# O Processo de Elaboração da Lista de Alvos Cibernéticos no Nível Tático

Ten Cel Com Vinícius Lacerda Vasquez*

**RESUMO**

A Guerra Cibernética envolve ações que contribuem para a consecução dos objetivos militares, sendo necessária sua integração no planejamento operacional. Neste sentido, este artigo tem o objetivo de apresentar uma proposta para o processo de elaboração da Lista de Alvos Cibernéticos durante o Exame de Situação do comandante tático. Para tanto, desenvolveu-se uma pesquisa qualitativa, de cunho descritivo, e empregou-se, além do método indutivo, um estudo bibliográfico e documental. A pesquisa foi, ainda, orientada no sentido de se compreender as adaptações necessárias ao processo de planejamento de fogos adotado pela doutrina militar terrestre brasileira em função das peculiaridades do ambiente operacional cibernético. A seleção das fontes de pesquisa fundamentou-se em artigos de autores de reconhecida importância no meio literário e acadêmico, bem como em publicações de elevado número de citações ou, ainda, em fontes abertas atuais e disponibilizadas em sítios eletrônicos. Desta forma, a metodologia de elaboração da Lista de Alvos Cibernéticos apresentada permite superar as peculiaridades do espaço cibernético, por meio do emprego de ferramentas auxiliares. Inicialmente, o espaço cibernético é avaliado sobre o prisma da dimensão informacional, a fim de facilitar a compreensão do ambiente operacional e a identificação dos alvos cibernéticos no Teatro de Operações. Em seguida, os alvos adquiridos são analisados empregando-se a taxonomia MACE. Por fim, os alvos identificados nas fases anteriores são selecionados e priorizados utilizando-se o método CRAVER, produzindo-se a Lista de Alvos Cibernéticos. Como conclusão, o artigo destaca a importância do método proposto, bem como apresenta sugestões para trabalhos futuros.

**Palavras-chave**: Busca de Alvos. Guerra Cibernética. Matriz CRAVER. Taxonomia MACE.

***Cyber-Target Listing Process on Tactical Level***

***ABSTRACT***

*The Cyber War involves actions that contribute to the achievement of military objectives, being necessary its integration in operational planning. Thus, this article aims to present a proposal for the Cyber-Target Listing methodology during the Military Decision Making Process. Therefore, qualitative research with a descriptive character was developed and, bibliographical and documentary research was employed, besides the inductive method. The research was also oriented to understand the necessary adaptations to the targeting process adopted by the Brazilian military doctrine due to the peculiarities of the cyber operating environment. The selection of research sources was based on articles by authors of recognized importance in the literary and academic circles, as well as publications with a high number of citations or on current open sources available on electronic websites. Thus, the Cyber-Target Listing methodology presented allows overcoming the peculiarities of the cyberspace, through the use of auxiliary tools. Initially, cyberspace is evaluated from the perspective of the informational dimension, to facilitate the understanding of the operating environment and the identification of cyber targets in the theater of operations. The acquired targets are then analyzed using the MACE taxonomy. Finally, the targets identified in the previous phases are selected and prioritized using the CARVER method, producing the Cyber-Target List. In conclusion, the article presents the validity of the proposed method, as well as suggestions for future work.*

***Keywords:*** *CARVER Matrix. Cyber Warfare. MACE Taxonomy. Targeting.*

Artigo recebido em 01/12/2019 e aceito para publicação em 1/01/2020

## 1 INTRODUÇÃO

A Guerra Cibernética tem se mostrado uma opção importante no rol de ações não cinéticas das operações militares. Isto foi motivado pela velocidade da revolução tecnológica recente que culminou na elevação do espaço cibernético à condição de domínio operacional. (US ARMY, 2010; USA, 2018).

Sua transversalidade aos demais domínios (marítimo, terrestre, aéreo e espacial), permite-lhe criar efeitos militares decisivos, produzindo vantagens e influenciando eventos em todos os ambientes operacionais. Entretanto, em um contexto de Operações no Amplo Espectro e à medida que surgem um número maior de atores no ambiente operacional, bem como aspectos relacionados às dimensões humana e informacional, verificase que a complexidade dos problemas enfrentados pelas forças militares aumenta. Para mitigar as consequências deste novo domínio na Defesa Nacional e contrapor os novos desafios apresentados às Forças Armadas na condução das operações militares contemporâneas, em 2008, o Ministério da Defesa incumbiu o Exército Brasileiro das tarefas de coordenar e de integrar as ações de Defesa Cibernética no país. (BRASIL, 2014; EXÉRCITO BRASILEIRO, 2014).

Contudo, com as peculiaridades do domínio cibernético e o fato do conceito de Guerra Cibernética ser uma concepção recente, a doutrina de emprego de suas ações ofensivas ainda carecem de amadurecimento. Neste contexto, este trabalho pretende estudar a aplicação de um método específico para a elaboração da Proposta de Lista de Alvos Cibernéticos (PLA Ciber), durante o Exame de Situação do comandante tático do elemento de Guerra Cibernética.

Para tanto, este artigo está organizado da seguinte maneira: esta primeira seção introdutória, seguida da segunda seção que descreve as peculiaridades do espaço cibernético, da Guerra Cibernética e suas possibilidades. Prossegue pela terceira seção, que introduz ferramentas que subsidiam as etapas do processo de busca de alvos cibernéticos. Quanto a tais etapas, a primeira delas objetiva avaliar o espaço cibernético sobre o prisma das camadas interdependentes física, lógica e cognitiva, facilitando a compreensão do ambiente. A segunda consiste no emprego da taxonomia MACE para a análise dos alvos adquiridos. A última etapa traduz-se na utilização do método CRAVER para a priorização e seleção dos alvos identificados nas fases anteriores. Encerrando o artigo, a quarta seção apresenta as conclusões do estudo, bem como apresenta propostas para trabalhos futuros.

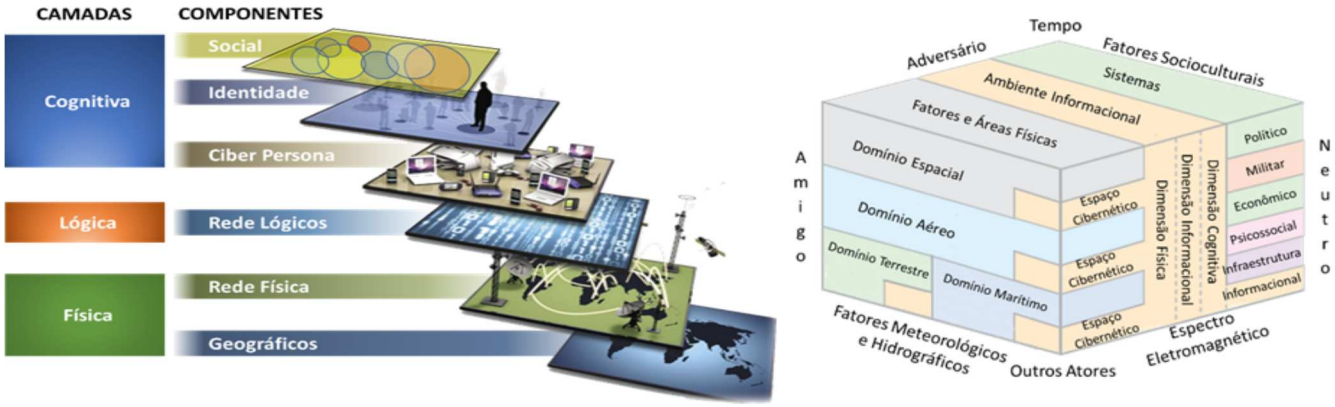
## 2 O ESPAÇO CIBERNÉTICO E A GUERRA CIBERNÉTICA

O espaço cibernético é um ambiente complexo que vai além dos limites organizacionais e das fronteiras nacionais (BRANDÃO; IZYCKI, 2019). Ele é resultante da interação de pessoas, softwares e serviços disponíveis na Internet por meio de dispositivos e redes de telecomunicações conectados a ela. (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012).

Na doutrina militar brasileira, o espaço cibernético é caracterizado por ser um ambiente virtual composto por dispositivos computacionais, conectados em redes ou não, onde as informações digitais transitam e são processadas ou armazenadas. Tais atributos criam um espaço operativo comum, integrando as dimensões física, informacional e humana no que se refere a sua dependência aos meios de tecnologia da informação e comunicações. (BRASIL, 2014; EXÉRCITO BRASILEIRO, 2017a; USA, 2018).

A complexidade desse ambiente pode ser minimizada por sua descrição segundo as três perspectivas da dimensão informacional, na qual o espaço cibernético está inserido. A figura 1 representa a inter-relação dessas camadas:

**Figura 1— Camadas do Espaço Cibernético e sua visão holística**




Fonte: US Army (2010); United Kingdom (2016), adaptador pelo autor. .

A camada física é caracterizada pelo hardware e pela infraestrutura computacional responsáveis pelo armazenamento, transporte e processamento de informações, distribuídos em um espaço geográfico. Seus componentes exigem medidas de segurança física, que podem ser aproveitados para a obtenção do acesso lógico. Ela também define a localização geográfica e a estrutura legal apropriada a ser aplicada nas operações militares, considerando que existem questões de propriedade e soberania ligadas aos domínios físicos e as fronteiras geopolíticas são facilmente ultrapassadas no ciberespaço.(UNITED KINGDOM, 2016; USA, 2018).

A segunda camada refere-se à rede lógica. Essa é uma abstração da camada física e consiste no código de programação, nos protocolos e nos dados que acionam os componentes de rede. Ela restringe o engajamento de seus alvos por meios inerentes ao espaço cibernético, ou seja, um dispositivo ou aplicação projetada para criar um efeito no ciberespaço ou através dele. (UNITED KINGDOM, 2016; USA, 2018).

A última camada é a cognitiva. Ela é responsável por conectar as pessoas ou grupos à sua forma de apresentação no espaço cibernético (ciber-persona). Ela reflete seus aspectos humanos e sociais, incluindo as contas de usuários (humanas ou automatizadas) e de grupos, bem como seus dados e relacionamentos. (UNITED KINGDOM, 2016; USA, 2018).

Essa gama de entidades que interagem nesse domínio para trocarem informações, faz com que ele seja determinante no planejamento operacional (US ARMY, 2019). Deste modo, é fundamental compreender as condições, circunstâncias e fatores que influenciam o ambiente operacional cibernético pois, por meio dele, é possível criar efeitos únicos e decisivos em todos os demais domínios (BRASIL, 2014; USA, 2018).

## 2.1 PRINCÍPIOS E CARACTERÍSTICAS DA GUERRA CIBERNÉTICA

Para alcançar tais objetivos, o vetor militar a ser utilizado é a Guerra Cibernética. Ela é definida pelas ações no espaço cibernético que amplificam as ações cinéticas e garantem liberdade de ação da força empregada, potencializando seus efeitos no Teatro de Operações. (BRASIL, 2012; EXÉRCITO BRASILEIRO, 2017a).

O termo Guerra Cibernética refere-se, ainda, ao planejamento e à execução das atividades cibernéticas nos níveis operacional e tático de uma operação militar. Ela corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de comando e controle (C2) do adversário. (BRASIL, 2014).

O seu emprego é pautado em quatro princípios relevantes: o efeito, a dissimulação, a rastreabilidade e a adaptabilidade. Os dois primeiros dizem respeito diretamente às ações ofensivas, enquanto os últimos às defensivas. O princípio do efeito remete à produção de impactos no espaço cibernético. Esses devem produzir vantagem em todos os níveis de decisão, afetando o mundo real, mesmo que não sejam cinéticos. A dissimulação trata das medidas a serem adotadas a fim de mascarar a autoria e o ponto de origem das ações ofensivas. A rastreabilidade, por sua vez, está relacionada à detecção das ações cibernéticas do oponente. E, por fim, o princípio da adaptabilidade consiste na capacidade da Guerra Cibernética em adaptar-se e manter a proatividade mesmo diante de mudanças súbitas e imprevisíveis no combate. (BRASIL, 2014).

Uma das principais características da Guerra Cibernética é a insegurança latente dos sistemas computacionais, que parte da premissa de que não há sistemas completamente seguros e que suas vulnerabilidades poderão ser exploradas. Assim, a Guerra Cibernética aproveita-se da ausência das amarras das limitações físicas de distância e espaço e ignora as fronteiras geográficas para conduzir suas ações em qualquer parte do globo. (EXÉRCITO BRASILEIRO, 2017a).

Também há de se observar que o desenvolvimento de armas cibernéticas possui um ciclo mais curto se comparado às tradicionais. Desta maneira, seu custo é inferior aos armamentos cinéticos convencionais. Isto proporciona um desbalanceamento de forças, em que Estados, organizações ou agentes com recursos financeiros limitados são capazes de perpetrar danos tão severos quanto os cometidos por entidades com maiores condições econômicas. (BRANDÃO; IZYCKI, 2019; EXÉRCITO BRASILEIRO, 2017a).

Outro aspecto interessante a ser constatado é a dualidade das ferramentas que podem ser usadas por atacantes e administradores de sistemas com finalidades distintas. Um software de identificação de vulnerabilidades tanto pode ser empregado para identificar falhas em um sistema para a adoção de medidas de proteção, quanto para apresentar oportunidades de ataque. (EXÉRCITO BRASILEIRO, 2017a).

Por este cenário, nota-se que uma operação cibernética pode empregar vários tipos de ataques, disseminados por diferentes vetores,

que exijam níveis de acesso distintos, tudo de forma combinada, sequencial ou simultânea, inclusive conjugar recursos cibernéticos e físicos (BERNIER, 2013). Desta forma, pode-se dizer que o sucesso das ações ofensivas cibernéticas depende do domínio de todo o ciclo de vida do ataque: reconhecimento, preparação, entrega do artefato, exploração, instalação,comando e controle e ações nos objetivos. (BRANDÃO; IZYCKI, 2019; HUTCHINS; CLOPPERT; AMIN, 2011).

Entretanto, é importante destacar que a Guerra Cibernética não tem um fim em si mesma. Ela é tipicamente empregada no contexto de uma Operação Militar, apoiando a condução de outros tipos de operação e contribuindo para a obtenção de um efeito desejado. Todavia, suas ações podem não gerar os resultados esperados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados. Devido a esta incerteza, cada operação deve ser planejada e acompanhada minuciosamente, considerando as particularidades do ciberespaço. (EXÉRCITO BRASILEIRO, 2017a).

## 2.2 GUERRA CIBERNÉTICA COMO MEIO NÃO CINÉTICO DE APOIO AO COMBATE

Para fins de aplicação do poder de combate, estão definidas três capacidades operativas: proteção, exploração e ataque. A atividade de proteção cibernética é de caráter permanente e refere-se à condução de tarefas para neutralizar as ações ofensivas do oponente sobre os ativos computacionais, redes de computadores e de comunicações. A de exploração tem o objetivo de preparar os alvos cibernéticos para ações futuras. Isso se dá por meio do mapeamento dos sistemas e dos ativos de informação presentes no espaço cibernético de interesse, bem como da identificação e exploração de suas vulnerabilidades. Por sua vez o ataque é caracterizado pela interrupção, negação, degradação, corrupção ou destruição de informações, de sistemas, de dispositivos ou de redes computacionais ou de comunicações do oponente. (EXÉRCITO BRASILEIRO, 2017a).

Das três capacidades operativas descritas acima, as ações de exploração e de ataque cibernético configuram a atuação não cinética da Guerra Cibernética. Seu emprego provoca efeitos no ambiente físico, podendo ser executados simultaneamente às ações cinéticas para causar resultados complementares sobre um mesmo alvo, sem o emprego do fogo cinético. (BRANDÃO; IZYCKI, 2019; EXÉRCITO BRASILEIRO, 2015, 2017a).

Em geral, estas ações afetam as propriedades básicas da segurança da informação: confidencialidade, integridade e disponibilidade. Desta forma, é imprescindível que a análise e o planejamento de Guerra Cibernética sejam orientados por estes elementos, permitindo seu emprego de maneira seletiva e pontual, engajando objetivos elencados pelos diversos níveis (estratégico, operacional e tático). Destaca-se, ainda, a possibilidade de se considerar outros atributos complementares, tais como: autenticidade, confiabilidade, conformidade, legalidade, não repúdio (irretratabilidade) e responsabilidade. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013; EXÉRCITO BRASILEIRO, 2017a, 2017b).

Com a capacidade de causar danos ou baixas nas estruturas físicas, nos centros de C2, nas redes de computadores, nos centros de comunicações, afetar o moral das tropas adversárias ou, ainda, reduzir a possibilidade do inimigo de explorar o ambiente operativo, é pelas ações de exploração e de ataque que a Guerra Cibernética se integra à função de combate Fogos (EXÉRCITO BRASILEIRO, 2015), cuja definição é:

> [...] um conjunto de atividades, tarefas e sistemas integrados, [que] permitem a aplicação e o controle de fogos, orgânicos ou não, integrados pelos processos de planejamento e coordenação. [...] Para isso, os sistemas de fogos devem estar integrados, considerando os meios conjuntos e incorporando a defesa antiaérea e a capacidade de realizar ações eletrônicas e cibernéticas. (EXÉRCITO BRASILEIRO, 2015, p. 1-1).

A responsabilidade da integração dos fogos com os atuadores não cinéticos é da célula de Coordenação de Fogos. Para tanto, ela conta com uma equipe multidisciplinar e especializada incumbida de avaliar todas as possibilidades e limitações dos meios disponíveis, buscando a eficácia do apoio de fogo. A tarefa de sincronização desses meios de intervenção no combate é encargo do Grupo Integrado de Seleção e Priorização de Alvos (GISPA). Dentre os elementos que podem integrar esse grupo, o Oficial de Ligação de Guerra Cibernética é responsável pelo assessoramento quanto às possibilidades dos atuadores dessa capacidade. (EXÉRCITO BRASILEIRO, 2017b).

Em relação aos elementos de Guerra Cibernética com capacidade ofensiva no nível tático, quando for ativada a Estrutura Militar de Defesa, esses poderão englobar uma Força Conjunta de Guerra Cibernética, como Força Componente, para executar as operações cibernéticas em proveito do Teatro de Operações ou da Área de Operações (TO/AO), bem como estruturas de Guerra Cibernética de cada uma das demais

Forças Componentes. Na Força Terrestre Componente (FTC), o planejamento e o assessoramento atinentes às ações cibernéticas ofensivas é encargo do comandante do Batalhão de Guerra Eletrônica, enquanto o comandante do Batalhão de Inteligência Militar é responsável pelas ações de Inteligência Cibernética. (BRASIL, 2011; EXÉRCITO BRASILEIRO, 2017a).

## 3 O PROCESSO DE BUSCA DE ALVOS CIBERNÉTICOS

O processo de busca de alvos é uma das tarefas que integram a função de combate Fogos e define a fase inicial do processo de planejamento de fogos. Ele é caracterizado por sua recursividade e continuidade, que perdura desde o tempo de paz e se prolonga ao logo de toda a campanha. Para tanto, engloba os processos de aquisição, de seleção e de análise de alvos. (EXÉRCITO BRASILEIRO, 2017b).

Sua execução vai além de possibilitar o apoio de fogo, favorecendo o emprego de outros vetores, incluindo os não cinéticos, tal como a Guerra Cibernética. Ela baseia-se nas diretrizes de fogos do escalão superior, sendo diretamente influenciada pela oportunidade, pela possibilidade de gerar efeitos colaterais e pela legalidade. No nível tático, ele inicia quando o comandante da força interpreta a missão e começa seu exame de situação (EXÉRCITO BRASILEIRO, 2017b).

Na Guerra Cibernética, sua concretização obedece à sistemática adotada na doutrina militar, sendo parte do planejamento detalhado do comandante do elemento de cibernética do escalão considerado. Entretanto, face às peculiaridades do espaço cibernético, fazem-se necessárias adaptações no seu modelo de planejamento, buscando criar soluções alternativas para contornar a complexidade do ciberespaço e sua rápida adaptação ao desenvolvimento das ações. (EXÉRCITO BRASILEIRO, 2017a).

Seu principal produto é a Proposta de Lista de Alvos Cibernéticos (PLA Ciber) que será consolidada pelos elementos de coordenação de fogos de cada escalão em presença na Lista Integrada Priorizada de Alvos (LIPA). (EXÉRCITO BRASILEIRO, 2017a).

A seguir, serão abordadas as três fases que compreendem o processo de busca de alvos: aquisição de alvos; análise de alvos; e seleção de alvos.

### 3.1 PRIMEIRA FASE: AQUISIÇÃO DE ALVOS CIBERNÉTICOS

A aquisição de alvos é um processo cíclico e consiste na detecção e localização de um objetivo com o detalhamento suficiente para permitir o efetivo emprego de armas. Ele inicia antes da campanha militar propriamente dita com a elaboração do Levantamento Estratégico de Área (LEA) e das pastas e listas de alvos e perdura durante todas suas fases. Nessas bases de dados, encontram-se os elementos que facultam o estudo detalhado da área e as informações conhecidas sobre os alvos de interesse, necessárias para o emprego das capacidades militares. (EXÉRCITO BRASILEIRO, 2001, 2017b).

Na análise de Guerra Cibernética, ele tem início com o recebimento dos planos e diretrizes do escalão superior. Nessa fase, o comandante e seu Estado-Maior buscarão entender, visualizar e descrever o ambiente operacional, especialmente o espaço cibernético, facilitando a compreensão da missão e a análise do problema. Para tanto, pode-se utilizar as técnicas de planejamento conceitual, bem como a análise dos fatores operacionais e de decisão, o que permite a revalidação contínua do planejamento. (EXÉRCITO BRASILEIRO, 2014).

Durante a definição do ambiente operacional cibernético, é natural considerar os meios de comunicações e de TI, bem como a informação em si. Entretanto, outras variáveis que também interagem com a informação e os ativos computacionais e de comunicação também devem ser ponderados, tais como indivíduos e organizações. (US ARMY, 2019).

Em sequência, devem ser identificados outros alvos potenciais existentes no interior da área de operações e de interesse da FTC, passíveis de exploração e de ataque cibernético. Nesta fase, a Inteligência terá papel fundamental no detalhamento dos componentes do alvo ou dos sistemas de alvos e suas vulnerabilidades. Como insumo, é utilizada a base de dados de alvos elaborada desde o tempo de paz. (EXÉRCITO BRASILEIRO, 2017b).

Nesta etapa, também são elencadas as Necessidades de Inteligência que comporão o Plano de Obtenção do Conhecimento. Para tanto, faz-se necessário considerar cada uma das camadas do espaço cibernético no seu estabelecimento, conforme apresentado de forma resumida no Quadro 1. Destaca-se, ainda, que o comandante do elemento de cibernética tático deve contar com meios variados de obtenção, além da fonte cibernética, para conseguir ou confirmar informações sobre os alvos a serem batidos. (EXÉRCITO BRASILEIRO, 2017b).

**Quadro 1 – Necessidades de Inteligência no Espaço Cibernético**

| Camada | Necessidades de Inteligência |
|---|---|
| Cognitiva | - Uso do espaço cibernético pelo oponente.<br>- Elementos ou entidades, da força oponente ou não, interessados ou com a capacidade de acessar dados e informações de interesse.<br>- Consumidores de dados e informações nas áreas de operações e de influência.<br>- *Hackers* e entidades presentes nas áreas de operações e de influência que podem ser cooptados.<br>- Relação dos atores locais com as camadas da rede física (telefonia celular, cibercafé, *LAN-Houses*) e da rede lógica (*sites* e aplicações).<br>- Influenciadores digitais capazes de interferir no ambiente operacional. |
| Lógica | - Páginas *web* que induzem ou tenham impacto social nas áreas de operações e de influência.<br>- Configurações de rede, softwares e sistemas criptográficos utilizados pelo oponente e suas possíveis vulnerabilidades.<br>- Endereços e protocolos pelos quais os dados de interesse podem ser acessados na Internet.<br>- Softwares utilizados na àrea de Operações.<br>- Métodos de intrusão e como eles podem ser mascarados. |
| Física | - Sistemas de C2 do oponente presentes nas áreas de operações e de influência.<br>- Pontos críticos de comunicações, presentes nas áreas de operações e de influência, que o oponente possa utilizar em seu proveito ou que possam servir de meio de entrada nas suas redes.<br>- Localização dos ativos de rede existente nas áreas de operações e de influência, tais como cabos de fibra ótica, pontos de troca de tráfego da Internet, locais públicos com pontos de acesso à Internet (cyber cafés e *LAN-Houses*), centros de processamento de dados e *intranets* militares ou governamentais.<br>- Medidas de segurança física implementadas que possam impedir o acesso a esses ativos. |

Fonte: US Army (2019), adaptado pelo autor.

Na camada Cognitiva, destaca-se que um indivíduo pode possuir várias ciber-personas que o representam de maneiras diferentes no ciberespaço, inclusive sem refletir suas características físicas reais. Por outro lado, uma única identidade cibernética pode ter vários usuários. Isto dificulta a atribuição de responsabilidades e demanda o apoio significativo da atividade de Inteligência para gerar a correta compreensão do ambiente operacional a fim de orientar o emprego da força ou criar o efeito desejado. (UNITED KINGDOM, 2016).

## 3.2 SEGUNDA FASE: ANÁLISE DE ALVOS CIBERNÉTICOS

Com a definição dos alvos potenciais a serem engajados, realiza-se a análise de suas caraterísticas e de seu relacionamento com os aspectos operativos da campanha militar. O estudo desses fatores auxilia na determinação de sua importância militar, a oportunidade para o ataque e a seleção do método de ataque mais conveniente para engajá-lo. (EXÉRCITO BRASILEIRO, 2017b).

A importância militar de um alvo é atribuída de acordo com a ameaça que este representa para o cumprimento da missão da força. Ela poderá vir especificada nas diretrizes no escalão superior ou deverá ser determinada durante os trabalhos de Estado-Maior, a quem compete apreciar a maneira que contribuem para atingir o Efeito Final Desejado ou colaboram para a conquista de Pontos Decisivos ou dos objetivos elencados pelo escalão enquadrante. Assim, será possível classificá-los de acordo coma sua natureza: estratégico, operacional ou tático. (EXÉRCITO BRASILEIRO, 2014, 2017b).

Para os passos seguintes, a taxonomia MACE (acrônimo de *Military Activities and Cyber Effects*) mostra-se uma ferramenta auxiliar valiosa. Ela consiste em um modelo criado pelo Centro de Pesquisa e Desenvolvimento de Defesa do Canadá para Pesquisa e Análise Operacional (DRDC CORA)para investigar o impacto dos efeitos cibernéticos nas decisões de comando e como integrar os recursos cibernéticos ao processo de planejamento operacional. Para isso, ela associa o tipo de ataque cibernético ao vetor de ataque e ao nível de acesso necessário para iniciá-lo, correlacionando-a com os tipos de adversário e os efeitos a serem produzidos. (BERNIER, 2013).

O Quadro 2 descreve as categorias, de interesse para este trabalho, que compõem a Taxonomia MACE:

**Quadro 2 – Descrição das seis categorias da taxonomia MACE**

| Categoria | Descrição |
|---|---|
| Ações Táticas | Ações táticas que produzem efeitos militares sobre o espaço cibernético. |
| Efeitos Cibernéticos | Descrição dos efeitos que podem ser produzidos no ambiente cibernético empregando os vários tipos de ataques cibernéticos. Compreendem a interceptação, modificação, degradação, fabricação e interrupção. |
| Tipos de Ataques | Abrange os tipos mais significativos de ataques cibernéticos, sejam eles passivos ou ativos. |
| Nível de Acesso | Descreve os diferentes níveis de acesso ao sistema ou rede, determinando as restrições impostas ao operador cibernético e os privilégios de acesso exigidos para cada tipo de ataque. São quatro: sem a necessidade de privilégios, necessidade de privilégios limitada, privilégio administrativo e acesso físico. |
| Vetores de Ataque | Relação dos métodos e das ferramentas usadas para se infiltrar em computadores e instalar o artefato malicioso. Dividem-se em mecanismos e ferramentas. |

Fonte: Bernier (2013), adaptado pelo autor.

A oportunidade para engajar um alvo cibernético está relacionada com suas características e limitações. Para tanto, o planejador deve, inicialmente, relacionar a ação tática a ser realizada com o efeito a ser provocado na dimensão informacional. (BERNIER, 2013; EXÉRCITO BRASILEIRO, 2017a, 2017b; US ARMY, 2019).

Por fim, a seleção do método de ataque procura a técnica operacional cibernética a ser empregada para se provocar o efeito desejado com o nível de acesso mínimo requerido, os vetores de ataque disponíveis, entre outros elementos que definem o alvo como compensador ou não. (BERNIER, 2013).

Como produto desta etapa, tem-se uma lista preliminar de alvos a serem engajados, que serão priorizados na fase seguinte. (EXÉRCITO BRASILEIRO, 2017b).

### 3.3 TERCEIRA FASE: SELEÇÃO DE ALVOS CIBERNÉTICOS

Nesta última fase, os meios do oponente identificados e analisados anteriormente serão relacionados nas listas de alvos disponíveis e priorizados de acordo com a avaliação de suas vulnerabilidades e da situação tática. Para tanto, propõe-se a utilização do método de priorização de alvos conhecido pelo acrônimo CRAVER (criticabilidade, recuperabilidade, acessibilidade, vulnerabilidade, efeitos e reconhecibilidade). (EXÉRCITO BRASILEIRO, 2017a, 2017b).

O quadro 3 apresenta as descrições de cada uma das seis categorias:

**Quadro 3 – Categorias do método de avaliação CRAVER**

| Categoria | Descrição |
|---|---|
| Criticabilidade | Refere-se à importância ou ao valor do alvo no contexto da campanha militar. É medido segundo o grau de comprometimento ou dos elementos críticos do ativo analisado. Ela depende de diversos fatores, tais como tempo para alcançar o efeito desejado, existência de sistemas legados e impacto sobre a funcionalidade do alvo. No campo da segurança da informação, a criticabilidade ainda corresponde à da confidencialidade, integridade ou disponibilidade do ativo informacional. |
| Recuperabilidade | É a capacidade de ser restabelecer a funcionalidade, total ou parcial, do alvo. É medido com base no tempo estimado para a recuperação do dano infligido ao ativo, considerando inclusive, a existência de *backup* do sistema ou dos dados.<br>A recuperabilidade é inversamente proporcional ao valor do alvo, ou seja, quanto maior a recuperabilidade de um alvo, menor a sua relevância para as operações. |
| Acessibilidade | Compreende a avaliação das condições que influenciam o acesso ao alvo para a realização do ataque. Está associada às medidas de segurança físicas e lógicas adotadas pelo oponente. Pode considerar, ainda, o grau de adestramento do pessoal de TI, da educação cibernética da tropa e a necessidade de acesso físico ao ativo. |
| Vulnerabilidade | Refere-se ao grau de conhecimento necessário e os meios disponíveis para a exploração do alvo, bem como sua suscetibilidade às diferentes formas de ataque. Deve considerar, ainda, a necessidade do desenvolvimento dos artefatos para a exploração ou do conhecimento de uma ou mais vulnerabilidades *Zero-Day*. |
| Efeitos | O alvo deve ser atacado apenas se os efeitos desejados estiverem coerentes com os objetivos que se deseja atingir. Ainda deve-se considerar as consequências, diretas ou indiretas, provocadas pelo ataque sobre as demais operações e a população local, levando em conta os riscos de efeitos colaterais, as restrições impostas pelo Direito Internacional Humanitário (DIH) e pelo Direito Internacional dos Conflitos Armados (DICA). |
| Reconhecibilidade | Traduz a capacidade de identificar um ativo como alvo. É avaliado o quão fácil é buscar e coletar informações sobre o alvo sem ativar as contramedidas de segurança. Deve considerar, ainda, a necessidade do acesso físico ao ativo. |

Fonte: Exército Brasileiro (2017b) e Schnaubelt, Larson, Boyer (2014), adaptado pelo autor.

Sua aplicação consiste na atribuição de pesos para cada um dos seis critérios, a fim de determinar o impacto sobre cada alvo, construindo-se uma matriz. A faixa de pontuação dos critérios é subjetiva, podendo ter seus limites inferior e superior definidos de acordo com a percepção do planejador. Após a valoração dos seis critérios em cada alvo, suas pontuações são somadas, determinando a prioridade do alvo. A pontuação final dos alvos também é relativa e a matriz pode ser reavaliada de acordo com a missão e os requisitos operacionais, bem como a percepção e experiência do planejador. (SCHNAUBELT; LARSON; BOYER, 2014).

### 3.4 PROPOSTA DE LISTA DE ALVOS CIBERNÉTICOS

Ao término do processo de busca de alvos cibernéticos, o Estado-Maior terá produzido a Proposta de Alvos Cibernéticos que substanciará a construção das Linhas de Ação do comandante tático de cibernética. Esta lista também será integrada ao planejamento dos demais meios de apoio de fogo pelos elementos de coordenação de fogos de cada escalão em presença, até a aprovação da Lista Integrada Priorizada de Alvos (LIPA). (EXÉRCITO BRASILEIRO, 2017a).

## 4 CONCLUSÃO

As ações de Guerra Cibernética geram efeitos nos domínios físicos e produzem a liberdade de ação necessária para a condução das operações militares. Assim, elas contribuem decisivamente para se alcançar o Efeito Final Desejado, os Pontos Decisivos ou conquistar objetivos táticos. Para tanto, a elaboração dos planos e ordens envolve uma metodologia particular que combina arte e ciência no intuito de solucionar o problema militar.

Como forma de auxiliar o planejamento detalhado do comandante tático do elemento de cibernética, este artigo abordou uma proposta de método de busca de alvos cibernéticos por meio da correlação da análise do ambiente operacional cibernético com duas ferramentas auxiliares: a

taxonomia MACE e a matriz CRAVER. Isto foi motivado devido à complexidade do domínio cibernético, potencializado por suas peculiaridades, e pelo fato do planejamento de fogos tradicional estar focado no emprego dos meios cinéticos.

Na fase de aquisição de alvos, a fim de proporcionar o entendimento do ambiente operacional cibernético, o ciberespaço foi observado sob o prisma da dimensão informacional, que o divide em três camadas interdependentes (física, lógica e social). Na fase de análise de alvos, foi empregada, a taxonomia MACE, a fim de se investigar o impacto dos efeitos cibernéticos nas decisões de comando e a integração dos recursos cibernéticos ao processo de planejamento operacional. Por fim, na fase de seleção dos alvos cibernéticos, foi empregada a matriz CRAVER na priorização de alvos elencados nas fases anteriores.

Estas três ferramentas associadas mostraram-se um método coerente para ser aplicado na elaboração da Proposta de Lista de Alvos Cibernéticos. Embora estas técnicas não sejam inéditas, a sua aplicação é inovadora no processo de busca de alvos cibernéticos.

Como proposta de trabalhos futuros, sugere-se a validação do modelo apresentado em exercícios e simulações, possibilitando a realização de estudos de caso. Após sua ratificação ou aperfeiçoamento, visualiza-se, ainda, a oportunidade de desenvolver-se um sistema dotado de inteligência artificial, capaz de realizar o processo de busca de alvos em curto espaço de tempo, permitindo a detecção, identificação, análise e distribuição dos dados sobre alvos compensadores de maneira automática. Tudo isto contribuirá para a evolução da doutrina militar no campo da cibernética e de planejamento de fogos.

## REFERÊNCIAS


ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2013.

BERNIER, M. **Military Activities and Cyber Effects (MACE) Taxonomy**: TM 2013-226. Ottawa: DRDC CORA, 2013.

BRANDÃO, J. E. M. D. S.; IZYCKI, E. A. Poder Ofensivo no Espaço Cibernético. In: ANDRADE, I. D. O., et al. **Desafios contemporâneos para o Exército Brasileiro**. Brasília, DF: Ipea, 2019. cap. 10, p. 241-273. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/180826_desafios_contemporaneos_para_o_exercito_brasileiro.pdf>. Acesso em: 28 ago. 2019.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas**: MD30-M-01. Brasília, DF: Ministério da Defesa, 2011. v. 1.

BRASIL. Ministério da Defesa. **Política de Defesa Cibernética**: MD31-P-02. Brasília, DF: Ministério da Defesa, 2012.

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

EXÉRCITO BRASILEIRO. **Estratégia**: C-124. 3. ed. Brasília, DF: Estado-Maior do Exército, 2001.

EXÉRCITO BRASILEIRO. **Processo de Planejamento e Condução das Operações Terrestres**: EB20-MC-10.211. Brasília, DF: Estado-Maior do Exército, 2014.

EXÉRCITO BRASILEIRO. **Fogos**: EB20-MC-10.206. Brasília, DF: Estado-Maior do Exército, 2015.

EXÉRCITO BRASILEIRO. **Guerra Cibernética**: EB70-MC-10.232. Brasília, DF: Comando de Operações Terrestres, 2017a.

EXÉRCITO BRASILEIRO. **Planejamento e Coordenação de Fogos**: EB70-MC-10.346. Brasília, DF: Comando de Operações Terrestres, 2017b.

HUTCHINS, E. M.; CLOPPERT, M. J.; AMIN, R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY, 6., 2011, Washington, DC. **Proceedings** […]. p. 113-125. Disponível em: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>. Acesso em: 23 ago. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27032:** Information Technology - Security Techniques - Guidelines for Cybersecurity. Geneva: ISO/IEC, 2012.

SCHNAUBELT, C. M.; LARSON, E. V.; BOYER, M. E. **Vulnerability Assessment Method Pocket Guide:** a tool for center of gravity analysis. Santa Monica, CA: RAND Corporation, 2014. 142 p.

UNITED KINGDOM. Ministry of Defence. **Cyber Primer**. 2. ed. Swindon: Development, Concepts and Doctrine Centre of Ministry of Defence, 2016. Disponível em: <www.gov.uk/mod/dcdc>. Acesso em: 5 set. 2019.

US ARMY. **Cyberspace Operations Concept Capability Plan 2016-2028:** TRADOC Pamphlet 525-7-8. Newport News: U.S. Army Capabilities Integration Center, 2010.

US ARMY. **Intelligence Preparation of the Battlefield:** ATP 2-01.3. Washington, DC: Department of the Army, 2019.

USA. Departament of Defense. **Cyberspace Operations:** JP 3-12. Washington: Departament of Defense, 2018.

*Artigo realizado a partir do trabalho de conclusão do Curso de Especialização em Planejamento de Guerra Eletrônica (CIGE) e de Guerra Cibernética em apoio às Operações em 2019 pelo Tenente Coronel de Comunicações Vinícius Lacerda Vasquez do Exército Brasileiro. E-mail: lacerda.vinícius@eb.mil.br.