ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP ART LUCAS MENUCI DE BRUM

A GUERRA CIBERNÉTICA E SUAS CAPACIDADES EM PROVEITO DO EMPREGO DE TECNOLOGIAS NA AQUISIÇÃO DE ALVOS NA FASE DETECTAR DA METODOLOGIA DE PROCESSAMENTO DE ALVOS

Rio de Janeiro

2022

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP ART LUCAS MENUCI DE BRUM

A GUERRA CIBERNÉTICA E SUAS CAPACIDADES EM PROVEITO DO EMPREGO DE TECNOLOGIAS NA AQUISIÇÃO DE ALVOS NA FASE DETECTAR DA METODOLOGIA DE PROCESSAMENTO DE ALVOS

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais como requisito parcial para obtenção do grau especialização em Ciências Militares.

Orientador: Cap Art Victor Gabriel **Bosch** Baptista

Rio de Janeiro

2022

Ficha catalográfica elaborada pelo Bibliotecário Francisco José de Paula Junior
CRB7/6686

B893

Brum, Lucas Menuci de.

A guerra cibernética e suas capacidades em proveito do emprego de tecnologia na aquisição de alvos na fase detectar da metodologia de processamento de alvos / Lucas Menuci de Brum – 2022.

39 f. : il.

Trabalho de Conclusão de Curso – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2022.

Orientação: Cap. Victor Gabriel Bosch Baptista

1. Guerra cibernética. 2. Espaço cibernético. 3. Capacidades. I Escola de Aperfeiçoamento de Oficiais. II Título.

CDD: 355

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

DIVISÃO DE ENSINO E PESQUISA / CURSO DE ARTILHARIA

Ao Cap Art LUCAS MENUCI DE **BRUM**

O Presidente da Comissão de Avaliação do TCC, cujo título é "A GUERRA CIBERNÉTICA E SUAS CAPACIDADES EM PROVEITO DO EMPREGO DE TECNOLOGIAS NA AQUISIÇÃO DE ALVOS DA FASE DETECTAR DA METODOLOGIA DE PROCESSAMENTO DE ALVOS", informa à Vossa Senhoria o seguinte resultado da deliberação: **APROVADO** com o conceito **MUITO BOM**.

Rio de Janeiro, RJ, 20 de setembro de 2022.

MÁRCIO DE LIMA AZENHA - Maj
Presidente

VICTOR GABRIEL BOSCH BAPTISTA - Cap
1º Membro

FELIPE MAGALHÃES COELHO DA SILVA - Cap
2º Membro

CIENTE:

LUCAS MENUCI DE BRUM - Cap
Postulante

RESUMO

A presente pesquisa, após a realização de consultas a bibliografias e manuais das Forças Armadas, identificou a inexistência de uma integração entre capacidades de Guerra Cibernética (Proteção, Exploração e Ataque) e meios tecnológicos empregados na fase de detecção, da metodologia de processamento de alvos “D3A” (Decidir, Detectar, Disparar e Avaliar). Assim, essa pesquisa tem como objetivo principal, o preenchimento dessa lacuna existente, buscando sugerir uma dinâmica de emprego conjunto das capacidades de Guerra Cibernética e meios, como, radares de vigilância e contrabateria e Sistemas de Aeronaves Remotamente Pilotadas (SARP), na fase de detecção da metodologia “D3A”, a fim the que as capacidades da Guerra Cibernética atuem em proveito desses meios tecnológicos de aquisição de alvos, com a proteção salvaguardando esses meios perante as possíveis ameaças cibernéticas, com a exploração levantando e confirmando dados acerca de alvos de interesse, através de sistemas tecnológicos e informacionais do oponente, e o ataque atuando para impedir ou dificultar a utilização de sistemas informacionais e de aquisição de alvos pelo inimigo.

Palavras-chave: Guerra Cibernética. Aquisição de Alvos. Detecção de Alvos. Ataque Cibernético. Proteção Cibernética. Exploração Cibernética. Defesa Cibernética.

ABSTRACT

The present research, after consulting bibliographies and manuals of the Armed Forces, identified the inexistence of an integration between Cyber Warfare capabilities, The Exploration, The Attack and The Protection, and technological means that are used in the detection phase of the target processing methodology “D3A” (Decide, Detect, Shoot and Evaluate). Thus, the main goal of this research is to fill this existing gap, seeking to suggest a dynamic of joint use of Cyber Warfare capabilities and technological means, such as surveillance and counter-battery radars and Remotely Piloted Aircraft Systems (SARP), in the detection phase of the “D3A” methodology. The main purpose is to use the capabilities of Cyber Warfare for the benefit of these technological means of target acquisition, with the protection safeguarding these means in the face of possible cyber threats, with the exploitation raising and confirming data about targets of interest, through the opponent's technological and informational systems, and the attack acting in order to prevent or hinder the use of enemy target acquisition systems and informational systems.

Keywords: Cyber Warfare. Target Acquisition. Target Detection. Cyber Attack. Cyber Protection. Cyber Exploitation. Cyber Defense.

SUMÁRIO

1. INTRODUÇÃO

O avanço da internet e da tecnologia permitiu a interconexão entre cidadãos de nações distantes, intensificou o fluxo de informações e disponibilizou inúmeros serviços online, nunca antes pensados. Por outro lado, trouxe consigo um novo conflito mundial, a guerra cibernética, na qual ataques cibernéticos são desencadeados, por um país ou nação, a fim dissolver os sistemas de computadores de outro, gerando danos significativos, similares ao de uma guerra real. (SINGER and FRIEDMAN, 2014).

O ataque cibernético com o *software* malicioso *Stuxnet*, que contaminou uma fábrica de enriquecimento de urânio iraniana em 2010, acelerando os reatores das centrifugas até que elas quebrassem, reafirmou a chegada da era da Guerra Cibernética, na qual, entre outros ataques, códigos mal intencionados são usados como armas cibernéticas, contaminando, propositalmente, setores tecnológicos estratégicos de um país, levando-o a sofrer muitas vezes não apenas danos no âmbito cibernético, mas também no âmbito físico.

Diante de todo esse cenário e visando atender à Estratégia Nacional de Defesa, que instituiu a responsabilidade da Defesa Cibernética para o Ministério da Defesa, por meio das Forças Armadas (FA), criou-se, em 2014, a Doutrina Militar de Defesa Cibernética, com a finalidade de propiciar uma unidade de pensamento sobre Defesa Cibernética e contribuir para a atuação conjunta das Forças Armadas (FA) na defesa do espaço cibernético brasileiro. (BRASIL, 2014).

O Ministério da Defesa, por sua vez, determinou que fosse desenvolvido no âmbito das FA, nível operacional e tático, o conceito de Guerra Cibernética, reforçando a importância do emprego de capacidades cibernéticas nas operações militares. (BRASIL, 2014).

Assim, a Guerra Cibernética, no âmbito das FA, foi definida como:

> Guerra Cibernética - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e

> Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2 . Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2017b, p. 19).

A atualização do Manual EB 70 MC 10.346 – Planejamento e Coordenação de Fogos (BRASIL, 2017b, p. 4-1) implementou o emprego da metodologia de processamento de alvos “D3A”, “Decidir”, “Detectar”, “Disparar” e “Avaliar”, com o objetivo de ordenar as tarefas atinentes ao sistema de apoio de fogo nas operações.

No contexto da metodologia “D3A”, foi implementada a utilização de tecnologias com o intuito de tornar mais eficazes e precisas as tarefas atinentes à fase “detectar”, estabelecendo o uso de radares e Sistemas de Aeronaves Remotamente Pilotadas (SARP), como meios de aquisição de alvos.

Diante da constante e audaciosa evolução dos ataques cibernéticos, das diretrizes emanadas pelo MD às FA, de desenvolver as capacidades de Guerra Cibernética e da implementação de meios tecnológicos na metodologia “D3A”, esta pesquisa tratará sobre a integração das capacidades da Guerra Cibernética trabalhando em proveito dos ativos tecnológicos empregados na fase “detectar”.

1.1 PROBLEMA

O emprego da Artilharia no combate moderno exige cada vez mais rapidez e precisão para identificar e impedir o uso dos fogos pelo inimigo. A necessidade de manter o grau de operacionalidade alinhada com as implicações de preservação da tropa e letalidade seletiva exigem, da atividade de contrabateria, medidas proativas e reativas que auxiliem no êxito da operação.

1.1.1 Antecedentes do problema

O Manual EB70-MC 10.346 – Planejamento e Coordenação de Fogos (BRASIL, 2017b), fonte de consulta nacional, que introduz o emprego da metodologia “D3A” nas operações, descreve todas as fases de processamento, “detectar”, “disparar”, “decidir” e “analisar”, de forma genérica, não entrando no âmbito do emprego da Guerra Cibernética em proveito dos seus processos.

O Manual EB70-MC 10.232 – Guerra Cibernética (BRASIL, 2017a), discorre sobre os fundamentos, estruturas e responsabilidades da Guerra Cibernética (G Ciber), bem como as atividades dessa em proveito das Funções de Combate e nas operações, mas não tangencia o nível a integração entre as capacidades da Guerra Cibernética com metodologias de processamento de alvos que fazem uso de tecnologia.

Os manuais ATP 3-09.12 – Field Artillery Target Acquisition (EUA, 2015a) e ATP 3-60 – Targeting (EUA, 2015b), do exército dos Estados Unidos, o qual utiliza a metodologia de processamento de alvos “D3A”, empregam em abundancia radares e SARP na busca de alvos e são dotados de obuseiros e sistemas de defesa antiaérea com alta tecnologia embarcada, também não se verificou uma abordagem clara do emprego de capacidades cibernéticas em proveito das suas metodologias de processamento de alvos.

O manual ROP-03-54 – Adquisición de Blancos de la Artillería de Campaña, do exército argentino, aborda profundamente metodologias de aquisição de alvos, discorrendo sobre os meios de aquisição e inteligência de artilharia, mas, assim como os demais manuais descritos acima, não integra o emprego de capacidades cibernéticas com o de meios tecnológicos na detecção de alvos.

1.1.2 Formulação do problema

Diante do uso de radares e SARP na fase de detecção da metodologia de processamento de alvos “D3A”, como as capacidades de Guerra Cibernética, ataque, proteção e exploração cibernética, podem atuar em proveito dessa metodologia, em prol da revisão do Manual EB 70 MC 10.346 – Planejamento e Coordenação de Fogos, a fim de mitigar vulnerabilidades e, analogamente, ações de ameaças cibernéticas?

1.2 OBJETIVOS

O objetivo geral visa alcançar em plenitude a elucidação do tema deste trabalho, almejando integrar as capacidades de Guerra Cibernética com as tarefas da fase “detectar”, a fim de proporcionar a preservação dos ativos tecnológicos empregados na referida Fase.

Os objetivos específicos serão estabelecidos a fim de se fasear a construção de conhecimentos necessários para a compreensão da metodologia de processamento de alvos “D3A”, dos fundamentos e capacidades de Guerra Cibernética e, por fim, da integração entre capacidades de guerra cibernética e o a metodologia “D3A”.

1.2.1 Objetivo Geral

A presente pesquisa tem por objetivo geral identificar como as capacidades da Guerra Cibernética, ataque, proteção e exploração cibernéticos, podem atuar em proveito da fase “detectar” da metodologia de processamento de alvos “D3A”.

1.2.2 Objetivos Específicos

A fim de alcançar o objetivo geral, foram elaborados os seguintes objetivos específicos:

- Descrever a metodologia de processamento de alvos “D3A”;
- Identificar o uso de radares e SARP na detecção de alvos no exército brasileiro e em exércitos de outros países;
- Evidenciar a ocorrência de ataques cibernéticos em meios tecnológicos voltados para a busca de alvos;
- Identificar os fundamentos da Guerra Cibernética de acordo com a doutrina militar vigente das FA brasileiras;
- Identificar as capacidades da Guerra Cibernética de acordo com a doutrina militar vigente das FA brasileiras;
- Identificar modelos de integração entre capacidades cibernéticas e meios de busca de alvos; e
- Inferir como as capacidades de Guerra Cibernética podem atuar em proveito da fase “detectar” da metodologia de processamento de alvos “D3A”.

1.3 QUESTÕES DE ESTUDO

As questões de estudo que serão abordadas pela pesquisa e nortearão o desenvolver do trabalho são:

- Quais os processos atinentes a fase de detecção da metodologia de processamentos de alvos “D3A”?
- Como são empregados os radares e os SARP em proveito da fase de detecção na metodologia de processamento de alvos “D3A”?
- Como foram elaborados e executados os ataques cibernéticos mais recentes sobre radares e sistemas semelhantes ao SARP?
- Quais são os fundamentos da Guerra Cibernética de acordo com a doutrina vigente nas FA?
- Quais são as capacidades da Guerra Cibernética de acordo com a doutrina vigente nas FA?
- Existe alguma doutrina de integração entre capacidades de Guerra Cibernética e meios tecnológicos de busca de alvos? e
- Como as capacidades de Guerra Cibernética podem atuar em proveito da fase “detectar” da metodologia de processamento de alvos “D3A”?

1.4 JUSTIFICATIVAS

Em 2008, A Estratégia Nacional de Defesa estabeleceu prioridade em três setores estratégicos para a Defesa Nacional: o Nuclear, o Cibernético e o Espacial. Dentre os setores citados, o setor Cibernético ficou a cargo do Ministério da Defesa, o qual, a fim de contribuir para a atuação conjunta das FA na defesa do espaço cibernético nacional, elaborou a Doutrina Militar de Defesa Cibernética. (BRASIL, 2017b, p. 17).

O advento de novas tecnologias pelo meio militar, facilitou o alcançar de objetivos militares, de forma cada vez mais precisa e eficaz, bem como aprimorou a medidas de defesa de seus ativos. Contudo, abriram-se, naturalmente, brechas para a atuação de ameaças cibernéticas provenientes de outras nações, grupos terroristas ou cibercriminosos com interesses diversos.

Nesse contexto, a Defesa Cibernética estabeleceu-se como atividade fundamental nas operações militares em todos os níveis de comando,

protegendo os ativos de informação da Força e negando o exercício do Comando e Controle ao inimigo. (BRASIL, 2017b, p. 13).

Os radares e os SARP empregados como meios tecnológicos no contexto da fase de detecção da metodologia de processamento de alvos “D3A”, representam importantes ativos da força que devem ser abrangidos pelas capacidades de Guerra Cibernética, a fim de se mitigar a exploração de suas possíveis vulnerabilidades por parte de ameaças cibernéticas.

Diante disso, o escopo deste trabalho vai ao encontro das diretrizes e prioridades da Estratégia Nacional de Defesa, bem como dos objetivos da Doutrina Militar de Defesa Cibernética, por se tratar de uma pesquisa voltada para a integração de capacidades cibernéticas (ataque, exploração e proteção) e meios tecnológicos empregados em operações militares que, diante do avançar dos conflitos no espaço cibernético, devem ser protegidos de possíveis ameaças atuantes no ambiente virtual.

2. REFERENCIAL TEÓRICO

Nesta fase, serão apresentadas, em sequência, os aspectos relacionados com o objeto de estudo do presente trabalho, buscando alinhar de forma lógica os conhecimentos que interrelacionados com o problema e com os objetivos levantado nos tópicos anteriores, a fim de se alcançar o resultado final esperado da presente pesquisa.

2.1 OS FUNDAMENTOS DA DOUTRINA DE EMPREGO DA FORÇA TERRESTRE

A Força Terrestre, a fim de bem cumprir os seus deveres constitucionais, enquadra-se em estratégias de emprego, valendo-se de princípios de guerra, bem como de táticas, técnicas e procedimentos como fontes para direcionar o seu preparo e emprego. (BRASIL, 2019, p 5-1).

Enquanto a estratégia militar tange o conceito de arte e ciência que consiste na previsão de emprego, preparação, orientação e aplicação da força militar os confrontos e hostilidades, os princípios de guerra são conceitos filosóficos provenientes de experiências militares em batalhas passadas, que orientam o planejamento dos comandantes da Força, diante das operações militares e situações com as quais se deparam. (BRASIL, 2019, p 5-1).

2.1.1 Estratégias de Emprego da Força Terrestre

As Estratégias de Emprego consistem em preceitos que guiam e orientam a Força. Esses preceitos consistem na ação direcionada do Poder nacional, com predominância da expressão militar, através de uma ação independente, uma aliança, a necessidade de uma ação defensiva, de dissuasão, ofensiva, de presença, de projeção de poder e de resistência. (BRASIL, 2019, p 5-1).

A Ação Independente consiste no emprego do Poder Nacional, de forma independente, quando forem abalados preceitos fundamentais e princípios da Constituição Federal, enquanto a Aliança, consiste no emprego em conjunto com o poder militar de um ou mais países. (BRASIL, 2019, p 5-1).

A Defensiva, materializa-se através de uma ação tomada, em caráter temporário, perante uma ameaça, até que se retome a ofensiva. Já a Ofensiva

trata-se da tomada de iniciativa nos conflitos, visando áreas de interesse ou territórios inimigos, a fim de se obter vantagens para futuras negociações. (BRASIL, 2019, p 5-2).

A Dissuasão traduz-se por meio manutenção de Forças com alto poder relativo de combate e operacionais, a fim de desestimular o inimigo a combater. Enquanto a Presença, trata-se na de uma ação de presença militar ou demonstração de capacidade de rápida ocupação de determinada área, ao longo de todo o território nacional e suas extensões, com foco no cumprimento das obrigações constitucionais da Força, entre outras atribuições. (BRASIL, 2019, p 5-2).

A Projeção de Poder, já está voltada para além do território nacional, buscando-se, por meio de ações no âmbito internacional, o respeito de instituições a nível global e países, a fim de desestimular agressores em potencial e em proveito de interesses nacionais no campo internacional. Já a Resistência, consiste em ações em longos conflitos, geralmente de baixa intensidade, empregando-se, na maioria das vezes, técnicas e táticas de guerra irregular. (BRASIL, 2019, p 5-2).

2.1.2 Os Princípios de Guerra no Emprego da Força Terrestre

A fim de se evitar que erros cometidos em conflitos passados sejam repetidos em situações que exijam o emprego da Força nos tempos atuais, foram elaborados preceitos filosóficos, para serem seguidos pelos comandantes militares, em todos os níveis, quando realizarem o planejamento de uma operação ou se depararem com problemas militares.(BRASIL, 2019, p 5-2).

Assim surgiram os Princípios de Guerra, que consistem em 13 (treze) preceitos que balizam as tomadas de decisão e planejamentos inerentes aos comandantes militares:

> **5.1.3** Os Princípios de Guerra são preceitos filosóficos decorrentes de estudos de campanhas militares ao longo da história e apresentam variações no espaço e no tempo. São pontos de referência que orientam e subsidiam os chefes militares no planejamento e na condução da guerra sem, no entanto, condicionar suas decisões.
>
> **5.1.4** O comandante, ao planejar e executar uma campanha ou operação, leva em consideração o que preconizam os princípios,

> interpretando-os e aplicando-os, criteriosamente, em face da situação-problema, decidindo quais são os prioritários. (BRASIL, 2019, p 5-1).

O princípio Objetivo, preconiza que o comandante deverá, ao definir um objetivo para ser alcançado, deverá defini-lo de forma clara, bem como estabelecer algo que seja alcançável pelos seus subordinados. A Simplicidade, que está, de certa forma relacionada ao Objetivo, refere-se ao fato de ser desejável que as ordens e documentos de emitidos pelo comandante contenham conceitos e claros e de fácil entendimento, de forma que fique nítido a intenção do comandante. (BRASIL, 2019, p 5-1 e 5-2).

A Ofensiva trata acerca de se ter iniciativa nas operações, antes da tomada da ofensiva pelo inimigo, determinando o ritmo das e direcionando o combate. Esse princípio tem como centelha a audácia do combatente, entusiasmado pelo espirito de corpo do grupo ao qual pertence. Relacionado a Ofensiva, a Surpresa consiste no empregar poder de combate em um local onde o inimigo não esteja pronto ou no qual ele se dê em conta quando não for mais possível empreender um contra-ataque eficaz. (BRASIL, 2019, p 5-2).

A Segurança preconiza medidas necessárias ao emprego dos meios da Força de forma a se evitar a perda da liberdade de ação e do poder de combate, ao mesmo tempo que se busca dificultar que inimigo mantenha a sua liberdade de ação, bem como impedir que venha a empregar a surpresa ou monitorar as forças amigas. (BRASIL, 2019, p 5-2).

A Economia de forças ou meios, traz como conceito o uso judicioso da força, bem como a eficiente descentralização dos meios, a fim de se obter o máximo do poder de combate em pontos e locais fundamentais, empregando-se somente o mínimo necessário para outras áreas menos importantes. Relacionado a esse princípio, tem-se o Princípio da Massa, que estabelece ser necessário se obter um acúmulo de forças, a fim de se obter uma preeminência decisiva sobre o oponente, na ocasião e ponto mais favoráveis às ações almejadas. (BRASIL, 2019, p 5-2).

A Manobra é definida pela habilidade de se organizar as forças ao ponto de se colocar o oponente em desvantagem, a fim de se alcançar os objetivos que, em outra disposição das tropas, causariam maiores perdas de efetivo e material. Assim, através desse princípio, pretende-se desequilibrar a coesão do oponente, por meio de ações que venham a surpreende-lo, buscando-se, por

meio de uma pressão constante, reduzir a habilidade de reação, de eficácia e de iniciativa de suas ações. (BRASIL, 2019, p 5-2 e 5-3).

O Moral está relacionado com o estado de espírito da tropa. Esse princípio preconiza a necessidade de se estimular, motivar, o indivíduo a ter uma atitude mental positiva direcionada ao bom cumprimento de sua missão. Assim, quando reunido em grupo, esse sentimento é fortalecido, sendo mais favorável ao enfrentamento do risco, ao desenvolvimento da disciplina, ao adestramento e à liderança por parte do comandante. (BRASIL, 2019, p 5-3).

A Exploração é definido como o aumento da intensidade das atitudes ofensivas, a fim de se estender o êxito obtido nas operações, possibilitando aproveitar as oportunidades que surgirem, empregando o poder de combate na sua capacidade plena, a fim de favorecer a obtenção dos efeitos desejados ao final do conflito. (BRASIL, 2019, p 5-3).

A Prontidão consiste na capacidade de operacionalidade de uma tropa, de estar pronta para agir ou reagir de forma eficiente e eficaz perante as situações durante um conflito. Esse princípio baseia-se nos fundamentos de doutrina, organização, adestramento, meios, instrução, recursos humanos e infraestruturas, necessários para que a Força obtenha a prontidão operativa. (BRASIL, 2019, p 5-3).

A Unidade de Comando, refere-se ao fato de ser essencial que o comando, a autoridade, seja atribuída a apenas um indivíduo. De forma a se obter a concentração de esforços de maneira integrada diante do amplo espectro das operações, visando alcançar um objetivo coletivo. (BRASIL, 2019, p 5-3).

A Legitimidade, trata acerca da necessidade de que todas as ações de uma força estejam embasadas em preceitos legais e em obrigações perante a comprometimentos assumidos por um Estado, bem como em dogmas e preceitos que fundamentam a Força, a fim de se atentar para a percepção que as sociedades nacional e internacional obterão acerca do emprego da tropa em determinado conflito. (BRASIL, 2019, p 5-3).

2.2 AS CONCEPÇÕES E CONCEITOS DAS OPERAÇÕES TERRESTRES

2.2.1 O Ambiente Operacional

O espaço no qual as forças militares atuam sofre as mais diversas interferências provenientes de características do ambiente e de situações que decorrem em paralelo às operações desencadeadas. Estas características, bem como as situações que se desenvolvem em paralelo às operações, influem diretamente, também, na forma que as forças militares são empregadas. (BRASIL, 2017c, p 2-2).

O conjunto destes fatores, que influenciam o espaço de atuação das forças militares, bem como a forma como serão empregadas define o conceito de Ambiente Operacional. (BRASIL, 2017c, p 2-2).

2.2.2. As Dimensões do Ambiente Operacional

O Ambiente Operacional, conjunto de fatores e situações, ao ser analisado, pode ser dividido em três diferentes dimensões: a dimensão humana, a dimensão física e a dimensão informacional. (BRASIL, 2017c, p 2-2).

A Dimensão Física trata-se dos fatores terreno e condições meteorológicas, que interferem diretamente no planejamento e forma de emprego da F Ter em determinado ambiente, devendo, esta, desenvolver capacidades para atuar nos mais diversos terrenos dentro e fora do país e sob as condições meteorológicas preponderantes nesses ambientes. (BRASIL, 2017c, p 2-2).

A Dimensão Humana representa os fatores que envolvem as massas populacionais que compõem o ambiente operacional de atuação de uma força militar. Reúne os fatores relacionados com a política, situação econômica e psicossocial locais. (BRASIL, 2017c, p 2-2).

Neste contexto, o foco da atenção com a dimensão humana refere-se a tomar-se todas as medidas necessárias, levando em consideração todos os aspectos da dimensão humana local, a fim de se mitigar ao máximo os efeitos colaterais das operações militares desencadeadas naquela localidade. (BRASIL, 2017c, p 2-3).

A Dimensão Informacional abrange todos os meios utilizados para criar, disseminar e agir sobre o espaço informacional que abrange a localidade onde se desenvolve uma operação militar e que buscam dominar narrativas a fim de conduzir a opinião da população local conforme os interesses dos que dominam esses meios. (BRASIL, 2017c, p 2-3).

Dessa forma, a fim de corroborar com o sucesso das operações militares, é muito importante que sejam desenvolvidas ações que visem alcançar o domínio da narrativa sobre os fatos que circundam a operação militar local, a fim de se levar a opinião pública a se tornar favorável a atuação da força militar naquela localidade. (BRASIL, 2017c, p 2-3).

2.3 A METODOLOGIA DE PROCESSAMENTO DE ALVOS “D3A”

A metodologia de processamento de alvos “D3A” é descrita, quanto sua finalidade de emprego, bem como as atividades desencadeadas nas fases que compõe os seus processos, no manual ATP 3-60 – *Targeting*, do Exército dos Estados Unidos da América.

A atualização do Manual EB70-MC 10.346 – Planejamento e Coordenação de Fogos, trouxe de forma similar a sistemática de emprego dessa metodologia, adaptando-a às necessidades e características das Forças Armadas brasileiras, sendo assim, a principal fonte de consulta para a compreensão dos processos atinentes a tal método de processamento de alvos.

A metodologia “D3A”, de acordo com o descrito no Manual EB70-MC 10.346 – Planejamento e Coordenação de Fogos, consiste na reunião das capacidades de detecção de alvos, na decisão acerca de qual meio deve ser empregado para bate-lo, na coordenação com outros sistemas e na avaliação de danos sobre o alvo, essa, quando empregada de forma criteriosa e eficaz, organiza as tarefas dos processos de planejamento e execução das operações, potencializando o apoio de fogo, levando à obtenção do efeito desejado. (BRASIL, 2017b, p. 4-1).

Essa metodologia é dividida em quatro fases, Decidir, Detectar, Disparar e Avaliar, as quais são desencadeadas de forma dinâmica, permitindo que sejam atualizadas em tempo real, conforme a evolução da ações, e leva em consideração todos os aspectos necessários para o planejamento do sistema de

fogos, exigindo a coordenação de vários elementos envolvidos na operação. (BRASIL, 2017b, p. 4-1).

2.3.1 A Fase Decidir

A fase decidir consiste no estabelecer de aspectos importantes para a fase de detecção, conforme definido no manual Manual EB70-MC 10.346 – Planejamento e Coordenação de Fogos:

> Estabelece as diretrizes para o planejamento e a execução das atividades de detecção e engajamento dos alvos, sincronizando essas ações com cada fase da manobra. Dessa forma, os trabalhos posteriores podem transcorrer com maior iniciativa dos escalões subordinados. (BRASIL, 2017b, p 4-3).

Nessa fase, para auxiliar o desencadear do apoio de fogo, são confeccionados a lista de alvos altamente compensadores (LAAC), a matriz guia de ataque (MGA), as tarefas essenciais de apoio de fogo (TEAF), a matriz de execução de apoio de fogo e a lista de alvos sensíveis, restritos e proibidos. Todos esses documentos servem de guia para o planejamento e execução dos fogos durante o desencadear das operações. (BRASIL, 2017b, p 4-3).

2.3.2 A Fase Detectar

A detecção é a fase na qual se desenvolvem as atividades atinentes a busca de alvos, ou seja, os processos de levantamento de informações quanto às características e a localização do alvo, devendo ser desenvolvida de forma conjunta, desde o levantamento até o estudo dos dados coletados, e desencadeada de forma continua, nas etapas anteriores, posteriores e durante a execução dos fogos. (BRASIL, 2017b, p. 4-16).

A metodologia empregada na fase de detecção é composta pelas atividades de detecção oportuna, na qual é determinada a existência de um alvo, identificação, das características principais do alvo, localização precisa e o monitoramento dos alvos de interesse. (BRASIL, 2017b, P 4-16).

2.3.2.1 Aquisição de Alvos

A aquisição de alvos ocorre a partir da coleta e busca de dados realizada pelos mais diversos meios de levantamento, sejam eles sensores humanos ou tecnológicos. Esses dados são compartilhados com uma célula responsável pelo planejamento do apoio de fogo da operação, a fim de que alvos de interesse sejam detectados e suas características identificadas para auxiliar os processos de planejamento e execução mais precisa dos fogos. (BRASIL, 2017b, p. 4-20).

Os dados levantados são provenientes dos relatórios confeccionados ao final de atividades de reconhecimento ou incursões realizadas em território inimigo, da interceptação de mensagens inimigas, dos sistemas de artilharia de Busca de Alvos e observação, dos radares de vigilância, das ações de operações especiais, da aviação militar e dos Sistemas de Aeronaves Remotamente Pilotadas (SARP). (BRASIL, 2017b, p. 4-20).

2.3.3 A Fase Disparar

A fase dispara consiste na análise acerca de qual dos alvos identificados na fase de detecção será engajado, e, conforme as ações pretendidas, como ele será batido, respeitando as restrições e diretrizes estabelecidas na fase decidir, de forma a alinhar as atividades desencadeadas na fase do disparo com os objetivos e intenções dos escalões superiores. (BRASIL, 2017b, p. 4-25).

Durante essa fase é desencadeado um processo de análise dos alvos localizados, que consiste, basicamente, no estudo das características dos alvos, determinação do efeito pretendido, da oportunidade de desencadeamento do ataque, escolha dos meios e método para bater o alvo. (BRASIL, 2017b, p. 4-27).

2.3.4 A Fase Avaliar

A fase avaliar consiste na etapa de verificação do resultado obtido, quanto aos efeitos alcançados após o engajamento de um alvo. Essa avaliação permite inferir a possibilidade de se atingir os objetivos pretendidos e o estado final desejado, podendo-se, caso não se tenha obtido um resultado a contento do

demandado pelos escalões superiores, retornar às fases anteriores detectar e disparar. (BRASIL, 2017b, p. 4-40).

Nessa fase, a situação dos alvos após ser batido é estimada por meio da taxa de danos de batalha (TDB), que é a avaliação dos danos causados, e da taxa de efetividade das munições (TEM), que, após a estimativa dos danos causados, permite avaliar a efetividade dos sistemas e munições empregados para o engajamento do alvo. (BRASIL, 2017b, p. 4-41 a 4-42).

A TDB pode ser inferida através dos meios para a avaliação de danos, que consistem nos mesmos sensores que realizaram a aquisição, os quais, após o desencadeamento dos fogos, informam os danos causados aos alvos. Essa taxa servirá para análise por parte da célula de fogos, a fim de que ela determine ou recomende o reengajamento do alvo, caso não se tenham alcançado os danos desejados. (BRASIL, 2017b, p. 4-42 a 4-43).

2.4 O CONCEITO DE GUERRA CIBERNÉTICA

A evolução da internet, uma rede de computadores conectados a partir dos pontos mais distintos do mundo, levou ao surgimento de um combate muitas vezes silencioso, mas com danos muitas vezes catastróficos para indivíduos, empresas, exércitos e até mesmo nações inteiras.

Diante da crescente onda de ataques cibernéticos, principalmente entre nações, a exemplo da incursão da força aérea israelense que, graças a inserção de um *software* malicioso, despistou o sistema de radares de vigilância sírio e atacou suas instalações militares sem que a aeronave fosse detectada, o termo Guerra Cibernética começou a ser utilizando em larga escala para caracterizar ações ofensivas e defensivas no espaço cibernético, envolvendo sistemas de tecnologia e informação. (JÚNIOR e DE SÁ, 2020, p. 12)

Acompanhando o cenário internacional de conflitos desencadeados no ambiente cibernético, em 2008, o foi aprovada pelo Governo brasileiro, a Estratégia Nacional de Defesa, a qual desencadeou os trabalhos de desenvolvimento do setor cibernético no país, deixando a cargo da Presidência da República, a segurança cibernética, e como responsabilidade do Ministério da Defesa, por meio das Forças Armadas, a Defesa Cibernética. (BRASIL, 2017a, p. 1-2).

Definidas as responsabilidades de desenvolvimento do setor cibernético o MD publicou, em 2014, Doutrina Militar de Defesa Cibernética (MD31-M-07), a qual definiu, entre outros aspectos, que os termos Guerra e Defesa Cibernética tenham conceitos similares, diferenciando-se apenas no que diz respeito ao nível de planejamento e execução das ações cibernéticas:

> 2.1.2 No contexto do Ministério da Defesa, as ações no Espaço Cibernético deverão ter as seguintes denominações, de acordo com o nível de decisão (conforme apresentado na figura 1):
> nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;
> nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e
> níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas. (BRASIL, 2014, p. 17).

A Guerra Cibernética, por fim, bem como a Defesa Cibernética, ficou definida como o conjunto de ações defensivas e ofensivas, desencadeadas no ambiente cibernético, em prol da proteção de sistemas de informação ou no intuito de se empregar meios de tecnologia da informação para dificultar a um adversário o emprego eficaz de seus sistemas de informação, degradando-os, corrompendo-os ou destruindo-os. (BRASIL, 2017a, p. 2-2).

2.4.1 As Capacidades da Guerra Cibernética

A definição de capacidade, de acordo com o Manual EB70-MC-10.232 – Guerra Cibernética é a habilidade necessária para se cumprir determinada tarefa**:**

> 3.3.1 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, 2017a, p. 3-4).

Diante dessa definição, as habilidades da Guerra Cibernético para cumprir com as missões a ela impostas são a Proteção Cibernética, o Ataque Cibernético e a Exploração Cibernética.

A capacidade de Proteção Cibernética consiste na habilidade de deter ataques e explorações cibernéticas que venham a ser desencadeados por ameaças cibernéticas, atores com motivação e capacidade de agir no ambiente cibernético, sobre os ativos informacionais e de tecnologia da Força. Essa capacidade deve ser realizada em caráter permanente a fim de se evitar a ocorrência de situações de crise ou conflito. (BRASIL, 2017a, p. 3-4).

O Ataque Cibernético é a capacidade de destruir, negar, corromper sistemas informacionais, redes de computadores e tecnologias usadas pelo inimigo, a fim de impedir que ele use com eficácia as ferramentas e habilidades cibernéticas em prol do cumprimento de suas missões, interferindo no seu poder de combate durante as operações. (BRASIL, 2017a, p. 3-4).

A capacidade de Exploração Cibernética está voltada para o levantamento de dados em proveito da produção de conhecimento e detecção de vulnerabilidades nos sistemas informacionais e tecnológicos do inimigo. As ações devem ser discretas, evitando deixar rastros para que o inimigo não perceba que os dados levantados, através da exploração dos seus sistemas, foram obtidos. (BRASIL, 2017a, p. 3-4).

2.5 OPERAÇÕES CIBERNÉTICAS NO CIBERESPAÇO

O C*iberespaço* é um ambiente de informação que é formado por redes interdependentes de tecnologia da informação e dados, redes de telecomunicações, sistemas de computador, bem como por processadores e controladores incorporados. (EUA, 2021, p 1-5).

As Operações Cibernéticas consistem no o uso de links e nós localizados em domínios físicos para realizar ações lógicas, ações cibernéticas, que causam efeitos no domínio alvo, ou seja, o uso de ferramentas ou programas de

computadores, com objetivo de criar efeitos dentro ou fora do ciberespaço. (EUA, 2021, p 2-1).

Essas ações, dessa forma, tornam-se essenciais para as operações militares, tendo em vista que o *ciberespaço* é um meio através do qual uma grande quantidade de dados e informações, resultante do uso de sistemas de comunicações, redes de computadores, sistemas de celulares, bem como redes e mídias sociais, podem ser obtidos do oponente ou até mesmo negados a ele. (EUA, 2021, p 1-5).

A principal função das Operações Cibernéticas é degradar, neutralizar, interromper e destruir as capacidades cibernéticas e informacionais do inimigo, de forma que as consequências de tais operações venham até mesmo a transcender o ciberespaço, resultando em efeitos que podem impactar o ambiente físico do inimigo. (EUA, 2021, p 1-15).

As operações cibernéticas podem atuar em sincronia com outras capacidades militares a fim de alcançar objetivos almejados pela Força, provendo aos comandantes informações que podem coloca-los em vantagem em relação às forças inimigas, gerando efeitos além do ciberespaço. (EUA, 2021, p 2-1).

2.5.1 Ações Cibernéticas

As Ações Cibernéticas consistem no emprego de uma ou mais tarefas especificas em conjunto com as capacidades cibernéticas, podendo ser divididas em quatro ações: Segurança, Defesa, Exploração e Ataque Cibernético. . (EUA, 2021, p 2-5)

2.5.1.1 Segurança Cibernética

A ação de Segurança Cibernética consiste na proteção do ciberespaço a fim de coibir acessos não autorizados direcionados para explorar ou degradar computadores, sistemas de comunicação, entre outros meios de tecnologia da informação, assim como as informações neles contidas, evitando que a avaliação, integridade, autenticação, confidencialidade e não repúdio destas informações, sejam afetados. . (EUA, 2021, p 2-6).

Algumas das ações relacionadas à segurança cibernética são: a criptografia de dispositivos de armazenamento de dados, a educação de recursos humanos quanto a medidas de segurança da informação, o gerenciamento de senhas, atualização e correção de *softwares*, bem como a restrição de acesso a *websites* suspeitos. (EUA, 2021, p 2-6).

2.5.1.2 Exploração Cibernética

A Exploração Cibernética consiste em ações desencadeadas no ambiente cibernético a fim de se obter inteligência, coleta de informações ou se obter dados necessários a fim de se apoiar futuras operações militares, visando buscar vantagens táticas e operacionais em relação ao oponente.

Estas ações são desenvolvidas dentro do ambiente cibernético inimigo com o propósito de se adquirir e manter o acesso a redes e sistemas de valor militar, sem que o inimigo desconfie que estas ações estejam sendo desencadeadas dentro do seu ciberespaço. (EUA, 2021, p 2-7).

2.5.1.3 Ataque Cibernético

O ataque cibernético consiste em ações desencadeadas no espaço cibernético a fim de gerar efeitos de negação de serviço, seja degradando, perturbando ou destruindo os sistemas de tecnologia de informação do inimigo. (EUA, 2021, p 2-7).

Estas ações produzem efeitos através do espaço cibernético podendo acarretar, até mesmo, resultados físicos sobre os ativos materiais e humanos do inimigo, modificando ou destruindo as capacidades cibernéticas inimigas que controlam ações no ambiente físico. (EUA, 2021, p 2-7).

Entre as ações mais comuns resultantes de um ataque cibernético estão a Negação de Serviço, a Degradação de Serviços, a Perturbação de Serviços, a Destruição e a Manipulação. (EUA, 2021, p 2-7).

A Negação de Serviços consiste em impedir o acesso e desencadeamento de operações no ambiente cibernético pelo oponente, negando-lhe a possibilidade de acessar seu ciberespaço, afetando os softwares e hardwares dos seus sistemas de tecnologia da informação por um período específico de tempo. (EUA, 2021, p 2-7).

A Degradação de Serviços consiste em ações que visam negar o serviço de sistemas de tecnologia da informação do oponente, através da degradação dos seus meios de Tecnologia da Informação, impossibilitando que utilizem as suas capacidades cibernéticas em prol de suas operações. (EUA, 2021, p 2-7).

A Perturbação de Serviços de Sistemas de Tecnologia da Informação do oponente consiste em atrapalhar o uso de seus meios de Tecnologia da Informação em parte, por um período de tempo determinando. Assemelha-se a Degradação de Serviços, mas enquanto a Degradação trata-se de uma interrupção em totalidade dos sistemas de TI do inimigo, a Perturbação gera efeitos apenas em parte. (EUA, 2021, p 2-7).

A Destruição de Sistemas de Tecnologia da Informação consiste em negar completamente e definitivamente o acesso do inimigo a seus meios de tecnologia da informação, maximizando o tempo que o oponente terá os serviços de seus sistemas de TI negados, bem como reduzindo a quantidade de meios disponíveis. (EUA, 2021, p 2-7).

Estas ações de destruição podem, inclusive, impor ao inimigo a interrupção definitiva dos seus sistemas computacionais, *hardwares*, *softwares* e redes, gerando perda de dados e informações que podem ser irreversíveis, reduzindo as suas capacidades cibernéticas para atuarem no ciberespaço. (EUA, 2021, p 2-7).

A Manipulação de Sistemas de Tecnologia da Informação consiste em uma forma de ataque, controle ou adulterações implementadas em informações, sistemas de informação e redes, que visão gerar efeitos no ambiente físico do inimigo, por meio, principalmente, da falsificação de dados e informações, entre outras técnicas similares. (EUA, 2021, p 2-7).

Estas ações buscam utilizar informações do adversário a fim de manipular dados e informações contidas nos sistemas informacionais e de tecnologia do oponente, buscando alcançar efeitos que resultem em danos no ambiente físico do inimigo. (EUA, 2021, p 2-7).

3. METODOLOGIA

3.1 OBJETO FORMAL DE ESTUDO

A presente pesquisa terá como objeto de estudo as capacidades da Guerra Cibernética em proveito da metodologia de processamento de alvos “D3A” na fase de detecção, caracterizando-se como exploratória do tipo observacional analítica, levando em consideração a necessidade de emprego dessas capacidades em prol da proteção dos meios de aquisição de alvos, ataque e exploração dos meios informacionais do inimigo, empregados na aquisição de alvos.

A variável independente consiste nos processos de aquisição de alvos da fase de detecção da metodologia “D3A”, enquanto as variáveis dependentes são as capacidades de ataque, exploração e proteção da Guerra Cibernética.

A fim de se alcançar o objetivo principal desse trabalho, será realizado um levantamento, em trabalhos científicos e manuais militares nacionais e de exércitos estrangeiros, a cerca de metodologias de emprego de capacidades cibernéticas em prol de processos e tecnologias de detecção e aquisição de alvos.

3.2 DELINEAMENTO DA PESQUISA

O estudo da presente pesquisa será do tipo exploratório com uso do método de abordagem dedutivo e do método de procedimentos comparativo, tendo em vista que serão realizadas consultas em trabalhos científicos, bem como em manuais militares nacionais e internacionais a fim de se chegar ao ponto de conclusão do trabalho sobre como as capacidades da Guerra Cibernética podem atuar em proveito da metodologia “D3A” na fase detectar.

Os procedimentos, bem como a sequência das ações desencadeadas para o levantamento dos dados da pesquisa, tiveram como ponto de partida a realização de uma pesquisa nas bibliografias das Forças Armadas a fim de se coletar informações já existentes acerca de metodologia de processamento e aquisição de alvos e de doutrinas de emprego de capacidades cibernéticas.

Posteriormente, essa pesquisa foi estendida a bibliografia das Forças Armadas dos Estados unidos da América e da Argentina, sendo seguida buscas

e levantamento de dados em trabalhos científicos por ocasião da conclusão de cursos de escolas militares e instituições de ensino civis.

O critério de inclusão e exclusão serão o ano de realização da pesquisa, nos últimos cinco anos, no caso de fontes provenientes de trabalhos científicos e a vigência e aplicabilidade, no caso de fontes advindas de bibliografia das forças armadas e de forças armadas estrangeiras, verificando se as doutrinas militares, relacionadas ao objeto de estudo da presente pesquisa, ainda estão vigentes e são eficientemente aplicáveis.

3.3 AMOSTRA

A amostra da presente pesquisa serão as Organizações Militares, grupos e seções do exército brasileiro e de exércitos estrangeiros que utilizam meios tecnológicos para a aquisição de alvos e que, preferencialmente, façam uso de metodologias de processamento de alvos semelhante a metodologia “D3A”.

3.4 PROCEDIMENTOS PARA A REVISÃO DA LITERATURA

Os procedimentos atinentes a revisão da literatura foram serão voltados para a realização de pesquisas em sites das Forças Armadas e em sites de exércitos estrangeiros, bem como em repositórios de trabalhos científicos de escolas militares, realizados pelos cursos da Academia Militar das Agulhas Negras, da Escola de Aperfeiçoamento de Oficiais, da Escola de Comando e Estado Maior do Exército e da Escola de Guerra Naval.

3.5 INSTRUMENTOS

A presente pesquisa será empregada como instrumento de pesquisa a consulta documental, bem como a análise dos conteúdos consultados, a fim de se realizar a coleta de dados que venham a consubstanciar o emprego de capacidades cibernéticas e de meios tecnológicos na aquisição de alvos, bem como a integração desses meios.

3.6 ANÁLISE DOS DADOS

A análise dos dados, após a fase de coleta realizada em manuais e trabalhos científicos, será direcionada para a verificação da atualidade e vigência das doutrinas expostas nas bibliografias militares consultadas, bem como na aplicabilidade das metodologias levantadas a partir dos trabalhos científicos pesquisados.

4. RESULTADOS

O presente capítulo tem por finalidade apresentar os resultados obtidos após realizada a revisão de literaturas que trazem conteúdos acerca dos assuntos discutidos neste trabalho, a fim de embasar a discussão dos resultados, bem como a conclusão e considerações finais, em busca de se alcançar uma solução para o problema apresentado nesta pesquisa.

4.1 A METODOLOGIA DE PROCESSAMENTO DE ALVOS D3A.

A Metodologia de Processamento de Alvos D3A, resume-se em procedimentos que visam organizar as ações necessárias para o a identificação dos alvos mais importantes, por meio da detecção, e sua posterior avaliação e engajamento, como resultado de uma atuação sincronizadas das funções de combate. (BRASIL, 2017b, p 4-1).

4.2 A FASE DETECTAR DA METODOLOGIA DE PROCESSAMENTO DE ALVOS D3A.

Na fase detectar da Metodologia de Processamento de Alvos D3A, atua-se com esforços em proveito da busca de alvos, visando determinar a existência de um alvo, por meio da detecção oportuna, e reunir o máximo de informações acerca dos mesmos, por meio da identificação, como a localização, a natureza, composição, dimensões, bem como outras características necessárias para a avaliação e engajamento dos alvos. (BRASIL, 2017b, p 4-15).

Nessa fase, verifica-se que são empregados, como meios de aquisição de alvos, isoladamente ou em conjunto com fontes humanas, relatórios de tropas amigas, interceptação de mensagens inimigas, meios tecnológicos de busca e coleta de dados sobre alvos, em prol de se verificar a existência, determinar a localização, as características, bem como realizar o monitoramento dos mesmos. (BRASIL, 2017b, p 4-20).

4.3 A GUERRA CIBERNÉTICA

A Guerra Cibernética atua com ações ofensivas e defensivas a fim de proteger os ativos de informação da Força, bem como negar ao oponente o uso de suas capacidades cibernéticas, dificultando a exploração cibernética, a aquisição de dados e informações acerca das tropas amigas, bem como mitigando que os ataques cibernéticos desencadeados contra os sistemas de comando e controle aliados. (BRASIL, 2017a, p 2-5).

A fim de cumprir com sua finalidade, a Guerra Cibernética atua com três capacidades básicas, o Ataque Cibernético, a Exploração Cibernética e a Proteção Cibernética. (BRASIL, 2017a, p 3-4).

Essas capacidades são desenvolvidas isoladamente ou em paralelo e atuam dentro do espectro de todos os tipos de operações, sejam elas, operações combinadas, ofensivas, defensivas ou de cooperação e coordenação com agências, permeando todas as funções de combate e trabalhando em prol de alcançar os objetivos da Força no âmbito não cinético dos conflitos militares. (BRASIL, 2017a, p 3-4).

4.4 A GUERRA CIBERNÉTICA E A FUNÇÃO DE COMBATE FOGOS.

A Guerra Cibernética pode atuar em conjunto com a Função de Combate Fogos, inserindo-se no contexto de aplicação da Metodologia de Processamento de Alvos D3A, atuando no espectro dos fogos não cinéticos em proveito dos objetivos almejados pelo F Cmb Fogos, podendo ser desencadeados como uma ação simultânea que vise gerar um efeito específico sobre um determinado alvo, gerando um efeito que reflita no âmbito do espaço cibernético ou no ambiente físico do oponente. (EUA, 2021, p 1-15).

A fim de se estabelecerem objetivos a serem alcançados pelas capacidades cibernéticas, deve ser elaborada uma lista de alvos cibernéticos com base na análise de Guerra Cibernética, que realiza um levantamento dos possíveis alvos para as ações de exploração e ataque, incluindo alvos que sejam de interesse da F Cmb F, tanto para o desencadeamento de um ataque por fogos não cinéticos quanto para o levantamento das características, localização e outros dados de interesse, sobre um determinado alvo. (BRASIL, 2017a, p 4-6).

5. DISCUSSÃO DOS RESULTADOS

O presente capítulo tem por finalidade discutir os resultados obtidos por meio da revisão de literaturas que trazem conteúdos acerca dos assuntos discutidos neste trabalho, visando embasar a conclusão e as considerações finais, em busca de se alcançar uma solução para o problema apresentado na presente pesquisa.

5.1 A METODOLOGIA DE PROCESSAMENTO DE ALVOS D3A.

Realizada uma análise nas fontes de referência acerca do assunto, verificou-se que no âmbito da Metodologia de Processamento de Alvos, tem-se o emprego de meios tecnológicos, como o uso de Sistemas de Aeronaves Remotamente Pilotados e de radares, de contrabateria e vigilância, como meios de busca e detecção de alvos. (BRASIL, 2017b, p 4-20).

Diante disso, se por um lado tem-se um aumento na precisão, eficiência e efetividade na detecção e levantamento das características e localização de alvos, por outro, o emprego dessas tecnologias pode representar um ambiente a ser explorado por forças adversas, a fim de se levantar possíveis vulnerabilidades que tais meios venham a apresentar. (BRASIL, 2017b, p 4-20).

5.2 A FASE DETECTAR DA METODOLOGIA DE PROCESSAMENTO DE ALVOS D3A.

O levantamento feito nas fontes bibliográficas mostrou que os principais meios tecnológicos utilizados para a aquisição de alvos nessa fase, podem apresentar vulnerabilidades, as quais podem vir a ser exploradas pelas forças inimigas, visando desencadear ações cibernéticas, negando, degradando, destruindo ou manipulando os meios de busca de alvos da Força. (BRASIL, 2017b, p 4-20).

Diante disso, as capacidades Guerra Cibernética podem, por meio da proteção cibernética, ser empregadas em conjunto com outros meios tecnológicos de aquisição, a fim de protege-los, por meio de ações cibernéticas, de possíveis ataques e explorações desencadeadas por forças inimigas no ambiente cibernético da Força. (BRASIL, 2017a, p 4-3).

Além da proteção cibernética, as ações desencadeadas pela exploração, podem ser direcionadas para a busca de alvos, de forma que essa capacidade venha a ser empregada como meio de aquisição de alvos, buscando ou coletando dados no ambiente cibernético inimigo, acerca da natureza, características, importância e localização de um alvo específico. (BRASIL, 2017a, p 4-3).

5.3 AS CAPACIDADES DA GUERRA CIBERNÉTICA

O estudo realizado permitiu verificar como as capacidades cibernéticas atuam em proveito da obtenção do efeito final desejado pelo Comandante da Força nas operações militares, bem como, ao serem empregados como atuadores não cinéticos, os efeitos gerados sobre a tropa inimiga. (BRASIL, 2017a, p 3-4).

O Ataque Cibernético consiste no emprego de programas, softwares, códigos de computador, que podem ser disseminados sobre os sistemas informacionais inimigo por meio de espectro eletromagnéticos ou por meio de dispositivos de rede, e, até mesmo empregados em ataques direcionados aos sistemas de armas de um adversário, dependendo das características de funcionamento destes sistemas. (BRASIL, 2017a, p 3-4).

O Ataque Cibernético pode atuar em conjunto com o Ataque Eletrônico quando o objetivo for atingir sistemas que se utilizam do espectro eletromagnético para a transmissão de voz e dados. Nesse contexto, cresce de importância o trabalho conjunto com capacidades que atuam no levantamento de informações e características de possíveis alvos cibernéticos, a exemplo disso, as capacidades da Função de Combate Inteligência. (EUA, 2021, p 1-15).

A Exploração Cibernética resume-se a ações ligadas a atividade de inteligência. A sua atuação tem como foco o levantamento de dados sobre o inimigo, seus sistemas de informação, de comando e controle e detectar possíveis alvos cibernéticos ou de artilharia, bem como levantar as suas características e localização, de forma a abastecer todas as Funções de Combate que possam se beneficiar dos dados e informações obtidas pelas ações de exploração. (BRASIL, 2017a, p 4-2).

A maior diferença entre esta capacidade e o Ataque Cibernético é que a Exploração Cibernética preza pela discrição em suas ações, de forma a evitar

que o oponente identifique que uma ação cibernética está sendo desencadeada no seu ciberespaço, de forma que as ações se tornem uma oportunidade para que o adversário rastreie a origem do ataque e obtenha informações suficientes para desencadear atividades de proteção, exploração ou ataque cibernético contra os ativos da tropa amiga. (EUA, 2021, p 1-15).

A Proteção Cibernética tem como foco mitigar que ações de exploração e ataque cibernético sejam desencadeados sobre o sistema de informações, de comando e controle, e demais ativos de tecnologia da informação da Força, incluindo como atividades de proteção a detecção, identificação e resposta a uma possível ação cibernética adversária. (BRASIL, 2017a, p 4-3).

A forma de atuação para proteger os ativos de tecnologia da Força, consiste em empregar o conceito de multicamadas de proteção, evitando, no caso de se detectar uma ação cibernética oponente, que o sistema alvo seja comprometido por complete antes que seja possível atuar em resposta ao ataque ou exploração desencadeada pelo inimigo no ciberespaço no qual atua a Força. (EUA, 2021, p 2-6).

5.4 A GUERRA CIBERNÉTICA E A FUNÇÃO DE COMBATE FOGOS

O Ataque Cibernético, atuando como atuador não cinético, em conjunto com a Função de Combate Fogos, é desencadeado a fim de atingir um determinado alvo, causando-lhe danos inclusive no ambiente físico, também são uma alternativa para a neutralização de um alvo localizado no interior de uma localidade, na qual se quer causar o mínimo de efeitos colaterais decorrentes do engajamento do mesmo. (EUA, 2021, p 1-15).

A Exploração Cibernética, por sua vez, pode atuar em proveito da aquisição de alvos, como meio de aquisição, buscando e coletando dados no ambiente cibernético inimigo, a fim de levantar, confirmar ou complementar conhecimentos provenientes de outras fontes, fornecendo as informações necessárias para consubstanciar as análises e a decisão acerca de alvos compensadores para o desencadeamento de fogos de artilharia. (BRASIL, 2017a, p 4-6).

6. CONCLUSÃO

Conforme a pesquisa realizada, constatou-se que não há uma proposta de integração entre as capacidades da Guerra Cibernética e a Metodologia de Processamento de Alvos “D3A” que vise direcionar a atuação de tais capacidades com as fases de tal metodologia, principalmente nas que empregam meios tecnológicos, como na fase detectar, por ocasião das ações de aquisição de alvos.

Verificou-se que as Capacidades da Guerra Cibernética são o Ataque Cibernético, a Exploração Cibernética e a Proteção Cibernética, e que estas atuam com a finalidade de degradar sistemas de informação e levantamento de dados do oponente, levantar dados de interesse para Força, a partir da exploração destes sistemas do adversário, bem como atuar na proteção dos sistemas de informação e levantamento de dados da tropa amiga.

Assim, diante dos dados levantados na presente pesquisa, propõem-se que a Capacidade de Ataque Cibernético atue a fim de degradar radares, SARP e meios tecnológicos de Busca de Alvos do inimigo, bem como negar o uso, pelo oponente, dos seus sistemas de fogos e de aquisição de alvos.

A Capacidade de Exploração Cibernética poderá ser empregada para levantar, dentro do espaço cibernético inimigo, dados, informações e características de alvos de interesse da Força, a fim de alimentar os seus sistemas de aquisição de alvos e fogos.

A Por fim, a Proteção Cibernética, poderá atuar com medidas para proteger os meios tecnológicos empregados na Aquisição de Alvos, os radares, SARP, e meios de Busca de Alvos da tropa amiga, mitigando as ações desencadeadas de ataque e exploração cibernética do oponente.

Por fim, o presente trabalho teve como finalidade estabelecer uma integração, uma proposta de foco, para a atuação das capacidades da Guerra Cibernética em prol da Metodologia de Processamento de Alvos “D3A”, não tendo como objetivo abranger os aspectos técnicos, a forma como serão desencadeadas as ações das capacidades de Guerra Cibernética, deixando esta temática voltada para o nível técnico como sugestão para a elaboração de trabalhos futuros.

REFERÊNCIAS BIBLIOGRÁFICAS

ARGENTINA. Exército Argentino. ROP-03-54 – **Adquisición de Blancos de la Artillería de Campaña**. 1ª. Ed. Buenos Aires, 2019.

BRASIL. Exército Brasileiro. **EB70-MC-10.232 – Guerra Cibernética.** 1ª. Ed. Brasília, DF, 2017a.

BRASIL. Exército Brasileiro. **EB70-MC-10.346 – Planejamento e Coordenação de Fogos.** 3ª. Ed. Brasília, DF, 2017b.

BRASIL. Exército Brasileiro. **EB70-MC-10.223 – Operações.** 5ª. Ed. Brasília, DF, 2017c.

BRASIL. Ministério da Defesa. **MD31-M-07 – Doutrina Militar de Defesa Cibernética.** 1ª. Ed. Brasília, DF, 2014.

BRASIL. Exército Brasileiro. **EB20-MF-10.102 – Doutrina Militar Terrestre.** 2ª. Ed. Brasília, DF, 2019.

DAMIÃO, ANDRÉ KOHLER. **Guerra Cibernética: Proteção Cibernética, Monitoramento de Redes e Sistemas e Levantamento de Vulnerabilidades.** 2018. Escola de Comando e Estado Maior do Exército, ECME, Rio de Janeiro, 2018.

DE CARVALHO, HAROLDO HEITOR. **A estrutura de Guerra Cibernética necessária para a proteção do centro de operações da Brigada de Artilharia Antiaérea: bases de uma proposta.** 2015. Escola de Comando e Estado Maior do Exército, ECME, Rio de Janeiro, 2015.

DE OLIVEIRA LOPES, LEONARDO. **A Defesa Cibernética na Seção de Mísseis IGLA.** 2014. Escola de Artilharia de Costa e Antiaérea, Rio de Janeiro, 2014.

EUA. Headquarters, Department of the Army. **FM 3-12 – Cyberspace Operations and Electromagnetic Warfare.** 2ª. Ed. Washington, DC, 2021.

EUA. Headquarters, Department of the Army**. ATP 3-09.12 – Field Artillery Target Acquisition.** 2ª. Ed. Washington, DC, 2015a.

EUA. Headquarters, Department of the Army. **ATP 3-60 – Targeting.** 2ª. Ed. Washington, DC, 2015b.

EUA. Headquarters, Department of the Army. **ATP 3-12.3 – Electronic Warfare Techniques.** 2ª. Ed. Washington, DC, 2019.

JUNIOR, Walmor C. L.; DE SÁ, Alan Oliveira. **Triggering Cyber-Electronic Attacks in Naval Radar Systems. 2020**. IMEKO TC-19 International Workshop on Metrology for the Sea, Napoles, Italy, p. 12 a 16, Outubro, 2020.

NEVES, Eduardo Borba; DOMINGUES, Clayton Amaral. **Manual de metodologia da pesquisa científica**. Rio de Janeiro: EB/CEP, 2007.

RODRIGUES, RODRIGO FALCI. **Possibilidades e limitações do emprego do SARP HÓRUS FT-100 na busca de alvos em operações de Garantia da Lei e da Ordem.** 2020. Escola de Aperfeiçoamento de Oficiais, ESAO, Rio de Janeiro, 2020.

SEGUNDO, CLÉCIO BORGES TAQUARY. **A Defesa Cibernética em ambientes de Infraestrutura Crítica e os riscos dos ataques cibernéticos.** 2019. Escola Superior de Guerra, ESG, Brasília, 2019.

SINGER, P. W.; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know,** Oxford University Press (UK), 2014.

VIEIRA, THIAGO P. DE BRITO. **On The Subspace Learning for Network Attack Detection.** 2013. 97 f. Tese (Doutorado) – Universidade de Brasília, UNB, Brasília, 2019.

APÊNDICE A

CAPITULO V
DETECTAR

5.4 MEIOS DE AQUISIÇÃO DE ALVOS

5.4.21 A GUERRA CIBERNÉTICA COMO MEIO DE AQUISIÇÃO DE ALVOS

5.4.21.1 O CONCEITO DE GUERRA CIBERNÉTICA

5.4.21.1.1 A Guerra Cibernética consiste no uso ofensivo e defensivo de informação e sistemas de informação a fim de negar as capacidades de Comando e Controle do inimigo, explorá-las, corrompê-las, degradá-las ou destruí-las.

5.4.21.1.2 Corresponde a ações que envolvem ferramentas de Tecnologia da Informação e Comunicações (TIC), visando desestabilizar ou tirar proveito dos sistemas de informação do oponente, defendendo os Sistemas de Informação próprios.

5.4.21.2 AS CAPACIDADES OPERATIVAS DA GUERRA CIBERNÉTICA

5.4.21.2.1 As capacidades operativas do Sistema de Guerra Cibernética são o Ataque Cibernético, a Exploração Cibernética e a Proteção Cibernética.

5.4.21.2.2 O Ataque Cibernético trata-se da capacidade de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos de redes de computadores e de comunicações do oponente.

5.4.21.2.3 A Exploração Cibernética consiste na capacidade 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.

5.4.21.2.4 A Proteção Cibernética consiste na capacidade de conduzir ações, por meio da detecção, identificação e resposta, a fim de 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. Trata-se de uma atividade de caráter permanente.

5.4.21.3 AS CAPACIDADES OPERATIVAS DA GUERRA CIBERNÉTICA COMO MEIO DE AQUISIÇÃO DE ALVOS

5.4.21.3.1 O emprego de meios tecnológicos na aquisição de alvos, como os radares de contrabateria e vigilância e os sistemas de aeronaves remotamente pilotadas (SARP), exige a atuação das capacidades operativas da Guerra Cibernética a fim de proteger os meios de aquisição de alvos da nossa Força, atacar os meios tecnológicos do oponente, empregados na busca de alvos, bem como explorar tais meios, a fim de se obter dados para a consubstanciar as atividades desenvolvidas nas demais fases da Metodologia de Processamento de Alvos D3A.

5.4.21.3.2 A capacidade que será empregada como meio de aquisição de alvos será a Exploração Cibernética, a qual atuará conduzindo atividades de busca ou coleta nos Sistemas de Tecnologia da Informação e Comunicações (TIC) e meios de Busca de Alvos do oponente, a fim de obter, entre outros, dados acerca da natureza, capacidades e localização de alvos de interesse para as nossas Forças, tomando todos os cuidados para que essas ações não sejam rastreadas pelo inimigo.

5.4.21.3.3 A capacidade Proteção Cibernética, por ser uma atividade permanente, também atuará nessa fase, neutralizando ataques e explorações cibernética conduzidas pelo oponente contra os nossos dispositivos computacionais, redes de computadores e de comunicações, e meios tecnológicos empregados na aquisição de alvos, com ações de guerra cibernética, face a situações de crise ou conflito, bem como com procedimentos e políticas de Segurança da Informação, visando mitigar possíveis vulnerabilidades dos nossos sistemas que possam vir a ser exploradas pelas forças inimigas.

APÊNDICE B

CAPITULO VI
DISPARAR

6.3 MEIOS ATUADORES

6.3.8 O CONCEITO DE GUERRA CIBERNÉTICA

6.3.8.1 A Guerra Cibernética consiste no uso ofensivo e defensivo de informação e sistemas de informação a fim de negar as capacidades de Comando e Controle do inimigo, explorá-las, corrompê-las, degradá-las ou destruí-las, tendo como capacidades operativas, já definidas no CAPÍTULO V, o Ataque Cibernético, a Exploração Cibernética e a Proteção Cibernética.

6.3.8.2 AS CAPACIDADES OPERATIVAS DA GUERRA CIBERNÉTICA EMPREGADAS COMO MEIOS ATUADORES

6.3.8.2.1 Nessa fase, a capacidade que será empregada como meio atuador será o Ataque Cibernético, com a finalidade de interromper, negar, degradar, corromper ou destruir sistemas de informação, de radares de contrabateria e vigilância inimigos, equipamentos de localização pelo som, SARP, bem como outros sistemas com capacidade de levantar dados e causar danos em ativos da nossa Força, agindo como meio atuador não cinético, com capacidade para causar, inclusive, danos físicos resultantes de ações desencadeadas no ambiente cibernético das forças inimigas.

6.3.8.2.2 A capacidade Proteção Cibernética, por ser uma atividade permanente, também atuará nessa fase, neutralizando ataques e explorações cibernética conduzidas pelo oponente contra os nossos dispositivos computacionais, redes de computadores e de comunicações, e meios tecnológicos empregados na aquisição de alvos, com ações de guerra cibernética, face a situações de crise ou conflito, bem como com procedimentos e políticas de Segurança da Informação, visando mitigar possíveis vulnerabilidades dos nossos sistemas que possam vir a ser exploradas pelas forças inimigas.

_____
LUCAS MENUCI DE BRUM
Capitão de Artilharia