ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM VINICIUS LUIS PALUDETO

A CAPACIDADE RELACIONADA À INFORMAÇÃO DE GUERRA CIBERNÉTICA NAS OPERAÇÕES DE INFORMAÇÃO

Rio de Janeiro
2020

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM VINICIUS LUIS PALUDETO

A CAPACIDADE RELACIONADA À INFORMAÇÃO DE GUERRA CIBERNÉTICA NAS OPERAÇÕES DE INFORMAÇÃO

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
2020

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 VINICIUS LUIS PALUDETO**

Título: **A CAPACIDADE RELACIONADA À INFORMAÇÃO DE GUERRA CIBERNÉTICA NAS OPERAÇÕES DE INFORMAÇÃO.**

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 – TC** Cmt Curso e Presidente da Comissão	
_____ **RAFAEL VILLAR OLIVEIRA - Cap** 1º Membro	
_____ **GLAUCO GONÇALVES DA SILVA - Cap** 2º Membro e Orientador	

_____
VINICIUS LUIS PALUDETO – Cap
Aluno

A CAPACIDADE RELACIONADA Á INFORMAÇÃO DE GUERRA CIBERNÉTICA NAS OPERAÇÕES DE INFORMAÇÃO

Vinicius Luis Paludeto*
Glauco Gonçalves da Silva**

RESUMO
A Dimensão Informacional tornou-se um novo espaço para exploração em um conflito bélico. As Operações de Informação (Op Info) vem sendo utilizadas como meio de potencializar um efeito desejado no campo de batalha, assim como servindo de escudo para os possíveis desdobramentos de uma operação tática. Nesse contexto o Espaço Cibernético tornou-se mais um meio a ser explorado em uma Op Info. Esse Artigo Cientifico tem como objetivo elencar quais atividades de Guerra Cibernética, como Capacidade Relativa a Informação, poderão ser utilizadas em proveito de uma Operação de Informação.

Palavras Chaves: Dimensão Informacional, Operação de Informação, Guerra Cibernética e Capacidades Relacionadas à Informação.

ABSTRACT
The Informational Dimension has become a new space for exploration in a conflict. Information Operations have been used as a means of enhancing a desired effect on the battlefield, as well as serving as a shield for the possible consequences of a tactical operation. In this context, the Cyber Space has become another means to be explored in an Information Operations. This Scientific Article aims to list which Cyber Warfear activities, such as Information Relative Capacity, can be used to benefit an Information Operation.

Keywords: Informational Dimension, Information Operation, Cyber Warfear and Information-Related Capabilities.

*Capitão da Arma de Comunicação. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2011. Pós Graduado Lato Sensu em Guerra Cibernética pelo Centro de Instrução de Guerra Eletrônica (CIGE) em 2014.
**Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2009. Pós Graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (AMAN) em 2019.

1. INTRODUÇÃO

As ações cibernéticas são atividades desenvolvidas para apreender, reter e explorar uma vantagem sobre oponentes ou potenciais adversários no espaço cibernético; objetivam, ainda, negar ou degradar a utilização de vantagem semelhante, quando obtida pelo oponente. Em suma, a atividade visa proteger os processos situacionais e decisórios próprios, bem como assegurar liberdade de atuação das forças amigas no espaço cibernético. Ainda que as ações cibernéticas exijam habilidades específicas definidas para executar os processos necessários, as Operações de Informação abordam a dimensão informacional de forma holística, exigindo que todas as operações sejam inter-relacionadas. Tal vetor como Capacidade Relacionada à Informação (CRI) contribuí para afetar a percepção e a tomada de decisão do adversário.

Portanto, quando desencadeada para influenciar um resultado cognitivo, as atividades cibernéticas são consideradas capacidades relacionadas à informação que devem ser sincronizadas e integradas pelas Operações de Informação. A utilização dessa capacidade permite que elementos da Força Terrestre (F Ter) garantam e mantenham a liberdade de ação no espaço cibernético para as forças amigas, enquanto busca explorá-la ou negá-la aos oponentes.

1.1 PROBLEMA

Com o objetivo de definir metas e diretrizes para a área de Defesa, o Governo Federal aprova em 2008 a Estratégia Nacional de Defesa (END). Os setores estratégicos Cibernético, Espacial e Nuclear foram atribuídos as Forças armadas e considerados essenciais para a Defesa Nacional:

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. (Brasil, 2008, p. 24).

O Exército Brasileiro recebeu a responsabilidade de desenvolver capacidades na Área de Cibernética para as Três Forças Singulares, entretanto ainda hoje não há uma doutrina consolidada de emprego das Capacidades da Guerra Cibernética (G Ciber) como CRI.

Portanto quais as atividades de Guerra Cibernética, como Capacidade Relacionada à Informação, podem ser desencadeadas em proveito das Operações de Informação?

1.2 OBJETIVOS

OBJETIVO GERAL

O objetivo geral deste trabalho é apresentar atividades de G Ciber nas Operações de Informação, aperfeiçoando a doutrina de G Ciber nas Op Info do Exército Brasileiro.

OBJETIVOS ESPECÍFICOS

Para atingir este objetivo geral, foram elencados os seguintes objetivos específicos:

1. Apresentar o Conceito de Guerra Cibernética (G Ciber), Capacidades Relacionadas à Informações (CRI) e Operações de Informação (Op Info).
2. Verificar as tendências mundiais no que se refere a G Ciber da Organização dos EUA, dos países do Tratado do Atlântico Norte (OTAN), da China e da Rússia,
3. Apresentar atividades de G Ciber, como CRI em Apoio a Op Info.

1.3 JUSTIFICATIVAS

No combate moderno, em um Ambiente denominado Volátil, Incerto, Complexo e Ambíguo *(Volatility, Uncertainty, Complexity and Ambiguity - VUCA)* tornou-se necessário obter a superioridade na Dimensão Informacional do Combate para que se possa alcançar um efeito na Dimensão Física e Humana. O Espaço Cibernético tornou-se um novo vetor para as Op Info, podendo influenciar significativamente o processo decisório.

Nesse contexto, pode-se utilizar atividades de Guerra Cibernética como Capacidades Relacionadas à Informação em apoio as Operações de Informação, sendo esta de extrema importância para o comandante empregá-la de maneira judiciosa e eficaz, para obter superioridade informacional, podendo influenciar e criar efeitos cinéticos na Dimensão Física e Humana.

2. REVISÃO DE LITERATURA

Para inicar a pesquisa deve-se definir alguns termos e conceitos importantes para o entendimento desse Artigo Científico.

2.1 A GUERRA DE INFORMAÇÃO

A revolução das Tecnologias de Informação e Comunicações (TIC), possibilitou aos Estados a gerência de redes informacionais complexas, refletindo assim na organização de suas atividades.

Segundo SILVA (2006, Pag. 11), a Tecnologia de Informação e Comunicações revolucionou o emprego dos diversos sistemas baseados em redes computadorizadas, os quais, ao serem empregadas para troca e armazenamento de informações, principalmente de dados financeiros, como a movimentação dos fluxos de capital, tornaram os países cada vez mais vulneráveis a ataques cibernéticos.

Nos conflitos armados, segundo SOUZA (2003, p. 14) a TIC permite, cada vez mais, realizar o sensoriamento de todos os meios amigos e inimigos envolvidos no conflito, permitindo processar os dados obtidos e compará-los com parâmetros pré-definidos, tornando-os informações relevantes.

Sendo assim, o objetivo da Guerra de Informação nos conflitos armados é a obtenção da superioridade de informação. O conceito de Guerra da Informação é descrito no MD35-G-01, Glossário das Forças Armadas:

> Conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos. (BRASIL, 2007, p.124).

Segundo DINARDO e HUGHES (1998, p. 43), um Estado deve permitir que suas forças armadas façam uso de todos os recursos nacionais e usem todos os setores da sociedade para obter mais informações que o seu oponente, ao mesmo tempo em que busca proteger seus próprios dados, a fim de garantir a capacidade de sobrevivência numa guerra de informação, quer seja em conflitos irregulares ou convencionais.

2.2 OPERAÇÕES DE INFORMAÇÃO

O Glossário das Forças Armadas (MD 35-G-01), define as Operações de Informação como:

> Ações coordenadas que concorrem para a consecução de objetivos políticos e militares. Executadas com o propósito de influenciar um oponente real ou potencial, diminuindo sua combatividade, coesão interna e externa e capacidade de tomada de decisão. Atuam sobre os campos cognitivo, informacional e físico da informação do oponente, e, também, sobre os processos e os sistemas nos quais elas trafegam, ao mesmo tempo em que procuram proteger forças amigas e os respectivos processos e sistemas de tomada de decisão. (BRASIL, 2007, p. 183).

Segundo CLARK (2010, p. 57), as Operações de Informações (Op Info) proporcionam aos comandantes alternativas dissuasórias não letais e flexíveis. A aplicação das Op Info dessa forma é viável tanto em relação a adversários estatais quanto a adversários não estatais. O grau de impacto dependerá da capacidade específica que o adversário possuir.

Ainda sobre as Op Info, segundo o Manual MD 31-D-03, Doutrina Militar de Comando e Controle (BRASIL, 2006, p. 41), apoiadas pela Inteligência, integrarão os meios da Guerra Eletrônica, das Operações Psicológicas, do Despistamento, da Segurança da Informação, da Destruição Física e da Guerra Cibernética, para negar informação, influenciar, explorar, degradar ou destruir as capacidades de Comando e Controle (C^2) do adversário, ao mesmo tempo em que protegem a capacidade de C^2 própria e amigas contra tais ações.

2.3 CAPACIDADES RELACIONADAS À INFORMAÇÃO

O Manual de Campanha EB20-MC-10.213, Operações de Informação (BRASIL, 2014 p. 4-2), define que as Capacidades Relacionadas à Informação (CRI) são aptidões requeridas para afetar a capacidade de oponentes ou potenciais adversários de orientar, obter, produzir e/ou difundir informações, em qualquer uma das três perspectivas da dimensão informacional (física, cognitiva ou lógica).

O Manual de Campanha EB70-MC-10.223, Operações (BRASIL, 2017 p. 4-5) complementa que as CRI contribuem para a condução das operações de informação (Op Info), destacando-se: Comunicação Social (Com Soc); Operações Psicológicas(Op Psc); Guerra Eletrônica (GE); Guerra Cibernética (G Ciber); e Inteligência(Intlg).

A publicação *Joint Publication (JP) 3-13, Information Operations (Washington, DC: U.S. Government Publishing Office [GPO], 27 Nov. 2012)*, *p. GL-3, define* Capacidade Relacionada à Informação como: “uma ferramenta, técnica ou atividade

empregada dentro de uma dimensão do ambiente informacional que pode ser usada para criar efeitos e condições operacionalmente desejadas.”

Portanto pode-se concluir que as Capacidades Relacionadas à Informação são atividades realizada na Dimensão Informacional, visando criar efeitos desejados nas três dimensões do combate (Físico, Humana e Informacional). Dentro desse conceito dar-se-á ênfase a algumas atividades de Guerra Cibernética capazes de criar esses efeitos no contexto de uma Operação de Informação.

2.4 GUERRA CIBERNÉTICA

Para conceituar Guerra Cibernética utilizar-se-á o Manual de Campanha EB70-MC-10.232, Guerra Cibernética (BRASIL, 2017 p. 2-2), que corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C² ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sistemas de Informação. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC.

O mesmo Manual de Campanha (EB70-MC-10.232) conceitua a Guerra Cibernética nas Operações Terrestres dentro das Operações de Informação:

> A guerra cibernética contribui com as operações de informação como uma capacidade relacionada à informação (CRI). Assim, possui áreas de superposição com as Op Info, mas sem vínculo de subordinação. As CRI são aptidões requeridas para afetar a capacidade de oponentes ou potenciais adversários de orientar, obter, produzir e/ou difundir informações, em qualquer uma das três perspectivas da dimensão informacional (física,cognitiva ou lógica)(BRASIL, 2017 p. 5-5).

2.5 TENDENCIAS MUNDIAIS NA UTILIZAÇÃO DA GUERRA CIBERNÉTICA

As principais potências mundiais já utilizam a Guerra Cibernética para atingir seus objetivos políticos, estratégicos e operacionais.

2.5.1 ESTADOS UNIDOS DA AMÉRICA

Segundo WALKER (2017, p.28-29), as Operações Cibernéticas compreendem o domínio global do ambiente de informações, considerando a interdependência dos dados, seja na internet, redes de comunicações, sistemas computacionais, processadores e controladores. Essa capacidade está focada em ações ofensivas e defensivas, sendo integradas em múltiplas linhas de esforço para afetar adversários e potenciais tomadores de decisão (UNITED STATES, 2014, p. II-9).

Ainda segundo WALKER (2017, p.28-29), Os Estados Unidos possuem um Centro Conjunto de Guerra de Operações de Informação (*Joint Information Operations Warfare Center – JIOWC)*, que é responsável desde o tempo de paz em coordenar o desenvolvimento tecnológico e ações estruturais conjuntas das capacidades relacionadas à informação, incluindo o setor cibernético. Sob a direção do *United States Strategic Command (USSTRATCOM), os* United States Cyber Command (USCYBERCOM), são responsáveis pela sincronização e coordenação das operações transregionais, bem como em coordenação com os comandos combatentes, *Joint Staff (JS)* e *Office of Secretary of Defense (OSD)* ligam-se com os demais departamentos (ministérios), agências e membros da base industrial de defesa dos *United States Government(USG)*, tudo em conjunto com o *Department of Homeland Security (DHS)* (UNITED STATES, 2013, p. IX).

2.5.1 RÚSSIA

A Rússia vem desenvolvendo e atualizando sua doutrina de emprego de Guerra Eletrônica e Guerra Cibernética desde os anos 90, e emprega em larga escala essas capacidades em operações convencionais ou em operações de informação.

Segundo ALENCAR (2010, p. 29), no que se refere ao estabelecimento de Estruturas de defesa em Guera da Informação, a Rússia criou em 1993, a Agência Federal do Governo para Comunicações e Informações *(Federal'naya Agenstvo Pravitel'stvennoy Svayazi i Informatsii – FAPSI)* uma grande organização de inteligência que trata, interna e externamente, da Guerra da Informação nos níveis político, econômico e no campo da ciência e tecnologia, podendo acessar informações no âmbito governamental e não governamental, no próprio país e no

exterior. Utiliza, para isso, os seus meios de inteligência de sinais distribuídos no seu próprio país e por suas embaixadas e consulados no exterior.

Segundo WALKER(2017, p. 30-31), as Operações Cibernéticas (*Кибер-Война*) são conduzidas de forma conjunta pelas tropas de guerra cibernética essencial para atingir os objetivos militares e políticos russos. No nível tático, a doutrina não concebe que as ações cibernéticas atuem isoladamente, pois fazem parte de um complexo de influências (GILES, 2011, p. 46). De acordo com Giles (2012, p. 46), em relação às Operações de Informação, a visão russa de Guerra da Informação é mais um conceito holístico que uma tradução literal que compreende Operações Cibernéticas, Guerra Eletrônica, Operações Psicológicas e Comunicação Estratégica. outra questão é a soberania da internet. O sistema russo requer um controle governamental sobre o que entra no espaço cibernético, considerando-se as fronteiras físicas do país.

2.5.2 CHINA

A China possui o maior número de pessoas que acessam a rede mundial de computadores (Internet) e o seu governo impõe um controle estatal sobre o conteúdo que sua população pode acessar, fazendo com que a mesma utilizem de técnicas de anonimização para acessar redes sociais como *Facebook* e *Instagram*.

A China encontrou no Espaço Cibernético uma maneira de equilibrar a balança de poder em relação a países dos ocidente como Estados Unidos e dos países da Europa.

Devido aos complexos sistemas computacionais utilizados pelas grandes potências ocidentais, a Guerra Centrada em Redes tornou-se uma solução viável para aquele país que exporta para o mundo inteiros componentes eletrônicos que são utilizados em diversos sistemas informatizados.

2.5.3 ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE (OTAN)

A OTAN (*North Atlantic Treaty Organization, NATO* em inglês) possui um Centro de Excelência para a Defesa Cibernética ativado formalmente em 14 de maio de 2008 denominado *NATO Cooperative de Cyber Defence Centre of Excellence* (NATO CCD COE), em Tallinn, Estônia.

O CCD COE é um esforço internacional para tentar aumentar a segurança dos seus sistemas computadorizados e de suas redes. Os principais mantenedores desse projeto são a Estônia e EUA, constantes alvos de ataques cibernéticos por parte da Rússia e China. Outros países como Alemanha, Hungria, Itália, Espanha, Holanda que fazem parte da OTAN também contribuem para o desenvolvimento do CCD COE. (PASINI, 2012, p.58)

Internamente os países da OTAN possuem estruturas próprias para atuação no Espaço Cibernético. Segundo WALKER(2017, p.29), a Alemanha está estabelecendo um comando cibernético de informações por meio da fusão de unidades cibernéticas da Forças Armadas (*Bundeswehr*). O Comando Cibernético e da Informação (*Kommando Cyber-und Informationsraum*) será o responsável por integrar os setores cibernéticos, a tecnologia da informação, a inteligência militar, a geoinformação e a comunicação operativa (IHS 360, 2016).

3. METODOLOGIA

A revisão bibliográfica sobre os assuntos Operações de Informação e Capacidades Relacionadas à Informação são de fundamental importância para o entendimento da maneira que a Guerra Cibernética pode ser empregada em uma Operação de Informação.

Quanto à forma de abordagem do problema, foram utilizadas os conceitos de pesquisa quantitativa, pois as referências numéricas obtidas por meio do questionário são fundamentais para a compreensão do problema.

Quanto ao objetivo geral, foi empregada a modalidade exploratória, tendo em vista ao conhecimento disponível, notadamente escrito, acerca do tema, o que exigiu uma ambientação inicial, seguida de questionário para uma amostra com especialidade de Guerra Cibernética.

Dentre as atividades cibernéticas, serão elencadas as que podem apoiar o êxito de uma Operação de Informação, ressaltando que algumas atividades dependendo do amparo legal, podem ser enquadradas como ilícitas ou que ferem o direito privado e/ou coletivo:

a. Utilização de Redes Sociais (Canal Oficial da Força) para o envio de mensagens institucionais e de atividades correntes.

b. Utilização de aplicativos de mensagem (BOTs) e e-mails (Técnica de SPAM) para difundir conteúdo para informar ou desinformar o inimigo.

c. Utilização da rede de móvel de uma região de interesse para localizar ou estimar a concentração de celulares em uma determinada área.

d. Utilização de Técnicas de OSINT (*Open Source Intelligence* – Pesquisa em Fontes Abertas), para coleta de dados de interesse.

e. Monitoração de Grupos fechados em mídias sociais e aplicativos de mensagem.

f. Disseminação de Malware para obtenção de dados negados e/ou inutilização/paralisação do sistema de C² do inimigo.

3.1 COLETA DE DADOS

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

Para atingir o objetivo, um questionário para estimar quais atividades de cibernética acima podem contribuir para uma Operação de Informação. O questionário ainda se propõem a verificar o conhecimento a cerca de uma Operação de Informação e das atividades de cibernéticas que podem ser utilizadas da mesma.

A amplitude do universo foi estimada a partir do efetivo de oficiais com o curso de Guerra Cibernética. O estudo foi limitado particularmente aos oficiais que realizaram o curso devido à especificidade da atividade de Guerra Cibernética.

Dessa forma, utilizando-se dados obtidos a população a ser estudada foi estimada em 86 militares (oficiais e sargentos das 3 Forças Armadas) que concluíram o curso de Guerra Cibernética entre os anos de 2016 e 2018. A fim de atingir uma maior confiabilidade das induções realizadas, buscou-se atingir uma amostra significativa, utilizando como parâmetros o nível de confiança igual a 90% e erro amostral de 10%. Nesse sentido, a amostra dimensionada como ideal (n_{ideal}) foi de 76.

A sistemática de distribuição dos questionários ocorreu de forma indireta (Formulário Online) para os 86 militares, que atendiam os requisitos. Entretanto, devido a diversos fatores, somente 58 respostas foram obtidas (74,35% de n_{ideal}), não havendo necessidade de invalidar nenhuma por preenchimento incorreto ou incompleto.

A partir do n_{ideal} (78), depreende-se que o tamanho amostral obtido (n=58) foi inferior ao desejado para o tamanho populacional dos potenciais integrantes da amostra, no entanto não inviabiliza, tampouco reduz a relevância desta pesquisa, haja vista a especialização da amostra.

Foi realizado um pré–teste com 4 (quatro) capitães-alunos da Escola de Aperfeiçoamento de Oficiais (EsAO), que atendiam aos pré-requisitos para integrar a amostra proposta no estudo, com a finalidade de identificar possíveis falhas no instrumento de coleta de dados. Ao final do pré-teste, não foram observados erros que justificassem alterações no questionário e, portanto, seguiram-se os demais de forma idêntica.

4. RESULTADOS E DISCUSSÃO

A Dimensão Informacional tornou-se um novo espaço para exploração em um conflito bélico, nesse contexto Operações de Informação vem sendo utilizadas como meio de potencializar um efeito desejado no campo de batalha. Assim o Espaço Cibernético tornou-se mais um meio a ser explorado em uma Op Info.

Forças Armadas de outros países possuem estruturas singulares para as Operações de Informação que se apoiam em alguma estrutura ou comando cibernético.

O questionário limitou-se a verificar quais atividades no espaço cibernético poderiam ser desencadeadas em apoio a uma Operação de Informação. Dentre os resultados obtidos constatou-se que:

Tabela 1 – Opinião dos Entrevistados sobre as atividades de Guerra Cibernética, como Capacidade Relacionada à Informação em Apoio as Op Info.

Atividades	Amostra	Ocorrência	Percentual
Utilização de Redes Sociais (Canal Oficial da Força) para o envio de mensagens institucionais e de atividades correntes.	58	35	60,3%
Utilização de aplicativos de mensagem (BOTs) e e-mails (Técnica de SPAM) para difundir conteúdo para informar ou desinformar o inimigo.		42	72,4%
Utilização da rede de móvel de uma região de interesse para localizar ou estimar a concentração de celulares em		32	55,2%

uma determinada área.		
Utilização de Técnicas de OSINT (*Open Source Intelligence* – Pesquisa em Fontes Abertas), para coleta de dados de interesse.	48	82,8%
Monitoração de Grupos fechados em mídias sociais e aplicativos de mensagem.	33	56,9%
Disseminação de Malware para obtenção de dados negados e/ou inutilização/paralisação do sistema de C² do inimigo.	30	51,7%
Engenharia Social, importante ferramenta para a obtenção de informação in-loco.	1	1,7%
Utilização de bots em redes sociais para mudar a percepção de um público.	1	1,7%
Invasão de dispositivos ou redes do alvo.	1	1,7%

Fonte: o Autor

As duas atividades de maior percentual de ocorrências, Utilização de aplicativos de mensagem (*BOTs*) e e-mails (Técnica de *SPAM*) para difundir conteúdo para informar ou desinformar o inimigo (72,4%) e Utilização de Técnicas de OSINT (*Open Source Intelligence* – Pesquisa em Fontes Abertas), para coleta de dados de interesse. (82,8%), são atividades de manipulação da informação e obtenção da mesma, respectivamente, ligadas Capacidade Operativa de Exploração Cibernética, conforme prescreve o Manual de Campanha EB70-MC-10.232, Guerra Cibernética:

> Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas. (BRASIL, 2017 p. 3-4).

Como conclusão parcial, a utilização de *OSINT* no Espaço Cibernético constitui uma das principais atividades de Guerra Cibernética em Apoio as Operações de Informação, na opinião do especialista. O Surgimento de Mídias/Redes sociais na última década, tornou o Espaço Cibernética uma imensa fonte de dados abertos. Segundo *RABELO (Website ,2017),* 2,8 bilhões de pessoas

utilizavam redes sociais até o final de 2016, quase 80% do tempo gasto em plataformas de redes sociais acontece no celular, 63% dos usuários do Facebook e do Twitter dizem que as plataformas servem como fonte de notícias sobre eventos e questões fora do âmbito de amigos e familiares, os usuários compartilharam mais de 40 bilhões de fotos (Instagram) e 500 milhões de tweets são enviados por dia. (Twitter).

Toda essa informação gerada através de mídias sociais quando filtradas e analisadas podem gerar informações relevantes para as Operações de Informação (conceito de *Big Data*).

Ainda sobre os resultados obtidos, tem-se que 3 (três) (5,2%) de militares que pertencem a Marinha do Brasil, 5 (cinco) (8,6)% de militares que pertencem a Força Aérea Brasileira e 50 (cinquenta) (86,2%) de militares pertencem ao Exército Brasileiro. Ainda constatou-se que 34 (trinta e quatro) (58,6)% dos militares questionados, conhecem ou já participaram de uma Operação de Informação.

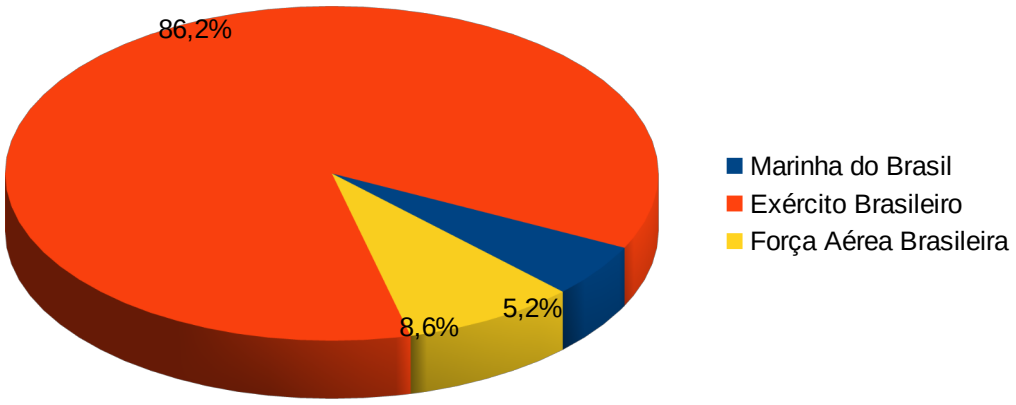

GRÁFICO 2 – Porcentagem dos Militares das 3 Forças Armadas que responderam o questionário.
Fonte: O autor

No questionário foi aberto um espaço para sugestões/comentário, no qual se destacaram os seguintes comentários:

a) *"Falta de atividades prática para manter o adestramento."*

b) "Diversas são as técnicas que o Guerreiro Ciber pode (e deve) utilizar para variar as formas de obtenção de informação. Esse trabalho realizado em uma

"Força-Tarefa", integrando GCiber, Inteligência, GE, FE e outros agentes, potencializa a penetração da equipe no ambiente real e cibernético com a finalidade desse trabalho de Op Info. Quanto mais técnicas empregadas, mais chance de sucesso."

c) *"entre as opções acima, a única que acredito que caiba às Op Ciber em apoio à uma Op Info seria a disseminação de malware, já que as outras utilizam o Espaço Cibernético, mas não são algo exclusivo das Op Ciber ou pertencem a outras capacidades (ex: GE), e o emprego do pessoal de Ciber nesse tipo de atividade que não requer conhecimento de Exploração e Ataque Cibernético os desvia de sua missão e adestramento. Além disso, cabe ressaltar que apesar de poder trabalhar em apoio às Op Info, as Op Ciber não são uma capacidade subordinada exclusivamente a elas, podendo ser utilizada em apoio à Inteligência, Manobra e outros."*

d) "Acredito que quando o assunto é op info, a cibernética e a inteligência se confundem. A cibernética, por conceito, significa realizar nossa vontade a partir da máquina. Ou seja, seria usar meios tecnológicos, fazendo-nos funcionar não como devem, mas como se quer, para inflingir uma ação. Acredito que quando se usa redes sociais, bots ou osint, o que se está fazendo é manipular informações, ou seja, inteligência. Quando se usa meios de TI com técnicas e conhecimentos especializados, para atingir um objetivo específico, aí sim seria Ciber."

Como afirmado nos comentários C e D, as atividades de Guerra Cibernética não são exclusivamente em apoio as Operações de Informação, elas podem ser desencadeadas em proveito a outras Funções de Combate (Manobra, Fogos, C², Inteligência e Proteção) ou a outras atividades específicas como Comunicação Social e como já visto no capítulo "Revisão da Literatura", as Op Info se apoiam em Capacidades Relacionadas à Informação (Comunicação Social, Operações Psicológicas, Guerra Eletrônica, Guerra Cibernética e Inteligência) para serem desencadeadas.

5. CONSIDERAÇÕES FINAIS

Quanto às questões de estudo e objetivos propostos no início deste trabalho, conclui-se que a presente investigação atendeu ao pretendido, apresentando quais atividades no Espaço Cibernético podem apoiar a célula de Op Info.

A revisão de literatura possibilitou concluir que alguns países centralizam a coordenação das Operações de Informação no seu mais alto escalão especializado em Cibernética, como por exemplo os Estados Unidos da América com o Comando Cibernético dos Estados Unidos (*United States Cyber Command USCYBERCOM)* e a Alemanha com o Comando Cibernético e da Informação (*Kommando Cyber-und Informationsraum*). Ainda há inciativas internacionais na criação de estruturas para discussão, proteção e dissuasão cibernética como o caso do *NATO Cooperative de Cyber Defence Centre of Excellence* (NATO CCD COE) – Estônia.

A opinião do militar especializado é de suma importância, na pesquisa pode-se constatar a sugestão de mais adestramento para a tropa e a importância de ter uma cadeia definida e de um fluxo de informação definido, pois a atividades de cibernética podem ser desencadeadas como Capacidade Relacionada à Informação, ou em proveito a outras Funções de Combate, como Inteligencia, Manobra e Comando e Controle.

Portanto, junto com outras Capacidades Relacionadas à Informação, a Guerra Cibernética tem aplicabilidade utilizando-se de diversas técnicas e ferramentas para apoiar uma Op Info, principalmente na obtenção de dados e difusão de informação por meio de mídias sociais.

REFERÊNCIAS

ALENCAR, Márcio Faccin de. **Guerra Cibernética: cenário atual e perspectivas.** Rio de Janeiro, 2010.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **EB70-MC-10.223 - Operações.** 5. Ed. Brasília, DF: 2017.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **EB20-MC-10.213, Operações de Informação.** 1. Ed. Brasília, DF: 2014.

BRASIL .Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. **EB70-MC-10.232 - Guerra Cibernética.** 1. Ed. Brasília, DF: 2017.

BRASIL. Presidência da República. **Política de Defesa Nacional.** Decreto Nr 5.484. 30 Jun 2005.

BRASIL. Ministério da Defesa. Estado-Maior de Defesa. **MD 31-D-03 Doutrina Militar de Comando e Controle.** 1a Ed. Brasília, DF: 2006.

BRASIL . MD. Estado-Maior de Defesa. **MD35-G-01, Glossário das Forças Armadas**. 1. Ed. Brasília, DF: 2007.

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. **EB70-MC-10.201 A Guerra Eletrônica na Força Terrestre**, 1. Ed., Brasília, DF, 2019.

BRASIL .Decreto nº 6.703, de 18 de dezembro de 2008 **.** Aprova a **Estratégia Nacional de Defesa**, e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008

CLARK, Blane R. **As Operações de Informações como um Elemento Dissuasório do Conflito Armado**. Militar Review. Ed. Brasileira, p. 57-65. Set-Out 2010.

GILES, K. **Information Troops: a Russian Cyber Command?** International Conference On Cyber Conflict. Estonia, 2011, p. 45-60.

JOINT PUBLICATION (JP) 3-13, **Information Operations** (Washington, DC: U.S. Government Publishing Office [GPO]), de 27 de novembro de 2012.

NETO, Ricardo Borges Gama. **Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação** .Revista Política Hoje - Volume 26, n. 1 (2017) - p. 201-217.

PASINI, Paulo César**. A Guerra Cibernética (G Ciber) e as Operações de Informação no Nível Operacional**. ECEME. 2012.

RABELO, Agnes. **Panorama mundial das redes sociais: 91 estatísticas que você precisa saber.** Disponível em: *"https://inteligencia.rockcontent.com/estatisticas-de-redes-sociais/"*. 9 de agosto de 2017. Acessado em 08/09/2020.

SOUZA, Carlos R. Pinto. **Guerra de Informação**. PADECEME. Rio de Janeiro, Nr 4, p.12 a 22.1º quadrimestre 2003.

SILVA**,** Gilmar Pereira. **Guerra Cibernética: preparo e emprego do Exército**, Riode Janeiro, 2006, 46 f.

UNITED STATES ARMY. (2014), **Cyber Eletromagnetic Activities**. FM 3-38. 12 de fevereiro 2014.

WALKER, Márcio Saldanha. **O papel da inovação tecnológica e da gestão conjunta do setor cibernético na integração das Operações de Informação no Brasil: comparação com Estados Unidos, Reino Unido, Alemanha e Rússia.** Revista da UNIFA, Rio de Janeiro, jul./dez. 2017.

	ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS **SEÇÃO DE PÓS-GRADUAÇÃO**

APÊNDICE "A"

QUESTIONÁRIO

O presente instrumento é parte integrante da especialização em Ciências Militares do Cap Com Vinicius Luis Paludeto, cujo tema é **A Capacidade Relacionada à Informação de Guerra Cibernética nas Operações de Informação.** Pretende-se, através da compilação dos dados coletados, fornecer subsídio para formulação de doutrina de Guerra Cibernética, como Capacidade Relacionada à Informação em apoio as Operações de Informação.

A fim de conhecer as atividades de Guerra Cibernética que possam ser desenvolvidas em apoio as Operações de Informação, o senhor foi selecionado, dentro de um restrito universo de especialistas em Guerra Cibernética, para responder as perguntas deste questionário. Solicito-vos a gentileza de respondê-lo o mais completamente possível.

A experiência profissional do senhor contribuirá de sobremaneira para a pesquisa. Será muito importante, ainda, que o senhor complemente, quando assim o desejar, suas opiniões a respeito do tema e do problema.

Desde já agradeço a colaboração e coloco-me à disposição para esclarecimentos através dos seguintes contatos:

Vinicius Luis Paludeto (Capitão de Comunicações – AMAN 2011)
Celular: (61) 98471-1569
E-mail: paludeto.vinicius@eb.mil.br

IDENTIFICAÇÃO

4. Qual Instituição o senhor(a) faz parte?
( ) Marinha do Brasil
( ) Exército Brasileiro
( ) Força Aérea Brasileira

5. O senhor(a) possui outra especialidade que contribua com as Operações de Informação além do Curso de Guerra Cibernética?
( ) Inteligência
( ) Guerra Eletrônica
( ) Operações Psicológicas
( ) Comunicação Social
( ) Inteligência de Imagens
( ) Inteligência do Sinal
( ) Outros:_____

6. O senhor(a) conhece ou já participou de uma Operação de Informação?
( ) Sim
( ) Não

ASPECTOS DOUTRINÁRIOS

7. Na opinião do senhor(a) quais atividades no Espaço Cibernético podem ser desencadeadas para apoiar uma Operação de Informação? (As opções abaixo são possibilidades, algumas atividades necessitam de amparo legal/jurídico)

( ) Utilização de Redes Sociais (Canal Oficial da Força) para o envio de mensagens institucionais e de atividades correntes.

( ) Utilização de aplicativos de mensagem (BOTs) e e-mails (Técnica de SPAM) para difundir conteúdo para informar ou desinformar o inimigo.

( ) Utilização da rede de móvel de uma região de interesse para localizar ou estimar a concentração de celulares em uma determinada área.

( ) Utilização de OSINT para coleta de dados.

( ) Monitoração de Grupos fechados em mídias sociais e aplicativos de mensagem.

( ) Disseminação de Malware para obtenção de dados negados e/ou inutilização/paralisação do sistema de C² do inimigo.

FECHAMENTO

8. Caso o senhor(a) queira deixe uma sugestão/comentário.

_____
_____
_____
_____

Obrigado pela participação.