínio, o espectro cibernético. Segundo Carreiro (2012), tais ações têm o objetivo de obter dados para uso criminoso e corruptivo, interrupção ou danos de alguns sistemas da informação, e ações já tipificadas como criminosas, como fraude, estelionato, chantagem, entre outros.

Recentemente, o ex-presidente dos Estados Unidos da América (EUA), Donald Trump, publicou em em suas redes sociais a seguinte frase (traduzida por este autor): “ Para deixarmos a América segura, nós precisamos colocar a segurança cibernética em uma prioridade maior”. Tal importância, dada pelo presidente da maior potência mundial, nos remonta a buscar o aprimoramento e evolução desse importante vetor

2.1 OS PRINCIPAIS CONCEITOS

A cibernética é uma dimensão nova dos campos de batalha, utilizada principalmente como disputa informacional no ambiente operacional. A base para o uso desta capacidade operacional envolve uma rede de estruturas de Tecnologia da Informação e Comunicações (TIC), a gestão e a proteção desses dados.

A Guerra Cibernética possui conceitos diferentes, mas que remontam aos mesmos termos de espaço virtual, exploração e proteção dos dados e gestão da

informação. No manual do Exército Brasileiro EB70-MC-10.232-Guerra Cibernética, a abordagem do conceito é:

> GUERRA CIBERNÉTICA - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. 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 às TIC. (BRASIL, 2017)

O mesmo manual aborda também sobre os níveis que cada decisão pode ser tomada no espaço cibernético:

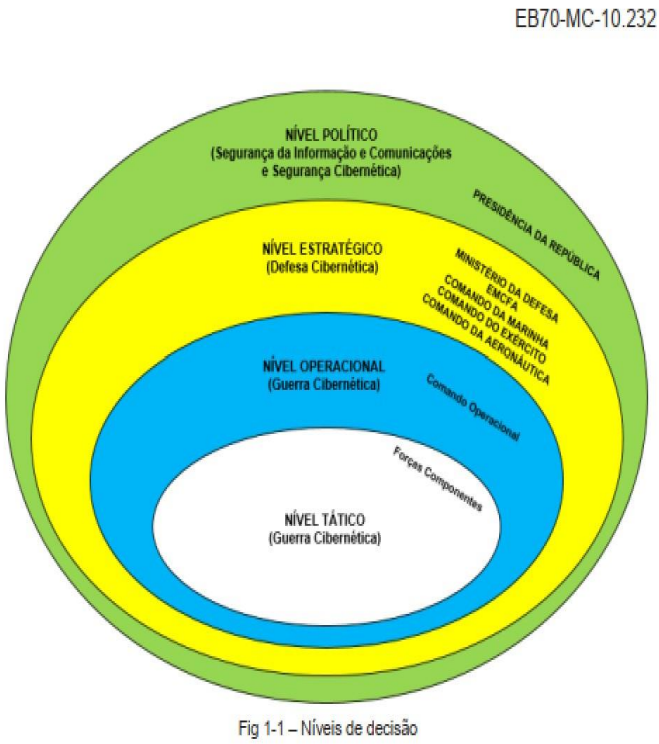

FIGURA 1 – Níveis Político, Estratégico, Operacional e Tático de decisão.
Fonte: Brasil (2017, p. 1-3).

No nível Tático, objeto deste trabalho, pode se observar que o Nível de Decisão engloba a Guerra Cibernética como um todo. Outrossim, é abordado os principais conceitos sobre o assunto:

Conceito	Definição
Ameaça cibernética	Causa potencial que pode inferir dano
Ativos de informação	Meios usados para gestão da informação
Defesa cibernética	Ações defensivas e ofensivas do nível estratégico para proteger nossos sistemas e comprometer do oponente
Espaço cibernético	Espaço composto pelos dispositivos onde tramitam as informações ou são armazenadas
Poder cibernético	Capacidade de criar vantagem em conflitos utilizando-se do espaço cibernético
Sistema de C2	Sistema de Comando e Controle que envolve os meios e a gestão da informação

QUADRO 1 – Conceitos de cibernética.

Fonte: Elaboração própria, segundo o Manual de Campanha EB70-MC-10.232.

2.2 A EVOLUÇÃO DA CIBERNÉTICA NO MUNDO

Como visto anteriormente, a cibernética surge pelo uso dos dispositivos conectados em redes, basicamente da exploração da internet, idealizado pelos EUA na metade do século XX. Desta forma, um dos precursores no assunto foi o país norte-americano que rapidamente desenvolveu suas capacidades para dominar o espaço cibernético.

Mas o uso do poder cibernético, em ação de Estado, em operações e conflitos militares veio a acontecer somente no ano de 2007 (grifo que este é um dado conhecido, porém é provável que tenha acontecido anteriormente seja no período da guerra fria, seja no ambiente das guerras travadas no Oriente Médio ao longo do início do século XXI).

Diante das evoluções do conflito, os EUA criaram o primeiro Comando de Guerra Cibernética em 2010, o USCYBERCOM, subordinado diretamente ao Ministério de Defesa norte-americano. Tal importância dada ao setor é comprovada pelo investimento em defesa, cujo valor chegou a 768 Bilhões de dólares aprovados pelo congresso em 2021.

> Planeja e conduz as atividades com objetivo de: direcionar as ações de defesa da informação, do Departamento de Defesa; preparar para operações no setor espacial e no ciberespaço; garantir a (EUA) liberdade de ação no espaço cibenético e negar aos adversários. (DEPARTMENT OF DEFENSE, 2010, tradução nossa)

Desde o ataque à Estônia em 2007, diversas ações foram registradas ao longo dos anos, como na Guerra entre Rússi e Geórgia em 2008 e do Irã em 2010 (PINHEIRO, 2018). Na esteira desses eventos e em consonância com os EUA, outros países desenvolveram suas forças cibernéticas para fazer frente ao novo espectro do conflito.

Rússia, China, Reino Unido lideram esse avanço ao lado dos EUA. A República Popular da China (RPC) vem desenvolvendo todos os campos da expressão militar do poder nacional para contrapor a balança de poder imposta pelos EUA nos últimos 30 anos. Da mesma forma, a Rússia não fica atrás nessa capacidade a medida que investe cada vez mais no setor.

> China e Rússia vêm se destacando dentre alguns países que estão encarando como ação estratégica estatal a formação do que analistas estão identificando como ‘guerreiros cibernéticos’. Fontes especializadas asseguram que os chineses estão decisivamente engajados nas tecnologias de desenvolvimento de vírus e worms, bem como na abertura de brechas de segurança na Internet. (PINHEIRO, 2008, p. 10)

Segundo a Harvard Kennedy School's, o ranking do poder cibernético em 2020 era o seguinte:

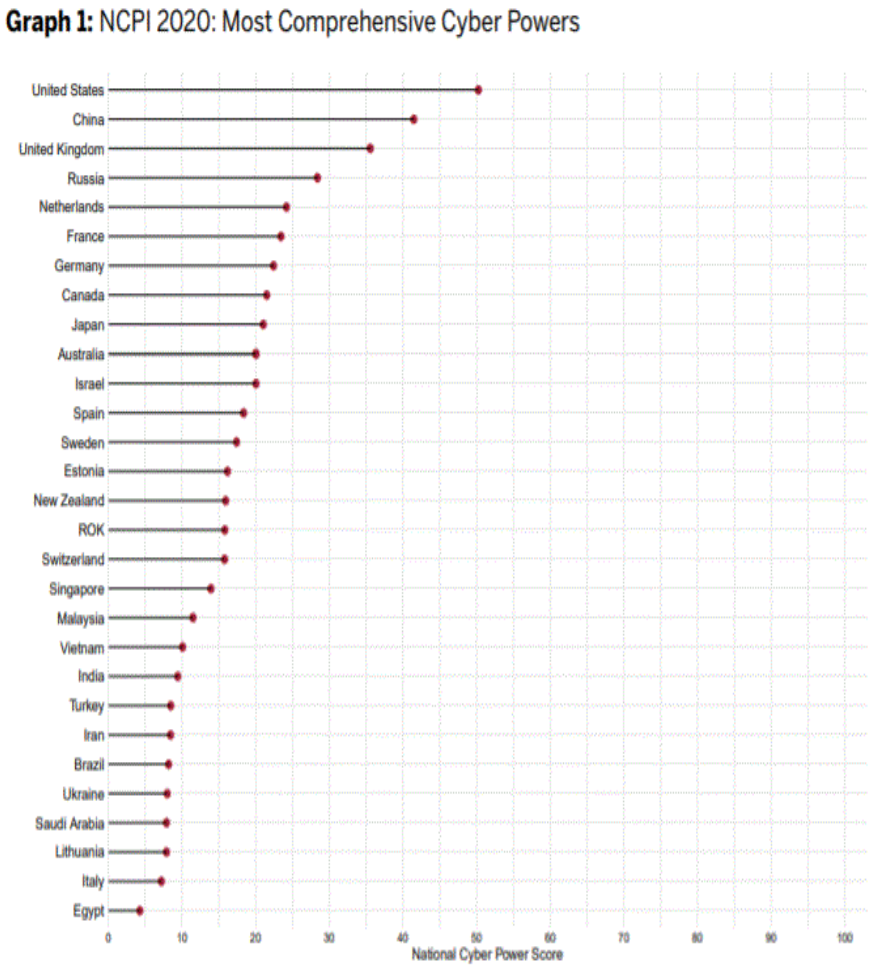

FIGURA 2 – Ranking nacional de poder cibenético.
Fonte: The Belfer National Cyber Power Index (NCPI) - Harvard Kennedy School's

Naturalmente, as grandes potências mundiais detêm as melhores posições no ranking de poder cibenético, fruto da capacidade de investir alto nesse setor, principalmente na criação de capacidades de defesa e ataque cibernéticos. Estímulo ao surgimento de “hackers cidadões” para espionar Estados sem envolvimento direto da nação atacante (muito usado pela Rússia nas guerras em seu entorno, a própria espionagem (com destaque para a CIA dos EUA) e a estruturação do poder cibernético nacional para maximizar essas capacidades são algumas das ações desses países.

Na parte da espionagem, um caso clássico da história cibernética mundial é do norte-americano Edward Snowden. Ex-funcionário da CIA, ele resolveu usar de seu acesso privilegiado para divulgar uma rede de espionagem a nível mundial que os EUA mantinham em constante vigilância, sobre os sistemas de tramitação das

informações à época. Tal fato veio a recrudescer ainda mais os interesses nacionais nas questões de defesa de seus ativos da informação.

Outros atores, ainda, merecem destaque no cenário mundial. A Coréia do Norte representa, por exemplo, a 4ª maior ameaça aos EUA (atrás de China, Rússia e Irã) (SANTOS, 2018). Apesar das restrições de internet internas e do pequeno tamanho, o desenvolvimento das suas capacidades cibernéticas, aliadas ao seu poder nuclear, entregam um importante poder de dissuasão no cenário mundial.

O Reino Unido detém o 4º maior poder cibernético mundial (conforme figura anterior) e possui importante aliado (EUA).

2.3 A EVOLUÇÃO DA CIBERNÉTICA NO BRASIL

O surgimento da preocupação com o domínio cibernético no Brasil surge com a Estratégia Nacional de Defesa (END), em 2008, que considerou este como um dos 3 vetores[1] a serem desenvolvido no país.

Cabe ressaltar que esta determinação surge após eventos importantes da história da cibernética, com países já tendo usado este espectro em combate para obter vantagem sobre o inimigo. O poder cibernético surge como um multiplicador da capacidade de um exército e a criação de uma doutrina, estrutura e graçãO de capacidades tornou-se essencial para manter o Brasil com uma boa posição geopolítica no cenário internacional.

A Diretriz Ministerial Nº 14/2009, de 09 de novembro de 2009, deu novo estímulo para a criação dessas capacidades, definindo fases para a implantação, sendo em uma primeira a definição, abrangência e objetivos e, em uma segunda fase, o detalhamento dos objetivos setoriais com ações estratégicas, assim como a proposta de estruturação de cada área. O vetor cibernético, destinado ao Exército, ficou a cargo do Estado Maior do Exército (EME) que logo criou o Núcleo do Centro de Defesa Cibernética.

A partir da criação do Núcleo, buscou-se criar uma estruturação de órgãos e divisão de responsabilidades na área de cibernética. Em um segundo momento, os

[1] Os 3 setores da END foram destinados às Forças Armadas, sendo o nuclear para a Marinha do Brasil, o espacial para a Força Aérea e o cibernético para o Exército Brasileiro.

órgãos criados buscaram gerar as capacidades e uma doutrina própria de emprego do poder cibernético, objetos estes que serão estudados no próximo capítulo.

2.4 AS AMEAÇAS DO ESPAÇO CIBERNÉTICO

Diante deste setor desafiador, capaz de multiplicar as capacidades de um exército, cabe destacarmos as ameaças possíveis. Nesse cenário, elas são executadas, em sua grande maioria, dentro de um anonimato que dificulta a identificação do atacante, e devem ser analisadas de forma criteriosa para proporcionar que as estruturas cibernéticas, voltadas para a segurança e proteção, estejam em condições de defender e reagir de forma oportuna.

O site *"https://www.blackberry.com/us/en"* é um conhecido endereço no ambiente cibernético com proposta de entrega de diversos produtos. Entre outros, a produção de relatório sobre as principais ameaças é uma importante análise do setor e pode servir de base para o estudo.

O Relatório das Ameaças BlackBerry, realizado por último em 2021, avalia as principais ameaças detectadas no ano anterior (no caso 2020), examinando as ações de cibersegurança. De forma geral, houve aprimoramento nas ações de ataque, como a utilização de *exploits* prontos (*softwares* que emulam ameaças) e, ainda, os tradicionais usos de *malspam*[2] e de *phishing*.

As ações podem ser feitas para ações criminosas ou mesmo por um Estado contra outro, visando obter vantagem sobre o oponente. Algumas observações do relatório são: ataque à rede elétrica na Ucrânia, contra os Jogos Olímpicos (Inverno, em 2018), nas eleições francesas (2017) e norte-americana (2020) (BLACKBERRY, 2021).

As ameaças podem trazer ao Estado brasileiro diversos tipos de problemas, desde o comprometimento de dados até a negação total de serviços essenciais como a ação para destruir o sistema lógico de uma hidrelétrica, a interrupção de um sistema essencial como do SUS ou o sequestro de informações classificadas. Dessa forma,

---

[2] *Malspam* é uma espécie de programa malicioso, conhecido comumente como malware (ou vírus) sendo entregue geralmente por e-mail. Uma melhora na forma de ataques a infraestrutura crítica foi detectada nas campanhas de *phishing*. Essa técnica consiste na adoção da engenharia social, para simular um evento aparentemente real e consegui implantar o dispositivo malicioso.

cabe ao Exército Brasileiro a criação de infraestrutura, física e lógica, para manter uma atualização constante frente às evoluções destas ameaças.

3. A ESTRUTURA BRASILEIRA DE GUERRA CIBERNÉTICA

A estruturação tem seu início no ano de 2005 com a Política Nacional de Defesa (PND), que começou a abordar o assunto relacionado ao setor cibernético. O foco foi na evolução dos meios e métodos da Tecnologia da Informação, apresentando inclusive algumas vulnerabilidades que poderiam afetar o Brasil. Tais assuntos permeiam os conceitos abordados sobre cibernética e indicam o despertar do país para este novo cenário.

Foi com a Estratégia Nacional de Defesa, de 2008 que o setor cibernético foi definido como um dos vetores estratégicos nacionais, surgindo o direcionamento das políticas de defesa para a necessidade de se estabelecer uma estrutura de defesa cibernética. O Exército, incumbido deste setor, ficou responsável por coordenar, em ligação com o Ministério da Defesa, a criação dessas estruturas capazes de gerar tais capacidades operativas.

Dessarte, em 2010, o Comando do Exército criou um núcleo para coordenar as ações iniciais deste novo domínio. O Núcleo do Centro de Defesa Cibernética teve como princípio, conforme descrito no site de projetos do Exército[3], a seguinte missão: “foi destinado ao desenvolvimento de doutrina de proteção dos próprios ativos, bem como na capacidade de atuar em rede, na de implementar pesquisa científica voltada ao tema e na indução da capacidade tecnológica nacional.” Assim, o Núcleo iniciou a estruturação, capacitação dos recursos humanos e formulação da base para a doutrina de cibernética.

A estruturação do setor cibernético ganhou maior vulto em 2012, com a criação e ativação do Centro de Defesa Cibernética (CDCiber), a partir do Núcleo criado em 2010. O setor cibernético voltou a ser estruturado em 2014, com a criação do Comando de Defesa Cibernética (ComDCiber e a Escola Nacional de Defesa Cibernética (ENaDCiber), fornecendo um nível de decisão ministerial (MD). Todas as criações foram feitas pelo Ministério da Defesa (MD) e coube ao Estado-Maior Conjunto das Forças Armadas (EMCFA) a coordenação das atividades que envolvem as Forças Armadas.

[3] Ao Escritório de Projetos do Exército (EPEx) compete atuar como órgão de coordenação executiva do Estado Maior do Exército (EME) para fins de governança do Portfólio Estratégico do Exército, constituindo-se no escritório de projetos de mais alto nível da Forca

Ainda em 2014, o MD publicou o primeiro manual de defesa sobre o assunto, o MD31-M-07 - Doutrina Militar de Defesa Cibernética, que estabeleceu os fundamentos básicos para proporcionar o pensamento sobre o assunto e contribuição para a construção da doutrina de cibernética no âmbito das três Forças. O manual estruturou os níveis de decisão e as responsabilidades sobre o assunto (Figura 1), forneceu diversos conceitos básicos que envolvem o setor cibernético e definiu o estabelecimento inicial do Sistema Militar de Defesa Cibernética (SMDC), estrutura responsável pela defesa do espaço cibernético.

3.1 O SISTEMA MILITAR DE DEFESA CIBERNÉTICA

O manual do MD de Doutrina Militar de Defesa Cibernética definiu um capítulo para conceituar o SMDC. Como fundamento, este sistema engloba toda estrutura, pessoal e doutrina essenciais para realizar a defesa no espaço cibernético, assegurando às Forças Armadas (FA) a utilização deste espectro para impedir ou dificultar ações contra os interesses da Defesa Nacional (BRASIL, 2014, p 13/36). Cabe, ainda, ao SMDC coordenar e proteger as infraestruturas críticas de interesse nacional.

O ComDCiber é o órgão central, de nível de decisão operacional, do SMDC e tem a responsabilidade de gerenciar o uso deste espectro, assim como fazer frente às ameaças e riscos que possam impedir ou negar tal utilização. O CDCiber é o seu braço tático, órgão onde se executam as ações no espectro cibernético e se mantém uma ligação com todos os órgãos nacionais de interesse para o setor. O CDCiber também contribui para a Defesa Nacional como sensor de inteligência, contribuindo com informações e alimentando o Sistema de Inteligência de Defesa (SINDE) (GUIMARÂES, 2017).

3.2 DOUTRINA DE GUERRA CIBERNÉTICA

Em 2017, o Exército publicou o manual EB70-10.232 - Guerra Cibernética, que consolidou toda a estruturação e conceituação que havia ocorrido desde a publicação da END em 2008 e posterior criação do CDCiber, em 2010. Um dos principais objetivos é de promover uma unidade de pensamento sobre o assunto para contribuir

com a atuação conjunta das Forças Armadas na defesa do espaço cibernético (BRASIL, 2017, p 1-1).

A Guerra Cibernética se consolida, desta forma, como um dos multiplicadores do poder de combate do Exército. Seguindo os níveis de decisão (Figura 1), o manual tem por objetivo estruturar o nível tático, local que o CDCiber se insere neste contexto, ficando o ComDCiber no nível operacional e estratégico. O Sistema de Guerra Cibernética do Exército (SGCEx) visa à proteção cibernética dos Sistemas de Comando e Controle do Exército e a capacidade de atuar no espectro cibernético.

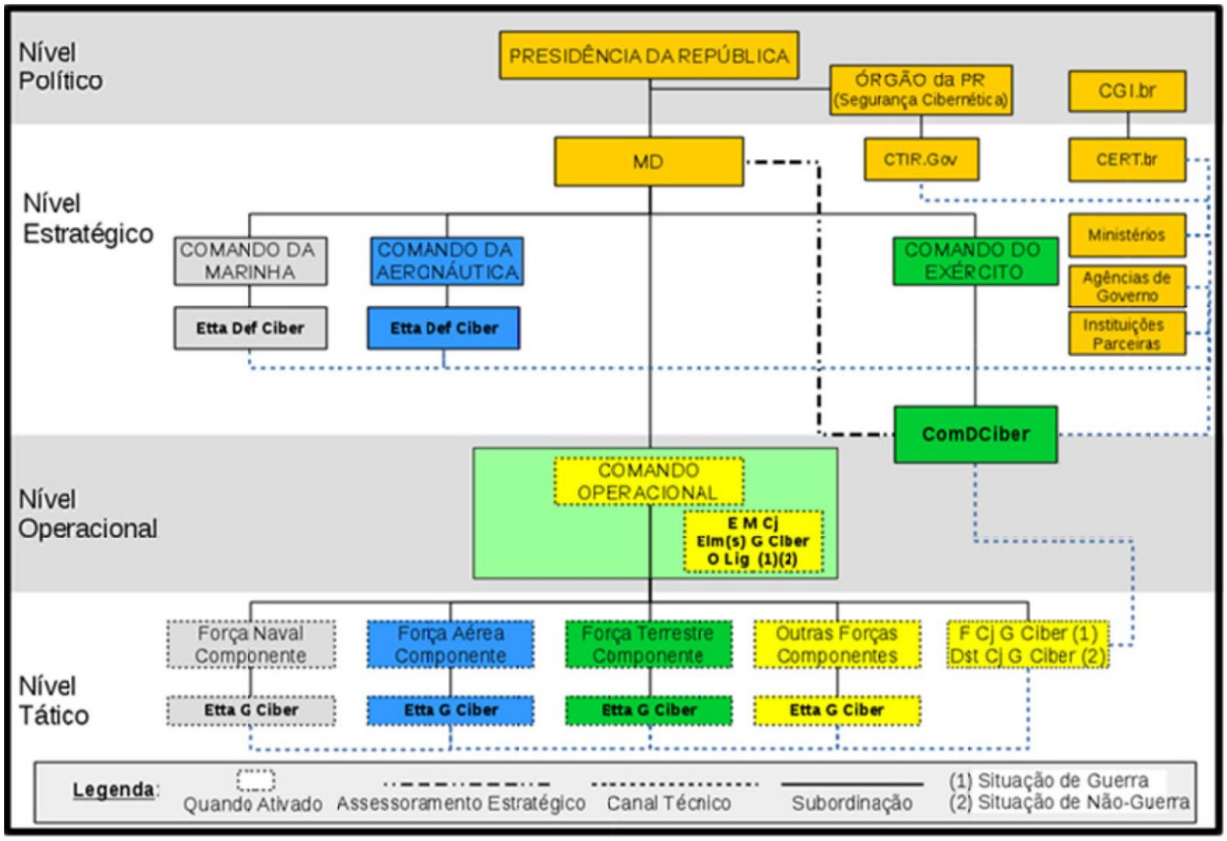

FIGURA 3 – SGCEX

Fonte: Brasil (2017, p. 3-1).

A figura 3 ilustra a concepção geral do SMDC. do qual o SGCEx faz. A divisão por níveis de decisão determina as responsabilidades e estrutura a Defesa Cibernética de forma nacional e abrangente, de modo a fazer frente às ameaças atuais e que porventura venham a surgir no futuro.

Em um nível político temos toda estrutura e defesa dos ativos da informação que envolvem a Presidência da República e as infraestruturas críticas, principalmente quanto a Segurança Cibernética. Essas estruturas críticas são aquelas que são sensíveis e podem desestabilizar o país em caso de sofrer danos em um eventual

ataque cibernético. O nível estratégico já engloba o Ministério da Defesa e tem relação com a Defesa Cibernética. Ambos os níveis de decisão permeiam toda administração pública, ministérios, órgãos e instituições parceiras.

No âmbito dos níveis mais baixo, operacional e tático, entramos nos conceitos de Guerra Cibernética, sendo restrito às Forças Armadas. A Força Terrestre Componente (FTC) será apoiado por uma Estrutura de Guerra Cibernética (Figura 3). Essa estrutura é composta pelos 1º Batalhão de Guerra Eletrônica, os Batalhões de Comunicações e Guerra Eletrônica, os Batalhões de Comunicações, o Batalhão de Inteligência Militar, a Companhia de Comando e Controle e as Companhias de Comunicações

3.2.1 Capacidades do SGCEx

As capacidades[4] do Exército multiplicam seu poder de combate de proporcionam melhores condições para atingir os objetivos. Dentro da capacidade cibernética, o Exército Brasileiro dividiu em 03 Capacidades Operativas (CO): Proteção Cibernética, Ataque Cibernético e Exploração Cibernética.

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

[4] Capacidade é a aptidão requerida a uma força ou organização militar, para que possa cumprir determinada missão ou tarefa. É obtida a partir do desenvolvimento de um conjunto de sete fatores determinantes, inter-relacionados e indissociáveis: doutrina, organização (e processos), adestramento, material (e sistemas), educação, pessoal e infraestrutura. (BRASIL, 2017, p 3-4)

	para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

QUADRO 2 – Capacidades Operativas do SGCEx.

Fonte: Manual de Campanha EB70-MC-10.232

O ataque cibernético é utilizado como forma de negar, destruir ou neutralizar um objetivo militar, geralmente ativos do inimigo como sistema de computadores, informações e até mesmo contra o sistema de armas. Entre as três, esta é a capacidade operativa mais acentuada e necessita estar sempre consistente com o arcabouço jurídico, principalmente em ações nos tempos de paz. Pode e deve ser utilizado em conjunto com a Guerra Eletrônica, por meio das ações e medidas de ataque eletrônico (MAE), potencializando uma ofensiva contra um oponente (BRASIL, 2017, p 4-2).

De acordo com o manual, estes ataques podem ocorrer por 03 formas principais: externos, internos e transitivos. Os externos são executados por elementos não ligados à instituição, os internos por pessoal interno à instituição, inclusivo os de forma física com elementos infiltrados e os transitivos são realizados contra alvos que possuem uma cadeia de confiança entre si.

A exploração cibernética tem por intenção buscar informações do oponente, a fim de alimentar a consciência situacional dos diversos níveis de comando, colaborando principalmente com a Inteligência militar. Cabe ressaltar que essas ações devem ser bem detalhadas pela possibilidade de deixar rastros, servindo, dessa forma, para alimentar o oponente com conhecimento e vulnerabilidades de nossas capacidades. Esta capacidade operativa também deve seguir o arcabouço jurídico, principalmente na relação a busca de informações não autorizadas pelo oponente (BRASIL, 2017, p 4-2).

A proteção cibernética se difere das duas anteriores por ser voltada para as ações de prevenção e Defesa Cibernética de nossas forças. Basicamente, a proteção é destinada a neutralizar a ameaça, o ataque e a exploração cibernética de um oponente. Esta é única ação permanente, segundo o manual de Guerra Cibernética, e tem a principal função de proteger, no âmbito do Exército Brasileiro, o Sistema de Comando e Controle do Exército (SC²Ex). é a proteção cibernética que vai possibilitar o Comando e Controle, negando o acesso ao oponente.

3.2.2 Proteção Cibernética

De caráter permanente, esta Capacidade Operativa do SGCEx é a única executada por todos os elementos que compõe a Estrutura de Guerra Cibernética (Figura 3), seja para o caso de compor uma FTC, seja para a situação de normalidade (paz) na proteção dos ativos das OM e das GU. As principais ações são de detectar uma ameaça, identificação e resposta oportuna.

De acordo com o manual de Guerra Cibernética, no contexto da proteção cibernética, podem ser executadas ações de ataque cibernético e exploração cibernética, principalmente com intuito de se simular as ameaças aos nossos sistemas, a fim de testar e avaliar o nível de proteção cibernética. Nesse sentido, foi criado o Simulador Nacional de Operações Cibernéticas (SIMOC), operado pelo Centro De Instrução de Guerra Eletrônica(CIGE), com sede em Brasília-DF. “Tal objetivo levou à criação do primeiro simulador de ataque cibernético no Brasil e à inserção de exercícios de defesa cibernética nas academias militares em todo o território nacional.” (LIMA, 2018).

As principais atividades e tarefas da proteção cibernética são:

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.

Atividade	Tarefa
	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 os administradores e gerentes determinem o que os indivíduos podem acessar, de acordo com sua [sic] 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 da 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.

QUADRO 3 – Atividades e tarefas de proteção cibernética.

Fonte: Manual de Campanha EB70-MC-10.232.

Podemos verificar no quadro acima, retirado do Manual de Campanha EB70-MC-10.232 Guerra Cibernética, que a proteção cibernética engloba todas as tarefas de defesa das infraestruturas físicas e lógicas, que permeiam o setor cibernético, principalmente as relacionadas aos ativos do Exército. A proteção cibernética está ligada á potencialização de todas as funções de combate, tanto para possibilitar o perfeito funcionamento como para evitar que as ameaças afetem as ações do Exército (BRASIL, 2017, p 4-5 a 4-7).

Conforme visto no Quadro 2, a proteção cibernética exerce a gestão da informação, com diversas tarefas especializadas que necessitam de uma capacitação técnica e que pode tornar essa capacidade em uma vulnerabilidade, caso não se tenham militares bem capacitados.

3.2.3 O Emprego das Capacidades Operativas pelas OM

A proteção cibernética é essencial para manter as capacidades do Exército no setor cibernético, principalmente frente às ameaças que evoluem a cada dia. Nesse sentido, o manual de Guerra Cibernética definiu os graus de responsabilidade para cada capacidade operativa:

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.

QUADRO 3 – Graus de responsabilidade.

Fonte: Manual de Campanha EB70-MC-10.232.

O Quadro 3 nos ajuda a entender o grau de responsabilidade para cada OM que compõe a Estrutura de Guerra Cibernética. O Batalhão de Guerra Eletrônica (BGE) do Exército, OM ímpar dentro do Exército Brasileiro, é a única com a responsabilidade de operar dentro das três Capacidades Operativas. Além desta capacidade, o BGE é a principal OM responsável pelas ações de Guerra Eletrônica dentro do Exército, fato que potencializa as ações de ataque cibernético, como visto acima. Algumas OM como os B Com GE e o BIM só não realizam o ataque cibernético. Porém, conforme o manual, todas essas OM tem responsabilidade de realizar as operações das tarefas relacionadas com a proteção cibernética.

O oficial de Comunicações formado na AMAN é o militar que adquiri a capacitação escolar sobre os assuntos relacionados a cibernética e que pode, posterior a sua formação, realizar os cursos técnicos de especialização. Será esse militar que irá compor os quadros de oficiais da maioria das OM citadas no Quadro 3, principalmente os B Com GE, B Com e Cia Com.

A OM de Comunicações, seja ela de valor Companhia ou de valor Batalhão, é a responsável por operar os meios de Comando e Controle e realizar as tarefas de proteção cibernética no âmbito de uma Grande Unidade (Brigada e Divisão de Exército). Assim, cresce de importância a capacitação desses oficiais de

Comunicações, pois necessitam ter a capacidade técnica de realizar todas as operações de proteção cibernética previstas no Quadro 2.

4. A CIBERNÉTICA COMO CAPACIDADE OPERATIVA DAS OM

O Catálogo de Capacidades do Exército foi publicado para subsidiar o Centro de Doutrina do Exército na consolidação do planejamento com base nas capacidades e nas definições das capacidades operativas. Todo o trabalho foi pautado para que o Exército possa atuar no amplo espectro dos conflitos, fazendo frente às ameaças dentro de áreas estratégicas.

FIGURA 4 – Capacidades
Fonte: Cátalogo EB20-C-07.001, p. 5).

O Planejamento Baseado em Capacidades (PBC) surge de uma evolução doutrinária do Exército Brasileiro, calcada na Estratégia Nacional de Defesa e na doutrina das principais potências dos países ocidentais. A identificação dos cenários e das ameaças são a base para a geração dessas capacidades.

De acordo com o Catálogo (Figura 4), a Capacidade Militar Terrestre (CMT) constitui um grupo de capacidades operativas com ligações funcionais, com objetivo de potencializar a aptidão da Força Terrestre no cumprimento de determinadas tarefas dentro de uma missão estabelecida.

A cibernética constitui a CMT número 09 (BRASIL, 2015, p 18) e tem, por definição, a necessidade de ser capaz de realizar as ações do meio cibernético, que envolvem os meios de Tecnologia da Informação e Comunicações, para superar os sistemas do oponente e defender os próprios. Abrange, essencialmente as ações de

ataque, exploração e defesa cibernética. O manual ainda faz ligação desta CMT com a de número 8 – Operações de Informação, ratificando seu uso como sensor de inteligência.

A Capacidade Operativa é, por definição, a aptidão requerida a uma força ou Organização Militar, para que possam cumprir sua missão. O Catálogo define as três divisões da Guerra Cibernética como três CO: CO35 – Exploração Cibernética, com foco na busca e otenção de dados nos Sistemas de Tecnologia da Informação de interesse, evitando, preferencialmente, ser rastreável; CO36 – Proteção Cibernética, capacidade de garantir o funcionamento de nossos ativos, neutralizando as ações de ataque e exploração; e CO37 – Ataque Cibernético, com a capacidade de conduzir ações para interromper, negar, degradar, corromper ou destruir informações do oponente.

As atividades são um conjunto de tarefas afins, reunidas pela semelhança de assunto, cujos resultados concorrem para o desenvolvimento de determinada função de combate. A eficácia dessas atividades se relaciona com a capacidade de identificação das capacidades operativas e na adequabilidade do emprego da força na solução dos problemas. As tarefas, por sua vez, são os conjuntos de ações que tem o objetivo geral de cumprir determinada missão. È durante a fase de planejamento que os comandantes identificam as tarefas a serem cumpridas e por meio de qual capacidade poderão cumprir a missão. A lista de atividades e tarefas relacionadas à Guerra Cibernética constam no manual EB70-MC-10.232 Guerra Cibernética.

As OM de Comunicações, conforme visto na definição de CO, ficam responsáveis por desenvolver essas aptidões dentro do cenário de cibernética. A Proteção Cibernética é a única permanente e executada por todas as OM de Comunicações (Quadro 3).

Nesse sentido, no intuito de avaliar se as OM têm obtido sucesso na geração dessa aptidão e com base no conhecimento dos oficiais de Comunicações egressos da AMAN, que obtiveram a capacitação inicial nos bancos escolares, foi confeccionado o questionário 1 (Apêndice 1). Este questionário tem o objetivo de analisar a percepção dos Comandantes (Cmt) e Chefes da Seção de Operações (S3) das diversas OM de Comunicações, que anualmente recebem novos oficiais da AMAN, sobre a geração das capacidades operativas, principalmente quanto à Proteção Cibernética.

Destarte, após uma pergunta sobre qual OM estava ligada ao respondente, a segunda pergunta foi se os Cmt e S3 das OM de Comunicações têm pleno conhecimento dos conceitos básicos, possibilidades e limitações da Guerra Cibernética descritos no manual EB70-MC-10.232 Guerra Cibernética:

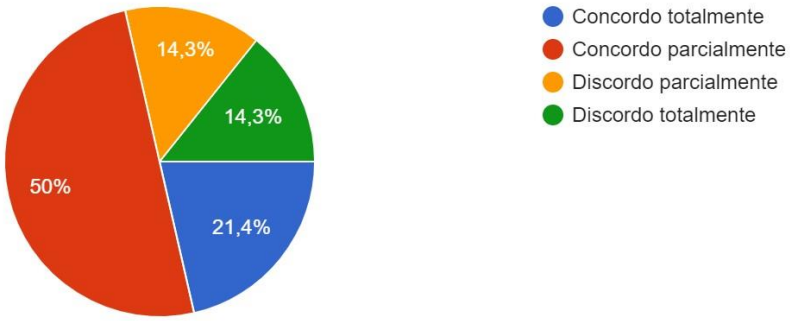

Gráfico 1 – Conhecimento acerca do manual

Fonte: O autor.

Conforme o Gráfico 1, a maioria desses militares considerou ter o conhecimento total ou parcial do manual, demonstrando o conhecimento destes militares sobre as atividades e tarefas necessárias a serem desenvolvidas nas OM para se obter a capacidade operativa desejada. Porém, cerca de 14% discordaram totalmente, denotando um alerta ao próprio comando da OM, por não saber sequer quais são as suas necessidades operativas, dificultando que tais objetivos sejam alcançados.

Após essa pergunta, as seguintes foram direcionadas a tarefas específicas de proteção cibernética, julgadas por esse autor como essenciais na manutenção do poder de combate da OM, por consequente da GU que a engloba, e na geração da aptidão necessária para se atingir a capacidade operativa.

Nesse contexto, a terceira pergunta foi sobre as tarefas – Defesa Ativa e Pronta, se TODOS os Of subalternos[5] têm a capacidade de detectar, identificar, avaliar e neutralizar as vulnerabilidades em uma rede de computadores ou sistemas de informação em uso no EB. Frente a essa ameaça, conseguem reagir ou assessorar seu Cmt de forma oportuna.

[5] Oficial dos postos mais baixos da carreira, 1º e 2º Tenentes.

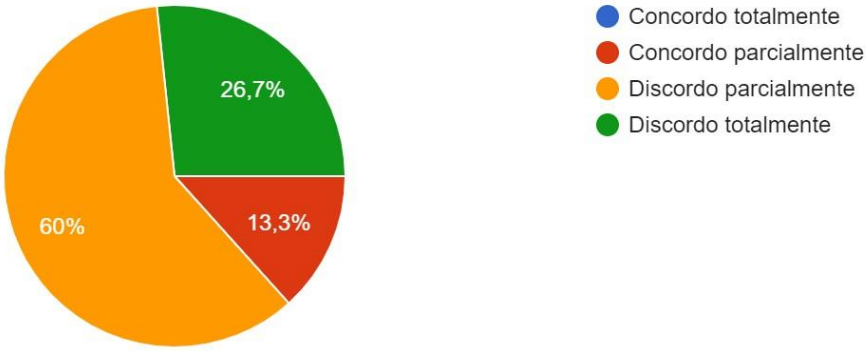

Gráfico 2 – Tarefa Defesa Ativa e Pronta

Fonte: O autor.

No gráfico acima podemos visualizar que quase 90% das respostas foram no sentido negativo, que não são todos os oficiais subalternos que tem a capacidade de executar esta tarefa. Um dado que fica ressaltado é que nenhum dos militares respondentes concordaram totalmente com a pergunta. A análise sumária deste gráfico aponta que, provavelmente, existe alguns militares na OM capazes de executar a tarefa mencionada, porém não todos.

Seguindo a lógica da pergunta três, a quarta pergunta foi sobre as tarefas Forense Digital e Teste de Artefatos Cibernéticos, se todos os Of subalternos têm a capacidade de coletar e examinar evidências digitais em redes e sistemas de informação de interesse do EB, além de testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos.

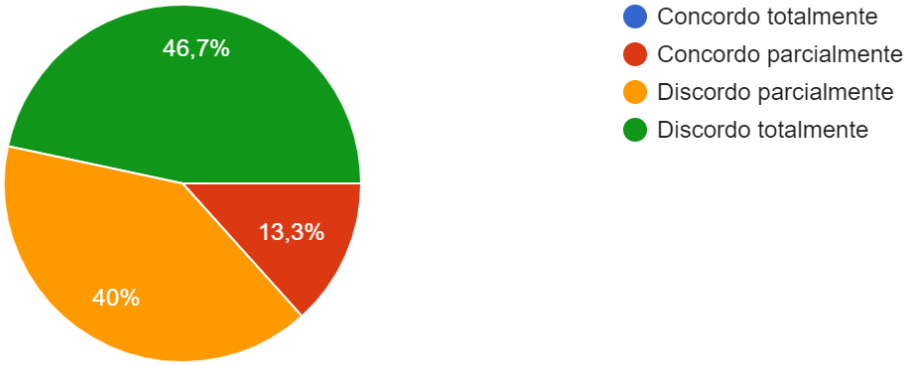

Gráfico 3 – Tarefa Forense Digital e Teste de Artefatos Cibernéticos

Fonte: O autor.

Ainda mais negativa, a tarefa apresentada foi respondida por quase 50% dos entrevistados como discordando completamente da afirmação e outros 40% discordaram parcialmente. Mais uma vez nenhum dos respondentes apontou com concordância total da assertiva.

A próxima pergunta foi em relação as tarefas de Controle de Acesso, Emprego de Criptografia e Segurança Física, se todos os Of subalternos têm a capacidade de determinar o que os usuários do sistema podem acessar e sua monitoração, utilizar técnicas e tecnologias de criptografia para aumentar a confiabilidade da rede criada e estabelecer condições para proteção física desses ativos.

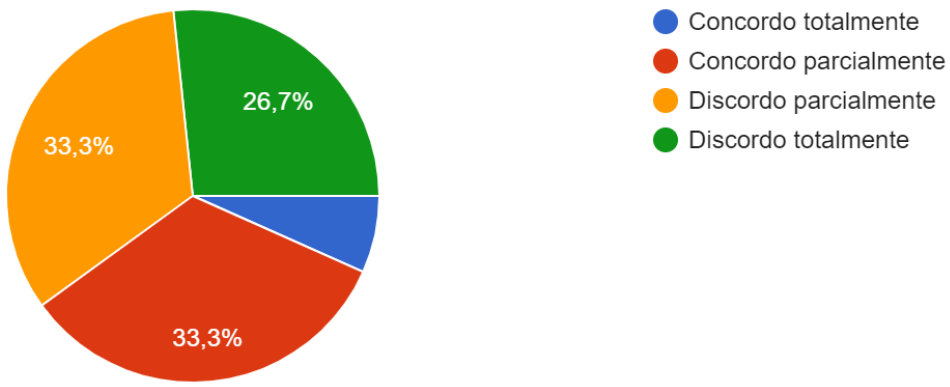

Gráfico 4 – Controle de Acesso, Emprego de Criptografia e Segurança Física
Fonte: O autor.

Essa tarefa tem uma maior facilidade de ser atingida por ser de fácil aprendizado e envolver a questão de segurança física (consideração do autor), porém, da mesma forma, a resposta foi negativa. Cerca de 60% dos respondentes apontaram para a falta de capacidade de todos os of subalternos cumprirem essa missão, provavelmente relacionado a parte gerencial da infraestrutura lógica. Nesta resposta foi obtido cerca de 34% de resposta positiva, indicando uma maior aptidão nesta tarefa para se atingir a capacidade operativa desejada.

A pergunta seguinte se referiu as tarefas de Gestão de Riscos, se todos os Of subalternos têm a capacidade de gerencias as relações dos ativos de informação com as vulnerabilidades/ameaças, executando e assessorando oportunamente no tratamento e monitoração destes incidentes/riscos.

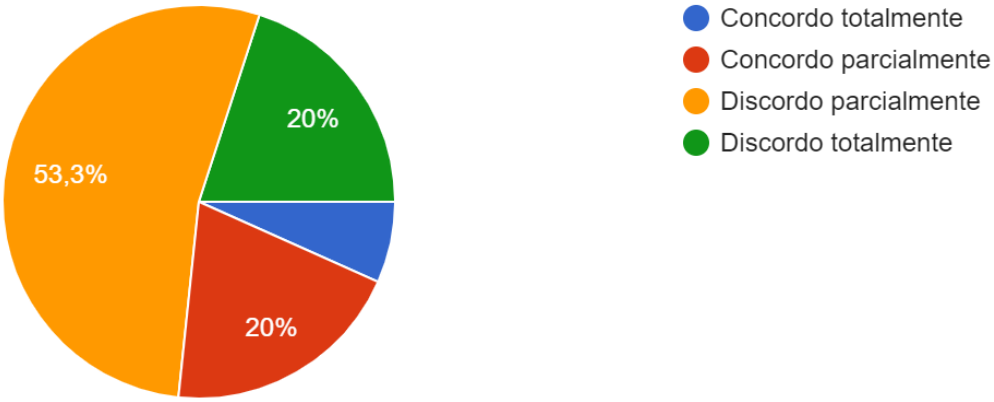

Gráfico 5 – Gestão de Riscos

Fonte: O autor.

Seguindo a percepção deste autor da pergunta anterior, a gestão é uma tarefa mais simples, que pode ser desenvolvida por uma capacitação básica, até mesmo em um autoaperfeiçoamento. O tratamento de incidentes requer maior capacidade, porém é de fácil obtenção com simples pesquisa na internet. Nesse sentido, as respostas foram negativas novamente, apontando para mais de 70% dos respondentes com a percepção que todos of subalternos não tem essa capacidade e menos de 30% concordaram, mesmo que parcialmente.

A pergunta sete foi sobre diversas tarefas que envolvem as condições dos Of subalternos de instalar um sistema de informações, realizar o gerenciamento e proteção deste sistema com controle de acesso, gestão da informação e tratamento de ameaças, tudo em conformidade com as tarefas descritas no manual.

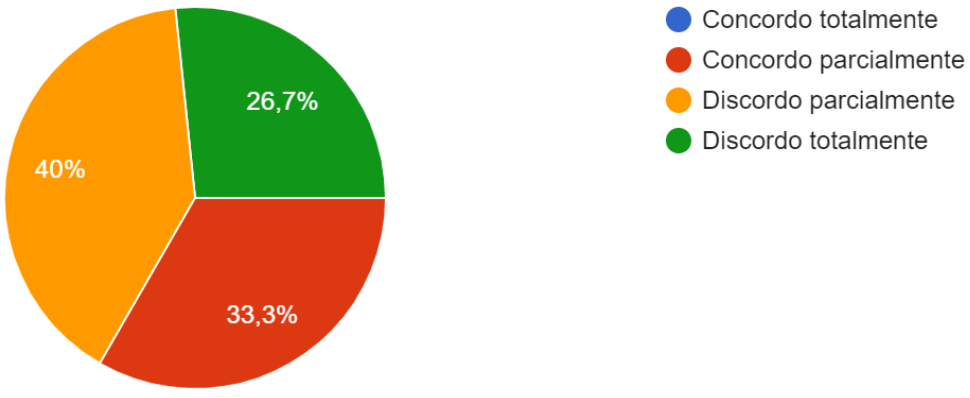

Gráfico 6 – Instalar e Gerenciar um Sistema

Fonte: O autor.

Seguindo a lógica das outras perguntas, essa se manteve no resultado negativo. Cerca de quase 70% dos respondentes apontaram para a falta de capacidade de todos os of subalternos de executarem essas tarefas, essenciais para o estabelecimento de um sistema. Apenas 33% concordaram parcialmente, sem nenhum apontamento para a concordância total com a afirmação.

A última pergunte foi destinada para a análise, com diversas assertivas, que deveriam ser marcadas para o caso de coincidência com a percepção que o respondente tinha sobre aquele tema.

Para a frase: “O conhecimento do Of subalterno em cibernética está ligado ao grau de interesse do mesmo no assunto.” Foi obtido um percentual de 93% positivo, indicando que as respostas do questionário indicam que a capacitação ocorre do interesse particular de poucos oficiais, em detrimento da capacitação completa desta capacidade operativa na AMAN.

A segunda assertiva: “Os Of subalternos de minha OM têm conhecimentos limitados ao básico de redes e TI” vai ao encontro das respostas anteriores e apontou que 60% dos respondentes concordam com a afirmação.

A afirmação três: “O conhecimento recebido na AMAN dos Of subalternos é adequado para as ações de proteção cibernética” liga-se diretamente a primeira e recebeu apenas 20% de respostas positivas. Tal concordância ratifica que a capacitação em cibernética nos bancos escolares não tem tido êxito na geração de tal capacidade.

A penúltima frase foi: “Poucos Of de minha OM têm condições de instalar, gerenciar e controlar um sistema de informação de forma segura e com capacidade de reagir às ameaças” que, nas mesmas linhas de raciocínio do problema, ratificou a percepção dos respondentes que não são todos os of subalternos capacitados para as tarefas de proteção cibernética, ficando com quase 90% de marcação.

Por último, a frase: “A carga horária de cibernética na AMAN serve apenas para fornecer um conhecimento inicial no assunto.” Gerou uma dúvida aos respondentes, com 60% da marcação positiva. Tal fato, gera a uma conclusão parcial que a capacitação da AMAN no setor cibernético gera efeitos, mas que devem ser aperfeiçoados pelo próprio militar ou por cursos de especialização.

Conclui-se, parcialmente, que a capacitação dos oficiais subalternos não tem atingido as necessidades operacionais das OM de Comunicações, principalmente quanto as tarefas que envolvem a geração da capacidade operativa proteção cibernética.

5. A FORMAÇÃO DO OFICIAL DE COMUNICAÇÕES DA AMAN

O PLADIS[6] do 2º ao 4º ano da AMAN, período de formação do cadete na arma de Comunicações, contempla uma carga horária total de 277 horas para a disciplina de cibernética, conforme Apêndice 3. Além desta carga horária, os cadetes têm as disciplinas iniciais de cibernética em âmbito comum aos outros cadetes, durante o período básico de formação.

No 2º ano do curso da AMAN os cadetes possuem uma carga maior, 120 horas, voltadas para as instruções relacionadas a instalação de um sistema, parte básica como IPV4[7], LAN/WAN, funcionamento das redes e equipamentos que fazem o roteamento dos dados (*switches*). Para aprender esses assuntos e com base nos cursos da Cisco[8], o cadete realiza os cursos CCNA I e CCNA II. O 2º ano está voltado para as instruções básicas, não atingindo de forma direta as tarefas de proteção cibernética previstas no manual de Guerra Cibernética, porém essenciais como fundamento base.

No 3º ano a carga horária é de 80 horas e o cadete já tem instruções voltadas para as capacidades objetivadas pelo manual de Guerra Cibernética. Assuntos como máquinas virtuais, uso do sistema operacional Linux, gerenciamento de usuário, registro de eventos, Backup, serviços web, entre outros. As tarefas que mais se relacionam à carga horária do 3º ano são gestão de riscos e de incidentes, controle de acesso e implementação de controles de segurança.

No 4º ano do curso de Comunicações da AMAN os cadetes têm 77 horas de carga horária e instruções mais avançadas como técnica de *hardening*[9], controle de acesso, as principais ameaças atuais e sobre engenharia social[10]. Essa carga horária está diretamente relacionada com as tarefas de proteção cibernética: segurança física, conformidade de SIC, defesa ativa, pronta resposta, entre outras.

Com base nas informações acima, podemos afirmar que a carga horária da AMAN está de acordo com o manual EB70-MC-10.232 Guerra Cibernética e direciona

[6] Plano das Disciplinas ministradas ao longo do curso de Comunicações da AMAN.
[7] Formato de endereço padrão que permite a comunicação entre os computadores.
[8] O Exército possui uma parceria com a Cisco para acesso a diversos cursos EAD.
[9] Técnica conhecida que blinda o sistema de acessos não autorizados, com identificação das principais ameaças e tratamentos necessários.
[10] Técnica usada para manipular usuários com interesse de permitir acesso ao sistema de informação.

os cadetes para obterem as aptidões necessárias para o desenvolvimento de quase todas as tarefas de proteção cibernética.

Neste intuito, foi distribuído o Questionário 2 aos oficiais subalternos formados na AMAN até o posto de 1º Tenente. A intenção foi de analisar se a carga horária de 277 horas foi suficiente para que esses militares conseguissem, na percepção deles próprios, atingir tais aptidões e capacidades.

Após uma pergunta inicial, para saber o ano de formação do militar, ratificando seu enquadramento como respondente, foi perguntado se o militar possuía pleno conhecimento dos conceitos básicos, possibilidades e limitações da Guerra Cibernética descritos no manual EB70-MC-10.232 Guerra Cibernética.

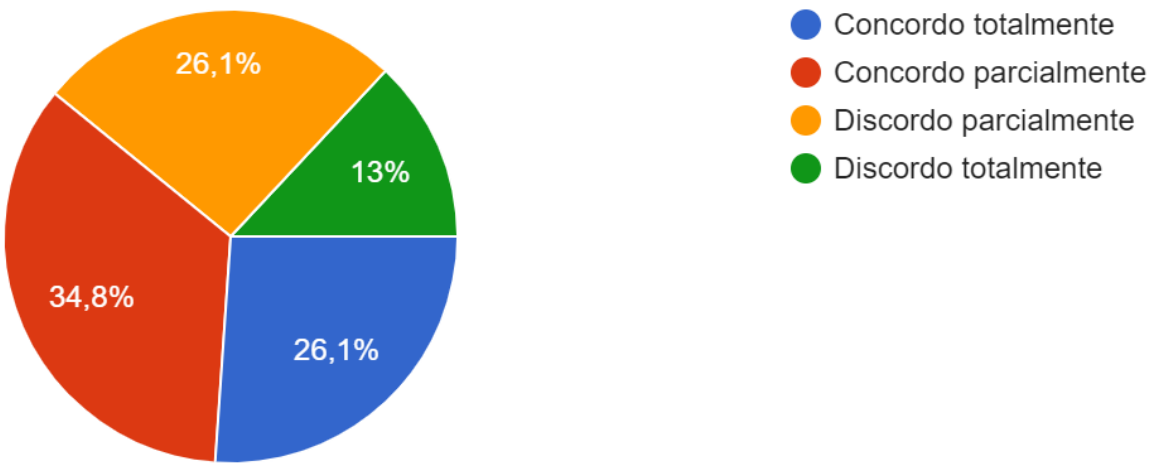

Gráfico 7 – Conhecimento do manual

Fonte: O autor.

A resposta da maioria dos respondentes, cerca de 61%, foi positiva. Ressalta-se que o manual de Guerra Cibernética foi publicado em 2017 e, assim, somente as turmas formadas a partir de 2018 puderem travar contato nos bancos escolares.

A próxima pergunta foi direcionada para a tarefa Defesa Ativa e Pronta Resposta, se o respondente considera ter a capacidade de detectar, identificar, avaliar e neutralizar as vulnerabilidades em uma rede de computadores ou sistemas de informação em uso no EB. Frente a essa ameaça, consegue reagir ou assessorar seu Cmt de forma oportuna.

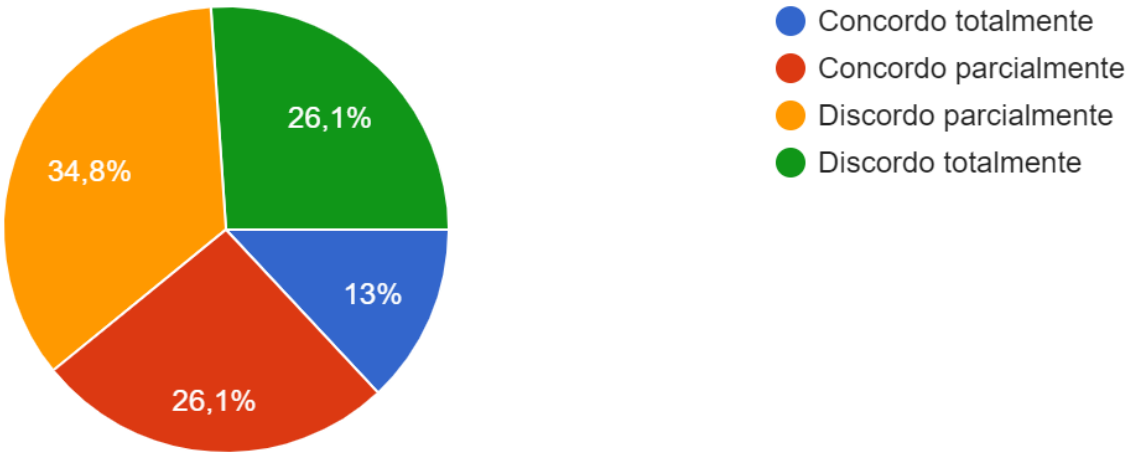

Gráfico 8 – Tarefa Defesa Ativa e Pronta Resposta

Fonte: O autor.

Da análise das respostas obtidas, pode se verificar que mais de 60% não possuem essa capacidade, sendo 26% nula. A tarefa de defesa ativa e pronta resposta é vista no 4º ano, porém de maneira superficial.

A pergunta 4 teve a assertiva relacionada com a tarefa Forense Digital e Teste de Artefatos Cibernéticos, onde se deveria ter a capacidade de coletar e examinar evidências digitais em redes e sistemas de informação de interesse do EB, além de testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos.

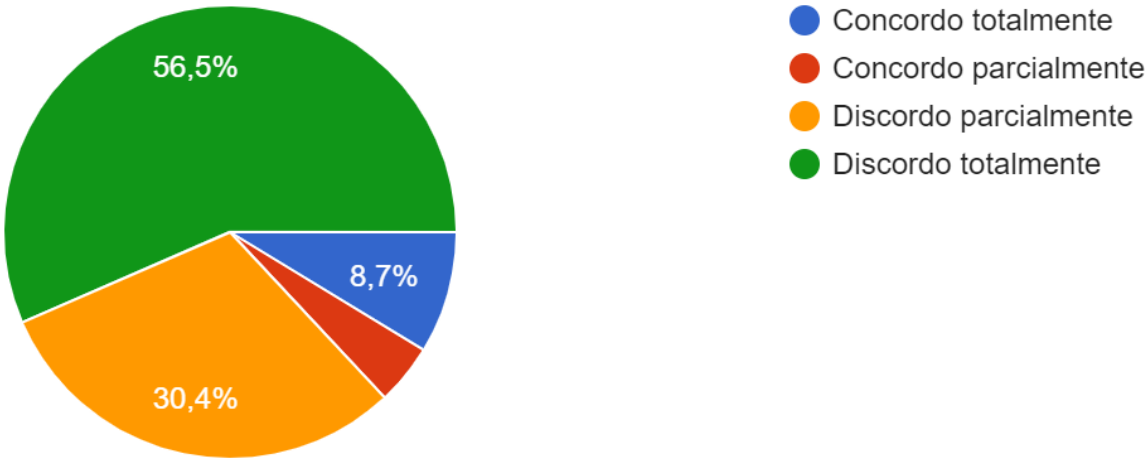

Gráfico 9 – Tarefa Forense Digital e Teste de Artefatos Cibernéticos

Fonte: O autor.

A pergunta que incluía a tarefa mais difícil, Forense Digital e Teste de Artefatos Cibernéticos, atingiu quase 90% de respostas negativas. Tal fato, com base em uma

avaliação parcial, ocorre pela não inclusão de disciplinas relacionadas a esta tarefa na AMAN. Da mesma forma, as respostas positivas são fruto do autoaperfeiçoamento.

Em sentido oposto à pergunta anterior, a pergunta 5 tinha uma conotação mais acessível, sendo em relação a tarefa Controle de Acesso, Emprego de Criptografia e Segurança Física, com a capacidade de determinar o que os usuários do sistema podem acessar e sua monitoração, utilizar técnicas e tecnologias de criptografia para aumentar a confiabilidade da rede criada e estabelecer condições para proteção física desses ativos.

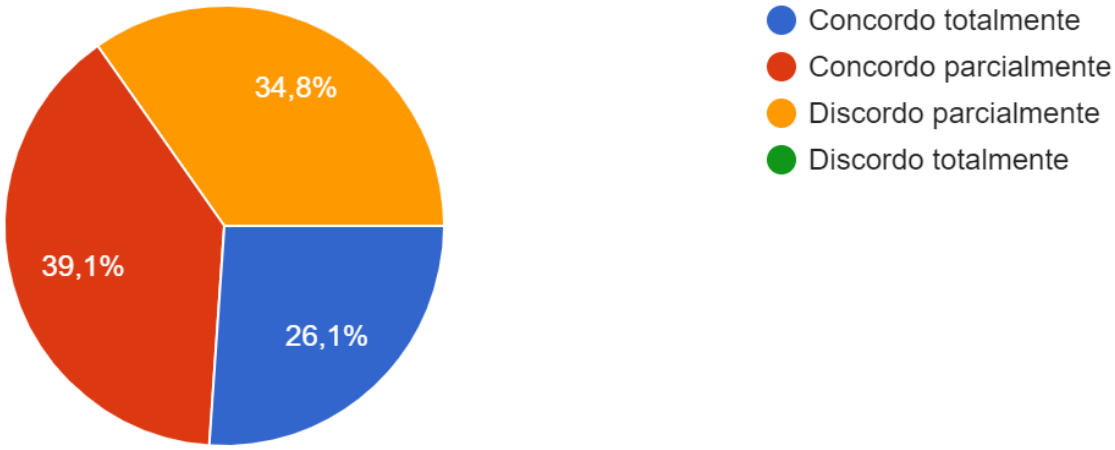

Gráfico 10 – Controle de Acesso, Emprego de Criptografia e Segurança Física
Fonte: O autor.

A resposta positiva de mais de 65% dos respondentes colabora para a conclusão parcial que essa capacidade foi ministrada e gerada na AMAN, ao longo dos 3 anos do curso de Comunicações. Cabe destacar que não houve marcação de discordância total com o item, demonstrando que a tarefa foi ministrada, mesmo que em curta carga horária.

A penúltima pergunta foi relacionada a tarefa Gestão de Riscos, se o respondente tem a capacidade de gerencias as relações dos ativos de informação com as vulnerabilidades/ameaças, executando e assessorando oportunamente no tratamento e monitoração destes incidentes/riscos.

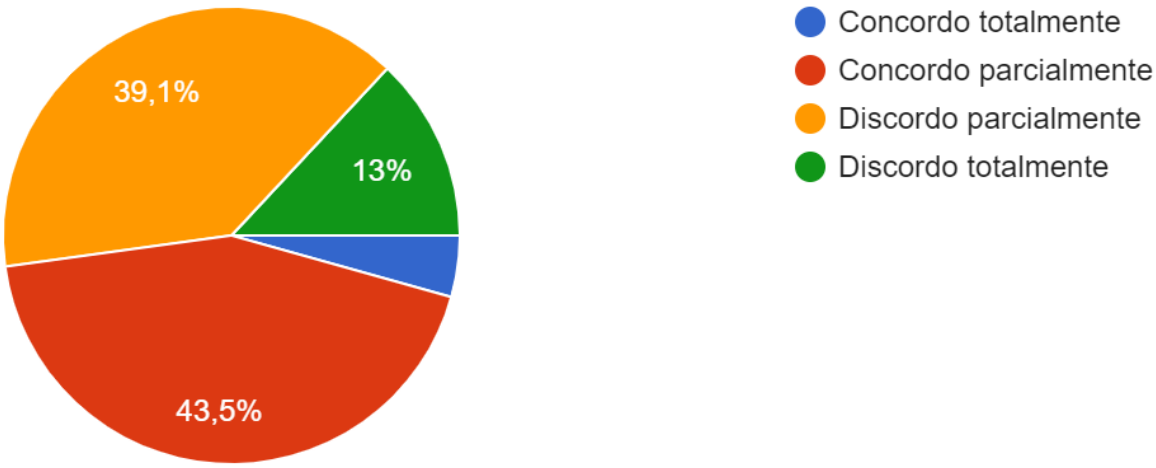

Gráfico 11 – Gestão de Riscos

Fonte: O autor.

Importante tarefa no escopo da proteção cibernética, a gestão de risco é obrigatória na manutenção de um sistema seguro. Assim, verifica-se que as respostas foram bem divididas, atingindo cerca de 50% positivas e 50% negativas.

Como última pergunta de relação com as tarefas, foi questionado o respondente sobre a capacidade de instalar um sistema de informações em rede, em minha OM de Com, realizar o gerenciamento e proteção deste sistema com controle de acesso, gestão da informação e tratamento de ameaças, tudo em conformidade com as tarefas descritas no manual de cibernética.

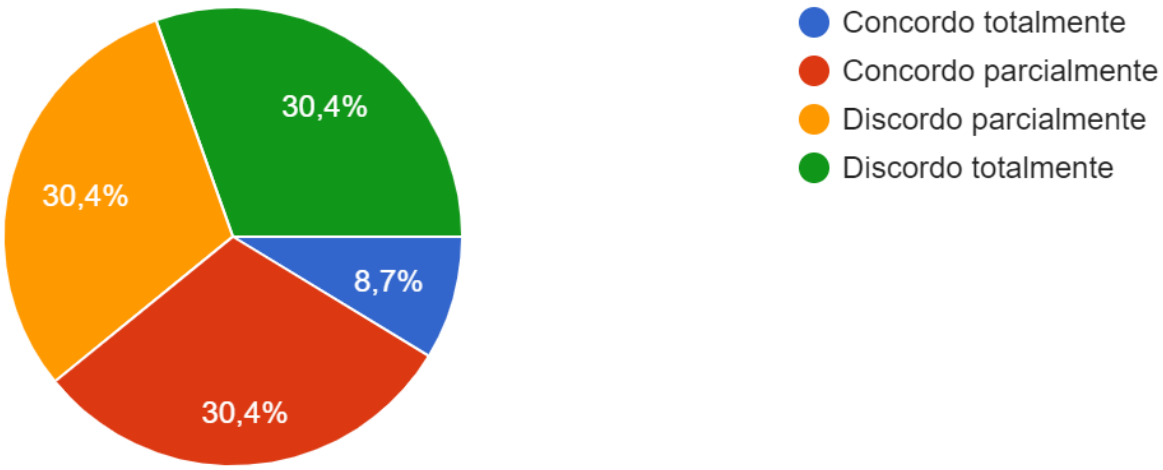

Gráfico 12 – Instalação e gerenciamento de um sistema

Fonte: O autor.

A tarefa básica de instalação e gerenciamento de um sistema tem o principal objetivo de analisar se o respondente adquiriu a capacidade fundamental na AMAN. Diante disto, menos de 40% dos militares tem a capacidade básica de realizar tais procedimentos.

No último item do questionário foram apresentadas assertivas para que o respondente fizesse a marcação daquelas que ele concordava. A primeira frase foi “Meu conhecimento em cibernética está mais ligado ao grau de interesse pessoal. O conhecimento recebido na AMAN foi básico”. Com cerca de 56% de respostas positivas a afirmação gerou dúvidas, reforçando que o conhecimento produzido na AMAN é além do básico, porém não muito avançado.

A segunda assertiva foi: “Meu conhecimento é básico, não sei instalar os softwares, gerenciar os ativos ou fazer tratamento das ameaças do setor”. Nesta afirmação buscou-se analisar a parte básica de operação de um sistema, onde somente 13% marcaram essa opção. O número é baixo para uma tarefa que requer mais experiência e contato com esse tipo de missão do que propriamente um conhecimento teórico.

A terceira afirmação foi “A carga horária de cibernética da AMAN tem TOTAL condições de capacitar o Asp Of a cumprir as missões descritas no manual de cibernética”. Seguindo esta lógica, a frase não foi concordada por nenhum dos respondentes, ficando com 0%. Tal fato se liga a afirmação 1, onde o conhecimento produzido na AMAN não é básico, possui ensinos lógicos e coerentes com o assunto, porém está longe de ser completo. A porcentagem “0”% é simbólica e evidencia sistematicamente que o ensino na AMAN não tem capacidade os oficiais de comunicações a desempenharem as funções de cibernética na tropa, particularmente quanto à proteção cibernética.

Como quarta assertiva, a indagação foi “Apesar de não ter muito conhecimento, tenho a capacidade de gerir uma missão de proteção dos ativos de informação, proteção do sistema e controle de acesso de usuários”. Marcada por apenas 17%, denota a falta de aptidão da maioria dos respondentes em capacidades mais avançadas.

Por último, em ligação com as assertivas 1 e 3, foi afirmado “Sem autoaperfeiçoamento, não é possível, ao longo da formação da AMAN, ter todas as capacidades descritas no manual. Apenas um conhecimento básico que deverá ser moldado e especializado em cursos específicos”. A comprovação que o conhecimento

gerado na AMAN necessita ser completado pelo autoaperfeiçoamento foi marcado por quase 80% dos respondentes.

Infere-se, parcialmente, que a instrução na AMAN tem curta carga horária para formar militares de Comunicações no setor cibernético. A proteção cibernética, capacidade operativa permanente do Exército possui diversas tarefas técnicas que devem ser de conhecimento do oficial subalterno, militar responsável pela instalação, gerenciamento e proteção dos sistemas de uma GU.

6. CONCLUSÃO

O espectro cibernético tem se mostrado cada vez mais fundamental nas operações militares. O sucesso das nossas operações está relacionada à segurança dos nossos ativos, das nossas informações e dos nossos meios, ficando evidente que a capacitação dos nossos militares nos assuntos relacionados à guerra cibernética é fundamental para tal. Destarte, a proteção cibernética é o ramo que se destaca neste ínterim e se transforma em um dos principais multiplicadores do poder de combate.

Em síntese, a capacitação dos oficiais da arma de comunicações na Academia Militar das Agulhas Negras se torna primordial para se atingir as capacidades operativas do Exército Brasileiro, em particular às relacionadas à guerra cibernética. Negar ao nosso oponente o acesso aos nossos ativos, explorar suas informações e atacar os meios constituem grandes vantagens militares que nossos militares precisam dominar.

Da análise deste trabalho foi possível identificar que o Exército Brasileiro vem conduzindo com afinco e grande capacidade de gestão a estruturação da cibernética no país. O Comando e Centro de Guerra Cibernética, aliado as capacitações da AMAN e cursos de especializações buscam produzir as capacidades operativas elencadas pelo Exército para fazer frente às ameaças atuais e vindouras.

Como resultado inicial, foi possível identificar que as ameaças são constantes e evoluem de forma exponencial, obrigando que as capacidades sejam geradas e atualizadas de forma frequente e sistemática. De forma estratégica, o Comando de Defesa Cibernética conduz a proteção de nossos ativos, realizando inclusive proteção de infraestruturas críticas e colaborando para manter a soberania nacional. No campo tático a responsabilidade recai sobre as Grandes Unidades, que desenvolvem as operações no menor nível e precisam executar principalmente a proteção cibernética.

Desta forma, verificou-se que a capacitação realizada na AMAN, nos assuntos relacionados à guerra cibernética, é essencial por ser o primeiro contato dos oficiais de comunicações com o assunto. Cabe ressaltar que estes oficiais terão apenas esta oportunidade para travar contato com o ensino desta matéria, exceto aqueles que forem realizar cursos de especialização no assunto. Assim, os oficiais que conduzirão a proteção cibernética das operações militares, no campo tático, necessitam adquirir tais capacidades operativas para fornecer a segurança nas operações das Grandes Unidades.

No intuito de identificar se tal objetivo vem sendo atingido, este trabalho identificou que a formação do conhecimento básico, na AMAN, vem sendo atingida com êxito, comprovadas pelas afirmações cosntantes do final dos questionários 1 e 2. Porém ficou também evidente a falta de profundidade que tais assuntos tem sido abordado em contrapartida com a necessidade de geração da capacidade operativa de cibernética, prevista no Catalogo de Capacidades Operativas do Exército Brasileiro.

Assim, o objetivo geral deste trabalho identificou que a capacidade desenvolvida pelo Asp Of de Com, egresso da AMAN, não tem sido suficiente para proteger os ativos e as informações que circulam entre os elementos da F Ter, particularmente atinentes ao setor cibernético. Tal resposta pode ser obtida em quase todas as perguntas respondidas nos questionários 1 e 2, mas fica evidente nas respostas das perguntas de número 2 dos questionários, relacionados à tarefa essencial para a proteção cibernética e que tiveram uma resposta negativa, total ou parcial, de quase 90% dos respondentes. Outra resposta que corroborou para se identificar esta afirmação é que nenhum dos respondentes assinalou a concordância com a afirmação “A carga horária de cibernética da AMAN tem TOTAL condições de capacitar o Asp Of a cumprir as missões descritas no manual de cibernética”.

Ainda, pode ser identificado e comprovado nas respostas das perguntas que uma pequena parte de respondente, tanto entre os oficiais de comunicações como pelos seus comandantes/S3, detém domínio do assunto, o que poderia refutar a conclusão apresentada. Porém a afirmativa, apresentada nos dois questionários, relacionada ao conhecimento do militar sobre cibernética ser relacionada ao seu grau de interesse e não à capacitação recebida, apresentou alto índice de concordância entre os respondentes, particularmente com os do primeiro questionaria que atingiram 93%.

Como conclusão final ficou evidenciado que a capacitação de cibernética nos bancos escolares da AMAN tem gerado capacidades operativas ao Exército Brasileiro em um nível inicial, porém, em concordância com o Manual de Campanha EB70-MC-10.232 Guerra Cibernética e o Catalogo de Capacidades Operativas, existe uma necessidade de maior aprofundamento nas questões técnicas, particularmente quanto as atividades e tarefas que geram a capacidade operativa de proteção cibernética.

Por fim, fruto desta pesquisa, conclui-se que se faz necessária incrementar os assuntos relacionados à guerra cibernética no currículo escolar da AMAN, buscando a conciliação das matérias com as atividades e tarefas descritas no EB70-MC-10.232, principalmente os de proteção cibernética. As ameaças deste espectro cibernético são cada vez mais preocupantes e tem a capacidade de acabar com a capacidade operativa de um exército e, para isso, é essencial que o Exército Brasileiro esteja em constante atualização para fazer frente à esse oponente.

REFERÊNCIAS

_____. Exército. **EB70-MC-10.232 Guerra Cibernética.** 1. ed. Brasília, DF, 2017.

_____. Exército. **EB20-MC-10.205 Comando e Controle.** 1. ed. Brasília, DF, 2015.

_____. Exército. **MD31-M-07 Doutrina Militar de Defesa Cibernética.** 1. ed. Brasília, DF, 2014.

ALFORD, Lionel D. Cyber Warfare: Protecting Military Systems. **Acquisition Review Journal**, Fort Belvoir, Fairfax County, VA, EUA, p. 100 – 120, 2000.

CARREIRO, Marcelo. **A Guerra Cibernética:** Cyberwarfare e a Securitização da Internet. Rio de Janeiro, RJ, 2012.

DAMIÃO, André Kohler. **Guerra Cibernética**: Proteção Cibernética monitoramento de redes e sistemas e levantamento de vulnerabilidades. Trabalho de Conclusão de Curso (Especialização em ciências militares) - Escola de Aperfeiçoamento de Oficiais. Rio de Janeiro, 2018.

DOS SANTOS, Marcel Deyvison Lima. **O emprego da proteção cibernética para ampliar a segurança nos postos de comando da Força Terrestre Componente.** Trabalho de Conclusão de Curso (Especialização em ciências militares) – Escola de Estado Maior, Rio de Janeiro, 2021.

DUTRA, André Melo Carvalhais. Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto. **IX Simpósio de Guerra Eletrônica**, 2007.

GOMES, M. G. F. M; CORDEIRO, S. S; PINHEIRO, W. A. A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle. **Revista Militar de Ciência e Tecnologia.** Rio de Janeiro, 2016.

GOMES, Mauro Guedes Ferreira Mosqueira; CORDEIRO, Sandro Silva; PINHEIRO, Wallace Anacleto. A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). **Rio de Janeiro**, 2016.

GUIMARÃES, Flavio de Queiroz. **Análise comparativa da estruturação do setor cibernético nacional em função das doutrinas cibernéticas internacionais**. Brasília. Trabalho de Conclusão do Curso de Guerra Cibernética para Oficiais. 2017.

MARCONDES, José Sérgio. **Segurança Cibernética**: O que é, Objetivos, Importância, Medidas. 2021. Disponível em: < https://gestaodesegurancaprivada.com.br/seguranca-cibernetica-o-que-e-objetivos-importancia-medidas/>. Acesso em: 04 de junho de 2021.

MONTEIRO, Luís. A internet como meio de comunicação: possibilidades e limitações. In: Congresso Brasileiro de Comunicação. 2001.

NICHOLSON, Andrew et al. SCADA security in the light of Cyber-Warfare. Computers & Security, v. 31, n. 4, p. 418-436, 2012.
LIMA, Victor Hugo. Hacktivismo e a Defesa Cibernética do Brasil. **Centro de Estudos Estratégicos do Exército – CEEEx**. Brasília. Vol 8 . março/maio 2018.

OLIVEIRA, Marcelo Mendes. **A defesa cibernética, o Exército Brasileiro e a gestão de projetos**. Rio de Janeiro. 2021.

PINHEIRO, Alvaro de Souza. **A Tecnologia da Informação e a Ameaça Cibernética na Guerra Irregular do Século XXI**. Padeceme**.** Rio de Janeiro, 2008.

BLACKBERRY. **Relatório de Ameaças 2021.** 2021. Disponível em: <https://www.blackberry.com/us/en/>. Acesso em 05 de junho de 2022.

BRASIL. **Estratégia Nacional de Defesa (END).** Brasília. 2008. Disponível em: <www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 01 de junho de 2022.

BRASIL. **Defesa Cibernética.** Disponível em: < http://www.epex.eb.mil.br/index.php/defesa-cibernetica> Acesso em: 24 de abril de 2022.

BRASIL. **Sistema Militar de Defesa Cibernética** <https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/sistema-militar-de-defesa-cibernetica-entra-em-vigor-nesta-terca-feira>. Disponível em 28 de abril de 2022.

GUERRA CIBERNETICA. **Guerra Cibernética e os conflitos na era da Informação.** Disponível em: < https://www.compugraf.com.br/guerra-cibernetica/#dba3t>. Acesso em: 24 de abril de 2022.

TECMUNDO. **Hackers vazam dados de 200 mil militares.** Disponível em: <https://www.tecmundo.com.br/seguranca/153022-hackers-vazam-dados-200-mil-militares-retaliacao-bolsonaro.htm > Acesso em: 15 de maio de 2022.

Questionário aos Cmt OM/Ex Cmt OM e S3 de Com

Este trabalho tem por objetivo identi car se a carga horária de Guerra Cibernética, durante a formação do Of na AMAN, está adequada para o cumprimento das ações de cibernética em operações.

Todas as perguntas estão fundamentadas no Manual EB70-MC-10.232 Guerra Cibernética

As perguntas se destinam aos Cmt OM/Ex Cmt OM e S3 de Com, para ser respondida sobre a percepção dos Of subalternos integrantes da OM e suas capacidades em gerir as TAREFAS descritas no manual supracitado.

1- Identifique qual Esc da F Ter o Sr comandou ou está comandando (ou E3):

- ☐ BCom GE
- ☐ BCom
- ☐ Cia Com

2- Tenho pleno conhecimento dos conceitos básicos, possibilidades e limitações da Guerra Cibernética descritos no manual:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

3- TAREFA – Defesa Ativa e Pronta Resposta - TODOS os Of subalternos têm a capacidade de detectar, identificar, avaliar e neutralizar as vulnerabilidades em uma rede de computadores ou sistemas de informação em uso no EB. Frente a essa ameaça, conseguem reagir ou assessorar seu Cmt de forma oportuna:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

4- TAREFA – Forense Digital e Teste de Artefatos Cibernéticos - TODOS os Of subalternos têm a capacidade de coletar e examinar evidências digitais em redes e

sistemas de informação de interesse do EB, além de testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

5- TAREFA – Controle de Acesso, Emprego de Criptografia e Segurança Física - TODOS os Of subalternos têm a capacidade de determinar o que os usuários do sistema podem acessar e sua monitoração, utilizar técnicas e tecnologias de criptografia para aumentar a confiabilidade da rede criada e estabelecer condições para proteção física desses ativos:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

6- TAREFA – Gestão de Riscos -TODOS os Of subalternos têm a capacidade de gerencias as relações dos ativos de informação com as vulnerabilidades/ameaças, executando e assessorando oportunamente no tratamento e monitoração destes incidentes/riscos:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

7- Na minha opinião, TODOS os Of subalternos de minha OM possuem condições de instalar um sistema de informações, realizar o gerenciamento e proteção deste sistema com controle de acesso, gestão da informação e tratamento de ameaças, tudo em conformidade com as tarefas descritas no manual de cibernética:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

8 - Marque as assertivas que coincidem com sua opinião:

☐ O conhecimento do Of subalterno em cibernética está ligado ao grau de interesse do mesmo no assunto.

☐ Os Of subalternos de minha OM têm conhecimentos limitados ao básico de rede e TI.

☐ O conhecimento recebido na AMAN dos Of subalternos é adequado para as ações de proteção cibernética

☐ Poucos Of de minha OM tem condições de instalar, gerenciar e controlar um sistema de informação de forma segura e com capacidade de reagir às ameaças

☐ A carga horária de cibernética na AMAN serve apenas para fornecer um conhecimento inicial no assunto.

Questionário aos Asp Of e Ten Com de AMAN

Este trabalho tem por objetivo identi car se a carga horária de Guerra Cibernética, durante a formação do Of na AMAN, está adequada para o cumprimento das ações de cibernética em operações.

Todas as perguntas estão fundamentadas no Manual EB70-MC-10.232 Guerra Cibernética

As perguntas se destinam aos Asp Of e Ten Com de AMAN e suas capacidades em gerir as TAREFAS descritas no manual supracitado.

1- Identifique qual seu ano de formação na AMAN.

- ☐ 2021
- ☐ 2020
- ☐ 2019
- ☐ 2018
- ☐ Outro

2- Tenho pleno conhecimento dos conceitos básicos, possibilidades e limitações da Guerra Cibernética descritos no manual EB70-MC-10.232 Guerra Cibernética:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

3- TAREFA – Defesa Ativa e Pronta Resposta - EU, como Of subalterno de uma OM de Com, tenho a capacidade de detectar, identificar, avaliar e neutralizar as vulnerabilidades em uma rede de computadores ou sistemas de informação em uso no EB. Frente a essa ameaça, consigo reagir ou assessorar meu Cmt de forma oportuna:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

4- TAREFA – Forense Digital e Teste de Artefatos Cibernéticos - EU, como Of subalterno de uma OM de Com, tenho a capacidade de coletar e examinar evidências digitais em redes e sistemas de informação de interesse do EB, além de testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos:.

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

5- TAREFA – Controle de Acesso, Emprego de Criptografia e Segurança Física - EU, como Of subalterno de uma OM de Com, tenho a capacidade de determinar o que os usuários do sistema podem acessar e sua monitoração, utilizar técnicas e tecnologias de criptografia para aumentar a confiabilidade da rede criada e estabelecer condições para proteção física desses ativos:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

6- TAREFA – Gestão de Riscos - EU, como Of subalterno de uma OM de Com, tenho a capacidade de gerencias as relações dos ativos de informação com as vulnerabilidades/ameaças, executando e assessorando oportunamente no tratamento e monitoração destes incidentes/riscos:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

7- Na minha opinião, EU TENHO TOTAL condições de instalar um sistema de informações em rede, em minha OM de Com, realizar o gerenciamento e proteção deste sistema com controle de acesso, gestão da informação e tratamento de ameaças, tudo em conformidade com as tarefas descritas no manual de cibernética:

- ◯ Concordo totalmente
- ◯ Concordo parcialmente
- ◯ Discordo parcialmente
- ◯ Discordo totalmente

8 - Marque as assertivas que coincidem com sua opinião:

☐ Meu conhecimento em cibernética está mais ligado ao grau de interesse pessoal. O conhecimento recebido na AMAN foi básico.

☐ Meu conhecimento é básico, não sei instalar os softwares, gerenciar os ativos ou fazer tratamento das ameaças do setor.

☐ A carga horária de cibernética da AMAN tem TOTAL condições de capacitar o Asp Of a cumprir as missões descritas no manual de cibernética.

☐ Apesar de não ter muito conhecimento, tenho a capacidade de gerir uma missão de proteção dos ativos de informação, proteção do sistema e controle de acesso de usuários.

☐ Sem autoaperfeiçoamento, não é possível, ao longo da formação da AMAN, ter todas as capacidades descritas no manual. Apenas um conhecimento básico que deverá ser moldado e especializado em cursos de especialização.