ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM PEDRO HENRIQUE DE OLIVEIRA SOUSA

ANÁLISE DO DESENVOLVIMENTO DE CAPACIDADES EM OPERAÇÕES CIBERNÉTICAS OFENSIVAS

Rio de Janeiro
2018

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM PEDRO HENRIQUE DE OLIVEIRA SOUSA

ANÁLISE DO DESENVOLVIMENTO DE CAPACIDADES EM OPERAÇÕES CIBERNÉTICAS OFENSIVAS

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

Rio de Janeiro
2018

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

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Com PEDRO HENRIQUE DE OLIVEIRA SOUSA**

Título: **ANÁLISE DO DESENVOLVIMENTO DE CAPACIDADES EM OPERAÇÕES CIBERNÉTICAS OFENSIVA**

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

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **DARDANO DO NASCIMENTO MOTA - Maj** Cmt Curso e Presidente da Comissão	
_____ **JULIANO BRANDÃO PALÁCIOS - Maj** 1º Membro	
_____ **CÉZAR FLORES MALHADA JÚNIOR - Cap** 2º Membro e Orientador	

_____
PEDRO HENRIQUE DE OLIVEIRA SOUSA – Cap
Aluno

1 INTRODUÇÃO

A Cibernética no Exército Brasileiro tem seu azimute apresentado pelo Catálogo de Capacidades, documento no qual o Exército norteia doutrina, estratégia e planejamento para cumprir seus objetivos quanto a contraposição de ameaças no amplo espectro dos conflitos. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2015)

Neste processo, novas capacidades são adquiridas e as existentes aperfeiçoadas, possibilitando a esta Força Armada atuar e dissuadir, de maneira gradativa e proporcional, a um problema militar, contribuindo para atender as demandas de segurança e defesa do País. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2015)

A Capacidade Militar Terrestre de Cibernética (CMT 09) é a reunião das Capacidades Operativas Exploração Cibernética (CO36), Proteção Cibernética (CO37) e Ataque Cibernético (CO38), nos quais tornam o Exército apto a cumprir suas missões obtendo um efeito estratégico, operacional ou tático. A capacidade operativa é obtida pela constatação de sete fatores indissociáveis conhecidos pelo DOAMEPI, cujo nome é o acrônimo para Doutrina, Organização, Adestramento, Material, Educação, Pessoal e Infraestrutura. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2015)

Das definições da Capacidade Militar Terrestre e das Capacidades Operativas surgem as atividades e tarefas, que permeiam o nível estratégico, operacional e tático, traduzindo-se nas ações de Guerra Cibernética a serem desempenhadas por uma tropa especializada na realização de uma determinada operação.

As ações de guerra cibernética têm como algumas de suas características a insegurança latente, a mutabilidade, a dualidade e a assimetria. Desta maneira, pode-se afirmar que nenhum sistema informatizado é 100% seguro, ou seja, fatores, condições e comportamentos podem ser alterados em função do tempo e pequenos elementos podem causar tanto impacto quanto grandes componentes. Afirma-se também que técnicas e ferramentas podem ser usadas tanto para proteção quanto para ataque. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2017)

Estas ações são divididas em proteção, exploração e ataque. A primeira visando a salvaguarda de seus sistemas, a segunda, com o objetivo de prover a inteligência oriunda da fonte cibernética; e a terceira, pretendendo obter efeitos em ativos de informação; sendo elas distribuídas nos níveis políticos, estratégicos, operacionais e táticos. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2017)

Especificamente nas atividades de ataque, as capacidades são descritas pelos verbos de interrupção, degradação, negação, corrupção de dados (corromper) e destruição de informações ou sistemas. Para essa atividade, são elencadas as tarefas, também chamada de fases, que norteiam como se devem chegar as capacidades descritas acima, são elas o reconhecimento, a investigação de informações por meio de fontes abertas; o escaneamento, que trata-se da descoberta de falhas; a exploração da vulnerabilidade, que se resume a obter acesso ou negar acesso a informações; a manutenção do acesso, que como o nome sugere é a manutenção da tarefa anterior e a cobertura de rastros, que é a ocultação de suas ações. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2017)

1.1 PROBLEMA

A situação-problema reside nas tarefas de escaneamento e exploração de vulnerabilidades. Para que essas tarefas sejam realizadas e consequentemente, uma operação seja bem-sucedida, faz-se necessário, em geral, o desenvolvimento de capacidades que o nível tático e operacional só descobrirão na fase de escaneamento.

Podemos citar como exemplo, uma tentativa de interromper um sistema computacional de infraestrutura crítica, ao realizar o reconhecimento e posteriormente o escaneamento, um determinado destacamento cibernético descobre que necessita desenvolver a capacidade em sistemas de automação industrial. Assim sendo, a próxima fase da atividade, que seria a exploração de vulnerabilidades, fica comprometida ao necessitar que se estude toda uma nova área de conhecimento específico, voltado para a compreensão sobre a forma de comando e controle das atividades automatizadas de uma infraestrutura crítica gerenciada por um sistema informatizado de automação industrial. A partir deste momento, este destacamento deve buscar meios para prosseguir no cumprimento de sua missão. Cabe ressaltar ainda que qualquer operação cibernética tem premissa de tempo, ou seja, o desenvolvimento desta capacidade deve ocorrer no momento em que se encontrou a vulnerabilidade ou deve-se pelo menos ter um mínimo preparo anterior para o que vai se encontrar.

Desta forma, este trabalho buscará responder o questionamento: **Quais são as capacidades específicas necessárias à realização das operações cibernéticas ofensivas?**

1.2 OBJETIVOS

O presente artigo tem como objetivo descrever as metodologias e os tipos de ataques cibernéticos e analisar o desenvolvimento de capacidades em operações cibernéticas ofensivas.

Para viabilizar a consecução do objetivo geral de estudo, foram formulados os seguintes objetivos específicos:

a) Apresentar a metodologia das capacidades utilizadas pelo Exército Brasileiro;
b) Discutir os tipos de ataques cibernéticos sobre a perspectiva do planejamento baseado em capacidades (PBC) do Exército Brasileiro; e
c) Analisar o desenvolvimento de capacidades em operações cibernéticas ofensivas quanto aos tipos que ataques cibernéticos.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

O Centro de Defesa Cibernética (CDCiber) nos anos de 2016 e 2017 deparou-se, tanto em operações quanto em eventos nos quais eram debatidos assuntos na área, em diversas ocasiões, esta demanda sugerida por equipes técnicas que, ao se deparar com problemas semelhantes, verificavam que não possuíam as capacidades desejáveis para a continuação do objetivo.

Ao verificar, por meio de pesquisas bibliográficas e documentais, muitas literaturas costumam mencionar as fases, as metodologias e os tipos de ataques cibernéticos, contudo, não se percebe que existem capacidades específicas voltadas para objetivos nos diversos níveis, que um destacamento cibernético pode necessitar.

Ventre (2011) corrobora a necessidade do desenvolvimento de capacidades específicas ao afirmar em sua obra que a probabilidade de ataques de grande porte voltados a nações, utilizando-se a premissa da surpresa e da guerra da informação, depende dos equipamentos (hardwares), dos programas (softwares) e do desenvolvimento das capacidades nas ferramentas, técnicas e táticas para surtirem o efeito desejado. Ventre (2011) afirma também que quanto mais avançada é a capacidade ofensiva, de modo análogo, maior é suas capacidades defensivas.

Ventre (2011) formula que na hipótese de serem levantados alvos militares visando seus ativos de informação e se valendo de um ataque surpresa, não há muito que fazer a não ser demandar um alto desenvolvimento de capacidades tanto em material (hardware/software) como em pessoal especializado.

Por fim pode-se contribuir para proporcionar esclarecimento no processo do ataque cibernético, de modo que os leitores do trabalho visualizem que a ação de ataque cibernético pode ser aprofundada em seus tipos e metodologias por meio do desenvolvimento de capacidades específicas às operações.

Deste modo o presente trabalho pode contribuir com a especificação das tarefas e atividades da ação de Guerra Cibernética ataque, produzindo uma lista de procedimentos para identificar metodologias, técnicas, táticas e procedimentos necessários para a execução e desenvolvimento de capacidades diante de uma operação cibernética ofensiva, como um anexo para o Planejamento de Operações Cibernéticas Ofensivas ao manual de Guerra Cibernética.

2 METODOLOGIA

Esta pesquisa científica de caráter qualitativo será baseada predominantemente na pesquisa documental e bibliográfica, sendo realizada nas seguintes etapas.

Na primeira etapa será realizada uma pesquisa documental e bibliográfica, sendo os dados, coletados na página eletrônica da biblioteca digital do Exército, com a finalidade de apresentar a metodologia das capacidades utilizadas pelo Exército Brasileiro.

Na segunda etapa serão coletados por meio de pesquisa exploratória na rede mundial de computadores os principais tipos de ataques cibernéticos com a finalidade de discutir esses ataques na ótica das metodologias apresentadas e quais capacidades específicas para o planejamento foram observadas.

Na terceira etapa, tendo por base os dados coletados na pesquisa documental, bibliográfica e por meio da rede mundial de computadores, serão analisadas o desenvolvimento das capacidades em operações cibernéticas ofensivas em 2 casos de estudo, com a finalidade de apresentar as metodologias de outros países em operações cibernéticas ofensivas e analisá-las sobre a ótica da metodologia do Exército Brasileiro.

Para a delineação da pesquisa, partiu-se da linha de raciocínio que a Cibernética permeia todas as arestas de nossa sociedade.

Desde a criação da rede mundial de computadores, a Internet, observamos a automação de processos e a diminuição de distâncias em um nível cada vez mais rápido.

No mundo atual, vemos toda a convergência de tecnologias criadas para facilitar a vida do homem. Em nossos dias atuais, passamos de simples servidores apresentando sítios (páginas) de internet para serviços em nuvens, compartilhamento de arquivos, redes sociais, interoperabilidade entre sistemas, automação de processos, inteligência artificial e Big Data. Como consequência disso a humanidade se adaptou e hoje estamos diante da sociedade da informação.

A cibernética, advêm desta evolução, no qual permitiu ao ser humano gerenciar e compartilhar informações, onde a linha que separa o mundo real do digital é cada vez mais frágil, de modo que os perigos originados pelas pesquisas nesta área, trouxeram assuntos como a segurança das informações e definição de políticas de segurança em diversos países.

O Brasil, em seu nível político, promove a segurança da informação e comunicações (SIC) e a segurança cibernética para sua sociedade da informação, coordenada pela Presidência da República e abrangendo toda a administração pública Federal. (MINISTÉRIO DA DEFESA, Brasília-DF, 2014)

Particularmente o seu Ministério da Defesa, desenvolveu no nível estratégico, com base na política de defesa cibernética, sua doutrina militar, onde especifica o espaço cibernético como o quinto domínio operacional, com a característica de que esse permeia os demais, que são interdependentes. (MINISTÉRIO DA DEFESA, Brasília-DF, 2014)

Desta forma, os níveis operacionais e táticos, são desenvolvidos por cada força armada, de acordo com a necessidade de cada domínio operacional, tendo o nível estratégico como o elemento de união entre elas.

No nível operacional e tático, a guerra cibernética é:

> 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 (STIC 2) do oponente e defender os próprios STIC 2. 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. (MINISTÉRIO DA DEFESA, 2014, pag 19/36)

É na guerra cibernética, que as atividades de proteção, exploração e ataque são divididas em tarefas. Especificamente na atividade de ataque, são definidas suas fases, o reconhecimento, escaneamento, exploração de vulnerabilidades,

manutenção do acesso e cobertura de rastros. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2017)

Na ação de ataque cibernético são definidos seus objetivos, a saber:

- Interromper;
- Negar;
- Degradar;
- Corromper; ou
- Destruir;

E em suas fases, são explanadas como chegarão a realização desses objetivos. Desta forma, é descrito o processo e a metodologia utilizada no Exército Brasileiro para a realização de um ataque cibernético. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2017)

O processo de ataque cibernético, portanto, se vale do reconhecimento e do escaneamento de informações ou sistemas no espaço cibernético, neste caso dimensionado a uma operação militar, e utilizando-se da exploração de vulnerabilidades realiza seu objetivo de interromper, negar, degradar, corromper ou destruir ativos de informação. Se for o caso, realiza a manutenção do acesso as essas informações ou sistemas e por fim, cobre os rastros deixados pelos ataques.

A tarefa da exploração de vulnerabilidades, se vale da complexidade da proteção do domínio cibernético, suas deficiências constituem-se no alvo compensador do ataque. Como exemplo destas deficiências, podemos citar: a falta de normas reguladoras; a falta de conscientização e do cumprimento às normas; a falta de capacitação; a falta de conhecimento da equipe de proteção; e a presença de sistemas legados.

A ausência de normas reguladoras constitui-se em um problema de ordem legislativa, com diversas consequências, onde uma deficiência pode ser aberta simplesmente por não haver uma padronização de processos de segurança.

A falta de conscientização e do cumprimento às normas já se caracteriza como um problema cultural, diversas vulnerabilidades que poderiam e deveriam ser facilmente corrigidas, acabam não sendo levadas em consideração como riscos aos ativos informacionais. O descumprimento das normas caracteriza-se também como uma exposição desnecessária do ativo a atores mal-intencionados. Felizmente a visibilidade dos impactos ocorridos por esta lacuna, tem feito a sociedade perceber a importância de se proteger. (National Cyber Security Strategy, 2016)

A falta de capacitação e de conhecimento da equipe de proteção é uma das vulnerabilidades mais exploradas, geralmente nesta deficiência não há complexidade em seu desenvolvimento, bastando utilizar ferramentas criadas pela dualidade do domínio cibernético. Esta deficiência caracteriza-se pela ausência parcial ou total dos níveis de segurança que devem existir no espaço cibernético. (National Cyber Security Strategy, 2016)

Os sistemas legados, isto é, sistemas antigos que necessitam funcionar em uma rede de ativos e que não mais recebem atualizações ou correções, são muito importantes e devem receber toda a segurança necessária no seu ciclo de vida. Infelizmente, nem todos os sistemas podem ser totalmente substituídos de tempos em tempos, alguns são críticos para qualquer negócio e infraestrutura, deste modo por utilizarem elementos que já passaram de sua época tecnológica, tornam-se alvos atrativos para a exploração de vulnerabilidades.

Assim sendo, a exploração de vulnerabilidades tem como alvo as deficiências da tarefa de proteção cibernética, onde percebemos que é extremamente abrangente e complexa.

O domínio da cibernética, passa por diversas e rápidas mudanças e transformações. Hoje nos encontramos caminhando para a Internet das coisas e para a interoperabilidade entre todos os sistemas com a rede mundial. A diversidade de sensores, acessórios, dispositivos e sistemas, constituem-se como um parque extremamente abrangente para a exploração de vulnerabilidades.

Ressalta-se as infraestruturas críticas, onde os sistemas se valem da Internet para serem interoperáveis. Setores como energia, transporte, financeiros, telecomunicações, saúde, alimentação, possuem ativos, dispositivos e sistemas dos mais diversos que configuram como alvos prioritários para a atividade de ataque cibernético.

Desta forma, ao sairmos das deficiências comuns existentes na proteção, nos deparamos com uma infinidade de possibilidades para a realização dos objetivos em uma operação militar das quais temos alvos de alto valor.

Para as possibilidades de ataque serem concretizadas, deve-se realizar o desenvolvimento de capacidades técnicas específicas para os diversos setores. É importante perceber que, para a evolução destas capacidades, torna-se fundamental reconhecê-las (quais são?) e até onde podemos progredir em seu domínio cognitivo.

A taxonomia de Bloom em seu domínio cognitivo nos mostra uma progressão cognitiva ao se desenvolver capacidades. Os níveis: conhecer; entender; aplicar; analisar; sintetizar; e criar, caracterizam-se como um bom parâmetro para interpretar o nível que a capacitação deve-se chegar. (Anderson, Krathwohl, Airasian, 2001)

Por fim, reconhecer quais são os desenvolvimentos de capacidades específicas para exploração de vulnerabilidades mais complexas constitui-se em um elemento fundamental ao processo do ataque cibernético, uma vez que com estas informações podemos utilizar os efeitos militares constituídos na doutrina e traduzi-los para os efeitos cibernéticos desejados em uma operação militar. (Military Activities and Cyber Effects Taxonomy, 2013)

3 RESULTADOS E DISCUSSÃO

A Polícia Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END), a Política Militar de Defesa (PMD) e a Estratégia Militar de Defesa contribuem para o norteamento e desenvolvimento da Doutrina Militar de Defesa. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

A Doutrina Militar de Defesa, lança as diretrizes para a geração de força adotada pelo Exército Brasileiro, mediante o Planejamento Baseado em Capacidades (PBC), tendo sua execução realizada pelo Preparo da Força Terrestre, no qual, busca gerar uma capacidade através do DOAMEPI. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

O entendimento do DOAMEPI, nesta primeira fase dos trabalhos, é de fundamental importância para a compreensão do desenvolvimento da capacidade requerida para o Poder Militar Terrestre. Com a exata noção de seus fatores, cumpre-se os requisitos essenciais para aquisição da capacidade operativa.

A doutrina como primeiro fator determina as bases para as demais, uma vez que por meio de produtos doutrinários se criam as missões, atividades e tarefas para a execução dos objetivos. Ressalta-se que da doutrina se derivam as normas, planos para adestramento, procedimentos para instruções em diversos níveis, aperfeiçoamento de estruturas e meios de maneira adequada, isto é, permeando os demais fatores do DOAMEPI. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

A organização como segundo fator configura-se como a composição de maneira metódica e racional para atingir resultados, agindo na estruturação da Força Terrestre. Ressalta-se que de acordo com o manual de Doutrina Militar Terrestre

(EB20-MF-10.102) o fator organização orienta os processos, no qual evitam capacidades redundantes quando empregadas. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

O adestramento é o terceiro fator que reúne todas as atividades do preparo, orientado por meio de planos, instruções e procedimentos que visam tornar a tropa apta e capaz para as missões, atividades e tarefas. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

O quarto fator que compreende o DOAMEPI é o material, no qual é compreendido por todo o aparato e sistemas do qual a tropa se vale para cumprir suas atribuições, acompanhando a evolução do conhecimento. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

A educação é o quinto fator, que envolve o processo de capacitação e habilitação individual, no domínio cognitivo, para que a competência seja adquirida. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014). Ressalta-se que na Capacidade Militar Terrestre de Cibernética (CMT 09), relacionando-se com a taxonomia de Bloom, o aprendizado de acordo com os verbos impostos tendem a ser prolongados pelas especificidades e multidisciplinaridade que envolve o domínio do Ciberespaço.

O pessoal como sexto fator, aborda toda a gerência dos recursos humanos, os ativos essenciais da Força Terrestre, para a plena competência na área da dimensão humana. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

As infraestruturas como último fator, engloba todos os aspectos estruturais para o desenvolvimento das capacidades requerentes da tropa, onde será possível alicerçar os demais fatores, em direção aos objetivos, missões, atividades e tarefas. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

Por consequência dos fatores acima expostos, a medição para fins de avaliação e acompanhamento do desenvolvimento de capacidades de uma tropa é realizado através do Preparo da Força Terrestre. De acordo com o Capítulo V da Concepção Estratégica do Exército (SIPLEX – Fase IV) as aferições são realizadas por meio de instruções, adestramentos, mobilizações, distribuição do pessoal, dotação do material, etc. Esta avaliação tem por finalidade tornar as Organizações Militares aptas a participarem de operações em amplo espectro, singulares, conjuntas ou combinadas de acordo com a concepção estratégica do Exército. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2017)

Conclui-se nesta primeira fase então, a elucidação de como a Força Terrestre se utiliza do DOAMEPI para seu desenvolvimento de capacidades.

No desenvolvimento deste trabalho, em sua segunda fase, cabe compreender também o desenvolvimento da capacidade operativa ataque cibernético (CO38), tendo como base o DOAMEPI empregado pelo Exército Brasileiro em seu preparo, uma vez que o Planejamento Baseado em Capacidades norteia toda a nova Doutrina Militar Terrestre.

O manual de Doutrina Militar Terrestre ampara que estando a Força Terrestre inserida na Era do Conhecimento, novas necessidades de capacitação são geradas como consequência da evolução doutrinária. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2014)

Desta forma, cabe uma percepção mais profunda no escopo da capacidade operativa ataque cibernético (CO38) no que se refere a parte de Doutrina do DOAMEPI.

O processo do ataque cibernético pode ser entendido como uma descrição técnica no qual elementos especializados em guerra cibernética terão de interpretar as missões recebidas pelo escalão superior e traduzi-los para os verbos identificados nas tarefas do ataque. Este processo é faseado e engloba as tarefas de reconhecimento, escaneamento, exploração de vulnerabilidades, manutenção de acesso e cobertura de rastros. (EXÉRCITO BRASILEIRO, BRASÍLIA-DF, 2017)

As tarefas descritas acima no entanto, são empregadas no desencadear da ação de ataque cibernético para o cumprimento de seu objetivo, não abrangendo a maneira de como se conduz o processo de ataque até estas fases.

Na área da Doutrina, toda operação cibernética ofensiva tem como foco a exploração de vulnerabilidades em pessoas, processos e tecnologias. Estas 3 dimensões no ciberespaço se interseccionam e fazem com que suas relações intrínsecas, criem uma complexidade que propicia brechas e erros em sistemas informacionais (Figura 1).

Figura 1: Pessoas, Processos e Tecnologias

Para que estas três áreas sejam alcançadas, os especialistas em guerra cibernética se utilizam dos pilares da segurança da informação, a saber: - Confidencialidade; Integridade; e Disponibilidade. Para a atuação nos pilares da segurança da informação, existem diversos verbos que amparam sua atividade dentro do escopo dos pilares, são exemplos deles:

- Interromper:
- Modificar:
- Degradar:
- Fabricar:
- Interceptar:

O manual de Guerra Cibernética, em consoante com a Doutrina Militar de Defesa Cibernética, atribui os verbos (interromper, negar, degradar, corromper e destruir) que evidenciam a finalidade das ações de ataque para o efeito militar desejado.

Em um próximo momento então, os especialistas necessitam relacionar o efeito militar desejado com os métodos para agir nos pilares da segurança da informação e assim, alcançar seu foco, isto é, executar uma tradução do efeito militar desejado para a atuação no pilar da segurança da informação.

Desta forma, apresenta-se abaixo uma matriz resumida dos efeitos militares em relação aos verbos que afetam a segurança da informação:

Militar Cibernético	Interromper	Negar	Degradar	Corromper	Destruir
Interrupção	X	X	-	-	-
Modificação	X	X	X	X	X
Degradação	X	-	X	X	-
Fabricação	-	X	X	X	-
Interceptação	-	-	-	-	-

Na figura 2 a seguir, temos como exemplo o efeito militar do verbo negar, sendo traduzido para os efeitos cibernéticos interromper e modificar:

Efeito Militar	Efeito Cibernético	Exemplo
Negar	Interrupção	Gerar *flood* em uma rede para causar falhas em *softwares* ou sistemas de modo a impossibilitar a comunicação de usuários com o servidor.
	Modificação	Modificar configurações de rede e do servidor, incluindo controles de acesso e tabelas de roteamento para negar acesso a um usuário específico.
	Um ataque de negação de serviço ao inserir uma grande quantidade de pacotes (fabricados) na rede com o objetivo de negar acesso.	

Figura 2: Tradução do efeito militar NEGAR para o efeito cibernético

Outro aspecto que deve ser levado em consideração no fator doutrina do DOAMEPI é o tempo para ser desencadeada as operações cibernéticas ofensivas, as missões desempenhadas pela capacidade operativa ataque cibernético (CO38) de acordo com as características e especificidades dos sistemas informacionais pode demorar longos períodos, sendo muitas vezes necessário a preparação do campo de batalha em tempo de paz. (United States Army War College – Strategic Cyberspace Operations Guide, 2016)

Ao se reunir as ideias acima apresentadas, verifica-se que o planejamento da operação cibernética ofensiva se desencadeiam no planejamento e preparação das seguintes atividades:

1. Planejamento do efeito militar desejado;
2. Tradução do efeito militar para o efeito cibernético;
3. Designação de requisitos, tempo e objetivos;
4. Planejamento das linhas de ação do ataque cibernético; e
5. Ordem de autorização.

Quanto aos outros fatores do DOAMEPI, cabe enfatizar em conjunto os fatores organização e pessoal, nos quais pela amplitude de conhecimentos necessários ao especialista em cibernética, pelo longo período para desenvolver as capacidades necessárias em relação ao pessoal e pelas diferentes especificidades das missões envolvidas nas operações cibernéticas ofensivas, pode ser viável a contratação de equipes civis, realizada por empresas do ramo, para desencadear operações militares ofensivas. Nestes fatores a gestão de recursos humanos em consonância com a carreira individual, deve buscar um termo ideal para que a instituição saia com o máximo de aproveitamento e o indivíduo com o máximo de capacitação.

Na parte de Material e Infraestrutura, cita-se que a rede mundial de computadores é uma colcha de retalhos de sub-redes e torna-se imprescindível a disponibilidade e manutenção de equipamentos de TI e soluções ofensivas em pronto emprego, para uma eventual utilização, o que torna a maneira do anonimato na Internet uma tarefa dispendiosa para instituições grandes como a Força Terrestre.

No fator adestramento, as equipes criadas para a capacidade cibernética ofensiva devem trabalhar ao máximo em sua integridade tática, uma vez que a maior adaptação possível de seus elementos faz com que diferentes problemas sejam solucionados da maneira mais rápida e menos custosa possível. Além disso, a falta de preocupação com a montagem de equipes para resolver um determinado problema num curto espaço de tempo, não favorece a sinergia dos envolvidos e podem tornar as operações cibernéticas ofensivas malsucedidas.

O fator educação do DOAMEPI é um dos mais sensíveis nas operações cibernéticas. A taxonomia de Bloom nos ajuda a mensurar o nível cognitivo que um especialista em cibernética deve chegar para conseguir desenvolver sua capacidade. Os níveis básicos para a capacidade ofensiva são conhecer, entender e aplicar, enquanto o nível intermediário seriam os de analisar e sintetizar. Neste estágio, o especialista cibernético ofensivo estaria somente na fase de reprodução de ataques cibernéticos já existentes, não sendo capaz ainda de poder executar sua capacidade plenamente. Os campos nos quais estaria apto seriam de somente preparar o campo de batalha no domínio cibernético e de aplicar as tarefas de reconhecimento, escaneamento, exploração de vulnerabilidades com limitações, manutenção do acesso com limitações e cobertura dos rastros com limitações. Para que o especialista tenha plena capacidade ele deveria chegar ao nível cognitivo avançado, ou seja, o nível cognitivo de criar, desta maneira, com a capacidade plenamente desenvolvida,

estaria apto a buscar vulnerabilidades nunca encontradas e ainda fabricar novos tipos de ataques cibernéticos. O que torna difícil no fator Educação no DOAMEPI é a longa curva de aprendizagem, que segundo dados médios de planejamento na parte cibernética, leva cerca de 2 ou 3 anos. (United States Army War College – Strategic Cyberspace Operations Guide, 2016)

Por fim, nesta segunda fase dos trabalhos, conclui-se que os tipos de ataques cibernéticos sob a ótica do DOAMEPI e o planejamento baseado em capacidades possuem aspectos bem diferentes do paradigma atual na Doutrina Militar Terrestre.

Na terceira fase, um estudo de caso foi escolhido para demonstrar a abordagem dos diferentes paradigmas elencados na fase anterior dos trabalhos.

O caso escolhido foi o *malware NotPetya (ou Nyetya)*, artefato cibernético malicioso utilizado na Ucrânia que teve como alvo as diversas organizações e instituições financeiras daquele país e uma narrativa do que ocorreu no fatídico dia 27 de Junho de 2017 é necessário para sua total compreensão. (MAYNOR e col., 2017)

Em 27 de Junho de 2017, ocorreu um dos ataques mais nocivos às instituições financeiras da Ucrânia e de alguns países da Europa, um ataque que se utilizava de um *ransonware*, *malware* que criptografa os dados de toda a máquina e exige um pagamento pelo resgate das informações, para se espalhar nas redes dos sistemas informacionais, causando consequentemente, o caos em várias infraestruturas críticas do país. Diversos meios de comunicações e países acusaram o governo russo de conduzir o ataque cibernético contra a Ucrânia. O governo russo nega veementemente as acusações recebidas. (HENLEY e SOLON, 2017)

Observando pela ótica do desenvolvimento de capacidades em uma operação cibernética ofensiva quanto a este tipo de ataque, pode-se analisar o DOAMEPI empregado pela força adversa, provavelmente russa, para a bem-sucedida operação ofensiva do ponto de vista do atacante.

Analisando o aspecto da doutrina na operação, no escopo estratégico, constata-se que a campanha de ataque cibernético se utiliza de conceitos de guerra híbrida, isto é, baseia-se na doutrina Gerasimov de utilização do máximo de meios indiretos e assimétricos de poder militar oculto para o alcance de seus objetivos. Desta forma, por meio de efeitos cibernéticos atuados nos pilares da segurança da informação, a força adversária logrou êxito em seu efeito político/militar desejado, degradando, corrompendo, interrompendo e destruindo ativos de infraestruturas críticas da Ucrânia. (BARTLES, 2016)

Nos fatores organização e pessoal, pela falta de informações a respeito do assunto devido ao sigilo das operações, não se pode constatar a organização de uma tropa constituída, entretanto, valendo-se ainda da doutrina Gerasimov e por meio de outras mídias noticiando eventos episódicos similares ao do estudo de caso, podemos mensurar esta organização, no qual possivelmente se valem de hackers oriundos do meio civil e alinhados com os pensamentos militares vigentes ou empresas do ramo, patrocinados pelo estado adverso.

Fontes de mídias chinesas e europeias em diversos outros eventos cibernéticos ofensivos e por meio da Inteligência de Ameaças Cibernéticas traçam um perfil do modus operandi de determinado *malware* e consequentemente conseguem identificar o grupo atuante naquela campanha. Neste evento específico, estudos realizados pelo Cisco Talos Intelligence Group e pela Kaspersky Labs, traçam por meio do código do artefato malicioso e de sua execução uma ameaça persistente avançada oriunda da Rússia, que desenvolveu inicialmente o código. (SONG, 2016; MAYNOR e col., 2017)

De modo análogo, o adestramento e a educação também não podem ser constatados pelo sigilo das operações, entretanto sabemos através de notícias que estes grupos se adestram por meio de campanhas desencadeadas por toda a rede mundial de computadores, desta maneira estão sempre percorrendo toda a taxonomia de Bloom e criando (nível cognitivo mais elevado) diversos métodos de ataque cibernético para utilizá-los em operações. (SONG, 2016)

A seguir, existem dois fatores do DOAMEPI que nas operações cibernéticas ofensivas são intrínsecos e se permeiam. O material e a infraestrutura verificados no estudo de caso, demonstra o nível elevado de adestramento da força adversa. O anonimato é de vital importância para a operação e foi executada de maneira que todas as invasões não fossem atribuídas a um determinado ator e a ameaça avançada se valeu ainda de um servidor na Letônia (país neutro para a Área de Operações estudada) para propagar o artefato malicioso. Desta forma, podemos aferir que a preparação do material e das infraestruturas utilizadas para o ataque, tenha sido antecedida por meses antes da ação no objetivo. (MAYNOR e col., 2017)

Por fim, para esta última fase dos trabalhos, podemos constatar pelo estudo de caso, que todo o DOAMEPI é evidenciado nas fases de consecução dos objetivos a serem realizados nas operações cibernéticas ofensivas.

4 CONCLUSÃO

Como conclusão deste trabalho, pode-se averiguar que o desenvolvimento de capacidades da Força Terrestre, proporcionado pelo DOAMEPI e seus fatores indissociáveis é um interessante meio para validar uma nova necessidade e um novo paradigma na Doutrina Militar Terrestre no que se refere a operações cibernéticas ofensivas.

As tarefas, atividades e as ações de ataque cibernético podem ser desenvolvidas com base no DOAMEPI, realizando-se algumas alterações pertinentes.

As alterações julgadas pertinentes não descartam de nenhuma maneira a doutrina vigente, mas busca evidenciar outros meandros que as características do domínio cibernético impõem para as operações militares.

O Estudo de Caso, realizado no trabalho busca elucidar o DOAMEPI e evidenciar a capacidade ofensiva sendo utilizada de sua forma plena. É importante ressaltar que apesar dos fatores serem indissociáveis, a base doutrinária que pretende-se evoluir é o fator inicial para a mudança pretendida.

Por fim, para responder ao questionamento inicial levantado no trabalho, pode-se responder que baseando-se pelo DOAMEPI e norteado pela Doutrina Militar Terrestre, as capacidades específicas necessárias para a realização das operações cibernéticas ofensivas são a evolução do fator doutrina, isto é, evoluindo-se o processo de ataque cibernético na tradução do efeito militar desejado para os verbos de atuação nos pilares de segurança da informação, tendo como foco a exploração de vulnerabilidades em pessoas, processos e tecnologias. A observação das nuances quanto aos fatores organização, material, infraestrutura no ciberespaço e, a percepção fundamental da importância da educação e do pessoal, tendo em vista o desenvolvimento do nível cognitivo e a gestão de recursos humanos. Doutrina, educação e pessoal, são os fatores do DOAMEPI que mais serão evoluídos com base nesta resposta.

REFERÊNCIAS

BRASIL. Ministério da Defesa. **MD-31-P-02: Política Cibernética de Defesa**. 1. ed. Brasília, DF, 2012.

BRASIL. Ministério da Defesa. **MD-31-M-07: Doutrina Militar de Defesa Cibernética**. 1. ed. Brasília, DF, 2014.

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

BRASIL. Exército. **EB20-MF-10.102: Doutrina Militar Terrestre**. 1. ed. Brasília, DF, 2014.

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

BRASIL. Exército. **Sistema de Planejamento do Exército – SIPLEX / Fase IV: Concepção Estratégica do Exército**. 1. ed. Brasília, DF, 2017.

ESTADOS UNIDOS, Center for Strategic Leadership. **United States Army War College – Strategic Cyberspace Operations Guide.** Philadelphia, 2016.

CANADA, Defence R&D. **Military Activities and Cyber Effects.** Ottawa, Ontario, 2013.

REINO UNIDO, HM Government. **National Cyber Security Strategy**. Londres, 2016.

VENTRE Daniel. **Cyberwar and information warfare.** ISTE Ltd and John Wiley & Sons, Inc. 2011.

ANDERSON Lorin W.; KRATHWOHL David R.; AIRASIAN Peter W.; CRUIKSHANK Kathleen A.; MAYER Richard E.; PINTRICH Paul R.; WITTROCK James Raths; WITTROCK Merlin C. **A Taxonomy for Learning, Teaching, and Assessing — A Revision of Bloom's Taxonomy of Educational Objectives.** Addison Wesley Longman, Inc. 2001.

BARTLES Charles K. Para Entender Gerasimov. In: **Military Review**, 2016. Disponível em: <https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/MilitaryReview_20160430_art010POR.pdf>. Acesso em: 1 Set 2018.

HENLEY, Jon.; SOLON Olivia. 'Petya' ransomware attack strikes companies across Europe and US. **The Guardian**, 2017. Disponível em: <https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe>. Acesso em: 1 Set 2018.

MAYNOR, David.; NIKOLIC, Aleksandar.; OLNEY Matt.; YOUNAN, Yves. The MeDoc Connection. **CISCO's Talos Intelligence Group Blog**, 2017. Disponível em: <https://blog.talosintelligence.com/2017/07/the-medoc-connection.html>. Acesso em: 1 Set 2018.

SONG, Long. Foreign media: In order to expand the network forces, Russia even secretly recruits criminals. **IT Times**, 2016. Disponível em: <http://www.ittime.com.cn/news/news_13375.shtml>. Acesso em: 1 Set 2018.