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

Maj Com **MARCEL** DEYVISON LIMA DOS SANTOS

O emprego da proteção cibernética para ampliar a segurança nos postos de comando da Força Terrestre Componente

Rio de Janeiro
2021

Maj Com **MARCEL** DEYVISON LIMA DOS SANTOS

O emprego da proteção cibernética para ampliar a segurança nos postos de comando da Força Terrestre Componente

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 Com Enio Corrêa de Souza

Rio de Janeiro
2021

S237e Santos, Marcel Deyvison Lima dos

O emprego da proteção cibernética para ampliar a segurança dos postos de comando da força terrestre componente. / Marcel Deyvison Lima dos Santos. – 2021.
49 f. : il. ; 30 cm.

Orientação: Enio Corrêa de Souza.
Trabalho de Conclusão de Curso (Especialização em Ciências Militares)—Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021.
Bibliografia: f. 47-49.

1. PROTEÇÃO CIBERNÉTICA. 2. FORÇA TERRESTRE COMPONENTE. 3. SEGURANÇA. I. Título.

CDD 355.4

Maj Com **MARCEL** DEYVISON LIMA DOS SANTOS

O emprego da proteção cibernética para ampliar a segurança nos postos de comando da Força Terrestre Componente

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 novembro de 2021.

COMISSÃO AVALIADORA

_____
Enio Corrêa de Souza – Ten Cel Com - Presidente
Escola de Comando e Estado-Maior do Exército

_____
Marco Antonio Barbosa – Ten Cel Com - Membro
Escola de Comando e Estado-Maior do Exército

_____
Carlos Otávio Macedo de Sousa – Ten Cel Inf - Membro
Escola de Comando e Estado-Maior do Exército

À minha esposa Hyanna e às minhas filhas Lara e Milena, que me forneceram a força e o equilíbrio necessários para vencer os desafios dessa difícil jornada.

AGRADECIMENTOS

A Deus, pela vida, pela saúde e pela força espiritual que me proporcionam a energia essencial para me manter firme na persecução dos meus objetivos pessoais.

À minha esposa Hyanna e às minhas filhas Lara e Milena que souberam compreender minha ausência nos momentos em que me dediquei ao aprimoramento profissional.

Ao meu pai, Nivaldo e à minha mãe Josedite, por ter perseverado na minha educação e dado todo o suporte necessário durante minhas jornadas.

Ao meu orientador, TC Enio pela confiança depositada e pelas orientações oportunas que foram imprescindíveis para a confecção do presente trabalho.

Aos militares do Centro de Defesa Cibernética, da Companhia de Comando e Controle e do Centro de Instrução de Guerra Eletrônica que colaboraram com esta pesquisa com bibliografias ou experiências profissionais.

Aos instrutores do Curso de Comando e Estado-Maior do Exército pelo profissionalismo em todas as instruções, servindo de exemplos a serem seguidos no percurso da minha carreira militar.

Aos companheiros de curso que colaboraram, direta ou indiretamente, com a conclusão desta pesquisa, ampliando minha capacidade cognitiva e elevando minha condição moral sempre que se fez necessário enquanto ombreamos a rotina da Escola Marechal Castello Branco.

“A evolução do homem passa, necessariamente, pela busca do conhecimento.” (Sun Tzu)

RESUMO

Na atualidade, as grandes potências estão desenvolvendo seus exércitos com as capacidades cibernéticas a fim de estarem aptas a combater na dimensão do ciberespaço, em virtude da rápida evolução tecnológica. Dentre essas capacidades está a da Proteção Cibernética, direcionada a proteger os sistemas operados em rede e que são fundamentais para a condução do combate. Em uma situação de emprego conjunto das Forças Armadas, é fundamental que a Força Terrestre Componente mantenha segura as informações transitadas nos Sistemas de Comando e Controle, para que os processos de tomada de decisão sejam realizados com maior confiabilidade e rapidez. Para tanto, é necessária a constante execução de tarefas que permitem a proteção dos Sistemas de Comando e Controle da FTC. A fim de ampliar a segurança desses sistemas, medidas adicionais de proteção devem ser adotadas para identificar as ameaças com maior rapidez e mitigar os riscos para as operações, no que tange às informações. Ainda, é relevante que a proteção cibernética seja cultuada em todos os escalões da Força Terrestre, seja nos tempos de paz ou de guerra.

Palavras-chave: Proteção Cibernética; Força Terrestre Componente; Segurança.

RESUMEN

Actualmente, las grandes potencias están desarrollando sus ejércitos con las capacidades cibernéticas con fin de ponerse en condiciones de combatir en la dimensión del espacio cibernético, debido a rápida evolución tecnológica. Entre las capacidades está la Protección Cibernética, destinada a proteger los sistemas operados en red y que san fundamentales para la conducción del combate. En una situación de empleo conjunto de las Fuerzas Armadas, es fundamental que la Fuerza Terrestre Componente mantenga segura las informaciones transitadas en los Sistemas de Mando y Control, para que los procesos de toma de decisión sean realizados con mayor confiabilidad y rapidez. Para tanto, es necesaria la constante ejecución de tareas que permitan la protección de los Sistemas de Mando y Control de la FTC. Con fin de ampliar la seguridad de eses sistemas, medidas a más de protección deben ser tomadas para identificar las amenazas con mayor rapidez y disminuir los riesgos para las operaciones, con relación a las informaciones. Todavía, es importante que la protección cibernética sea cultivada en todos los escalones de la Fuerza Terrestre, sea en los tiempos de paz o de guerra.

Palabras clave: Protección Cibernética; Fuerza Terrestre Componente; Seguridad;

LISTA DE ABREVIATURAS

AFCYBER	Comando Cibernético da Força Aérea dos EUA
AFP	Administração Pública Federal
ARCYBER	Comando Cibernético do Exército dos EUA
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
CC Op	Centro de Coordenação de Operações
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 FTC	Comandante da Força Terrestre Componente
CO	Capacidades Operativas
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
F Cte	Força Componente
FTC	Força Terrestre Componente
FTP	Serviço de Transferência de Arquivo

IA	Inteligência Artificial
IME	Instituto Militar de Engenharia
MARFORCYBER	Comando Cibernético da Marinha e dos Fuzileiros Navais dos EUA
OCCA	Operações de Cooperação e Coordenação com Agências
PC	Posto de Comando
PIM	Programa de Instrução Militar
PR	Presidência da República
RENASIC	Rede Nacional de Segurança da Informação e Criptografia
ROD	Rede Operacional de Defesa
RPC	República Popular da China
RPDC	República Popular Democrática da Coreia
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
SISCOMIS	Sistema de Comunicações por Satélite
SMDC	Sistema Militar de Defesa Cibernética
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
USCYBERCOM	Comando Cibernético dos Estados Unidos da América
USSTRATCOM	Comando Estratégico dos Estados Unidos da América
VoIP	Voz sobre IP
VPN	Rede Virtual Privada
VUCA	*volatility*, *uncertainty*, *complexity and ambiguity*

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1. INTRODUÇÃO

O espaço cibernético tem sido amplamente empregado nos conflitos da atualidade como um dos meios pelos quais os Estados em beligerância buscam obter vantagens sobre seu oponente. Em um mundo cada vez mais dependente da tecnologia em rede, as preocupações com a segurança da informação no Exército Brasileiro tornam-se crescentes, especialmente no tocante às informações que transitarão nos sistemas de comando e controle da Força Terrestre, em caso de um conflito envolvendo o Brasil.

Os eventos de ataques cibernéticos têm crescido nas últimas décadas e essas ameaças atraíram a atenção das autoridades políticas e militares de diversos países, conforme pode ser observado na seguinte citação: “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). Com isso, o mundo passou a vivenciar o emprego da Guerra Cibernética (G Ciber) nos conflitos: “São oferecidos comumente três incidentes internacionais como exemplos precursores de ataques virtuais como armas militares: o ataque à Estônia (2007), à Geórgia (2008) e ao Irã (2010)” (CARREIRO, 2012, p.11).

De acordo com o Manual de Campanha do Exército Brasileiro EB70-MC-10.232 - Guerra Cibernética, o Brasil, como nação soberana, necessita estar em condições de se contrapor às ameaças externas e complementa:

> “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)

Eventos de ataques cibernéticos aos sistemas do Exército Brasileiro indicam a existência de vulnerabilidades que ameaçam a segurança das informações, como pode ser observado na seguinte publicação de maio de 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). Dessa forma, a proteção adequada dos sistemas de comando e controle do Exército Brasileiro, na atualidade,

torna-se fundamental para manter a capacidade de defesa do país contra possíveis ameaças externas no futuro.

Em uma Força Terrestre Componente (FTC), a segurança da informação torna-se ainda mais relevante, pois a obtenção de dados pela força oponente, em um conflito, poderá influenciar sobremaneira no resultado das operações, como pode ser verificado na seguinte citação extraída do Manual de Campanha do Exército Brasileiro EB70-MC-10.225 – Força Terrestre Componente sobre a importância dos Sistemas de Comunicações e de Tecnologia da Informação (TI):

> "São fundamentais para a obtenção e a manutenção da superioridade de informações e da consciência situacional – fatores que conduzem ao sucesso das operações militares. A proteção desses sistemas deve ser uma preocupação constante, uma vez que elas se constituem em alvos compensadores para as ações do oponente e tendem a ser progressivamente degradadas no decorrer das operações." (BRASIL, 2019, p. 5-7)

Assim, o Exército Brasileiro possui, atualmente, o desafio de ampliar o grau de segurança das informações transitadas nos sistemas de comando e controle a fim de estar preparado para enfrentar as ameaças cibernéticas nos conflitos que porventura poderão surgir no futuro, conflitos estes cada vez mais dependentes da tecnologia da informação e comunicações, como pode ser observado pelo estudo prospectivo dos cenários de defesa para os anos de 2020 a 2039, realizado pelo Ministério da Defesa:

> "Com as operações militares centradas em redes e, como tal, dependentes de sistemas de comunicação e informação, haverá incremento da guerra cibernética. A necessidade de garantir o uso do domínio informacional e impedir que o oponente o faça (Superioridade da Informação) se incrementará. Ataques cibernéticos serão também utilizados contra infraestruturas nacionais – governamentais, econômicas e militares – que suportam o esforço de guerra." (BRASIL, 2017, p.21)

2. METODOLOGIA

Conforme a classificação de Vergara (2013), a pesquisa será qualitativa, quanto à abordagem; exploratória, quanto aos fins; bibliográfica e documental, quanto aos meios; e aplicada quanto à natureza. Qualitativa porque se pretende analisar os dados obtidos em documentos para identificar as principais ameaças aos Sistemas de Comando e Controle da Força Terrestre Componente e, com isso, buscar formas de mitigar os riscos de segurança, sem a necessidade de quantificar qualquer dado coletado. Exploratória porque as ameaças estão em constante evolução para cumprir sua finalidade de ataque aos sistemas computacionais e, por esse motivo, não há muito conhecimento produzido acerca das atuais ameaças, sendo as principais,

objetos dessa análise. Bibliográfica porque buscar-se-á em materiais já publicados, como livros, jornais e revistas, os principais conceitos acerca do emprego da proteção cibernética nos sistemas corporativos e como é possível mitigar os riscos proporcionados pelas ameaças. Documental porque serão utilizados os documentos do Exército Brasileiro para compreender o Sistema de Comando e Controle da Força Terrestre Componente. Por fim, a pesquisa será aplicada porque visa a resolução de problemas para ampliar a segurança dos postos de comando da Força Terrestre Componente, ante às ameaças cibernéticas.

Tendo em vista a metodologia a ser aplicada, a pesquisa tomará por base os aspectos qualitativos para a melhor compreensão dos riscos para o Sistema de Comando e Controle da Força Terrestre Componente e, com isso, buscar soluções para mitigá-los. Esses aspectos qualitativos limitam o desenvolvimento deste trabalho, em que serão abordados apenas os que forem considerados pelo autor os mais importantes para a atualidade. Assim sendo, a análise dos dados obtidos estará sujeita à interpretação pessoal deste oficial, o que poderá gerar dissidência com relação à outras interpretações ou mesmo à realidade.

A seguir, será analisado o emprego da proteção cibernética para ampliar a segurança dos postos de comando da Força Terrestre Componente, destacando as possíveis medidas de mitigação dos riscos nas futuras operações da Força Terrestre.

3. A ESTRUTURA CIBERNÉTICA NO EXÉRCITO BRASILEIRO

A evolução tecnológica proporcionou o advento dos computadores, os quais poderiam ser configurados de modo que se comunicassem entre si formando uma rede. De acordo com Lopes (2015), essa rede de computadores permitiu que recursos computacionais fossem partilhados entre máquinas distantes entre si geograficamente que, posteriormente, fez-se necessária uma melhor organização devido ao crescimento de usuários e o surgimento de novos recursos. Com um progressivo crescimento das redes de computadores, criou-se de forma espontânea, imprevisível e autorregulada a “rede das redes”, denominada de “internet”. Nessa rede, de domínio público, qualquer pessoa com um computador razoável que tivesse o *software* TCP/IP instalado poderia se conectar a um sítio sem qualquer tipo de regulação.

Por conseguinte, a internet evoluiu e passou a ser empregada em larga escala nos mais diversos setores da sociedade. Segundo Lins (2013), a internet proporcionava, em um primeiro período, aplicações de uso privado para troca de mensagens, murais eletrônicos e transferência de arquivos. Em um segundo período, caracterizado pela abertura da rede ao público, promovia o uso do "hipertexto, das páginas e dos sítios, em que as informações, predominantemente textuais, passaram a ser interligadas das formas mais variadas mediante os *hyperlinks*", surgindo nesse momento o conceito de navegação. O terceiro período, com o incremento da velocidade do tráfego de dados no acesso em banda larga, passou-se a utilizar as aplicações voltadas para o relacionamento interpessoal, permitindo o compartilhamento de conteúdo de imagem e áudio digital. No quarto e atual período, as possibilidades aumentaram consideravelmente, abrangendo as redes sociais, a computação em nuvem, a aplicação no setor financeiro, entre outras diversas utilidades.

Entretanto, o uso indiscriminado da internet possibilitou também o acesso não-consentido a outros computadores, pessoais ou corporativos, ou a outros equipamentos ligados em rede, como servidores e *switches*. Esses acessos indevidos caracterizaram os ataques cibernéticos que, de acordo com Carreiro (2012), tinham como objetivo a obtenção de dados para corrupção, a interrupção de sistemas de informação, danos a computadores, fraude, invasão, entre outros.

Em que pese alguns autores associarem o surgimento das redes de computadores à necessidade militar dos Estados Unidos da América (EUA), para garantir a integridade da rede norte-americana de comunicações frente a ameaça nuclear da União da Repúblicas Socialistas Soviéticas (URSS), durante a Guerra Fria (LOPES, 2015, p. 18), a sociedade internacional passou a interpretar as redes de computadores como um meio de obter vantagens em conflitos a partir de 2007, nos ataques cibernéticos à Estônia[1] (CARREIRO, 2012, p. 8), corroborando para um melhor entendimento do conceito de Guerra Cibernética. Devido sua grande relevância no cenário atual, esse conceito foi difundido rapidamente em escala global, passando a ser empregado na doutrina das Forças Armadas de diversos países, incluindo o Brasil.

[1] Sites governamentais e de empresas locais da Estônia foram tiradas do ar ou alteradas para exibir conteúdo diferentes dos originais – método de ataque conhecido por *defacement*. (CARREIRO,2012)

3.1 A GUERRA CIBERNÉTICA

“O ambiente cibernético pode ser considerado um novo domínio ou palco de batalha, depois da terra, do mar, do ar, do espaço exterior e do espectro eletromagnético” (SALDAN, 2011). Os conflitos da atualidade ampliaram o nível de complexidade, comparados aos do século passado, pois exigem uma gama de capacidades, as quais possuem grande relevância para o sucesso nos conflitos (GOMES; CORDEIRO; PINHEIRO; 2016). Dentre essas capacidades, estão as cibernéticas que têm destaque na dimensão informacional do ambiente operacional, baseada em uma rede interdependente de infraestruturas de Tecnologia da Informação e Comunicações (TIC) e dados (BRASIL, 2017).

Segundo Pinheiro (2008), o entendimento mais divulgado sobre o conceito de Guerra Cibernética é expresso da seguinte forma:

> “Guerra Cibernética corresponde ao uso ofensivo e defensivo de informações e sistemas de informação para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes computadorizadas.” (PINHEIRO, 2008 apud CAMPEN; DEARTH; GODDEN; 1996)

O Manual de Campanha EB70-MC-10.232 - Guerra Cibernética, do Exército Brasileiro, faz uma abordagem mais completa e mais apropriada desse conceito para as operações militares da Força Terrestre:

> “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)

3.1.1 A Guerra Cibernética no cenário internacional

Como visto anteriormente, a Guerra Cibernética se tornou mais relevante para a evolução dos conflitos a partir do ano de 2007, com o ataque cibernético à Estônia. Desde então, tornou-se uma tendência a nível mundial a utilização do meio cibernético

para se obter vantagens contra oponentes no campo de batalha, como na Guerra Russo-Georgiana[2], em 2008, e na Guerra do Irã[3], em 2010.

De acordo com Pinheiro (2008), os ataques cibernéticos provocaram o desenvolvimento das estruturas sistêmicas dos Estados Nacionais para proporcionar-lhes adequados níveis de Segurança da Informação.

> "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)

Portanto, a evolução no espaço cibernético estimulou a transformação das Forças Armadas de diversos países a fim de se obter as capacidades militares nessa área. Para uma melhor percepção sobre o cenário atual dessa transformação, serão apresentadas a seguir as perspectivas sobre o domínio cibernético dos seguintes países: EUA, China, Rússia e Coreia do Norte.

3.1.1.1 *Estados Unidos da América*

Durante a década de 1990, os Estados Unidos da América preocuparam-se em compreender o termo Guerra da Informação e sua influência para os planejamentos nos assuntos de defesa e política. Com isso, "os EUA e aliados procuraram explorar melhor essas infraestruturas de informação global em evolução, visando tecnologias com intuito militar" (SANTOS, 2018).

> "Assim, com o crescente destaque do espaço cibernético em assuntos de cunho estratégico, cada vez mais os Estados têm se empenhado na regulação do ciberespaço como um novo domínio estratégico. Dessa maneira, políticas e estratégias nacionais de países como Estados Unidos, França, Reino Unido e Alemanha servem como exemplos do uso de políticas referentes à defesa cibernética, já que com a era da informação, as redes e os dados cada vez mais ganharão espaço de destaque nas estratégias político-militares dos Estados" (SANTOS, 2018).

O rápido aumento de ataques cibernéticos contribuiu para que os EUA intensificassem a relevância da defesa no ciberespaço para os assuntos militares. Por

---

[2] Na Guerra Russo-Georgiana, em 2008, foram realizados ataques similares aos da Estônia, em 2007: *defacement* de sites oficiais, como do Parlamento Georgiano e Negação de Serviço (DDoS), tirando do ar sites do presidente e do Ministro do Exterior. Sites russos e da Ossétia do Sul também foram atingidos. (CARREIRO, 2012)

[3] Na Guerra do Irã, em 2010, foi elaborada uma ferramenta específica, o *worm* Stuxnet, que foi programado para atingir e danificar centrífugas nucleares iranianas por meio de pen drives contaminados. (CARREIRO, 2012)

conseguinte, os EUA passaram a considerar o ciberespaço como um domínio próprio para a guerra (SANTOS, 2018).

> “Com o intuito de facilitar as operações no ciberespaço, o Departamento de Defesa precisaria de uma estrutura organizacional adequada. Em relação à postura defensiva, seria importante que os EUA fossem dinâmicos e rápidos na resposta a ataques cibernéticos. Para isso, o Pentágono, por meio do seu Comando Cibernético (USCYBERCOM) implantou um sistema que mantém software de segurança e firewalls atualizados e uma linha de proteção de Inteligência que o governo fornece às defesas especializadas” (SANTOS, 2018).

Santos (2018) relata que a visão americana sobre o ciberespaço é a de que este é um domínio onde o combate acontece e que deve ser dominado. Para tanto, foi estabelecido na Estratégia Cibernética do Departamento de Defesa dos Estados Unidos (DoD), de abril de 2015, que o Departamento de Defesa seria responsável por defender os EUA de ataques cibernéticos, durante os períodos de paz, crise ou conflito, expondo pontos importantes para se atingir os objetivos daquela pasta de defesa. Dentre esses pontos, destacam-se:

> “(...) a criação de capacidades de segurança cibernética efetivas e a possibilidade de operações cibernéticas no intuito de defender redes. Além disso, é importante ressaltar a capacidade de defender o país contra ataques cibernéticos e também fornecer suporte a planos operacionais” (SANTOS, 2018).

Assim, o governo dos EUA tem envidado esforços para a defesa da nação contra ameaças cibernéticas, sendo o Comando Cibernético dos EUA (USCYBERCOM) o elemento central do processo para elevar o nível de proteção das redes governamentais e militares, orientando como o serviço militar deve treinar, equipar e comandar suas forças para a missão cibernética (LYNN III, 2010).

> “Devido à atitude progressista da Força Aérea norte-americana em aspirar ao papel de liderança no ciberespaço, em 23 de junho de 2009, o Departamento de Defesa dos Estados Unidos estabeleceu um comando subunificado [subordinado ao Comando Estratégico dos EUA – USSTRATCOM], o USCYBERCOM, localizado em Forte Mead, no Estado americano de Maryland. O quartel-general coordena esforços no DoD de combater ameaças e garantir liberdades no espaço cibernético.” (SANTOS, 2018)

No tocante à missão do USCYBERCOM, o Departamento de Defesa dos EUA estabelece que esse Comando:

> “planeja, coordena, integra, sincroniza e conduz atividades para: direcionar as operações e a defesa de determinadas redes de informação do Departamento de Defesa; prepara-se, quando dirigido, para conduzir operações espaciais no ciberespaço em todo o espectro para permitir ações em todos os domínios, garantir a liberdade de ação dos EUA/aliados no ciberespaço e negar o mesmo aos adversários” (DEPARTMENT OF DEFENSE, 2010, tradução nossa).

Segundo Santos (2018), em outubro de 2016, as autoridades do USCYBERCOM intensificaram suas atividades com a Força de Missão Cibernética do Comando dos EUA (CMF).

> “As Forças de Missão Cibernética do USCYBERCOM se alinham com a estratégia do Departamento de Defesa. Ainda, os grupos da Força da Missão Cibernética são responsáveis por dar suporte às operações do Departamento e possuem suas próprias atribuições. As equipes que formam a Força Nacional de Missão Cibernética são responsáveis pela defesa da nação em uma atividade adversária. As equipes das Forças de Combate da Missão Cibernética têm o papel de conduzir operações cibernéticas militares em apoio aos comandos combatentes. Já as equipes da Força de Proteção Cibernética defendem as redes de informação e preparam as forças cibernéticas para o combate. Também fazendo parte dos grupos da Força de Missão Cibernética, as equipes de Suporte Cibernético fornecem apoio extensivo e de idealização às equipes da Missão Nacional e da Missão de Combatente” (SANTOS, 2018)

Para apoiar o USCYBERCOM nas operações de guerra cibernética, os EUA criaram os Comandos Cibernéticos das Forças Singulares, sendo elas: o Comando Cibernético da Força Aérea (AFCYBER); o Comando Cibernético da Marinha e das Forças dos Fuzileiros Navais dos EUA (MARFORCYBER); e o Comando Cibernético do Exército (ARCYBER) (SANTOS, 2018).

O Comando Cibernético do Exército dos EUA tem fundamental importância para o combate terrestre nas missões norte-americana da atualidade, frente às ameaças de seus oponentes, de forma a lhes permitir uma maior agilidade de tomada de decisão em um esforço conjunto (SANTOS, 2018).

> “O Comando Cibernético do Exército (ARCYBER), estabelecido em 1 de outubro de 2010, é a linha de frente de defesa contra hackers, violação de dados e invasões de rede. O Comando também é responsável por manter e desenvolver superioridade tecnológica em meio a mudanças de ameaças em que o ciberespaço e a tecnologia podem apresentar-se” (SANTOS, 2018).

O ARCYBER combate as ameaças cibernéticas globais, defende as redes militares, protege as plataformas de armas do Exército e colabora na proteção da infraestrutura crítica norte-americana (ARCYBER, 2019). Com isso, a missão do ARCYBER é definida da seguinte forma:

> “O Comando Cibernético do Exército é responsável por manter agressivamente a segurança do ciberespaço e conduzir operações integradas de guerra eletrônica, informação e ciberespaço, garantindo a liberdade de ação através do ciberespaço e do ambiente de informações.” (ARCYBER, 2019, tradução nossa).

Portanto, o governo norte-americano tem verificado, na última década, um aumento das ameaças cibernéticas em todo o mundo, identificando adversários estatais e não-estatais dos EUA e de seus aliados. Estas ameaças exigem do Comando de Defesa Cibernética e das Forças Armadas um contínuo desenvolvimento

de capacidades cibernéticas com a finalidade de garantir seus interesses (SANTOS, 2018).

3.1.1.2 *República Popular da China*

A República Popular da China (RPC) tem desenvolvido capacidades no ciberespaço com foco na coleta de informações e nas ações que provoquem danos nas infraestruturas dos seus adversários, causando-lhes prejuízos econômicos. (SANTOS, 2018).

> "A China está interessada em assuntos relacionados a guerra cibernética porque pode ampliar seu poder nacional, ou seja, o que pode ser entendido por Washington como uma ameaça para os Estados Unidos. Em *reports* recentes do Congresso americano a respeito do poderio da China, o Pentágono nota uma expansão de capacidades no domínio cibernético, o que desperta a procura de um melhor entendimento na estratégia de guerra cibernética chinesa" (SANTOS, 2018)

A transformação das Forças Armadas da RPC, para a obtenção das capacidades cibernéticas, se deu início a partir da Guerra do Golfo, com o objetivo de fomentar a dominância chinesa na Ásia, assim como sua crescente influência a nível global (SANTOS, 2008).

> "É evidenciado que os estrategistas chineses adotaram a RMA [Revolução nos Assuntos Militares], e acreditavam que o futuro da guerra seria paulatinamente dependente da negação ou degradação do fluxo de informações do adversário. Os efeitos dessa decisão após uma década são bastante expressivos, e suas capacidades de atuar no ciberespaço foram ampliadas devido ao rápido crescimento econômico. Ademais, as capacidades cibernéticas chinesas tiveram crescimentos expressivos na promoção de defesa em redes de ataque e operações ofensivas contra adversários, como foi evidenciado por Richard Lawless, um subsecretário Adjunto de Defesa para Ásia e Pacífico em 2007" (SANTOS, 2018).

Diante da sua ampliação da capacidade ofensiva no domínio cibernético, a China adotou medidas para se preparar contra os ataques de adversários que tentassem impedir seu avanço. Essas medidas foram: a) criação de um grupo de cidadãos *hackers*; b) espionagem cibernética, incluindo software e hardware de computadores dos EUA; c) elaboração de medidas necessárias para defender seu próprio ciberespaço; d) criação de unidades militares de guerra cibernética; e e) realização de um cerco à infraestrutura dos EUA com bombas-lógicas (SANTOS, 2018).

> "De acordo o *report* Anual do Congresso norte-americano, *Military and Security Developments Involving the People's Republic of China* do ano de 2017, sobre as capacidades cibernéticas, é apresentado que nos anos recentes o Exército Popular de Libertação tem enfatizado uma maior importância no espaço cibernético como um novo domínio de segurança

> nacional e de área como competição estratégica. Com base no que foi apresentado pelo *white paper* da China de 2015, o país identificou o ciberespaço como um dos quatro 'domínios críticos de segurança', ao lado dos [sic] marítimo, espacial e nuclear. Desta maneira, o Exército continua a desenvolver pesquisas a respeito do ciberespaço e de como podem explorar novas formas estratégicas no mesmo. Com o estabelecimento da Força de Suporte Estratégica, uma organização que foi estabelecida em 2015 e responsável por unir capacidades espaciais o espaço, cibernéticas e eletrônicas, pode ter representado um primeiro passo no desenvolvimento de forças cibernéticas e criar eficiências capazes para realizar os ataques e defesa da organização" (SANTOS, 2018).

Santos (2018), refere-se à obtenção das capacidades cibernéticas pelo Exército Popular de Libertação como uma crescente, tendo em vista a importância dada pela RPC ao assunto com base no cenário atual.

> "A China continua a desenvolver capacidades de dissuadir, deter e anular possíveis intervenções. Acerca das operações de informações são tidas como um elemento fundamental para controlar habilidades no moderno espectro de batalha. Os autores do Exército citam essa capacidade como uma "informação de bloqueio ou 'domínio da informação' como sendo um fator fundamental para definição de condições necessárias e conseguir a superioridade no ar e mar e terra também. O conceito de 'bloqueio de informação' se faz presente através do emprego do militar e não militares instrumentos do poder de estado no campo de batalha, e que estão inclusos o ciberespaço e o espaço" (SANTOS, 2018)

3.1.1.3 *Rússia*

Após a extinção da URSS, em 1991, a Rússia enfrentou um período pelo qual sua capacidade de desenvolvimento científico, principalmente no campo de computadores pessoais e redes de computadores, era quase inexistente. Entretanto, a Rússia passou por um amplo processo de revolução da informação proporcionando um aumento considerável de cidadãos russos com acesso à internet (SANTOS, 2018).

O Estado russo verificou a importância dos sistemas de informação, a partir da última década do século XX, com o desenvolvimento da internet e a origem de novas tecnologias de comunicação (SANTOS, 2018).

> "Em 2000, foi adotada a Doutrina Militar da Federação Russa que simbolizou pela primeira vez que a segurança computadorizada necessitava de novos instrumentos e estratégias. Diferentemente das estratégias que eram adotadas pelas nações ocidentais, para os quais o ciberespaço era o contexto principal em considerar novos sistemas informatizados de combate e defesa. Desde o princípio os russos reconheceram a necessidade de suas forças armadas de operarem no 'espaço de informação', como também reconheciam as ameaças enfrentadas pelo exército russo.
> Adotada em setembro de 2000, a Doutrina de Segurança da informação da Federação Russa, que ainda está vigorando atualmente, ressalta a importância da dimensão militar na questão da informação. Desse modo, a segurança de informação é vista como um fundamento para a segurança do Estado, pois é possível identificar as 'armas de informação' como instrumentos que possibilitam conseguir objetivos políticos" (SANTOS, 2018).

Com base na Doutrina de Segurança da Informação da Federação Russa, verificou-se a necessidade do desenvolvimento de uma política militar de informação e contenção estratégica de conflitos no espaço da informação, em virtude da previsão da realização de tarefas específicas por parte do departamento de defesa no espaço de informação, da execução de tarefas de longo prazo para manter a monitoração das ameaças e o desenvolvimento das capacidades para combatê-las (SANTOS, 2018).

Assim, a Rússia reconhece o ciberespaço como um novo campo estratégico militar, mas com o exército russo desempenhando um papel além do contexto militar, isto é, atuando em outras expressões do poder nacional, de forma que as ações cibernéticas externas são vistas como ameaças sociais, políticas e civilizacionais do ocidente, inseridas no conceito do “espaço de informação” (SANTOS, 2018).

> “Cada vez mais a Rússia em níveis operacionais tentará desenvolver instrumentos que possibilitem alcançar seus objetivos, incluindo medidas que visem ampliar o poder cibernético, defesa cibernética e capacidades ofensivas. Desse modo, será necessário que envolva uma maior coordenação de atividades entre vários atores na realização das mais variadas tarefas em nível operacional” (SANTOS, 2018)

3.1.1.4 *Coreia do Norte*

Apesar de ser o país com a menor presença na internet do mundo, a República Popular Democrática da Coreia (RPDC), nome oficial da Coreia do Norte, é o governo que representa a 4ª maior ameaça para a potência hegemônica (EUA), atrás somente da China, Rússia e Irã, nessa ordem (SANTOS, 2018).

Nesse contexto, a Coreia do Norte vem desenvolvendo suas capacidades cibernéticas, aplicando recursos significativos no setor, a fim de buscar uma vantagem decisiva na península coreana sem adotar ações militares convencionais. Essa medida é uma das alternativas utilizadas pelo governo da RPDC para causar danos ou prejuízos aos seus oponentes a um baixo custo, criando dificuldades para uma retaliação, vistos os empecilhos para se confirmar um ataque cibernético como uma ação militar norte-coreana (JUN; LAFOY; SOHN; 2015).

> “De acordo com o relatório intitulado de Serviço de Pesquisa do Congresso de 2015, no que tange a organização de operações cibernéticas norte-coreanas, é exposto que o regime de Kim são [sic] sediadas no Bureau Geral de Reconhecimento, mais especificamente o Bureau 121. O Bureau serve como uma espécie de central para que as operações clandestinas da Coreia do Norte. Diante disso, o Exército Popular da Coreia tem como finalidade planejar as unidades cibernéticas e podem coordenar conjuntamente com Bureau. A Força Cibernética da Coreia do Norte foi estimada entre 3000 e 6000 hackers treinados em operações cibernéticas, sendo que a maiorias

> desses guerreiros pertencem ao Bureau e o staff do Exército Popular norte-coreano (SANTOS, 2018)".

"A unidade cibernética mais importante é a Boreau 121, e sua gama de serviços incluem operações cibernéticas ofensivas e defensivas, espionagem cibernética, exploração de redes entre outros" (SANTOS, 2018).

Dessa forma, deve-se levar em consideração o desenvolvimento de capacidades cibernéticas pela Coreia do Norte, com objetivos na expressão militar contra seus oponentes, evidenciando, assim, a relevância dessas capacidades no preparo e no emprego das forças militares em todo o mundo na atualidade.

3.1.2 A Guerra Cibernética no Brasil

> "O número de ataques cibernéticos tem crescido no Brasil desde 2001, tendo como alvos bancos, agências governamentais, organismos internacionais, e partidos políticos. Devido à fragilidade na defesa deste espaço nacional, o país também tem sido alvo de espionagem de modo recorrente (...)." (LIMA, 2018)

Os ataques ou tentativas de intrusões de diversos lugares do mundo contra os sistemas brasileiros corroboraram para uma maior atenção ao tema, fazendo-se necessária a implantação de estruturas e estratégias de defesa e segurança cibernética (GOMES; CORDEIRO; PINHEIRO; 2016).

Com isso, o Brasil incluiu na Estratégia Nacional de Defesa de 2008 o setor cibernético, destacando-o como um dos setores de importância estratégica para a defesa do país, após passados sete anos do primeiro ataque cibernético (LIMA, 2018).

Tal medida não dissuadiu os atacantes, ao contrário, as ações cibernéticas contra os sistemas do Estado brasileiro aumentaram em número e em complexidade.

> "Em junho de 2011, diversos portais governamentais brasileiros, como o da Presidência da República, da Receita Federal e da Petrobras, foram alvos de ataques cibernéticos assumidos pelo grupo Lulz Security Brazil. Segundo o próprio grupo divulgou no Twitter, este ataque teria sido um protesto contra a corrupção e o aumento dos combustíveis. No mesmo período, o grupo Fatal Error Crew, que já havia atacado o portal da Presidência em janeiro de 2011, divulgou o endereço de 500 portais de prefeituras e câmaras municipais atacadas.
>
> Diante de tais fatos e de medidas práticas adotadas pelo governo brasileiro, novas políticas e documentos têm sido criados e aprovados, com vistas a definir uma política cibernética para o país: a Estratégia Nacional de Defesa, o Livro Verde sobre Segurança Cibernética no Brasil e a recente Política Cibernética de Defesa." (GOMES; CORDEIRO; PINHEIRO; 2016)

Por conseguinte, o Ministério da Defesa (MD) aprovou a Doutrina Militar de Defesa Cibernética, com a finalidade de proporcionar uma "unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a

atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético" (BRASIL, 2014).

> "Com a publicação dos referidos documentos, adveio o estabelecimento do objetivo de criar um Sistema Militar para Defesa Cibernética, a introdução de defesa cibernética em exercícios das juntas militares e simulações de combate. 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)

De acordo com Lima (2018), o Simulador Nacional de Operações Cibernéticas (SIMOC) passou a ser operado no Centro de Instruções de Guerra Eletrônica (CIGE), em Brasília-DF, para a capacitação de militares na área em prol da defesa do Brasil. Em 2014, o Estado-Maior do Exército criou o Centro de Defesa Cibernética (CDCiber) e organizou as funções para os órgãos do setor cibernético:

ÓRGÃO	LOCAL	FUNÇÃO
CDCiber	Brasília-DF	Organização do Centro de Defesa Cibernética
		Arcabouço documental
		Gestão de pessoal
CITEx	Brasília-DF	Planejamento e execução da Segurança Cibernética
CDS	Brasília-DF	Estrutura de apoio tecnológico e desenvolvimento de sistemas
IME	Rio de Janeiro-RJ	Estrutura de pesquisa científica na área cibernética
CCOMGEx	Brasília-DF	Estrutura de Capacitação e de preparo e emprego operacional (Força Cibernética)
CIE	Brasília-DF	Estrutura para produção do conhecimento oriundo da fonte cibernética
RENASIC	Brasília-DF	Rede Nacional de Segurança da Informação e Criptografia

QUADRO 1 – Funções atribuídas aos órgãos do setor cibernético do Brasil.

Fonte: Elaboração própria, segundo Lima (2018).

Como forma de integrar as ações das Forças Armadas, foi criado o Comando de Defesa Cibernética (ComDCiber), em 2016, sendo caracterizado como o Comando Conjunto de Defesa Cibernética na estrutura regimental do Exército Brasileiro. A missão destinada ao ComDCiber é:

> "planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética [SMDC], sendo seu órgão central, com o objetivo de assegurar o uso efetivo do espaço cibernético pelas Forças Armadas brasileiras e impedir ou dificultar sua utilização contra interesses da Defesa Nacional." (BRASIL, 2016)

Nesse contexto, o Sistema Militar de Defesa Cibernética (SMDC) foi concebido de forma a designar as atribuições para os Órgãos de estado e de governo vinculados

à defesa nos diversos níveis de decisão, descrito a seguir no quadro 2 e representado na figura 1.

NÍVEL	ATRIBUIÇÕES
Nível Político	Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, coordenadas pela Presidência da República (PR) e abrangendo a Administração Pública Federal (APF) direta e indireta, bem como as infraestruturas críticas da informação dos setores público e privado.
Nível Estratégico	Defesa Cibernética, a cargo do Ministério da Defesa, interagindo com a PR e APF.
Níveis operacional e tático	Guerra Cibernética, denominação restrita ao âmbito interno das Forças Armadas.

QUADRO 2 – Atribuições segundo os níveis de decisão.

Fonte: Cerávolo; Ferreira Neto (2015, p. 82).

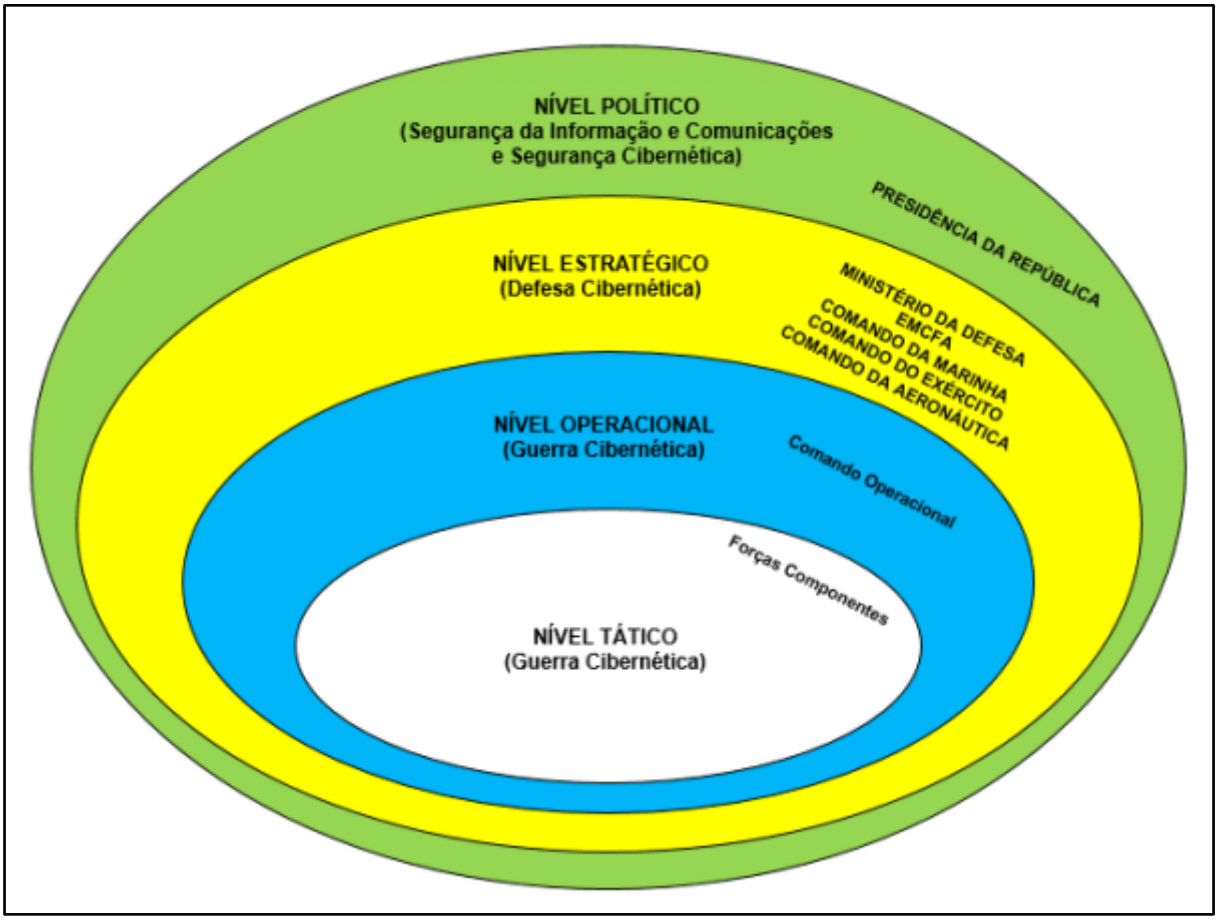


FIGURA 1 – Níveis de decisão.

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

No nível tático, o SMDC contempla o Sistema de Guerra Cibernética do Exército (SGCEx), conceituado como:

> "um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de guerra cibernética, assegurando o seu uso efetivo pelo Exército Brasileiro,

> bem como impedindo ou dificultando a utilização do espaço cibernético pelo oponente.” (BRASIL, 2017)

O SGCEx tem como objetivo a proteção cibernética do Sistema de Comando e Controle do Exército, de forma a assegurar a capacidade de atuar em rede com segurança, assim como a coordenar e a integrar a proteção das infraestruturas críticas da informação sob responsabilidade do Exército (BRASIL, 2017).

Dessa forma, a capacidade militar terrestre cibernética do Exército Brasileiro foi desenvolvida no SGCEx com base em um conjunto de sete fatores determinantes, interrelacionados e indissociáveis, denominados por DOAMEPI: doutrina, organização (e processos), adestramento, material (e sistemas), educação, pessoa e infraestrutura (BRASIL, 2017). Tal capacidade é composta por três capacidades operativas (CO): a proteção cibernética, o ataque cibernético e a exploração cibernética, descritas no quadro 3.

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

QUADRO 3 – Capacidades do SGCEx.

Fonte: Brasil (2017, p. 3-4).

3.2 A CAPACIDADE OPERATIVA DE PROTEÇÃO CIBERNÉTICA

A proteção cibernética é uma capacidade operativa da Guerra Cibernética que “Visa neutralizar o ataque e a exploração cibernética oponentes contra os dispositivos computacionais, as redes de computadores e de comunicações amigos” (BRASIL, 2017, p. 4-3). Ainda, “no âmbito do Exército Brasileiro, a proteção cibernética tem o

propósito de proteger as redes do Sistema de Comando e Controle do Exército (SC2Ex) [sic]" (BRASIL, 2017, p. 4-3).

As ações de proteção cibernética "incluem a detecção, a identificação e a resposta a ações que foram realizadas ou que estão prestes a serem conduzidas pelo oponente" (BRASIL, 2017, p. 4-3). Essas ações são executadas a partir da realização de determinadas tarefas que, segundo Gomes e colab. (2016), proporcionam maior grau de proteção cibernética ao sistema de comando e controle desdobrado em apoio à determinada operação militar. Gomes e colab. (2016) ainda reforça que "O emprego de todas as ferramentas e procedimentos de segurança disponíveis, somado a uma boa auditoria, são a mistura certa para a eficiência do trabalho do administrador de redes de C2".

Assim, de acordo com Brasil (2017, p. 3-4), uma força ou organização militar deve possuir a capacidade de cumprir sua missão ou tarefa, sendo, nesse caso específico, a aptidão requerida para empregar a proteção cibernética.

O Manual de Campanha do Exército Brasileiro EB70-MC-10.232 – Guerra Cibernética descreve as tarefas e ações da atividade de proteção cibernética, no contexto da Guerra Cibernética, conforme o quadro 4.

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 4 – Atividades e Tarefas de Guerra Cibernética (Proteção Cibernética).

Fonte: Brasil (2017, p. 4-4).

Algumas atividades das funções de combate têm seus efeitos potencializados com o apoio da Guerra Cibernética, sobretudo na execução da atividade de proteção cibernética (BRASIL, 2017, p 4-5). Dentre as atividades que se correlacionam com a atividade de proteção cibernética, destacam-se como as principais:

Função de Combate	Ações correlacionadas à Proteção Cibernética
Movimento e Manobra	- Garantir a segurança das redes de comando e controle e infraestruturas de TIC para apoiar o movimento e a manobra, propiciando a sincronização das ações cinéticas, proporcionando ao comandante a

Função de Combate	Ações correlacionadas à Proteção Cibernética
	segurança, a liberdade de ação na operação e importantes vantagens no espaço de batalha.
Proteção	a) Manter a disponibilidade, integridade, confiabilidade e autenticidade das informações que trafegam ou que são armazenadas nos sistemas de informação. b) Buscar a garantia da segurança e do funcionamento das infraestruturas críticas nacionais localizadas no interior da área de operações da FTC.

QUADRO 5 – Atividades das Funções de Combate correlacionadas à Proteção Cibernética.

Fonte: Elaboração própria, segundo Brasil (2017).

"As ações cibernéticas são aplicáveis no amplo espectro dos conflitos. Normalmente a G Ciber participa das combinações simultâneas de atitudes realizadas pela FTC" (BRASIL, 2017). Nesse contexto, a Proteção Cibernética é importante na garantia do perfeito funcionamento dos sistemas e das estruturas críticas de informação e comunicações e na salvaguarda de bancos de dados estratégicos (BRASIL, 2017).

Nas operações ofensivas,

> "as ações de proteção cibernética têm caráter permanente em todas as fases da operação. A proteção cibernética dos sistemas de informação é essencial para o seu eficaz exercício durante o ataque. Redundâncias e outros mecanismos contra falhas de segurança dos sistemas de informação devem proporcionar a continuidade da missão." (BRASIL, 2017, p. 5-3)

Nas operações defensivas, a manutenção das ações de proteção cibernética em relação aos sistemas de informação costuma ser crítica. Entretanto, a proteção cibernética deve prevalecer entre as demais ações de Guerra Cibernética, pois em uma defesa móvel são características: o intenso fluxo de informações; a rapidez na tomada de decisões e na difusão de ordens; e a coordenação de todas as funções de combate em tempo e espaço (BRASIL, 2017, p. 5-3).

As Operações de Cooperação e Coordenação com Agências (OCCA) também exigem maior ênfase nas ações de proteção cibernética, em que as ligações com as agências devem ser mantidas pelo ComDCiber e pelos órgãos regionais encarregados pela proteção e operação dos sistemas corporativos, como o Centro de Telemática do Exército (CITEx), os Centros de Telemática de Área (CTA) e os Centros de Telemática (CT) (BRASIL, 2017, p. 5-4).

3.3 AS PRINCIPAIS AMEAÇAS CIBERNÉTICAS DA ATUALIDADE

Nos últimos anos, houve um aumento da dependência de sistemas baseados em rede e da internet, ampliada com o evento da pandemia causada pelo COVID-19. Essa realidade criou um ambiente favorável para o crescimento do número de ataques cibernéticos em âmbito mundial (BLACKBERRY, 2021).

Ao mesmo tempo em que os grupos de ameaças mercenários atuaram com o objetivo de obter vantagens financeiras, agentes e organizações estatais e não-estatais terceirizavam seus ataques cibernéticos com a finalidade de causar danos aos seus oponentes (BLACKBERRY, 2021).

Nesse cenário, torna-se relevante a identificação das principais ameaças da atualidade para que as estruturas de Guerra Cibernética voltadas para a atividade de proteção estejam preparadas para a adoção das medidas mais adequadas, de forma a evitar ou minimizar os possíveis danos aos sistemas operados pela Força Terrestre.

O Relatório de Ameaças BlackBerry de 2021 examinou os maiores eventos de cibersegurança de 2020 e identificou o aprimoramento das ferramentas de ataque, sendo os mais relevantes para essa pesquisa a utilização de *kits* de *exploits* prontos, *softwares* de emulação de ameaças como o *Cobalt Strike*, utilitários *AdFind* e *SharpHound* e campanhas de *malspam* e *phishing*.

Os *kits* de *exploits*, segundo BlackBerry (2021), funcionam como um vetor automático de infecção, utilizados desde 2006. Ainda complementa:

> “São usados primariamente para distribuir malware padronizado, explorando sistemas sem patches/vulneráveis para acionar um download drive-by. Em termos simples, os KEs [Kits de Exploits] tentam detectar uma vulnerabilidade em um aplicativo relacionado a um navegador e depois explorá-la para baixar e executar um payload malicioso. Os payloads por download podem ser kits de exploit ou as campanhas que os alavancam.
> Os kits de exploit também continuam a avançar em termos de complexidade e cobertura de vulnerabilidades, conforme mostrado pelo kit de exploit Purple Fox. As atualizações recentes do Purple Fox incluíram CVEs e capacidades de rootkit usadas para evitar detecção e dificultar análises.” (BLACKBERRY, 2021)

“O Cobalt Strike é um software de emulação de ameaças com recursos e suportes completos, que ainda está em desenvolvimento ativo” (BLACKBERRY, 2021). Por meio desse *software* os atacantes realizam acesso remoto aos dispositivos ligados em rede e, atualmente, ainda é uma das ferramentas mais comuns de teste de penetração, segundo BlackBerry (2021).

O utilitário de linha de comando *AdFind* é empregado para enumerar informações como computadores no domínio, objetos de confiança, usuários em que uma senha não é necessária e outras informações potencialmente úteis, de acordo com BlackBerry (2021). “Os agentes de ameaças usam o Adfind para obter informações para sondar adicionalmente ou se mover lateralmente em um ambiente infectado” (BLACKBERRY, 2021). Outro utilitário de enumeração é o *SharpHound*, utilizados para mapear relacionamentos não vistos em um domínio, permitindo ao atacante encontrar o caminho mais curto, e às vezes mais fácil, para obter os privilégios de administrador de domínio em um ambiente de rede (BLACKBERRY, 2021).

O *Malspam* é um programa malicioso, também conhecido como vírus ou *malware*, que é entregue por e-mail.

> “As campanhas de malspam variam desde usar alvos abrangentes e indiscriminados até empreendimentos altamente específicos e sofisticados, com foco em uma ou duas pessoas importantes. Considerando a popularidade avassaladora do e-mail, o malspam continua a ser um risco”. (BLACKBERRY, 2021)

O Relatório de Ameaças BlackBerry de 2021 também identificou um incremento dos ataques contra infraestrutura crítica a partir de diversas campanhas de *phishing*. Essas campanhas são realizadas pela adoção de técnica de engenharia social utilizada para enganar usuários por meio de mensagens aparentemente reais e obter credenciais para acesso aos sistemas. Durante a pandemia do coronavírus, em 2020, campanhas de *phishing* foram executadas visando a consecução de objetivos estratégicos de países, relacionados à pesquisa, ao desenvolvimento e ao transporte de vacinas contra a COVID-19:

> “Outra ameaça à infraestrutura crítica relacionada à pandemia são ataques contra organizações que desenvolvem vacinas contra a COVID-19. As campanhas começaram já em abril de 2020 e são bem diferentes dos incidentes de ransomware com motivação financeira. Esses ataques têm foco em espionagem e exfiltração de dados e acredita-se que sejam patrocinados primariamente por estados-nação. Em julho de 2020, o National Cyber Security Centre do Reino Unido advertiu sobre campanhas de phishing em grande escala atribuídas à APT29 (também chamada de CozyBear), cujos alvos eram instalações de pesquisa sobre COVID-19. Depois que as credenciais foram obtidas, os adversários usaram malwares WellMess e WellMail para furtar dados.
> De acordo com a IBM, outra campanha, voltada para uma rede de transporte de vacinas, começou em setembro. Envolvia e-mails de phishing direcionados com precisão para organizações de transporte na tentativa de furtar informações relacionadas a compra e planejamento de movimentação da vacina. A AstraZeneca, desenvolvedora de uma das principais vacinas potenciais, foi alvo em novembro de atacantes, supostamente da Coreia do

> Norte. Os adversários, disfarçados como recrutadores, estavam enviando documentos maliciosos disfarçados como descrições de cargos" (BLACKBERRY, 2021)

O relatório apontou também que os EUA acusaram agentes do serviço secreto russo de realizar ataques cibernéticos com alta visibilidade que incluíam: ataques à rede elétrica da Ucrânia, comprometimento de sistemas para os Jogos Olímpicos de Inverno de 2018 e interferência (esforços de *hack-and-leak*) nas eleições francesas de 2017 (BLACKBERRY, 2021). Ainda, o consultor de segurança nacional norte-americano acusou a China de interferência no período anterior à eleição presidencial dos EUA em 2020.

Fruto dos fatos indicados no Relatório de Ameaças BlackBerry 2021 e outras fontes pesquisadas, este autor alerta para uma melhor preparação e planejamento das operações da Força Terrestre do Brasil para se obter o êxito na prevenção de ameaças cibernéticas. Ante o desenvolvimento de novas técnicas e ferramentas de ataque, é necessário contínuo monitoramento do cenário e o entendimento sobre os impactos dos eventos atuais em todo o mundo.

3.4 CONCLUSÕES PARCIAIS SOBRE A ESTRUTURA CIBERNÉTICA NO EXÉRCITO BRASILEIRO

A atividade de Proteção Cibernética torna-se cada vez mais complexa com o passar tempo, pois o surgimento de novas tecnologias, a utilização de novos dispositivos e outras inovações aumentam os desafios para a garantia da segurança dos sistemas operados em rede.

De forma parcial, pode-se concluir que a Proteção Cibernética é fundamental para a segurança das informações nos conflitos da atualidade. Sua relevância tem alcance global e a atualização e o desenvolvimento da doutrina militar brasileira com capacidades cibernéticas compatíveis às doutrinas das potências militares internacional é imprescindível.

As ameaças cibernéticas estão em constante evolução e seus objetivos visam provocar distúrbios e prejuízos de toda ordem a fim de se obter vantagens diversas, dentre essas, as militares.

Os estudos sobre as ameaças permitiram identificar a intensificação de ataques que se aproveitam das vulnerabilidades existentes com foco na falha de

procedimentos na operação de dispositivos ligados em rede, como o *malspam*, e outros que são voltados para as deficiências existentes nos sistemas operacionais, programas e *softwares* instalados, como os *kits* de *exploits*. Nesse sentido, ressalta-se a importância do aperfeiçoamento do emprego da proteção cibernética para a melhor consecução dos objetivos da Força Terrestre no cumprimento de suas missões nas operações.

4. O SISTEMA DE COMANDO E CONTROLE DA FORÇA TERRESTRE COMPONENTE

4.1 A FORÇA TERRESTRE COMPONENTE

> "Força Terrestre Componente (FTC) – é o componente terrestre adjudicado ao Comando Operacional do Teatro de Operações/Área de Operações. Os escalões da F Ter a quem se pode atribuir a condição de FTC são: o Corpo de Exército, a Divisão de Exército e a Brigada;" (BRASIL, 2019)

O conceito de Força Terrestre Componente do Manual de Campanha EB70-MC10.225 Força Terrestre Componente é apropriado à atual realidade dos conflitos, em que as ameaças de um mundo volátil, incerto, complexo e ambíguo (VUCA – *volatility*, *uncertainty*, *complexity and ambiguity*) "exigem que o preparo das Forças Armadas seja baseado em capacidades conjuntas" (BRASIL, 2019).

O Manual complementa esse conceito da seguinte forma:

> "A concepção de emprego das Forças Armadas tem como um fundamento básico a ação conjunta de forças navais, terrestres e aéreas. As diferentes forças agregam capacidades específicas às ações no amplo espectro do conflito, propiciando ao conjunto um rendimento maior do que a soma do rendimento de suas partes, caso atuassem sem o necessário comando unificado.
> As operações conjuntas exigem das forças singulares a adoção de estruturas flexíveis, adaptáveis, modulares, elásticas e sustentáveis, que rapidamente possam ser integradas às demais forças. A FTC deve integrar e sincronizar os meios da Força Terrestre ao esforço conjunto, contribuindo para o sucesso das operações, visando à eficácia sem, entretanto, negligenciar a doutrina e as especificidades do Exército Brasileiro." (BRASIL, 2019)

Desta forma, verifica-se a evolução das Forças Armadas Brasileira em consonância com as reais necessidades ligadas à defesa da Pátria, à garantia dos poderes constitucionais e da lei e da ordem, conforme prevê a Constituição Federal de 1988. A fim de acompanhar essa evolução, a Força Terrestre, representada pelo escalão designado como FTC como parte integrante de operações conjuntas no emprego das Forças Armadas, vivencia um período de transformação pelo qual tem

ampliado suas capacidades militares para enfrentar os desafios do presente e do futuro.

Ainda segundo O Manual de Campanha EB70-MC10.225 Força Terrestre Componente, o processo de emprego da FTC é flexível, isto é, constituído como um escalão da F Ter para se ajustar às peculiaridades de cada situação. Para um melhor exercício de comando e controle, é essencial a organização do Estado-Maior, pois permitirá coordenar, sincronizar e compartilhar informações entre seus integrantes. Tal organização é efetivado pela composição de células do Centro de Coordenação de Operações (CC Op) e as seções do Estado-Maior.

As células do CC Op são “um conjunto de pessoal e equipamento organizado por função de combate ou por horizonte temporal de planejamento, de forma a facilitar o exercício do C²” (BRASIL, 2019). Assim, é possível definir como Células Funcionais aquelas que reúnem pessoal e equipamento por funções de combate e como Células de Integração aquelas que grupam pessoal e equipamento por horizonte temporal de planejamento.

As seções do Estado-Maior compõem as Células Funcionais e de Integração, de forma que militares com formações e especializações diferentes executem suas tarefas em conjunto em cada célula, facilitando a coordenação e o sincronismo entre elas. As Células Funcionais são divididas nas seguintes funções de combate: Comando e Controle, Inteligência, Movimento e Manobra, Fogos, Proteção e Logística (BRASIL, 2019).

4.1.1 A Função de Combate Comando e Controle na FTC

A Célula Funcional responsável por coordenar e sincronizar forças e atividades da Função de Combate Comando e Controle é a Célula de Comando e Controle. Essa célula normalmente é constituída, pela Seção de C², Seção de Comunicação Social, Seção de Assuntos Civis, Seção de Operações de Informação do Estado-Maior da FTC, pelo Elemento de Guerra Eletrônica e por elementos de Operações Cibernéticas e de Geoinformação (BRASIL, 2019).

A Função de Combate Comando e Controle integra todo o processo de emprego da FTC em operações, tendo em vista que o Cmt, como elemento central desse processo, e o Estado-Maior da FTC direcionam e coordenam as tarefas incluídas em todas as Funções de Combate (BRASIL, 2019).

> “O C² é, simultaneamente, ciência e arte que trata do funcionamento de uma cadeia de comando. É o exercício da autoridade e da direção que um comandante tem sobre as forças sob o próprio comando, para o cumprimento da missão designada.
> O C² envolve três componentes imprescindíveis e interdependentes: a autoridade, o processo decisório e a estrutura. Na FTC, o exercício da autoridade e do processo decisório cabe ao comandante da FTC, assessorado por seu EM, através da estrutura existente, que inclui pessoal, material, instalações, equipamentos e tecnologias necessárias ao exercício da atividade de C².” (BRASIL, 2019)

Assim sendo, na opinião deste autor, a correta realização das tarefas da Função de Combate Comando e Controle proporcionará um melhor planejamento e decisões mais adequadas nas operações, que poderão refletir no sucesso no cumprimento das missões da FTC.

Dentre as tarefas da Função de Combate Comando e Controle está a de Instalar, Explorar, Manter e Proteger os Sistemas de Comunicações, cuja importância é citada pelo Manual de Campanha EB70-MC 10.225 Força Terrestre Componente da seguinte forma:

> “A condução das operações no ambiente operacional terrestre é impossível sem a existência de sistemas de comunicações e de Tecnologia da Informação (TI) adequados e confiáveis. A arquitetura e a eficiência dos sistemas de comunicações e TI empregados pela FTC implicam diretamente na capacidade operativa da F Cte, possibilitando o fluxo adequado de informações e, consequentemente, uma tomada de decisão mais precisa e oportuna pelos comandantes nos diversos níveis.” (BRASIL, 2019)

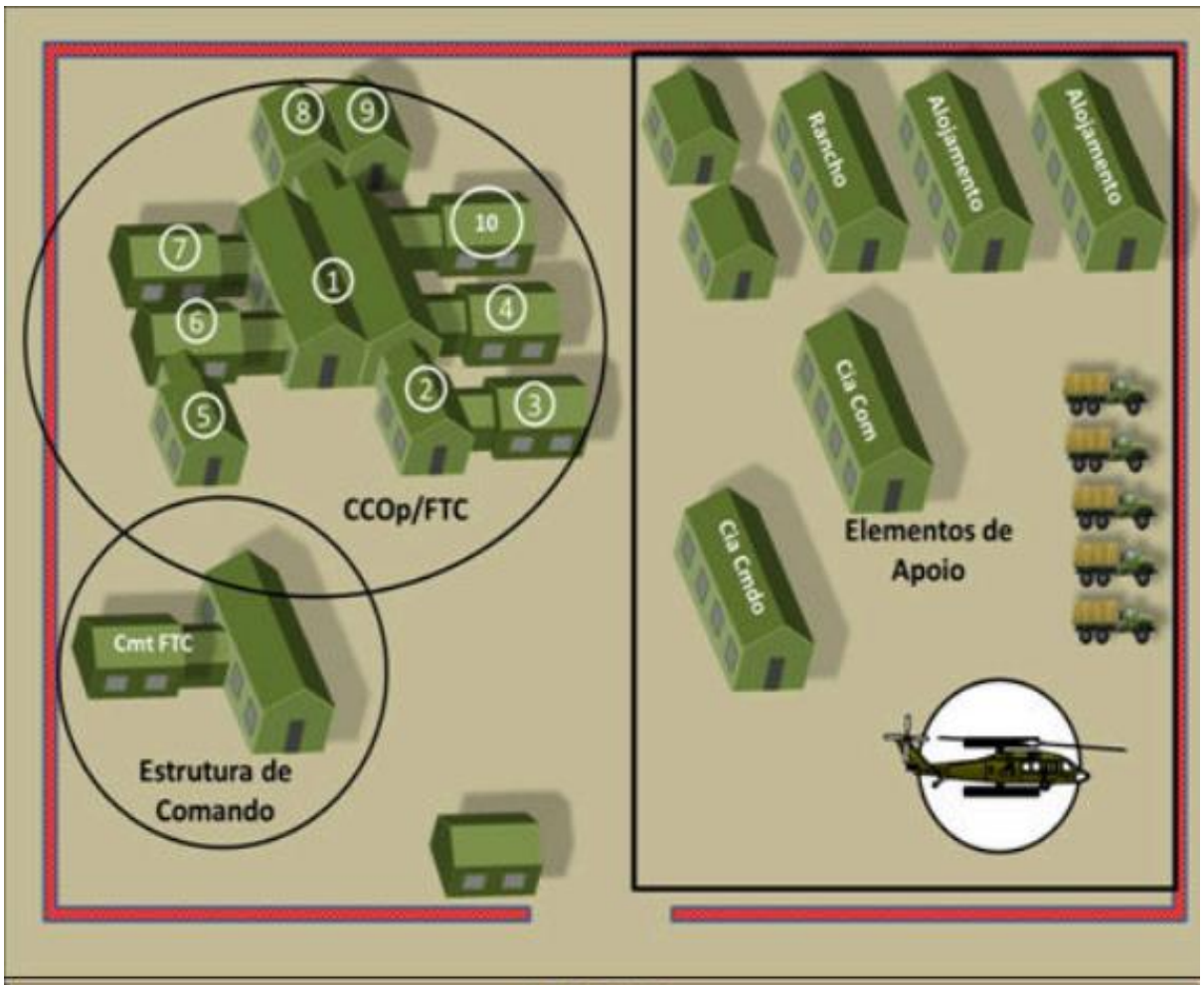
Verifica-se, dessa forma, que a proteção dos sistemas de comunicações e TI dos postos de comando da FTC, de maneira a proporcionar confiança e eficiência à atividade de comando e controle, é preponderante para que o processo de tomada de decisão do Comandante seja realizado com maior rapidez e oportunidade, aumentando as probabilidades de sucesso no jogo do acaso dos conflitos.

4.1.2 Os postos de comando da FTC

> “O Posto de Comando (PC) é o local onde o comando e o EM FTC desempenham as suas atividades. Para a organização do PC, deve-se considerar o efetivo do Estado-Maior e das necessidades da operação, conforme a determinação do comandante, assessorado pelo Chefe do Estado-Maior (Ch EM).
> Normalmente, o PC é composto pela estrutura de comando, pelo CC Op e por elementos de apoio (...). As principais atividades desempenhadas no PC da FTC são as seguintes: a) preparação e manutenção das Estimativas Correntes e do Cenário Operativo Comum; b) elaboração e disseminação de planos e ordens; c) controle das operações; d) avaliação das operações; e) coordenação com os escalões superior, subordinado e com as outras forças componentes; f) condução da gestão do conhecimento e gestão das

> informações; e g) realização da administração do próprio PC.” (BRASIL, 2019)

Para a execução das suas atividades, o Posto de Comando é estruturado de forma a permitir uma melhor integração das Células, como pode ser observado em um exemplo na figura 2.



LEGENDA

1 – Célula de Operações Correntes/ Célula de Movimento e Manobra
2 – Célula de Operações de Médio Prazo
3 – Célula de Planos de Longo Prazo
4 – Célula de Comando e Controle
5 – Célula de Proteção
6 – Célula de Logística
7 – Célula de Fogos
8 – Célula de Inteligência
9 – Área Destinada ao Armazenamento e Processamento de Material Sigiloso
10 – Elemento de Apoio de Comunicações ao CCOp

FIGURA 2 – Esboço de Posto de Comando da FTC.

Fonte: Brasil (2019, p. A-1).

A instalação, exploração, manutenção e proteção das estruturas de Comunicações e Tecnologia da Informação dos postos de comando da FTC é de responsabilidade das Organizações Militares de Comunicações e Guerra Eletrônica (B Com, B Com GE, Cia C2 ou Cia Com), de acordo com a composição da FTC (BRASIL, 2017).

Nesse sentido, é importante salientar que os operadores dos diversos sistemas das Organizações Militares supracitadas estejam capacitados adequadamente para a realização das tarefas no PC da FTC, sobretudo na proteção cibernética das estruturas de TI interligados em rede, por serem alvos de ataques cibernéticos.

Ressalta-se que o aprimoramento das técnicas de ataque cibernético exige novas e contínuas adaptações relacionadas à capacitação do pessoal empregados na atividade de operação e proteção dos sistemas, estendendo, sempre que possível, o treinamento e a atualização de todos os militares envolvidos nas operações da FTC. Essa necessidade já é uma realidade na atualidade, tendo em vista que os equipamentos de comunicações e informação em todos os escalões estão mais dependentes da tecnologia em rede, sendo, portanto, sujeitos a ataques.

4.2 O SISTEMA DE COMANDO E CONTROLE DA FTC

> “O sistema de C² é o componente da Função de Combate Comando e Controle que tem por objetivo ampliar a capacidade do Cmt FTC de conduzir as operações. Ele é organizado de forma a: apoiar a tomada de decisão; coletar, gerar, manter e difundir informações relevantes, auxiliando o entendimento e a concepção de uma visão por parte dos comandantes em todos os níveis; preparar e transmitir ordens e diretrizes; e estabelecer os meios pelos quais os comandantes comunicam, colaboram e facilitam o funcionamento das equipes ou elementos a eles subordinados.” (BRASIL, 2019)

Os elementos que compõem o Sistema de Comando e Controle da FTC, representados na Figura 3, possuem devida importância para as operações, conforme descrito pelo Manual EB70-MC-10.225 Força Terrestre Componente:

> “devem ser integrados de forma a ampliar a capacidade do Cmt FTC e da força como um todo, de conduzir o Processo Operativo, possibilitando atingir a principal finalidade dessa Função de Combate: o exercício do comando para integrar os demais elementos do Poder de Combate Terrestre” (BRASIL, 2019).

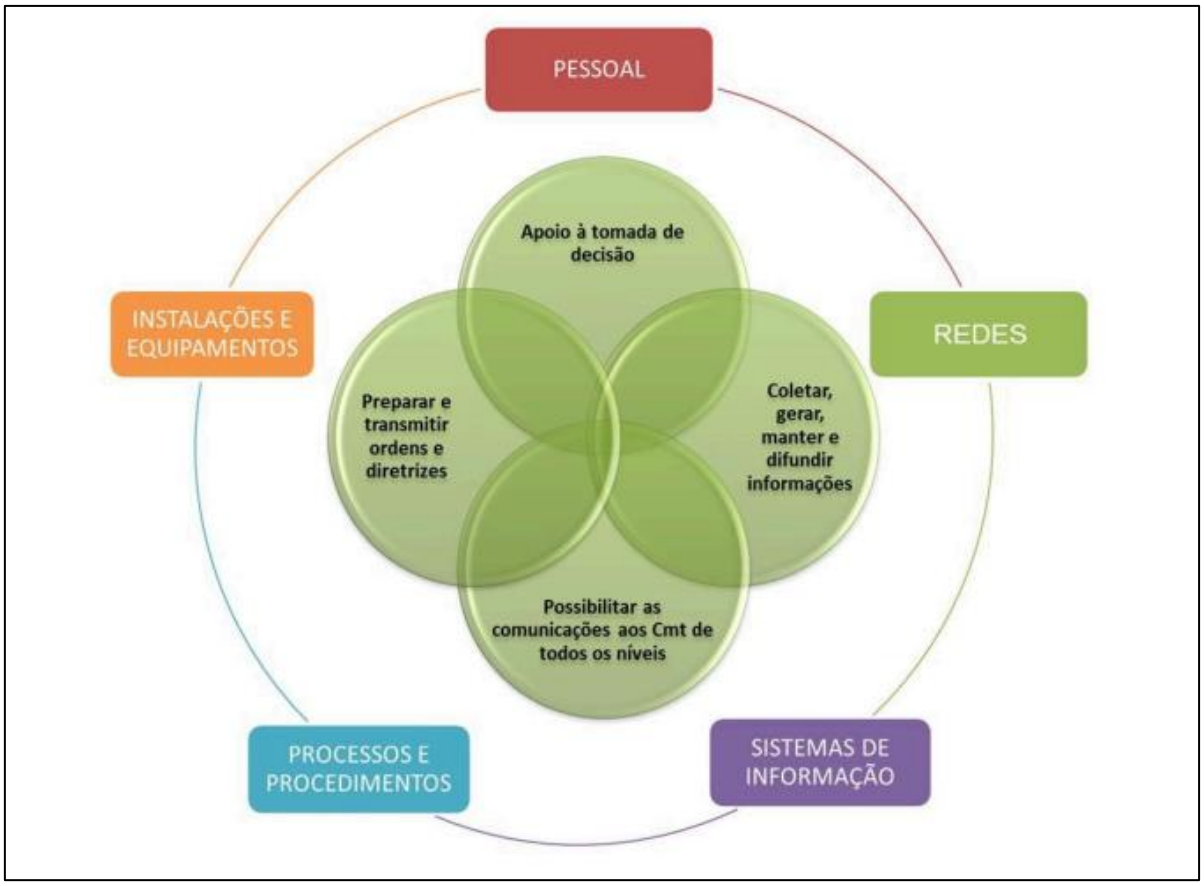


FIGURA 3 – Sistema de Comando e Controle com seus Componentes e Funções.

Fonte: Brasil (2019, p. 5-5).

O principal componente do sistema é o “pessoal capacitado e treinado para a realização das atividades da Função de Combate Comando e Controle” (BRASIL, 2019).

Os Sistemas de Comunicações e TI, segundo o Manual EB70-MC-10.225 Força Terrestre Componente,

> “Proporcionam ao Cmdo FTC a capacidade de transmitir informações e controlar as operações dos seus elementos de emprego. São fundamentais para a obtenção e a manutenção da superioridade de informações e da consciência situacional – fatores que conduzem ao sucesso das operações militares. A proteção desses sistemas deve ser uma preocupação constante, uma vez que elas se constituem em alvos compensadores para as ações doponente [sic] e tendem a ser progressivamente degradadas no decorrer das operações.
> Os Sistemas de Informação consistem em equipamentos destinados a coletar, processar, armazenar, apresentar e a disseminar as informações. Nesse conceito podem ser incluídos computadores e equipamentos de comunicações, bem como os procedimentos para a sua utilização. Esses sistemas, quando integrados a redes bem estruturadas e confiáveis, permitem o compartilhamento extensivo de informações, o planejamento colaborativo, o controle da execução das operações e sua avaliação efetiva, no âmbito da FTC”. (BRASIL, 2019)

Os Sistemas de Informação do SC²FTC

> “consistem em equipamentos destinados a coletar, processar, armazenar, apresentar e a disseminar as informações. Nesse conceito podem ser incluídos computadores e equipamentos de comunicações, bem como os procedimentos para a sua utilização. Esses sistemas, quando integrados a redes bem estruturadas e confiáveis, permitem o compartilhamento extensivo de informações, o planejamento colaborativo, o controle da execução das operações e sua avaliação efetiva, no âmbito da FTC”. (BRASIL, 2019)

Os processos e procedimentos são utilizados no âmbito da FTC para ampliar “sua efetividade, potencializando a capacidade de trabalho do EM FTC ou possibilitando acelerar o ritmo das operações” (BRASIL, 2019).

As Instalações são os locais em que o sistema é estruturado e Equipamentos são os dispositivos de TI necessário para o exercício da atividade de Comando e Controle. (BRASIL, 2019)

O Sistema de Comando e Controle da FTC (SC²FTC) constitui parte do Sistema de Comando e Controle da Força Terrestre (SC²FTer) para as operações conjuntas com as demais Forças Armadas. O SC²FTer é uma estrutura do Sistema de Comando e Controle do Exército (SC²EX) que “tem por finalidade o apoio integrado ao processo de comando e controle no preparo e no emprego operativo da F Ter, desde o tempo de paz” (BRASIL, 2015) e integra as funções de combate.

De acordo com o Manual de Campanha EB20-MC-10.205 Comando e Controle, do Exército Brasileiro, a interoperabilidade entre as Forças Armadas é possível, principalmente, por meio do Sistema de Comunicações por Satélite (SISCOMIS), pelo qual sua estrutura permanente permite a realização de enlaces a longa distância. Esse meio satelital é empregado pelo Estado-Maior Conjunto das Forças Armadas (EMCFA) para o estabelecimento da Rede Operacional de Defesa (ROD), que é descrita como uma rede segregada “que proporciona grande segurança para o fluxo de informações necessário à condução de operações conjuntas”. Assim, o Centro de Comando e Controle da Força Terrestre Componente (CC² FTC) se integra aos demais Centros de Comando e Controle das Forças Componentes e aos Centros de Comando e Controle dos Comandos Operacionais ativados.

Para permanecer em condições de ser empregado em qualquer tempo e circunstância, o Ministério da Defesa hospeda no seu Centro de Comando e Controle (CC²MD) os seguintes serviços e sistemas:

> “a) acesso à ROD; b) voz sobre IP (VoIP); c) correio eletrônico operacional; d) serviço de transferência de arquivo (FTP); e) rede privada virtual (VPN); f) acesso às redes internas de comunicações e de dados das FA; g) acesso seguro à internet; h) sistema de videoconferência; e i) sistemas de apoio à decisão” (BRASIL,2017).

Este autor considera que o emprego de meios satelitais para proporcionar a interoperabilidade entre as Forças Componentes oferece relativa segurança para as operações, nas situações em que a força oponente não dispõe de equipamentos para realizar ataques contra esses meios. Por outro lado, o combate moderno tem demonstrado que já não há limitações para ações de ataque contra os meios satelitais a partir de novas tecnologias, pelas quais permitem interferir e degradar o fluxo de informações.

4.3 A PROTEÇÃO CIBERNÉTICA NA FTC

A fim de limitar o risco das operações, decorrente da ação do oponente, as tarefas de proteção cibernética são importantes para garantir a integridade do poder de combate disponível ao Cmt FTC para o cumprimento de sua missão, segundo o Manual EB70-MC-10.225 Força Terrestre Componente.

O Manual reconhece que as ameaças à FTC

> "São as atividades de qualquer natureza, que podem ser desencadeadas por forças oponentes ou adversas, que visam a comprometer ou a superar as medidas de salvaguarda do conhecimento adotadas pela FTC e por seus elementos de emprego. Além da busca por dados e conhecimentos sigilosos da FTC (incluindo a espionagem), podem ocorrer na forma de:
> a) coleta de dados ou conhecimentos ostensivos;
> b) sabotagem – provocando danos de modo intencional contra instalações ou material de interesse para a FTC, com a finalidade de afetar sua capacidade operativa;
> (...)
> d) propaganda adversa – conjunto de ações de cunho psicológico, desencadeado por meio da manipulação de meios de comunicação, buscando persuadir determinado público e obter atitudes desfavoráveis ao C Cj e à FTC." (BRASIL, 2019)

Nesse sentido, as ameaças são direcionadas "contra os indivíduos detentores dos dados e dos conhecimentos ou contra tudo o que serve como suporte a esses indivíduos (documentos, materiais, meios de comunicações e TI, áreas e instalações)" (BRASIL, 2019).

> "As ameaças ao pessoal não são direcionadas somente aos integrantes da FTC que detenham conhecimentos sensíveis, mas também àqueles que tenham acesso aos conhecimentos – ainda que de forma indevida. As ameaças mais expressivas são:
> a) espionagem, inclusive mediante recrutamento de pessoal do Cmdo/EM FTC (passam a ser agentes adversos consciente ou inconscientemente);
> b) terrorismo, atingindo pessoal da FTC de maneira seletiva, em função da importância dos cargos que ocupam; e

> c) propaganda adversa, cujo objetivo mais comum é o de buscar a queda do moral e da disciplina entre os integrantes das forças amigas.
> A espionagem contra a FTC objetiva a obtenção do conhecimento protegido, inclusive o transmitido pelos meios de comunicações e TI, normalmente, quebrando cifras e decifrando códigos. A sabotagem pode gerar danos que redundem na perda da documentação e de material ou na impossibilidade de utilização de áreas, instalações, meios e equipamentos, conduzindo à impossibilidade de prosseguimento na linha de ação da FTC – como no caso de produzir interrupção da comunicação e troca de dados entre os elementos de emprego, por exemplo.” (BRASIL, 2019)

A proteção cibernética na FTC tem foco na salvaguarda de informações sensíveis, ante a interceptação do oponente, e a eliminação da possibilidade deste de interferir nas redes amigas. “Os meios de transferência digital de dados e os sítios para postagem e disseminação de informações estão entre os focos para a proteção e a preservação da superioridade de informações” (BRASIL, 2019).

Assim, a mitigação dos riscos exige uma contínua avaliação das ameaças e o levantamento de vulnerabilidades pela Célula de Proteção da FTC, de forma a manter o Cmt e o EM FTC informado sobre os possíveis óbices para a operação.

4.4 CONCLUSÕES PARCIAIS SOBRE O SISTEMA DE COMANDO E CONTROLE DA FTC

Infere-se parcialmente que o Sistema de Comando e Controle da FTC está sujeito a ataques cibernéticos de uma força oponente em combate. Os elementos que constituem os SC²FTC (pessoal, sistemas de comunicações e TI, sistemas de informação, processos e procedimentos e instalações e equipamentos) possuem vulnerabilidades que possibilitam a realização de ataques.

Dentre esses elementos, destacam-se os sistemas de TI e de Informação, que necessitam estar em constante atualização para impedir invasões aos sistemas, e o pessoal, que são exigidas as capacitações e treinamentos adequados para a correta operação e os procedimentos para se evitar a obtenção de vantagens pela força oponente.

Ainda, é necessário que haja uma sinergia entre a célula de proteção e a célula de comando e controle na mitigação dos riscos de ataques cibernéticos, de forma que as medidas preventivas sejam tomadas ainda na fase de planejamento e as melhores soluções sejam tomadas no decorrer da operação.

5. CONCLUSÃO

A Proteção Cibernética tem ganhado grande relevância para o sucesso das operações conjuntas das Forças Armadas brasileiras e a Força Terrestre mantém-se em uma constante evolução de forma a ampliar sua capacidade de proteger os sistemas de informação e comunicações no espaço cibernético fundamentais para o exercício do comando e controle da FTC nas operações.

Em síntese, a FTC, no contexto das operações conjuntas, deve prever em todas as suas fases do processo operativo de emprego, as capacidades de proteção cibernética na sua estrutura de informação e comunicações, sobretudo nos sistemas de C2 operados em rede em seus postos de comando, de forma a permitir maior amplitude da consciência situacional do comandante, a fim de que sua decisão seja a mais precisa e oportuna quanto possível, além de possibilitar maior confiabilidade das informações que tramitam nesses sistemas.

Como resultado, identificou-se uma crescente da importância da proteção cibernética para a Força Terrestre, desde os dias de paz, materializado no Comando de Defesa Cibernética (Com D Ciber), o qual mantém ativado o Comando Conjunto de Defesa Cibernética com a finalidade de identificar as ameaças e mitigar os riscos delas advindas, empregando todas as suas capacidades disponíveis na atualidade.

Ainda, observou-se um aumento considerável do número de ataques cibernéticos em todo o mundo nos últimos anos, incluindo os ataques aos sistemas das Forças Armadas brasileiras, voltadas principalmente para as vulnerabilidades existentes na dimensão física (novos dispositivos de rede, servidores, entre outros) e para as falhas de segurança ligadas à dimensão humana (engenharia social, erros operacionais, entre outros).

Diante da evolução dessas ameaças, conclui-se que se torna necessária a obtenção de novas capacidades, o que gera uma demanda maior de investimentos para desenvolvimento de sistemas mais seguros e eficientes, com materiais de última geração e pessoal adequadamente capacitado.

Verificou-se que prevenção de ataques nem sempre é possível, no entanto o aprimoramento das técnicas de proteção como a utilização de Inteligência Artificial (IA) favoreceria uma maior rapidez e eficiência na identificação da ameaça e inibição dos ataques. A Inteligência Artificial pode proporcionar uma monitoração da rede

sobre o comportamento de usuários e sistemas, padrões de acesso e comportamentos anormais ou maliciosos.

É relevante o emprego de equipamentos capazes de proporcionar confiabilidade e rapidez de operação, de forma a permitir maior velocidade na solução de problemas e minimizar os prejuízos de um ataque cibernético, além do permanente desenvolvimento dos aplicativos dos Sistemas de C2, mantendo-os em constante atualização, frente ao surgimento de novas ameaças cibernéticas, a fim de mitigar as possibilidades de ataques aos sistemas de comando e controle da FTC.

Outrossim, é imprescindível a contínua atualização e capacitação pessoal com relação à utilização mais segura dos meios computacionais, envolvendo todos os militares que compõem uma FTC e que estão sujeitos a um ataque cibernético de uma força oponente, seja na operação de dispositivos vinculados ao Sistema de C2, seja no uso de dispositivos particulares que se configuram em alvos para a obtenção de informações e portas de acesso aos sistemas, constituindo-se em riscos para as operações. Tal atualização e capacitação são possíveis já em tempos de paz a partir da inclusão de instruções voltadas para a conscientização desses riscos e treinamento de proteção cibernética em todos os Estabelecimentos de Ensino e no Programa de Instrução Militar (PIM) para a formação dos militares temporários.

Por fim, fruto da presente pesquisa, conclui-se que a proteção cibernética tem sido fundamental para a consecução dos objetivos da Força Terrestre, na atualidade, e sua importância tende a aumentar no futuro, em que a realidade das operações se encaminha para uma dependência absoluta da rede de computadores, com a demanda da informação em tempo real para a tomada de decisão mais rápida e eficiente. Dessa forma, observada a grande relevância desse tema, esta pesquisa necessita de novos estudos de forma a complementar e manter atualizada a Força Terrestre sobre as possibilidades de se ampliar, cada vez mais, a capacidade de emprego da proteção cibernética nos Postos de Comando da FTC, contribuindo para a incessante busca do mais elevado nível de segurança da informação.

REFERÊNCIAS

ARMY CYBER. **About army cyber command: the army's frontline of cyber warfare.** 2019. Disponível em: <https://www.goarmy.com/army-cyber/about-armycyber-command.html>. Acesso em 05 de junho de 2021.

BLACKBERRY. **Relatório de Ameaças 2021.** 2021. Disponível em: <https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-pt.pdf>. Acesso em 06 de junho de 2021.

BRASIL. **Estratégia Nacional de Defesa.** Brasília. 2008. Disponível em: <www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 05 de junho de 2021.

_____. Exército. Comando de Operações Terrestres. **EB70-MC-10.225 Força Terrestre Componente.** 1. ed. Brasília, DF, 2019.

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

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

_____. Ministério da Defesa. **Cenários de Defesa 2020 – 2039:** sumário executivo. Brasília, DF, 2017.

_____. Ministério da Defesa. **Comando Conjunto na Defesa Cibernética.** Brasília, DF, 2017. Disponível em: <https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/comando-conjunto-na-defesa-cibernetica#:~:text=O%20Comando%20de%20Defesa%20Cibern%C3%A9tica%20%28Com%20D%20Ciber%29,dificultar%20sua%20utiliza%C3%A7%C3%A3o%20contra%20interesses%20da%20Defesa%20Nacional.>. Acesso em 06 de junho de 2021.

_____. Ministério da Defesa. **MD31-M-08 Doutrina Militar de Defesa Cibernética.** 1. ed. Brasília, DF, 2014.

_____. **Política Nacional de Defesa.** Minuta. Brasília. 2020. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf>. Acesso em 10 de abril de 2021.

CARREIRO, Marcelo. **A Guerra Cibernética:** Cyberwarfare e a Securitização da Internet. Rio de Janeiro, RJ, [n.d].

CERÁVOLO, Luiz E. S.; FERREIRA NETO, Walfredo B. **Defesa Cibernética no Brasil**: distribuição de competências nas operações interagências. In: Defesa Nacional. Ano CIII, n. 828, 3. quadrimestre, 2015. pp. 65-90.

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.

DEPARTMENT OF DEFENSE. **U. S. Cyber Command.** Washington, DC, USA, 2010. Disponível em:<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf>. Acesso em 05 de junho de 2021.

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 (C2). **Revista Militar de Ciência e Tecnologia.** Rio de Janeiro, n. 2, vol. 33, p. 11-18. 2016.

JUN, J.; LAFOY, S.; SOHN, E. **North Korea's cyber operations: strategy and responses.** USA: Center for strategic international studies, 2015. Disponível em: < https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations>. Acesso em 02 de junho de 2021.

LIMA, Victor Hugo. Hacktivismo e a Defesa Cibernética do Brasil. **Centro de Estudos Estratégicos do Exército – CEEEx**. Brasília. Vol 8 (2). março/maio 2018.

LINS, Bernardo Felipe Estellita. A evolução da internet: uma perspectiva histórica. **Cadernos Aslegis**. Brasília, n. 48, p. 11-45, 1. Quadrim. 2013.

LOPES, Pedro Filipe Terra. **A evolução das redes de computadores e as filosofias tecno-políticas nos finais do século XX**: para uma genealogia dos novos *media*. Dissertação (Mestrado em Ciências da Computação) - Faculdade de Letras da Universidade do Porto, Porto. 2015.

LYNN III, William J. Defending a new domain: the Pentagon's cyberstrategy. **Foreign Affairs**, setembro/outubro 2010. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-newdomain>. Acesso em: 05 de junho de 2021.

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: 07 de junho de 2021.

PINHEIRO, Alvaro de Souza. A Tecnologia da Informação e a Ameaça Cibernética na Guerra Irregular do Século XXI. **Padeceme.** Rio de Janeiro, n. 18, p. 4-11, 2. Quadrim. 2008.

SACRAMENTO, Lucas Rocha. **Hardening em Linux:** Aperfeiçoamento da segurança do PFSENSE visando aumentar a segurança de borda nas organizações militares. Orientador: JULIANO BRANDÃO PALÁCIO. 2018. Trabalho de Conclusão de Curso (Especialização em ciências militares) - Escola de Aperfeiçoamento de Oficiais. Rio de Janeiro, 2018.

SALDAN, Eliane. **Doutrina precisa definir guerra cibernética**. Disponível em: https://www.conjur.com.br/2011-ago-06/guerra-cibernetica-urgentemente-definicao-doutrina. Acesso em: 26 maio 2021.

SANTOS, Phillipe Dautro dos. **Ciberespaço como domínio de operações militares**: A perspectiva dos Estados Unidos da América. Orientador: Prof. Dr. AUGUSTO WAGNER MENEZES JÚNIOR. 2018. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Federal da Paraíba, João Pessoa, 2018.

TECMUNDO. **Hackers vazam supostos dados de 200 mil militares em retaliação a Bolsonaro**, 11 maio 2020. Disponível em: <https://www.tecmundo.com.br/seguranca/153022-hackers-vazam-dados-200-mil-militares-retaliacao-bolsonaro.htm>. Acesso em: 10 de abril de 2021.