ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM FELIPE RODRIGUES DE VASCONCELLOS

PRINCÍPIOS E EMPREGO DE FOGOS CIBERNÉTICOS

Rio de Janeiro
2018

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM FELIPE RODRIGUES DE VASCONCELLOS

PRINCÍPIOS DE EMPREGO DE FOGOS CIBERNÉTICOS

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Guerra Cibernética

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 FELIPE RODRIGUES DE VASCONCELLOS**

Título: **PRINCÍPIOS DE EMPREGO DE FOGOS CIBERNÉTICOS**

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

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

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

_____
FELIPE RODRIGUES DE VASCONCELLOS – Cap
Aluno

PRINCÍPIOS DE EMPREGO DE FOGOS CIBERNÉTICOS

Felipe Rodrigues de Vasconcellos
Juliano Brandão Palácio

RESUMO

A função de combate fogos é uma das seis adotadas pelo Exército Brasileiro e reúne atividades, tarefas e sistemas inter-relacionados que permitem o emprego coletivo e coordenado de fogos cinéticos e não cinéticos. O emprego dessa capacidade é regido por quatro princípios previstos na doutrina do Exército Brasileiro: centralização do comando e descentralização da execução; Oportunidade e continuidade do fogo; obtenção e manutenção da superioridade; e profundidade. Contudo, alguns autores discordam dessa definição e sugerem a adoção de princípios diferentes, mais afetos aos fogos cibernéticos. Dessa maneira, o objetivo desse trabalho foi identificar os princípios de emprego de fogos não cinéticos, decorrentes de um ataque cibernético. Para tanto, foi distribuído um questionário aos especialistas em guerra cibernética das Forças Armadas com a finalidade de ratificar/retificar os princípios listados no manual FOGOS EB20-MC-10.206, tomando como referência a pesquisa de outros autores. O resultado alcançado revela que os princípios atualmente aceitos na doutrina brasileira devem ser alterados, pois não atendem às particularidades do domínio cibernético, devendo ser adotados os seguintes: discrição, perícia, prontidão, adaptabilidade e precisão.

Palavras-chave: Guerra Cibernética, fogos, princípios, doutrina

ABSTRACT

The fires combat function is one of six adopted by the Brazilian Army and brings together activities, tasks and interrelated systems that allow the collective and coordinated use of kinetic and non-kinetic fires. The use of this capacity is governed by four principles foreseen in the doctrine of the Brazilian Army: centralization of command and decentralization of execution; Opportunity and continuity of fire; obtaining and maintaining superiority; and depth. However, some authors disagree with this definition and suggest the adoption of different principles, more affect to cyber

fires. In this way, the objective of this work was to identify the principles of the use of non-kinetic fires, due to a cyber attack. In order to do so, a questionnaire was distributed to specialists in cyber warfare in the Armed Forces, with the purpose of ratifying / rectifying the principles listed in the FOGOS EB20-MC-10206 manual, taking as reference the research of other authors. The result achieved reveals that the principles currently accepted in Brazilian doctrine must be changed, since they do not meet the particularities of the cyber domain, and the following should be adopted: discretion, expertise, readiness, adaptability and precision.

Keywords: Cyberwar, fires, principles, doctrine

1 INTRODUÇÃO

A tecnologia da informação é uma área “púbere” do conhecimento humano quando comparada a ciências mais maduras como a matemática, física ou a botânica. Pouco mais de 40 anos transcorreram desde a transmissão da mensagem enviada pelo professor Leonard Kleinrock da Universidade da Califórnia ao *Stanford Research Institute*. As poucas letras que chegaram ao destinatário em outubro de 1969 ganharam assento nos livros de história como o primeiro e-mail enviado pela rede de computadores. (WIKIPEDIA,2017)

Do uso instável e restrito dos anos 1960 ao fenômeno universal dos dias atuais, a tecnologia da informação avançou com passos largos e orientados a transformar a maneira como a sociedade se relaciona. Inúmeras oportunidades surgiram, principalmente com a consolidação da internet, e o setor bélico, como tantos outros, percebeu a necessidade de incorporar os benefícios desse novo ramo.

O espaço cibernético passou a ser visto como um novo ambiente para atividades bélicas devido a sua capilaridade nos demais domínios (terrestre, aéreo, marítimo e espacial) e pela íntima relação com as infraestruturas críticas, garantindo um efeito cinético a eventuais ataques cibernéticos, como a paralisação de uma usina ou a interrupção do fornecimento de energia de uma cidade. Esse tipo de efeito depende do judicioso emprego de ações cibernéticas ofensivas através do uso de fogos não cinéticos, como *botnets, malware* ou *trojans*.

Esses recursos passam a compor o arcabouço de opções de um comandante militar, podendo atuar complementarmente ao uso dos fogos cinéticos, largamente empregados em combates passados e com doutrina sedimentada.

Esse conjunto de armas (cinéticas e não cinéticas) compõem uma das sete funções de combates adotadas pelo Exército Brasileiro, denominada FOGOS (BRASIL, 2017b). Tal função possui uma série de procedimentos e princípios definidos nos manuais da Força Terrestre, como os “princípios de emprego dos sistemas de fogos”, que servem de base para a execução e planejamento do uso das armas contra um alvo definido. (BRASIL, 2015)

Esses princípios são “pontos de referência que orientam e subsidiam os chefes militares no planejamento e na condução da guerra sem, no entanto, condicionar suas decisões”. Cabe aos comandantes nos diversos níveis de decisão, ao planejar e executar uma campanha ou operação, levar “em consideração o que preconizam os

princípios, interpretando-os e aplicando-os criteriosamente em face da situação, decidindo quais irá privilegiar, em detrimento de outros. (BRASIL, 2014c)

Diante da relevância da adoção de princípios que traduzam a realidade de uma operação militar para orientar de maneira acertada os planejamentos futuros, é necessário avaliar se a doutrina referente ao emprego de fogos, atualmente adotada pelo Exército Brasileiro, está aderente à nova capacidade inserida pela guerra cibernética através dos seus fogos não cinéticos.

1.1 PROBLEMA

A doutrina da função de combate FOGOS cita largamente o uso de fogos não cinéticos, mais especificamente aqueles decorrentes da “guerra cibernética, guerra eletrônica, operações de apoio à informação, dentre outros que, não implicando a execução de fogo cinético nem caracterizando o emprego de elementos de manobra ou de proteção”. (BRASIL, 2015)

Todavia, a utilização de cada meio supracitado é carregada de especificidades decorrentes das técnicas e tecnologia que se apoiam e do alvo a que são direcionados. Como exemplo, uma ação de apoio à informação tem como mote principal a dimensão humana, por sua vez, um ataque cibernético tem como escopo principal a dimensão informacional (BRASIL, 2017b).

Dessa forma, surge a seguinte problemática de pesquisa: Quais os princípios de emprego dos sistemas de fogos cibernéticos?

OBJETIVOS

Para responder o problema proposto, espera-se alcançar o seguinte objetivo: identificar os princípios de emprego de fogos não cinéticos, decorrentes de um ataque cibernético.

Ao perseguir o objetivo geral, acredita-se que os seguintes objetivos específicos serão alcançados:

a) atualizar os princípios de emprego de fogos para adequar a realidade dos fogos não cinéticos decorrentes de um ataque cibernético;

b) apresentar propostas de atualização do manual “Doutrina Militar de Defesa. MD51-M-04”;

c) Identificar os princípios de emprego do sistema de fogos cibernéticos mais relevantes.

Para tanto, a delimitação do presente trabalho é a identificação dos princípios de emprego dos fogos não cinéticos no nível tático em ações ofensivas do Exército Brasileiro.

1.2 JUSTIFICATIVAS E CONTRIBUIÇÕES

A Estratégia Nacional de Defesa do Brasil (END) de 2008 estabeleceu três áreas estratégicas para o país: cibernética, espacial e nuclear. Cada força armada ficou responsável por fomentar um desses setores, cabendo ao Exército Brasileiro o fomento e condução da cibernética a nível nacional. Diante desse desafio, a força terrestre inseriu entre seus projetos estratégicos a “Defesa Cibernética”, dedicando especial atenção para a capacitação de recursos humanos, criação de órgãos e desenvolvimento de normativas. (BRASIL, 2008)

Ao contrário de algumas áreas, onde foi possível tomar como referência as lições aprendidas de outras Forças Armadas para construir uma doutrina autóctone fundamentada nas boas práticas realizadas pelo mundo, com a cibernética essa dinâmica não foi possível, pois até as nações mais desenvolvidas estão dando os primeiros passos nesse setor.

A doutrina que baliza essa nova capacidade está em construção e precisa ser cuidadosamente desenhada para conduzir o setor ao encontro das diretrizes estabelecidas pela END e garantir às FA o uso bélico das possibilidades oferecidas pela cibernética. Especial atenção deve ser dada aos princípios impostos nestes regulamentos, pois serão os fundamentos para o planejamento e emprego das atividades futuras.

2 METODOLOGIA

Para colher subsídios que permitissem formular uma possível solução para o problema, o delineamento desta pesquisa contemplou leitura analítica e fichamento das fontes, questionários, argumentação e discussão de resultados.

Quanto à forma de abordagem do problema, utilizaram-se, principalmente, os conceitos de pesquisa **quantitativa**, pois as referências numéricas obtidas por meio dos questionários foram fundamentais para a compreensão da opinião dos militares.

Quanto ao objetivo geral, foi empregada a modalidade **exploratória** através da

análise da bibliografia existente, aplicação de questionários destinados a uma amostra com experiência profissional, afim de coletar a opinião de especialistas no assunto.

2.1 REVISÃO DE LITERATURA

O emprego dos fogos é regido por quatro princípios consolidados na doutrina militar brasileira, são eles: (BRASIL, 2015)

1) Centralização do comando e descentralização da execução - Esse princípio é autoexplicativo, mas a doutrina destaca que a centralização da execução é necessária para a obtenção do emprego em massa dos fogos, mas uma excessiva centralização dificulta a capacidade de intervenção na operação, já que todos os meios empregados de uma vez, não daria margem para um escalão ser apoiado por outro, caso a situação tática exija.

2) Oportunidade e continuidade do fogo - O princípio da oportunidade e continuidade do fogo leva em conta o caráter dinâmico e mutável do ambiente operacional, que exige dos sistemas de fogos velocidade de reposta para ser eficaz contra os alvos. O comando e controle para as ações de avaliação e tomada de decisão entre os diferentes níveis de decisão e a velocidade na transmissão das informações geradas entre os sistemas de busca de alvos e o sistema de armas que será empregada, são elementos essenciais para garantir maior velocidade no emprego dos fogos.

3) Princípio da obtenção e manutenção da superioridade - O princípio da obtenção e manutenção da superioridade impõe a conquista da superioridade de fogos em determinado local e momento, conforme a necessidade tática, garantindo ao comando uma maior liberdade para o cumprimento da missão. Destarte, é preciso buscar o ponto mais vulnerável do sistema de apoio de fogo inimigo e concentrar o ataque nesse local com vistas a anular a capacidade de fogos inimiga.

4) Princípio da profundidade - O emprego dos fogos deve ser capaz de atingir o inimigo em profundidade durante todo o combate, com foco nas organizações operativas, sistemas de comando e controle, de apoio de fogos e logística, “para o qual se exigirá um adequado escalonamento em profundidade de apoio de fogo em função de seus alcances e suas características”.

Esses quatro princípios se referem ao emprego de fogos, sem distinção entre cinéticos e não cinéticos. Com objetivo de identificar apenas os princípios de emprego

de fogos cibernéticos, uma espécie do gênero não cinético, VASCONCELLOS (2018) analisou casos históricos de ataques cibernéticos, bem como a perspectiva de alguns autores sobre o assunto, tudo sobre quatro prismas: possibilidades e restrições da guerra cibernética, capacidades do Exército Brasileiro (organização) e o sistema de apoio de fogos. Essa análise permitiu ao autor identificar oito princípios, retificando o que está atualmente previsto na doutrina militar da força terrestre, conforme lista abaixo:

1) Amplitude do ataque - Um ataque com atuador cibernético atinge inúmeros alvos, dentro ou fora do escopo imposto pelo atacante, com isso o alcance dos efeitos produzidos pela arma cibernética é bastante abrangente. Por exemplo, o APT batizado como Ghostnet infectou 1295 computadores em 103 países, ilustrando a capilaridade desse tipo de arma (BBC, 2009). Até mesmo em casos que o alvo era extremamente específico, como o Stuxnet, foram identificados efeitos em inúmeros dispositivos hospedados em diferentes países. Isso acontece, devido a capacidade de locomoção lateral do código malicioso e pela capacidade do *payload* em afetar qualquer dispositivo que possua a vulnerabilidade explorada pela ameaça. (SHEARER, 2017)

Na técnica de DDoS essa característica é ainda mais patente. Devido a própria natureza da ação é necessário um ataque amplo, contra inúmeros alvos para obter o efeito de indisponibilidade de um serviço, conforme ocorrido nos episódios da Geórgia e Estônia, quando servidores de inúmeras intuições foram afetadas pela ação ofensiva. (CLARKE, 2015)

Essa característica conduz ao **princípio da amplitude. Seguir esse princípio significa empregar armas cibernéticas que permitam resultados abrangentes, com grande quantidade de alvos em potencial.** (VASCONCELLOS, 2018)

2) Dificuldade na identificação da origem - A identificação da autoria de um ataque cibernético não é comum, pelo contrário, a história mostra que em grande parte das ações ofensivas a vítima não consegue reunir provas suficientes para comprovar a autoria da ação. Isso ocorre devido a característica dos protocolos e da própria internet, que permitem o emprego de técnicas antirastreamento, como o uso de proxy, vpn e da rede tor. (SILVA, 2017)

Casos como o night dragon, Titan Rain, Gauss e Duqu são exemplos de APT, cuja autoria não foram determinadas (SANCHES ,2017). De maneira semelhante ocorre com a técnicas de DDoS, que, mesmo sendo bastante ruidosa, pode ter sua

origem camuflada, conforme observado nos ataques contra a Geórgia e Estônia (CLARKE, 2015). Essa característica é buscada não só em ações de estado, mas também por grupos *hackers*, como o Ouroburus, que sequestrou satélites para dificultar a identificação da origem de seus ataques. (TIMES, 2015)

Essa característica conduz ao princípio da **discrição. Seguir esse princípio significa empregar armas cibernéticas com técnicas e procedimentos que dificultem a identificação da autoria do ataque, prejudicando a resposta inimiga.** (VASCONCELLOS, 2018)

3) Necessidade de elevado conhecimento técnico - O emprego de fogos cibernéticos demanda elevado conhecimento técnico por parte do executante, pois a mínima variação na configuração do artefato malicioso pode alterar o efeito desejado no alvo, gerando resultados improváveis (APT). Além disso, os *softwares* e sistemas estão agregando mais funcionalidades e se tornando mais complexos para atender as novas demandas dos usuários. (OWENS et al, 2009)

Uma arma cibernética para ser eficaz tem que encontrar uma falha no sistema alvo, que permita a sua exploração e execução do *payload* para realizar uma ação desejada. Encontrar essas vulnerabilidades é uma tarefa que exige grande conhecimento técnico por parte dos atacantes, pois, muitas vezes, é necessário descobrir uma falha desconhecida inclusive pelos desenvolvedores de determinado sistema (OWENS et al, 2009). O APT Stuxnet, por exemplo, lançou mão de quatro vulnerabilidades inéditas (zero-day) para cumprir sua finalidade, exigindo uma equipe com destacada capacidade técnica. É por isso que em países onde a domínio cibernético é encarado como uma potencial arena de combate, como o Brasil e a Coréia do Norte, a seleção e preparação dos guerreiros cibernéticos é um tema presente na agenda das Forças Armadas. (CLARKE, 2015)

Para empregar as armas cibernéticas citadas nessa pesquisa (DDoS e APT) é necessário enorme expertise dos atacantes. Montar e gerenciar uma *botnet* não é uma tarefa trivial, muito menos tornar um APT efetivo, é indispensável conhecer as características dos protocolos para a fase de coleta dados e o funcionamento dos Sistemas Operacionais no desenvolvimento de *rootkits* (APT), para citar apenas duas das fases de uso dessa arma cibernética. (FIVE, 2011)

Essa característica conduz ao princípio da **perícia. Seguir esse princípio significa empregar armas cibernéticas com elevado refinamento técnico para**

viabilizar a sobreposição da defesa inimiga e encontrar vulnerabilidades que permitam o alcance do efeito desejado. (VASCONCELLOS, 2018)

4) Preparação do campo de batalha - O emprego da capacidade cibernética ofensiva exige certo grau de preparação para tornar a arma disponível para emprego, haja vista a necessidade de estudar o alvo com relativa antecedência para encontrar uma vulnerabilidade que viabilize o ataque. Essa característica torna a variável tempo um limitador importante das ações cibernéticas, pois essa preparação pode levar meses até que sejam alcançadas as condições necessárias para o ataque. Até mesmo quando a técnica utilizada é um tanto menos refinada, como o DDoS, há a necessidade de algum tempo de preparação para "cooptar" dispositivos e montar uma ou mais *botnets*. (SANS, 2015)

Conhecedores dessa necessidade, alguns países preparam seus artefatos cibernéticos e o "campo de batalha" desde o tempo de paz, instalando *backdoors* e realizando reconhecimentos nas estruturas potencialmente inimigas ou vendendo roteadores para serem acessados quando o conflito for deflagrado. (CLARKE, 2015)

Essa característica conduz ao princípio da **prontidão. Seguir esse princípio significa preparar o "campo de batalha" (espaço cibernético) com antecedência, preferencialmente antes do conflito ser deflagrado, garantindo a disponibilidade das armas cibernéticas durante o combate.** (VASCONCELLOS, 2018)

5) Adaptabilidade do ataque - O domínio cibernético garante ao atacante, muitas vezes, o acompanhamento em tempo real dos efeitos produzidos pelo ataque, permitindo a realização de alterações no artefato, caso o alvo adote medidas corretivas para proteger o seu sistema. (OWENS et al, 2009)

Conforme ocorre com o emprego das armas cinéticas, quando um míssil é interceptado pela defesa antiaérea oponente, no espaço cibernético se espera que a defesa adote medidas para interromper o ataque em curso. A técnica de DDoS, por exemplo, pode se tornar ineficaz caso seja implementado um filtro para bloquear os pacotes de determinada origem. Nessa situação, o atacante pode e deve adotar medidas para suplantar essa barreira e manter a eficácia da ação. (SANS, 2015)

Por mais que grande parte dos ataques seja precedida de um reconhecimento dos alvos, nada impede que o oponente altere algum parâmetro do seu sistema, tornando-o mais seguro ou com características diferentes. Nessa situação o atacante deve preparar sua arma cibernética para se adaptar a condições imprevistas, capaz

de encontrar outras vulnerabilidades, um novo canal de acesso à rede alvo (APT) ou qualquer outra medida que supere o novo cenário imposto pela defesa adversária.

Essa característica conduz ao princípio da **adaptabilidade. Seguir esse princípio significa adaptar a arma cibernética para continuar efetiva, mesmo diante de um novo cenário, como a ação corretiva de uma vulnerabilidade pela vítima.** (VASCONCELLOS, 2018)

6) Necessidade de atenção aos efeitos colaterais - O efeito colateral é bastante comum em uma ação cibernética ofensiva e pode ser, inclusive, o resultado desejado com o ataque. Quando o efeito colateral é identificado e faz parte da estratégia do emprego da arama cibernética não há problemas, porém existem os efeitos colaterais não desejados, que são difíceis de prever e podem trazer prejuízos a população civil, a países sem envolvimento com o conflito e até mesmo ao próprio atacante. (OWENS et al, 2009)

Para evitar qualquer efeito indesejado o emprego das armas cibernéticas deve primar pela precisão, cabendo aos responsáveis um planejamento diligente sobre os possíveis desdobramentos do ataque. Para atingir esse objetivo é indispensável a atenção ao princípio da perícia, pois apenas profissionais com grande conhecimento técnico conseguem prever com certa exatidão qual o comportamento de uma arma não cinético no espaço cibernético e como limitar seu espectro de atuação. (OWENS et al, 2009)

Essa característica conduz ao princípio da **precisão. Seguir esse princípio significa realizar ações precisas, com pleno entendimento das consequências diretas e indiretas do uso da arma cibernética, evitando que sejam causados danos indesejáveis a terceiros e à própria infraestrutura.** (VASCONCELLOS, 2018)

7) Necessidade de comando e execução centralizada - O comando de uma operação ofensiva deve ser unificado para evitar que as ações de tropas diferentes interfiram umas nas outras. Para viabilizar esse controle, deve haver um comandante único em algum ponto da cadeia de comando que tenha ciência de todos os eventos praticados por uma força no espaço cibernético, cabendo a ele orquestrar todas as capacidades disponíveis com objetivo de evitar fogo amigo ou interferência. (GRAHAM, 2016)

A execução centralizada também deve ser buscada, pois o emprego de armas cibernéticas exige a participação de profissionais com habilidades em diferentes

campos da informática, além de especialistas no setor ou infraestrutura alvos. (controle de danos) Como as ações no espaço cibernética não demandam proximidade física, nada impede que os militares responsáveis por executar a ação ofensiva permaneçam reunidos trocando informações técnicas e buscando sinergia para vencer as barreiras técnicas impostas pelas características do domínio cibernético e pelos dispositivos de segurança presentes nas redes e sistemas. (GRAHAM, 2016)

Essa característica conduz ao princípio do **comando e execução centralizado. Seguir esse princípio significa realizar ações com comando único e execução centralizada, evitando que as medidas de tropas diferentes interfiram umas nas outras, além de garantir a sinergia necessária na execução das ações ao concentrar os especialistas em um único ponto de atuação.** (VASCONCELLOS, 2018)

8) Necessidade de continuidade do fogo - Uma arma cibernética busca corromper a integridade, disponibilidade e/ou confidencialidade dos seus alvos. Contudo essas características são extremamente voláteis e, na maioria das ocasiões, dependem de uma ação contínua por parte do atacante para manter o efeito desejado. (OWENS et al, 2009)

Ao contrário de uma ponte que demanda um tempo razoável para ser reconstruída após ser bombardeada, um servidor se torna disponível no segundo seguinte ao término de um ataque DDoS. Com isso, para atingir e manter o efeito desejado um atacante deve planejar o emprego de suas armas cibernéticas de maneira contínua para não permitir que o alvo volte a utilizar seus sistemas. (SANS, 2015)

Essa característica conduz ao **princípio da continuidade. Seguir esse princípio significa realizar ataques persistentes, cujo efeito dure o período necessário para atingir o efeito desejado.** (VASCONCELLOS, 2018)

Comparando os princípios atualmente aceitos no manual FOGOS EB20-MC-10.206 do EB e os sugeridos por VASCONCELLOS (2018), é possível traçar a seguinte comparação:

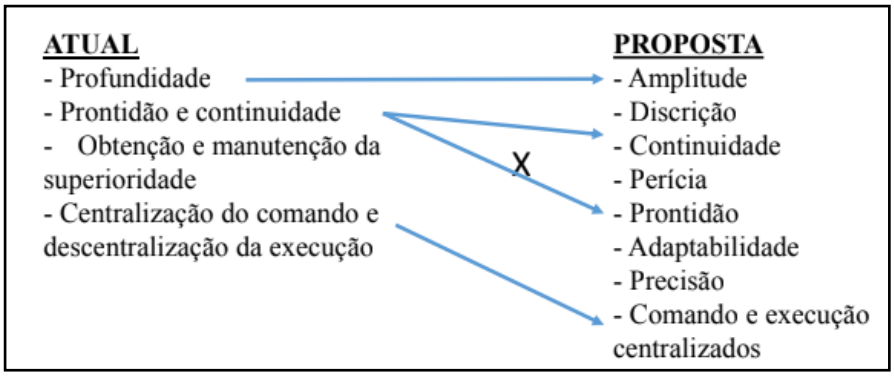

Figura 01 – Comparação entre os princípios listados no manual EB20-MC-10.206 e os propostos por VASCONCELLOS (2018)
Fonte: o autor

O princípio profundidade é semelhante ao conceito de amplitude; o princípio prontidão e continuidade foi desmembrado em dois; e o princípio centralização do comando e descentralização da execução foi alterado para comando e execução centralizados.

Para avaliar se os princípios de emprego dos fogos cibernéticos propostos por VASCONCELLOS (2018) estão alinhados com a realidade, foi conduzida uma pesquisa de opinião com especialistas em guerra cibernética.

2.2 COLETA DE DADOS

Na sequência do aprofundamento teórico a respeito do assunto, o delineamento da pesquisa contemplou a coleta de dados através de questionário.

2.2.1 Questionário

A amplitude do universo foi estimada a partir do efetivo de oficiais e sargentos que concluíram o curso de guerra cibernética do Exército, ofertado pelo Centro de Instrução de Guerra Eletrônica, que capacita o militar a exercer atividades no setor cibernético.

Como o tema da pesquisa abrange uma área ainda pouco madura nas Forças Armadas brasileiras e o número de especialistas capacitados para realizar ações ofensivas é relativamente pequeno, foi possível submeter o questionário para 59 militares, que atualmente possuem a especialização em guerra cibernética.

Cabe uma ressalva sobre a qualidade das opiniões coletadas através do questionário. Dentro do rol de atividades da Guerra Cibernética, as ações de proteção e exploração são mais comumente executadas em detrimento do ataque cibernético,

isso se deve a fatores como: falta de amparo jurídico, hipóteses de emprego das FA, tecnicidade da atividade e falta de uma cultura institucional para fomentar esse tipo de ação. Diante desse cenário, apesar da população selecionada ser a melhor fonte de dados para uma pesquisa sobre esse tema nas FA brasileiras, é preciso levar em conta que grande parte dos participantes nunca participou de uma ação cibernética ofensiva real, limitando-se apenas ao conhecimento teórico e treinamentos simulados.

Com a finalidade de identificar possíveis falhas no instrumento de coleta de dados, foi utilizado um questionário piloto com 03 capitães-alunos da Escola de Aperfeiçoamento de Oficiais (EsAO), que faziam parte da população selecionada. Ao final do pré-teste, não foram observados erros que justificassem alterações no questionário e, portanto, seguiram-se os demais de forma idêntica.

3 RESULTADOS E DISCUSSÃO

Buscou-se compreender a opinião dos oficiais e sargentos especialistas em guerra cibernética das Forças Armadas brasileiras através da distribuição de um questionário de percepção dos princípios de emprego dos fogos cibernéticos, cujo modelo consta no Apêndice “A” deste trabalho. Ao todo foram distribuídos 59 questionários, dos quais 54 para militares do Exército Brasileiro, 01 para militares da Marinha do Brasil e 04 para militares da Força Aérea Brasileira. Foram respondidos adequadamente 43 questionários, não havendo a necessidade de descartar nenhuma reposta por erro de preenchimento. A distribuição da ferramenta de coleta de dados ocorreu por canal eletrônico, entre os dias 13 e 14 de junho de 2018.

O primeiro item do questionário solicitava a identificação do participante, com objetivo de permitir um eventual contato futuro para mitigar dúvidas sobre o seu preenchimento. Houve a preocupação de não obrigar a resposta desse item, garantindo a possibilidade de anonimato aos que assim preferiam.

Na questão 02 foi perguntado aos militares: “levando em consideração que um ATAQUE CIBERNÉTICO compreende ações para INTERROMPER, NEGAR, DEGRADAR, CORROMPER ou DESTRUIR sistemas computacionais do oponente, qual a sua experiência com esse tipo de atividade?”

TABELA 1 - Opinião absoluta e percentual do total da amostra acerca da experiência em ações cibernéticas ofensivas

Grupo / Avaliação	Amostra	
	Valor absoluto	Percentual
Nunca realizei	3	7%
Realizei apenas para fins didáticos, poucas vezes	20	46,5%
Realizei apenas para fins didáticos, com frequência	16	37,2%
Realizei ações reais, poucas vezes	4	9,3%
Realizei ações reais, com frequência	0	0,0%
TOTAL	43	100,0%

Fonte: o autor

A reposta da amostra revela que poucos militares (4/9,3%) realizaram ações ofensivas em um cenário real. Esse fato pode ser explicado devido a dois principais fatores, o primeiro diz respeito ao pouco conhecimento das capacidades cibernéticas por parte dos militares em função de comando e de estado-maior, e que não demandam o emprego dor recursos disponíveis pela cibernética. O outro fator é a inexistência de conflitos externos, que justifiquem o uso de fogos cibernéticos contra um alvo real.

Se a resposta da amostra revelou que poucos realizaram ações ofensivas em um cenário real, por outro lado, o percentual de militares que utilizaram técnicas dessa natureza para fins didáticos chega a 83,7%, revelando que a grande maioria dos participantes tem algum tipo de experiência nessa arena, o que reforça a relevância dos resultados encontrados através do instrumento de coleta de dados.

Outro dado revelador é que 9% dos especialistas em guerra cibernética nunca realizou esse tipo de ação, expondo uma falha na formação dos guerreiros cibernéticos, que deixam o curso de G Ciber sem praticar algumas das técnicas essenciais ao seu futuro ofício.

Na questão 03 foi apresentada a seguinte questão aos militares: “Princípios são pontos de referência que orientam e subsidiam os chefes militares no planejamento e na condução da guerra sem, no entanto, condicionar suas decisões. São os pilares que sustentam o sucesso de uma operação. Levando em conta essa definição, aponte quais os princípios mais relevantes em uma ação cibernética ofensiva”. Foram listados os seguintes princípios: amplitude, discrição, perícia, prontidão, adaptabilidade, precisão, comando e execução centralizados, continuidade, profundidade, obtenção e manutenção da superioridade e centralização do comando e descentralização da

execução. Foi facultado aos militares escolher quantos princípios achassem necessários, podendo selecionar todos os 11 ou nenhum

TABELA 2 - Opinião absoluta e percentual do total da amostra acerca dos princípios de emprego dos fogos cibernéticos

Grupo / Avaliação	Amostra	
	Valor absoluto	Percentual
Amplitude	7	16,3%
Discrição	36	83,7%
Perícia	35	81,4%
Prontidão	28	65,1%
Adaptabilidade	24	55,8%
Precisão	35	81,4%
Comando e execução centralizados	8	18,6%
Centralização do comando e descentralização da execução	18	41,9%
Continuidade	21	48,8%
Obtenção e manutenção da superioridade	13	30,2%
Profundidade	21	48,8%

Fonte: o autor

A resposta dos participantes foi a seguinte: amplitude 16,3% (7), discrição 83,7% (36), perícia 81,4% (35), prontidão 65,1% (28), adaptabilidade 55,8% (24), precisão 81,4% (35), comando e execução centralizados 18,6% (8), centralização do comando e descentralização da execução 41,9% (18), continuidade 48,8% (21), obtenção e manutenção da superioridade 30,2% (13) e profundidade 48,8% (21). O gráfico abaixo mostra o resultado obtido.

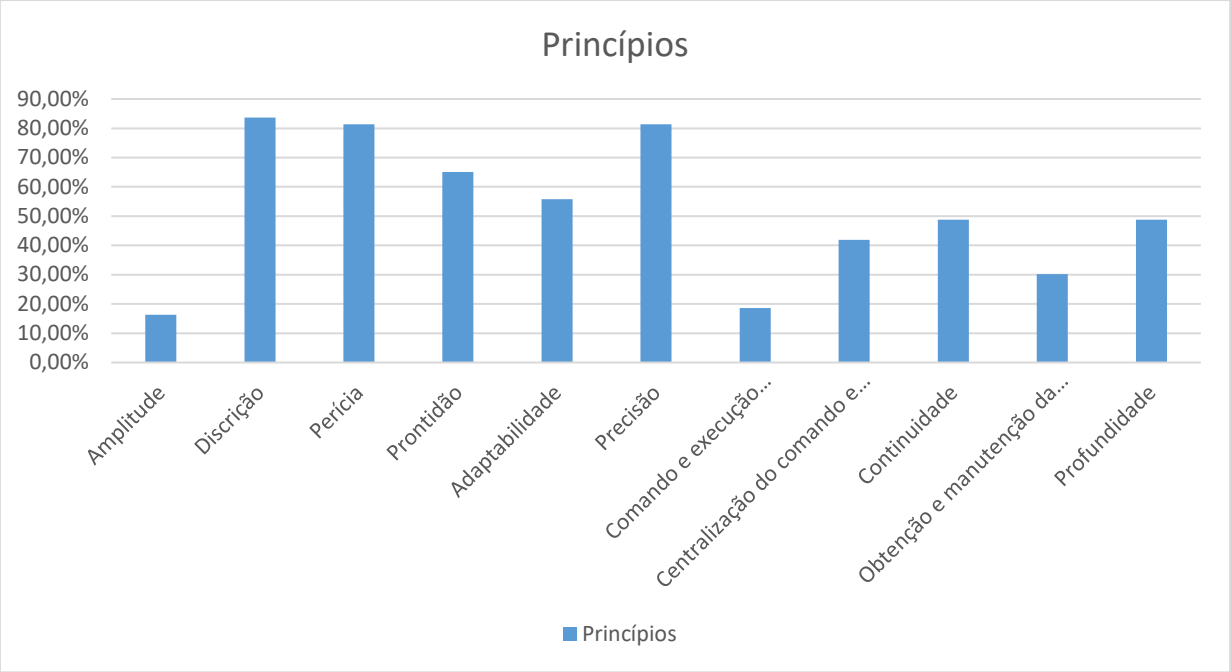

Figura 02 – Percentual de resposta da amostra para cada princípio de emprego de fogos cibernéticos
Fonte: o autor

Os seguintes princípios foram escolhidos por mais da metade dos participantes: discrição, perícia, prontidão, adaptabilidade e precisão. Com isso, é possível afirmar que esses cinco princípios foram ratificados pela amostra, como pontos de referência aos chefes militares no planejamento do emprego de fogos cibernéticos.

Por outro lado, os princípios menos selecionados pela amostra foram: amplitude (16,3%), comando e execução centralizados (18,6%) e obtenção e manutenção da superioridade (30,2%).

O objetivo desse item era confirmar ou refutar os princípios de emprego dos fogos cibernéticos sugeridos no referencial teórico, com base na opinião dos especialistas integrantes da amostra.

A quarta e última questão apresentava a seguinte pergunta: “Dos princípios listados acima, qual o senhor considera mais relevante em uma ação cibernética ofensiva?”.

TABELA 3 - Opinião absoluta e percentual do total da amostra acerca dos princípios de emprego dos fogos cibernéticos mais relevantes

Grupo / Avaliação	Amostra	
	Valor absoluto	Percentual
Discrição	15	34,9%
Perícia	11	25,6%

Prontidão	8	18,6%
Precisão	6	14%
Centralização do comando e descentralização da execução	2	4,7%
Adaptabilidade	1	2,3%
TOTAL	43	100,0%

Fonte: o autor

A resposta da amostra foi a seguinte: discrição (34,9%), perícia (25,6%), prontidão (18,6%), precisão (14%), centralização do comando e descentralização da execução (4,7%) e adaptabilidade (2,3%).

O objetivo desse item foi identificar qual princípio é o mais relevante para ser levado em conta durante o planejamento de emprego dos fogos cibernéticos.

4 CONSIDERAÇÕES FINAIS

No contexto bélico, uma função de combate é um conjunto relativamente homogêneo de atividades e tarefas afins, que atendem a uma finalidade comum em uma operação militar (BRASIL, 2014). A função de combate fogos é uma das seis adotadas pelo Exército Brasileiro e reúne atividades, tarefas e sistemas inter-relacionados que permitem o emprego coletivo e coordenado de fogos cinéticos e não cinéticos. (BRASIL, 2015)

O emprego dos fogos é regido por quatro princípios largamente aceitos e consolidados na doutrina militar brasileira, são eles: Centralização do comando e descentralização da execução; oportunidade e continuidade dos fogos; obtenção e manutenção da superioridade; e profundidade (BRASIL, 2015). A doutrina trata esses princípios como universais para o uso de fogos cinéticos e não cinéticos, mesmo com a reconhecida diferença entre o domínio cibernético e os demais (terrestre, marítimo, aéreo e espacial). Diante dessa constatação e com base em pesquisa bibliográfica de ações cibernéticas ofensivas ocorridas contra estados, VASCONCELLOS (2018) sugeriu oito novos princípios em substituição aos já existentes, são eles: Amplitude, discrição, perícia, prontidão, adaptabilidade, precisão, comando e execução centralizados e continuidade.

Com base nos princípios atualmente aceitos pela doutrina do EB e nos propostos pelo trabalho supracitado, surgiu o problema que norteou essa pesquisa: Quais os princípios de emprego dos sistemas de fogos cibernéticos?

Para responder a proposição apresentada foi realizada uma leitura analítica e fichamento das fontes, seguida pela distribuição de questionários para militares especializados em guerra cibernética, com objetivo de identificar a percepção da amostra sobre quais os princípios de emprego dos fogos cibernéticos efetivamente se aplicam em uma ação ofensiva.

As respostas obtidas através do instrumento de coleta de dados permitiram concluir quais os princípios, de fato, se aplicam ao emprego de fogos cibernéticos, são eles:

a) Discrição - empregar armas cibernéticas com técnicas e procedimentos que dificultem a identificação da autoria do ataque, prejudicando a resposta inimiga.
b) Perícia - empregar armas cibernéticas com elevado refinamento técnico para viabilizar a sobreposição da defesa inimiga e encontrar vulnerabilidades que permitam o alcance do efeito desejado.
c) Prontidão - preparar o “campo de batalha” (espaço cibernético) com antecedência, preferencialmente antes do conflito ser deflagrado, garantindo a disponibilidade das armas cibernéticas durante o combate.
d) Adaptabilidade - adaptar a arma cibernética para continuar efetiva, mesmo diante de um novo cenário, como a ação corretiva de uma vulnerabilidade pela vítima.
e) Precisão - realizar ações precisas com pleno entendimento das consequências diretas e indiretas do uso da arma cibernética, evitando que sejam causados danos indesejáveis a terceiros e à própria infraestrutura.

Dessa maneira, segundo a percepção da amostra ouvida, dos princípios atualmente aceitos na doutrina do Exército, apenas prontidão se aplica aos fogos cibernéticos e dos propostos por VASCONCELLOS (2018), continuam valendo os princípios da discrição, perícia, prontidão, adaptabilidade e precisão. A figura abaixo resume as retificações sugeridas.

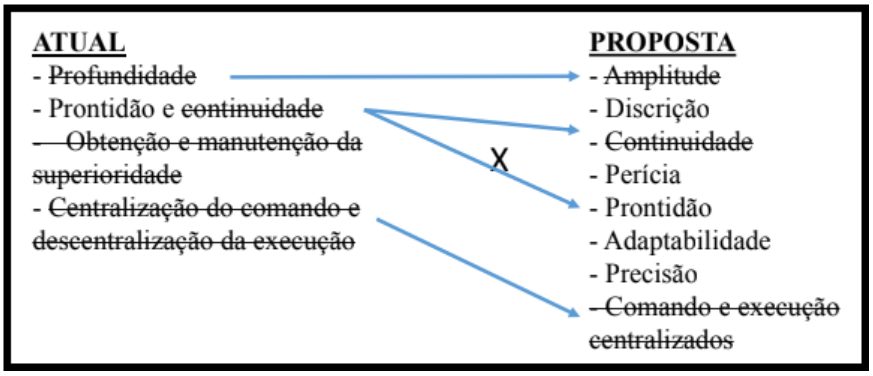

Figura 03 – Comparação entre os princípios atualmente aceitos na doutrina brasileira e os propostos por VASCONCELLOS (2018)
Fonte: o autor

O instrumento de coleta de dados permitiu alcançar o objetivo principal da pesquisa que era: identificar os princípios de emprego de fogos não cinéticos, decorrentes de um ataque cibernético. Com base nos resultados alcançados, sugere-se ao Centro de Doutrina do Exército a retificação dos princípios atualmente adotados pela doutrina militar brasileira e listados no manual EB20-MC-10.206.

Para trabalhos futuros, sugere-se que seja realizado um estudo de caso onde haja o planejamento do emprego de fogos cibernéticos em um contexto bélico, empregando o Simulador de Operações de Guerra Cibernética (SIMOC) para medir a eficácia e eficiência das ações planejadas sob a sombra dos cinco princípios sugeridos neste artigo.

REFERÊNCIAS

BBC. **Major Cyber spy network uncovered**. 2009. Disponível em: http://news.bbc.co.uk/2/hi/americas/7970471.stm. Acessado em 18 mar 2018.

_____. Comando de Operações Terrestres. **Operações EB70-MC-10.223**. 5ª ed Brasília, 2017.

_____. Estado Maior do Exército. **Doutrina Militar Terrestre EB20-MF-10.102**. 1ª ed. Brasília, DF, 2014a.

_____. Estado Maior do Exército. **Fogos. EB20-MC-10.206**. 1ª ed Brasília, 2015

_____. Ministério da Defesa. **Doutrina militar de Defesa Cibernética MD-31-M-07**. Brasília, 2014b.

_____. Ministério da Defesa, **Estratégia Nacional de Defesa.** Brasília, 2008.

CLARKE, Richard A. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015.

FIVE, COMMAND. **Advanced Persistent Threats: A Decade in Review**. 2011. Disponível em: https://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf. Acessado em: 27 mar 2018.

História da Internet. WIKIPÉDIA, a enciclopédia livre. Flórida: Wikipedia Foundation. Disponível em: <https://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet>. Acesso em: 04 nov. 2017

OWENS, W. A. DAM, K. W. LIN, H. S. (edit). **The national academies. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.** Washington-EUA, 2009. Disponível em: https://www.nap.edu/read/12651/chapter/1. Acessado em: 03 mar 2018.

SANCHES, J. L. T. **El ciberespacio como entorno operativo**. Notas de aula. Master en Ciberdefensa. Universidad de Alcalá, 2017

SANS, INSTITUTE. **Security 504: Hackers Tools, Techniques, Exploits & Incident Handling**. 2015.

SHEARER. JARRAD. **W32. Stuxnet**. Symantec, 2017. Disponível em: https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. Acessado em: 31 mar 2018.

SILVA, Wagner. **Anonimização e desanonimização**. Curso de Guerra Cibernética, 10-14 de jul 2017. Notas de Aula.

TIMES, FINANCIAL. **Russian group accused of hacking satélites**. 2015. Disponível em: https://www.ft.com/content/50b1ff84-571d-11e5-9846-de406ccb37f2 . Acessado em: 22 nov 2017

VASCONCELLOS, Felipe. **Principios para el empleo de armas cibernéticas**. Universidad de Alcalá. Alcalá, 2018.

APÊNDICE "A" –QUESTIONÁRIO DE PERCEPÇÃO DE OPINIÃO

Princípios de emprego de fogos cibernéticos

Este questionário é parte do meu Trabalho de Conclusão do Curso de Aperfeiçoamento de Oficiais de Comunicações, cujo escopo é identificar quais são os princípios de emprego dos fogos cibernéticos em uma operação militar. Para que o resultado alcançado seja relevante, foram selecionados para responder esse instrumento de coleta de dados todos os militares especializados em Guerra Cibernética das FA.

A contribuição do Senhor é muito importante e ajudará a Força Terrestre na pesquisa científica. A partir dela, pretende-se coletar importantes subsídios para aperfeiçoar o emprego ofensivo da G Ciber, adequando a doutrina atual às reais necessidades das Forças Armadas.

Pretende-se, ao final do trabalho, identificar quais os princípios de emprego de fogos cibernéticos devem ser levados em consideração durante o planejamento de uma ação cibernética ofensiva. Desde já agradeço a contribuição prestada.

Cap Felipe Rodrigues de VASCONCELLOS, da EsAO.

1) Nome completo (OPCIONAL)

_____

2) Levando em consideração que um ATAQUE CIBERNÉTICO compreende ações para INTERROMPER, NEGAR, DEGRADAR, CORROMPER ou DESTRUIR sistemas computacionais do oponente, qual a sua experiência com esse tipo de atividade?
   a. Nunca realizei
   b. Realizei apenas para fins didáticos, poucas vezes
   c. Realizei apenas para fins didáticos, com frequência
   d. Realizei ações reais, poucas vezes
   e. Realizei ações reais, com frequência

3) Princípios são pontos de referência que orientam e subsidiam os chefes militares no planejamento e na condução da guerra sem, no entanto, condicionar suas decisões. São os pilares que sustentam o sucesso de uma operação. Levando em conta essa definição, aponte quais os princípios mais relevantes em uma ação cibernética ofensiva.MARQUE QUANTAS OPÇÕES JULGAR NECESSÁRIO.
   a. AMPLITUDE: Seguir esse princípio significa empregar armas cibernéticas que permitam resultados abrangentes, com grande quantidade de alvos em potencial.
   b. DISCRIÇÃO: Seguir esse princípio significa empregar armas cibernéticas com técnicas e procedimentos que dificultem a identificação da autoria do ataque, prejudicando a resposta inimiga.
   c. PERÍCIA: Seguir esse princípio significa empregar armas cibernéticas com elevado refinamento técnico para viabilizar a sobreposição da defesa inimiga e encontrar vulnerabilidades que permitam o alcance do efeito desejado.
   d. PRONTIDÃO: Seguir esse princípio significa preparar o “campo de batalha” (espaço cibernético) com antecedência, preferencialmente antes do conflito ser deflagrado, garantindo a disponibilidade das armas cibernéticas durante o combate.
   e. ADAPTABILIDADE: Seguir esse princípio significa adaptar a arma cibernética para continuar efetiva, mesmo diante de um novo cenário, como a ação corretiva de uma vulnerabilidade pela vítima.
   f. PRECISÃO: Seguir esse princípio significa realizar ações precisas, com pleno entendimento das consequências diretas e indiretas do uso da arma cibernética, evitando que sejam causados danos indesejáveis a terceiros e à própria infraestrutura.
   g. COMANDO E EXECUÇÃO CENTRALIZADOS: Seguir esse princípio significa realizar ações com comando único e execução centralizada, evitando que as medidas de tropas diferentes interfiram umas nas outras, além de garantir a sinergia necessária na execução das ações ao concentrar os especialistas em um único ponto de atuação.
   h. CENTRALIZAÇAO DO COMANDO E DESCENTRALIZAÇÃO DA EXECUÇÃO: Seguir esse princípio significa realizar ações com comando único e execução descentralizada, pois uma excessiva centralização dificulta a capacidade de intervenção na operação.
   i. CONTINUIDADE: Seguir esse princípio significa realizar ataques persistentes, cujo efeito dure o período necessário para atingir o efeito desejado.
   j. OBTENÇÃO E MANUTENÇÃO DA SUPERIORIDADE: Seguir esse princípio significa buscar a superioridade de fogos em determinado local e momento, conforme a necessidade tática, garantindo ao comando uma maior liberdade para o cumprimento da missão.
   k. PROFUNDIDADE: Seguir esse princípio significa atingir o inimigo em profundidade durante todo o combate, com foco nas organizações operativas, sistemas de C^2, de apoio de fogo e logística, para o qual exigirá um adequado escalonamento em profundidade de apoio de fogo em função de seus enlaces e suas caracteríticas.
   l. OUTRO

4) Dos princípios listados acima, qual o senhor considera mais relevante em uma

ação cibernética ofensiva?

a. Amplitude
b. Discrição
c. Perícia
d. Prontidão
e. Adaptabilidade
f. Precisão
g. Comando e execução centralizados
h. Continuidade
i. Profundidade
j. Obtenção e manutenção da superioridade
k. Centralização do comando e descentralização da execução