ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM MICHELL MEDEIROS SANTOS

CONVERGÊNCIA ENTRE ATIVIDADES DE GUERRA CIBERNÉTICA E GUERRA ELETRÔNICA NO 1º BATALHÃO DE GUERRA ELETRÔNICA NAS OPERAÇÕES:

CENTRO DE OPERAÇÕES DO 1ºBGE

Rio de Janeiro
2020

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM MICHELL MEDEIROS SANTOS

CONVERGÊNCIA ENTRE ATIVIDADES DE GUERRA CIBERNÉTICA E GUERRA ELETRÔNICA NO 1º BATALHÃO DE GUERRA ELETRÔNICA NAS OPERAÇÕES:

CENTRO DE OPERAÇÕES DO 1ºBGE

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

CONVERGÊNCIA ENTRE ATIVIDADES DE GUERRA CIBERNÉTICA E GUERRA ELETRÔNICA NO 1º BATALHÃO DE GUERRA ELETRÔNICA NAS OPERAÇÕES:
CENTRO DE OPERAÇÕES DO 1ºBGE

Michell Medeiros Santos[*]
Rafael Villar Oliveira[**]

RESUMO
No presente trabalho, buscou-se apresentar uma visão sobre a importância da integração da Guerra Eletrônica com a Guerra Cibernética no nível tático. Sua finalidade é alertar quanto a necessidade de integrar essas duas fontes de informação dentro do 1º BGE, que atualmente é a única Unidade capaz de operacionalizar atividades tanto no espaço eletromagnético, quanto no espaço cibernético, bem como propor a transformação do atual COGE do 1º BGE em COGEC, incluindo a Guerra Cibernética, como forma de enriquecer o conhecimento produzido e integrar as fontes em questão. Para tanto, esse artigo foi desenvolvido, de fevereiro a junho de 2020, por meio de uma pesquisa quantitativa, utilizando-se, também, o recurso da leitura analítica e de questionário. Além do material colhido nos diversos manuais e outros trabalhos científicos, o relatório de pesquisa conta com a experiência individual vivida pelo autor como oficial integrante do 1º BGE por 8 (oito) anos. Apresenta comentários sobre o aumento da importância da Guerra Cibernética no cenário atual e a importância da integração dessas duas fontes de informação para as Operações de Informação. São abordados aspectos teóricos da Guerra Eletrônica, Guerra Cibernética e Operações de Informação. Discorre-se sobre a integração das duas fontes de informação no COGEC como forma de gerar um conhecimento mais significativo e não perder o banco de dados dessa integração que, até então, só acontece no escalão superior, externo ao 1º BGE. Na conclusão, as ideias expressas ao longo do trabalho são ratificadas, enfatizando a importância da operacionalização do COGEC.

Palavras-chave: Guerra Eletrônica. Guerra Cibernética. Operações de Informação. 1º BGE. Integração.

ABSTRACT
In this work, we sought to present a view on the importance of integrating Electronic Warfare with Cyber Warfare at the tactical level. Its purpose is to alert as to the need to integrate these two sources of information within the 1st EWB, which is currently the only Unit capable of operationalizing activities both in electromagnetic space and in cyber space, as well as proposing the transformation of the current EWOC of the 1st EWB in ECWOC, including the Cyber War, as a way to enrich the knowledge produced and integrate the sources in question. For this purpose, this article was developed, from February to June 2020, through a quantitative research, also using the resource of analytical reading and questionnaire. In addition to the material collected in the various manuals and other scientific works, the research report relies on the individual experience lived by the author as an official member of the 1st EWB for 8 (eight) years. It presents comments on the increasing importance of Cyber War in the current scenario and the importance of integrating these two sources of information for Information Operations. Theoretical aspects of Electronic Warfare, Cyber Warfare and Information Operations are addressed. We discuss the integration of the two sources of information in ECWOC as a way of generating more significant knowledge and not losing the database of this integration, which, until then, only happens in the upper echelon, external to the 1st EWB. In conclusion, the ideas expressed throughout the work are ratified, emphasizing the importance of operationalizing ECWOC.

Keywords: Electronic Warfare. Cyber War. Information Operations. 1st BGE. Integration.

[*] Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2011. Pós-graduado em Guerra Eletrônica (2012) e Guerra Cibernética (2014) pelo Centro de Instrução de Guerra Eletrônica (CIGE).
[**] Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2009. Pós-graduado em Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica (CIGE) em 2012.

1 INTRODUÇÃO

O manual de Operações de Informação EM-20-MC10.213, de 2014, traz o seguinte entendimento das ações cibernéticas e eletromagnéticas:

> [...] as ações cibernéticas e eletromagnéticas são atividades desenvolvidas para apreender, reter e explorar uma vantagem sobre oponentes ou potenciais adversários, tanto no espaço cibernético como no espectro eletromagnético e, simultaneamente, negar e degradar ao adversário utilização dessa vantagem [...] (BRASIL, 2014, p. 4-9)

Em suma, ambas as atividades visam proteger os processos situacionais e decisórios próprios, bem como assegurar liberdade de atuação das forças amigas nos espaços respectivos.

No mesmo manual, em outro momento, é dito o seguinte:

> Ainda que as ações cibernéticas e eletromagnéticas exijam habilidades específicas definidas para executar os processos necessários, as Op Info abordam a dimensão informacional de forma abrangente, exigindo que essas operações sejam inter-relacionadas. Tais vetores se apoiam mutuamente e a integração das referidas capacidades são um facilitador, uma vez que contribuem para afetar a percepção e a tomada de decisão do adversário. Portanto, quando desencadeadas para influenciar um resultado cognitivo, as atividades cibernéticas e os componentes eletromagnéticos são consideradas capacidades relacionadas à informação que devem ser sincronizadas e integradas pelas Operações de Informação. A integração desses recursos permite que elementos da Força Terrestre (F Ter) garantam e mantenham a liberdade de ação no espaço cibernético e no espectro eletromagnético para as forças amigas, enquanto buscam explorá-la ou negá-la aos oponentes. (BRASIL, 2014, p. 4-9)

1.1 PROBLEMA

Atualmente, o 1º Batalhão de Guerra Eletrônica (1º BGE) atua em todo o território nacional, realizando atividades de Guerra Eletrônica (GE) e, mais recentemente, de Guerra Cibernética (G Ciber) apoiando diversos tipos de operações, como: Defesa Externa, Garantia da Lei e da Ordem (GLO), Operações de Informação (Op Info) dentre outras em apoio a F Ter, ao Ministério da Defesa (MD) e à Órgão Governamentais.

Com essa nova capacidade, o 1º BGE necessitou adequar sua doutrina de emprego visto que o seu Centro de Operações de Guerra Eletrônica (COGE) acostumou-se a trabalhar somente com a GE. Com o advento da G Ciber, adaptações e coordenações precisaram e precisam ser feitas para que a GE e a G Ciber possam trabalhar em conjunto de forma eficiente.

Visto que a integração das atividades de Guerra Eletrônica e Guerra Cibernética são uma necessidade do 1º BGE, quais mudanças estruturais e doutrinárias devem ser realizadas no COGE para apoiar as Operações de Informação em apoio a F Ter, MD e Órgãos Governamentais?

1.2 OBJETIVOS

A fim de contribuir com a convergência das informações advindas da GE e G Ciber nas operações táticas, o presente estudo pretende apresentar uma proposta de Centro de Operações de Guerra Eletrônica e Cibernética (COGEC) para implementação no 1º Batalhão de Guerra Eletrônica.

Para atingir esse objetivo geral, foram levantados os seguintes objetivos específicos:

a) Realizar uma revisão bibliográfica sobre a integração das atividades de Guerra Eletrônica e Cibernética no âmbito internacional e nacional;
b) Propor o funcionamento do COGEC do 1º BGE para atender as capacidades operacionais de GE e G Ciber, tendo como base as Op Info em apoio à F Ter; e
c) Discutir a estrutura e composição do COGEC do 1º BGE, baseado nas Op Info em apoio à F Ter, MD e Órgãos Governamentais.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

Conforme Manual de Operações de Informação EM-20-MC10.213 (2014), as Op Info se definem da seguinte forma:

> As Operações de Informação (Op Info) consistem na atuação metodologicamente integrada de capacidades relacionadas à informação, em conjunto com outros vetores, para informar e influenciar grupos e indivíduos, bem como afetar o ciclo decisório de oponentes, ao mesmo tempo protegendo o nosso. Além disso, visam a evitar, impedir ou neutralizar os efeitos das ações adversas na Dimensão Informacional. (BRASIL, 2014)

Dentro dessa atuação metodologicamente integrada de capacidades relacionadas à informação, levantam-se dois importantes vetores de informação que são a guerra eletrônica e guerra cibernética.

O Manual de Emprego da Guerra Eletrônica C34-1 (2009), faz o seguinte destaque relativo a atuação da Guerra Eletrônica na história dos conflitos:

> Durante a 1ª Guerra Mundial (I GM), ocorreram vários eventos históricos, nos quais as ações de busca de interceptação, monitoração e bloqueio das comunicações por meios eletromagnéticos mostraram ao mundo que a tecnologia aplicada no desenvolvimento dos equipamentos eletroeletrônicos não podia estar distante do emprego das armas em terra, mar e ar. (BRASIL, 2009, p. 1-2)

Já o Manual de Guerra Cibernética EB-70-MC10.232, 1ª Ed., de 2017, define fonte cibernética como:

> Recurso que possibilita a obtenção de dados no espaço cibernético, utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A fonte cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de inteligência. (BRASIL, 2017, p. 2-2)

Nesse sentido, o presente estudo se justifica por tentar operacionalizar a integração de duas capacidades relacionadas a fontes de informação no nível tático, promovendo assim um entendimento melhor e mais ágil do cenário de determinada operação e mitigando os possíveis danos do inimigo.

O trabalho pretende, ainda, reformular o funcionamento do Centro de Operações do 1º BGE, adequando-o a nova capacidade de Guerra Cibernética atribuída ao Batalhão.

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 necessidade do 1ºBGE.

Quanto ao objetivo geral, foi empregada a modalidade analítica, tendo em vista a análise de diversos fatores, levantados em questionário, buscando dados em manuais e com especialistas na área para que se chegasse a uma linha de ação que solucionasse o problema levantado.

2.1 REVISÃO DE LITERATURA

Iniciamos o delineamento da pesquisa com a definição de termos e conceitos, a fim de viabilizar a solução do problema de pesquisa, sendo baseada em uma

revisão de literatura no período de jan/2014 a jan/2020. Essa delimitação baseou-se na necessidade de adequação do COGE do 1º BGE trabalhar não só com Guerra Eletrônica, mas também com a nova capacidade de obtenção de informação em operações que é a Guerra Cibernética.

O limite anterior foi determinado pela criação do 1º BGE, visto que antes disso, a então 1ª Cia GE não possuía a capacidade de Guerra Cibernética. Com a criação do 1º BGE e a ativação da Companhia de Guerra Cibernética nessa data, surgiu essa nova capacidade do Batalhão exigindo também outras medidas para que o Batalhão pudesse operacionalizar suas capacidades de forma eficiente, entre elas repensar a aplicação do COGE.

Foram utilizadas as palavras-chave guerra eletrônica, guerra cibernética, guerra da informação, operações de informação, sinais e ciberespaço, juntamente com seus correlatos em inglês e espanhol em sítios eletrônicos de procura na internet, na biblioteca digital do Exército, biblioteca de monografias da Escola de Aperfeiçoamento de Oficiais (EsAO) e da Escola de Comando e Estado-Maior do Exército (ECEME), sendo selecionados apenas os artigos em português e inglês. O sistema de busca foi complementado pela coleta de manuais de campanha referentes ao tema, do EB e dos EUA, em período de publicação diverso do utilizado nos artigos.

Quanto ao tipo de operação militar, a revisão de literatura limitou-se a operações de não-guerra, com enfoque majoritário nas participações do 1ºBGE em apoio a F Ter, MD e Órgãos de Segurança Pública em apoio ao Governo Federal.

a. Critério de inclusão:

- Estudos publicados em português relacionados à Guerra Eletrônica e Guerra Cibernética;

- Manuais e livros que retratam a importância da Guerra da Informação nos dias atuais; e

- Estudos qualitativos sobre o emprego da GE e G Ciber.

b. Critério de exclusão:

- Estudos que abordam a GE e a G Ciber no nível estratégico e político; e

- Estudos e reportagens que abordam as duas capacidades citadas no campo da investigação pontual de determinados fatos.

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 que servem ou já serviram no 1ºBGE. O estudo foi limitado particularmente aos oficiais da arma de comunicações, oriundos da Academia Militar das Agulhas Negras, possuidores do curso de Guerra Eletrônica ou Guerra Cibernética e que, de preferência, já tenham participado de alguma operação pelo 1º BGE devido ao assunto abordado.

Dessa forma, utilizando-se dados obtidos nos questionários, a população a ser estudada foi estimada em 17 militares. 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 15.

Apesar de o COGE normalmente ser composto por capitães ou oficiais superiores, a amostra contemplou também oficiais subalternos, visto que os mesmos, por vezes também exerceram função de integrante do COGE em operações. Dessa feita, foram distribuídos questionários para 22 oficiais que já serviram no 1ºBGE com os requisitos citados no parágrafo anterior.

A amostra foi selecionada somente no 1º BGE devido a especificidade da pesquisa que necessita que os militares tenham visto como funciona a sistemática de análise de GE no 1º BGE em uma operação. A sistemática de distribuição dos questionários ocorreu de forma direta (pessoalmente) e indireta (via grupo de aplicativo) para 22 militares que atendiam os requisitos. Entretanto, devido a diversos fatores, somente 20 respostas foram obtidas (90,9% dos questionários enviados), não havendo necessidade de invalidar nenhuma por preenchimento incorreto ou incompleto.

A partir do n_{ideal} (15), depreende-se que o tamanho amostral obtido (n=20) foi superior ao desejado para o tamanho populacional dos potenciais integrantes da amostra e, portanto, enriquece a relevância desta pesquisa, haja vista a especialização da amostra.

3 RESULTADOS E DISCUSSÃO

3.1 A GUERRA DA INFORMAÇÃO

A revolução das Tecnologias da Informação e Comunicações (TIC) possibilitou aos Estados a gerencia de redes informacionais complexas, refletindo assim, na organização de suas atividades. Sobre as TIC, PASINI (2012) faz a seguinte consideração:

> Nesse sentido, segundo SILVA (2006, p.11) a Tecnologia da 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. (PASINI, 2012, p.26)

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.

Nesse contexto, 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)

Quanto a busca de informações, PASINI (2012), faz a seguinte menção:

> [...] 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. (PASINI, 2012, p. 28)

3.2 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, 2015, p. 196)

Para CLARK (2010), as Op Info são vistas da seguinte forma:

> As Operações de Informações (Op Info) proporcionam ao comandante 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. (CLARK, 2010, p. 57)

Ainda sobre as Op Info, segundo o Manual de EB-20-MC10.213 (2014), Operações de Informação, diz o seguinte:

> As Op Info contribuem para a obtenção da superioridade de informações e integram capacidades relacionadas à informação, destacando-se: a Comunicação Social (Com Soc); as Operações de Apoio à Informação (OAI); a Guerra Eletrônica (GE); a Guerra Cibernética (G Ciber); e a Inteligência (Intlg). (BRASIL, 2014, p. 3-1)

Portanto a integração de ações de Guerra Eletrônica (GE) e Guerra Cibernética (G Ciber) são de grande importância para o êxito das Operações de Informação uma vez que, no nível estratégico, as Op Info tem como objetivo dissuadir e no nível operacional e tático tem como objetivo obter a superioridade das informações vindo a diminuir a combatividade da força inimiga.

3.3 CONVERGÊNCIA ENTRE A GUERRA ELETRÔNICA E A GUERRA CIBERNÉTICA NOS ESTADOS UNIDOS

O Manual FM 3-12 Cyberspace and Electronic Warfare Operations (2017), definiu as atividades cibernéticas e eletromagnéticas – em inglês *Cyber Eletromagnetic Activities* (CEMA), como um direcionamento na forma de operar no Espectro Eletromagnético e no Espaço Cibernético.

Segundo NETO (2017), o CEMA é definido como um esforço unificado onde as operações de ciberguerra e eletrônica devam ser integradas e sincronizadas, percebidas como um ambiente operacional único.

A seguir, tem-se outra citação do último manual americano citado em que se fala sobre a integração das funções de combate no ciberespaço e os seus riscos quanto a sua vulnerabilidade aos adversários:

> Um ambiente operacional é um composto de condições, circunstâncias e

> influências que afetam o emprego de capacidades e influenciam as decisões do comandante. O ciberespaço, as variáveis operacionais, as variáveis de missão e as dimensões do ambiente de informações compartilham um relacionamento complexo dentro de um ambiente operacional. Os estados-maiores executam tarefas e missões no e através do ciberespaço para apoiar as funções de combate. O ciberespaço apoia, habilita e integra operações para funções de combate no ambiente operacional em todos os domínios.
> Embora o ciberespaço permita recursos de comunicação, ele também cria vulnerabilidades críticas para que adversários e inimigos ataquem ou explorem. A complexidade, o baixo custo de entrada, os recursos amplamente disponíveis, o investimento tecnológico mínimo necessário e a facilidade de anonimato no ciberespaço permitem que inimigos e adversários causem danos graves. A disponibilidade expandida de tecnologia comercial de prateleira fornece aos adversários uma tecnologia cada vez mais flexível e acessível para se adaptar a propósitos militares. Barreiras baixas para o uso do ciberespaço diminuem significativamente a lacuna de capacidade tradicional entre os Estados Unidos e os adversários, permitindo-lhes colocar em campo recursos cibernéticos sofisticados. (FM 3-12, 2017, p. 1-16, tradução nossa)

Ainda, segundo NETO (2017), o ciberespaço é definido da seguinte forma:

> É um “ambiente” artificial caracterizado por uma complexa e não centralizada rede de emissões e transmissores de informações, composta não apenas pela Internet (rede mundial de computadores), mas também por redes privadas (intranets) e telecomunicações em geral. Utiliza meios físicos (ex: cabos de fibra ótica), wireless e espaciais (satélites). É redundante destacarmos a importância da internet e das outras redes para as economias nacionais e para os governos. O mais importante agora é destacarmos o aumento incessante das transmissões de rede “sem fio” pelo mundo, especialmente após o surgimento de *smartphones* e *tablets*. Emissões eletromagnéticas para comunicação, não importa se seja por rádio, internet ou data link, em termos físicos é a mesma, diferenciando o nível de frequência (bandas) em que ocorre. O ciberespaço e as emissões eletromagnéticas hoje são os principais meios de transmitir informações e conhecimento, sejam elas individuais, coletivas, civis ou militares. Na realidade, podemos afirmar que as redes de computadores e de comunicação, no século XXI, tornaram-se a mesma coisa. Há uma ampla convergência tecnológica entre computadores, comunicações, equipamentos eletrônicos, software e criptografia. O aumento da importância crescente dos sistemas de wireless para a internet traz consequências óbvias para a guerra eletrônica. (NETO, 2017, p. 213)

Dentro desse contexto da importância crescente dos sistemas wireless para a internet e suas consequências para a guerra eletrônica, PORCHE (2013) reforça essa ideia da seguinte forma:

> [...]convergência tecnológica generalizada entre computadores, comunicações, dispositivos eletrônicos e sensores - convergência tanto no nível do dispositivo quanto no nível da infraestrutura de suporte - o iPhone tem todas essas funções. Com o tempo, as infraestruturas usadas para cibernética, Guerra Eletrônica (GE) e Operações no Espectro Eletromagnético se tornarão indistinguíveis - a convergência tecnológica está permitindo que nossos ativos de rede se tornem nossos ativos EW e vice-versa. [...]
> Esses elementos resultam em convergência operacional. Operações

> Cibernéticas e Eletromagnéticas estão cada vez mais utilizando os mesmos recursos, por exemplo, ambos contam com ativos de inteligência de sinais e gerenciadores de espectro. A interdependência é tal que as Operações Cibernéticas são essenciais para a GE e Operações no Espectro Eletromagnético integrados. As capacidades de GE têm utilidade para ataque e defesa de plataformas, sistemas e redes. Essas capacidades estão sendo empregadas em conjunto (em combinações muito sofisticadas) para atingir os objetivos necessários. (PORCHE, 2013, p. 49).

3.4 CONVERGÊNCIA ENTRE A GUERRA ELETRÔNICA E A GUERRA CIBERNÉTICA NO BRASIL

A GE e a G Ciber, conforme já dito anteriormente, atuam no campo das Op Info de forma que, integradas, podem obter uma vantagem sobre os oponentes e proteger o nosso sistema de comando e controle.

Sobre isso, o Manual EB-20-MC10.213 (2014), Operações de Informação, faz a seguinte menção à integração de Ações Cibernéticas e de Guerra Eletrônica:

> Normalmente, as ações cibernéticas e eletromagnéticas são atividades desenvolvidas para apreender, reter e explorar uma vantagem sobre oponentes ou potenciais adversários, tanto no espaço cibernético como no espectro eletromagnético e, simultaneamente, negar e degradar ao adversário a utilização dessa vantagem e proteger o nosso processo decisório, particularmente o sistema de comando e controle. (BRASIL, 2014, p. 4-9)

Esse mesmo Manual, um pouco mais a frente, diz que a integração da G Ciber com a GE permite que elementos da F Ter garantam e mantenham a liberdade de ação no espaço cibernético e eletromagnético para as nossas forças, enquanto buscam explorá-la e negá-la aos oponentes. Com isso, percebe-se que a integração das duas fontes de informação é algo essencial para o êxito das operações da F Ter. (BRASIL, 2014)

No contexto do Ministério da Defesa, as ações no espaço cibernético deverão ter as seguintes denominações, de acordo com o nível decisório da Sistemática de Planejamento de Emprego Conjunto das Forças Armadas (SisPECFA).

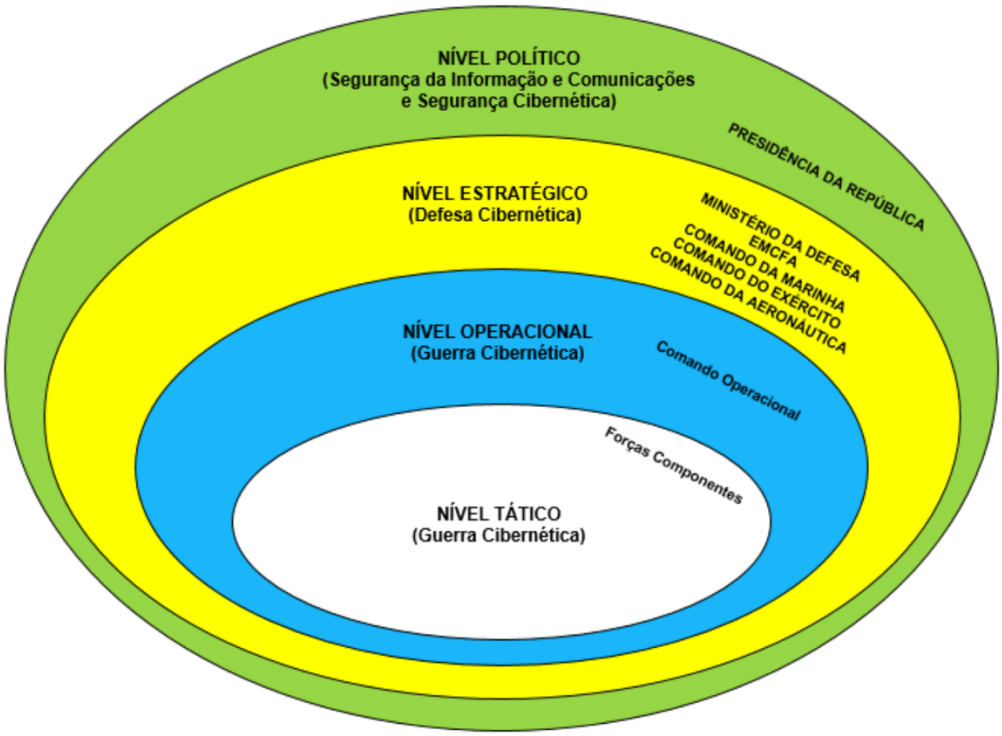

Figura 1 - Níveis de decisão
Fonte: BRASIL, 2017.

Dentro do conceito operativo do Exército em amplo espectro, as ações ofensivas de G Ciber no nível tático são conduzidas no âmbito das unidades de Guerra Eletrônica por meio das frações respectivas, sobretudo em razão da convergência conceitual e funcional, além de certa similaridade entre os alvos atuais atinentes às duas atividades.

As funções operativas de G Ciber são conduzidas pelo emprego de *malwares*[1] e *spywares*[2]. As funções de GE, por outro lado, desencadeiam-se por meio de radiação, retransmissão, exploração, execução de procedimentos e adoção de tecnologias associadas ao espectro eletromagnético.

Nas ações ofensivas de G Ciber, os *malwares* são inseridos nas redes computacionais do oponente na forma de programas, os quais são por elas assimilados e passam a desempenhar suas finalidades hostis (ataque de negação de serviços ou exploração).

Nas ações de GE, a ingerência nas redes oponentes dá-se eletromagneticamente, seja pela aquisição deliberada, reflexão ou retransmissão

---

[1] Software deliberadamente programado e distribuído para causar danos a um sistema computacional.

[2] Software que tem o objetivo de observar e roubar informações de um sistema computacional.

dos sinais emitidos ou pela radiação de energia eletromagnética com destino às antenas dos sistemas eletrônicos oponentes.

A maior parte dos sistemas táticos atuais, sejam de telecomunicações ou de sensoriamento, são integrados logicamente, formando extensas redes com considerável capacidade computacional e mobilidade, essa última característica decorrente dos enlaces baseados na emissão de sinais eletromagnéticos.

Nesses casos, o espectro eletromagnético é o principal ponto comum entre as atividades de GE e G Ciber. Portanto, ainda que atuando em domínios distintos, com objetivos e alvos diversos, há necessidade de planejamento conjunto e sincrônico das ações de GE e G Ciber, sob pena de eventual interferência, por exemplo, das ações de GE sobre as atividades desenvolvidas pela G Ciber em redes onde o espectro eletromagnético é o canal no qual elas têm suporte.

Como casos de convergência entre GE e G Ciber, citam-se as ações ofensivas sobre redes de comunicação móvel de voz e dados, sobre redes de computadores que empreguem protocolos de comunicação sem fio (como o IEEE 802.11x), entre outras.

3.5 O 1º BATALHÃO DE GUERRA ELETRÔNICA

O 1º BGE, normalmente, desdobra seus meios em três estruturas definidas: o Posto de Comando (PC), os Centro de Operações de Guerra Eletrônica (COGE) e os Postos de Guerra Eletrônica (PGE).

Segundo o Manual EB-70-MC10.247 (2020), o Posto de Comando (PC) é a estrutura de C2 que reúne material e pessoal incumbidos das atividades de planejamento e condução das operações táticas de GE. Compete ao PC do 1º BGE, ligar-se ao Comando da Força Terrestre Componente (FTC), desse receber as ordens e, para ele, remeter os resultados das ações de GE, além de planejar e conduzir a manobra da OM. Devido as peculiaridades de algumas operações, como as de GLO, algumas vezes esse PC fica caracterizado por um O Lig integrado ao Estado-Maior da FTC.

Esse último manual citado também faz a seguinte definição de COGE:

> Os Centros de Operações de Guerra Eletrônica (COGE) são instalações de C2 desdobradas e operadas pelas subunidades e frações de GE, destinadas às atividades de coordenação e condução das ações de GE

> executadas pelas frações respectivas. O COGE, justaposto ao PC da OM GE, denomina-se COGE Principal. As frações de GE, por seu turno, desdobrarão Centros de Operações de Guerra Eletrônica Avançados (COGE Avçd) em suas áreas de responsabilidade. Compete ao COGE Principal ligar-se ao PC, convertendo os planos, ordens e diretrizes recebidas do Comando da FTC em planos de GE, condizentes e adequados aos meios de sensoriamento e ataque disponíveis nos postos que lhe são afetos. O COGE Principal realiza a análise final de GE a partir dos relatórios e alarmes produzidos pelos COGE Avçd, produzindo e encaminhando Conhecimentos de Inteligência, relatórios e alarmes ao Comando do Escalão enquadrante. [...]
> [...] Os postos de GE tática são compostos de plataformas especializadas, desdobradas e exploradas por especialistas de GE, nos quais são instalados os equipamentos e os sistemas de MAGE e MAE. (BRASIL, 2020, p. 2-3)

3.6 DISCUSSÃO

O 1º BGE foi criado em 2014 com o intuito de atender as demandas do Exército quanto as operações que necessitassem de Guerra Eletrônica. Grandes eventos como a Copa das Confederações de 2013, Copa do Mundo de 2014, Olimpíadas de 2016 e várias outras operações como a ocupação do Complexo do Alemão, Complexo da Maré e a Intervenção Federal na cidade do Rio de Janeiro-RJ mostraram que essa demanda era verdadeira e não conseguiria ser suprida pela então 1ª Cia GE.

Ao mesmo tempo em que surgiu essa demanda maior pela GE, começou a surgir também o advento da G Ciber que, pela similaridade da atividade, demandou a criação da Companhia de Guerra Cibernética no 1º BGE. O objetivo dessas duas companhias era atender ao Exército nas demandas táticas de GE e G Ciber.

Com o passar do tempo e a operacionalidade da Cia GE e da Cia G Ciber, verificou-se experimentalmente em algumas operações que a junção dessas fontes de informação poderia gerar um produto satisfatório para as Op Info. Verificou-se que isso já ocorria na Central de Inteligência (quando ativada) mas, devido a demanda do 1º BGE nunca ser sempre do mesmo escalão superior, esse conhecimento gerado nessa Central somente era recordado quando o era o mesmo escalão superior empregado. Porém, por muitas vezes, acontecem operações no mesmo local, mas o escalão empregado é diferente. Com isso, as informações buscadas daquele local são reestabelecidas para essa nova operação somente na parte de GE, pois esta também ficou guardada no COGE Principal do 1º BGE, mas o conhecimento vindo da integração da GE com a G Ciber não, visto que o COGE possui capacidade apenas de processar informações de GE.

Diante desse problema, foi feito um questionário com alguns oficiais que já serviram no 1º BGE e possuem o curso de Guerra Eletrônica e/ou de Guerra

Cibernética no intuito de validar essa possibilidade de transformação do COGE em COGEC, vindo a guardar não só o conhecimento vindo do Espectro Eletromagnético mas também o conhecimento vindo do Espaço Cibernético e, sempre que possível, gerar um produto útil da junção das informações vindas das duas fontes e guarda-las no 1º BGE para operações futuras no mesmo local/cenário.

Inicialmente, perguntou-se qual o Posto do entrevistado e verificou-se que, do universo que respondeu ao questionário, 10% eram Maj, 55% Cap e 35% 1º Ten.

Dentre esses 20 militares que responderam o questionário, verificou-se também que 90% dos militares possuem o curso de Guerra Eletrônica e somente 20% possuem o curso de Guerra Cibernética. Nesse dado pode-se ver que, apesar de o curso de Guerra Cibernética ter sido ministrado pela primeira vez em 2012, o 1º BGE ainda possui uma deficiência grande em oficiais especialistas em G Ciber.

Após isso, foi perguntado se esses militares já haviam participado de alguma operação em função de GE ou G Ciber e, como foi verificado que todos já haviam participado, perguntou-se também se nessas operações em que participaram, haviam outras equipes realizando a outra atividade que o militar não estava realizando (GE ou G Ciber). Nesse último questionamento, verificou-se que a grande maioria (90%) dos questionados tiveram a oportunidade sim de estar trabalhando nas fontes de Guerra Eletrônica ou Cibernética enquanto outro militar, na mesma operação, estava contribuindo com a outra fonte que ele não estava monitorando. Isso mostra que, apesar de não haver tantos oficiais no 1º BGE especializados em Guerra Cibernética, a demanda por essa fonte é praticamente a mesma da demanda de Guerra Eletrônica.

O próximo questionamento perguntou aos militares qual o nível de importância que eles davam a integração das atividades de Guerra Eletrônica e Guerra Cibernética, conforme GRÁFICO 1 a seguir:

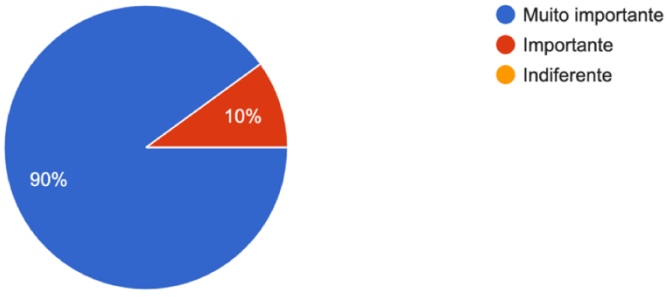

GRÁFICO 1 - Nível de importância da integração da GE e G Ciber
Fonte: O autor

Dentre as respostas, verificou-se que 18 deles consideram a integração muito

importante, sendo que 2 consideram importante e ninguém considerou indiferente.

Com essas respostas, pôde-se observar que para a maioria dos militares empregados e missões táticas de GE e G Ciber, a integração dessas duas fontes de informação é considerada de alta relevância para o êxito da missão.

Dando continuidade a linha de pensamento do trabalho, o próximo questionamento foi: considerando que em uma operação seja empregada uma equipe de GE e outra de G Ciber, as duas do 1ºBGE, o sr considera importante uma integração, além da já feita na Central Intlg, das informações obtidas pelas duas fontes (tendo em vista o uso desse conhecimento em operações futuras na mesma região, mas que o escalão apoiado não seja o mesmo)?

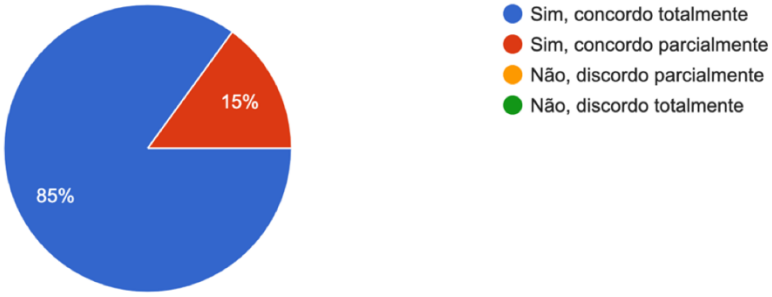

GRÁFICO 2 - Nível de importância da integração de GE e G Ciber no 1º BGE
Fonte: O autor

Conforme GRÁFICO 2 acima das respostas, conseguiu-se reforçar a ideia já levantada de que realmente o 1º BGE precisa de uma integração das fontes que ele emprega em missão (Guerra Eletrônica e Guerra Cibernética) além da integração já feita na Central de Inteligência das operações restando apenas debater como que se pode operacionalizar essa situação.

A 7ª questão levantada foi: visto que o 1º BGE possui uma Cia G Ciber e uma Cia GE para operacionalizar os dois ramos de levantamento de informação, o sr considera importante a adaptação do COGE para um COGEC (Centro de Operações de Guerra Eletrônica e Cibernética) dentro do 1º BGE em que essas informações possam ser discutidas para a construção de um conhecimento? Com 95% dos militares que responderam o questionário concordando com esse modo de operacionalização, ratificou-se a proposta levantada no artigo em questão, reforçando todas as ideias anteriores levantadas e reforçando a ideia de que um COGEC integrando as duas fontes poderá enriquecer o conhecimento já feito em algumas ocasiões nas Centrais de Inteligência e, ao mesmo tempo, guardar esse conhecimento gerado para operações futuras, independente do escalão ou órgão enquadrante do 1º BGE.

Como ultimo questionamento, foi perguntado se o militar acredita que a composição mínima para o COGEC proposto seria de 1 (um) oficial especialista em GE, 1 (um) oficial especialista em G Ciber e 1 (um) oficial integrador.

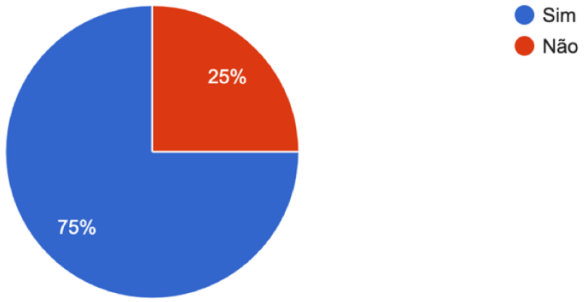

GRÁFICO 3 - Proporção de especialistas que concordam com a proposta do COGEC

Fonte: O autor

Essa proposta foi feita tendo em vista que o analista, tanto de GE quanto de G Ciber, é um oficial. Portanto, visto que a informação que chegará nesse COGEC Principal virá dos COGE Avçd e do analista que Cibernética, que também são oficiais e, respeitando a hierarquia funcional do Exército, acreditou-se que essa seria a proposta mais viável. Apesar da concordância da maioria, houveram outras poucas opiniões em diversas linhas de ação diferentes com algumas falando que dependeria do tipo de missão, outra desconsiderando o oficial integrador, outra desconsiderando os especialistas em GE e G Ciber e uma última propondo também o apoio de ST/Sgt especialista também nesse COGEC.

Como ultima pergunta, foi perguntado se havia alguma sugestão ao trabalho que está sendo desenvolvido. Das considerações feitas, pôde-se ressaltar duas que reforçam a ideia da proposta.

Na primeira, o militar disse que “O trabalho das duas capacidades, quando integrado, proporciona o planejamento mais adequado de busca de alvos considerando ambas as possibilidades. Ademais, o resultado do trabalho tendo sido considerado ambos os produtos das capacidades em uma única análise, facilita o trabalho, reduz esforços e resulta um informe mais robusto”. Diante do exposto por esse militar, se reforça a ideia de que as duas fontes de informação, quando integradas, podem produzir um conhecimento mais rebuscado, caracterizado na análise do militar como “um informe mais robusto” facilitando, por muitas vezes, a busca de alvos.

O segundo militar expressou a seguinte opinião: “Interessante a criação de um banco de dados único no COGEC visto que as duas capacidades, GE e Ciber,

diferem unicamente nas fontes de alimentação". Nessa afirmação, pode-se buscar o que foi exposto anteriormente sobre a similaridade das capacidades. Talvez em uma análise mais detalhada, chegue-se a conclusão de que as capacidades não se diferem somente quanto a fonte de alimentação, mas é inegável que essas possuam certa similaridade. Caso não possuíssem o Exército não estaria as operacionalizando, no nível tático, dentro da mesma OM (1ºBGE). O segundo ponto levantado pelo militar questionado foi o banco de dados único. Sabemos que, assim como a memória de operações anteriores do mesmo local, a concepção de um banco de dados único facilitará o trabalho dos militares envolvidos nas operações e, como dito pela primeira opinião, tudo isso também reduzirá esforços e resultará em informes mais robustos.

Terminado o questionário, pôde-se notar que a maioria das opiniões e situações levantadas com os militares empregados em missões de Guerra Eletrônica e Guerra Cibernética seguem a mesma direção geral que é a importância da integração da Guerra Eletrônica e Guerra Cibernética, não só nos escalões mais elevados, mas também no nível tático, sempre visando o melhor aproveitamento desse poder de combate nas operações.

4 CONSIDERAÇÕES FINAIS

Quanto às questões de estudo e objetivos propostos no início deste trabalho, conclui-se que a presente investigação atendeu ao pretendido, ampliando a compreensão sobre a convergência das atividades de Guerra Eletrônica e Guerra Cibernética no 1º BGE nas operações.

A revisão de literatura possibilitou concluir que a relevância da integração da Guerra Eletrônica com a Guerra Cibernética era de fundamental importância para degradar o sistema de Comando de Controle inimigo e para manter a liberdade de ação os espaços cibernético e eletromagnético nas operações, conforme citação retirada do manual de Op Info do Exército Brasileiro.

Dessa forma, entende-se que para chegar a esses objetivos, é necessário manter a superioridade das informações. Uma das formas de obter essa superioridade é integrando as fontes de informação, dentre elas a GE e a G Ciber.

O estudo dos manuais e a busca por dados mostrou que essa integração ocorre, mas somente nos níveis operacional, estratégico e político.

A criação do 1º BGE e o surgimento da Companhia de Guerra Cibernética nessa OM fizeram com que as fontes de GE e G Ciber, no nível tático, ficassem

todas sob um mesmo comando.

Estando essas duas fontes de informação sob o mesmo comando, surge o questionamento de por que as informações advindas das duas fontes se integram somente quando há uma Central de Inteligência em proveito de alguma operação ou em um Estado-Maior fora do 1º BGE sendo que as duas fontes pertencem a mesma Unidade.

Diante desse questionamento, verificou-se que a transformação do COGE em COGEC atenderia essa demanda e assim as informações das duas fontes poderiam ser trocadas para a elaboração de um conhecimento mais robusto e o banco de dados dessas fontes permaneceriam no Batalhão e não com o Estado-Maior enquadrante de cada missão, visto que o 1º BGE nem sempre apoia o mesmo escalão superior. O fluxo de informações seguiria o organograma apresentado abaixo:

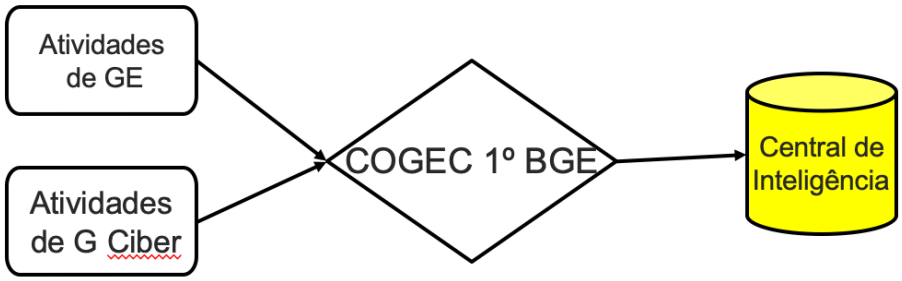

FIGURA 2 - FLUXO DE INFORMAÇÕES DO 1º BGE EM MISSÕES
Fonte: O Autor

Através do questionário distribuídos a militares especializados e que servem ou já serviram no 1º BGE, pôde-se constatar que tal transformação seria de grande valia para o Batalhão e que o produto gerado através de conhecimento e informes tornaria mais eficiente a produção de um conhecimento maior no âmbito Célula de Inteligência. Além disso, esse conhecimento gerado, com a criação do COGEC, ficará armazenado dentro do 1º BGE, podendo ser empregado em qualquer nova missão, independente do escalão superior enquadrante.

Como ultimo questionamento a ser ratificado por esse trabalho, foi verificado através do questionário também que a proposta de 1 (um) oficial especialista em Guerra Eletrônica, 1 (um) oficial especialista em Guerra Cibernética e 1 (um) oficial integrador seria a composição mínima para a constituição desse COGEC. Conforme já levantado e ratificado pela maioria dos questionados, tal configuração se mostrou útil devido a necessidade de cada especialista receber os dados dos seus postos

avançados empregados na operação e o oficial integrador fazer a junção dessas informações produzindo o conhecimento mais robusto, sendo tal estrutura aplicável tanto em operações da F Ter, como também em apoio ao MD e à Órgãos Governamentais.

Conclui-se, portanto, que é inegável a necessidade da integração das fontes de Guerra Eletrônica e Guerra Cibernética no nível tático, dentro do 1º BGE. A integração as duas fontes, que são os dois braços operacionais do Batalhão, deve se operacionalizar através da transformação do COGE em COGEC, fazendo assim, com que o conhecimento não se perca devido ao elemento que faz a junção ser externo ao 1º BGE e que esse conhecimento gerado seja mais significativo, se mostrando mais útil e tornando as Op Info mais eficientes.

REFERÊNCIAS

BRASIL. Ministério da Defesa. Estado-Maior de Defesa. MD35-G-01, **Glossário das Forças Armadas**. 5. Ed. Brasília, DF. 2015.

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

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. EB70-MC-10.247, **A Guerra Eletrônica nas Operações**. 1. Ed. Brasília, DF. 2020.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. C 34-1 **Emprego da Guerra Eletrônica**. 2. Ed. Brasília, DF. 2009.

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

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

DINARDO R. L. e HUGHES D. J**. Algumas Reflexões de Prudência Acerca da Guerra da Informação.** Militar Review. Ed. Brasileira, p. 40-49. 4º quadrimestre 1998.

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.

PORCHE III, Isaac R et all. **Redefining Information Warfare Boundaries for an Army in a Wireless World**. RAND Corporation. 2013.

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

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

UNITED STATES. Headquarters. Department of the Army. FM 3-12, **Cyber Space and Electronic Warfare Operations**. Apr, 2017.

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

APÊNDICE A - QUESTIONÁRIO

Esse formulário tem por objetivo levantar informações com os oficiais que já serviram no 1ºBGE para a adaptação do COGE para COGEC (Centro de Operações de Guerra Eletrônica e Cibernética) do 1º BGE tendo em vista a capacidade tática de Guerra Cibernética que o BGE adquiriu com a ativação da Cia G Ciber.

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

Michell Medeiros Santos (Capitão de Comunicações – AMAN 2011)

Celular: (61) 98128-0238

E-mail: michell.santos@eb.mil.br

IDENTIFICAÇÃO

1. Qual seu posto/graduação atual?

_____

2. O sr possui o curso de Guerra Eletrônica?

   ( ) Sim

   ( ) Não

3. O sr possui o curso de Guerra Cibernética?

   ( ) Sim

   ( ) Não

ASPECTOS OPERACIONAIS

4. O sr já participou de alguma operação em alguma função de Guerra Eletrônica ou Guerra Cibernética?

   ( ) Sim

   ( ) Não

5. Caso tenha respondido "Sim" na pergunta anterior, nessas operações, houveram outras equipes realizando a outra atividade? Por ex: se o sr estava

levantando informações de GE, tinha alguém levantando informações pelos meios cibernéticos?

( ) Sim

( ) Não

6. Qual o nível de importância que o sr considera a integração dessas duas atividades?

   ( ) Muito importante

   ( ) Importante

   ( ) Indiferente

7. Considerando que em uma operação seja empregada uma equipe de GE e outra de G Ciber, as duas do 1ºBGE, o sr considera importante uma integração, além da já feita na Central Intlg, das informações obtidas pelas duas fontes? (Tendo em vista o uso desse conhecimento em operações futuras na mesma região mas que o escalão apoiado não seja o mesmo)
   ( ) Sim, concordo totalmente
   ( ) Sim, concordo parcialmente
   ( ) Não, discordo parcialmente
   ( ) Não, discordo totalmente

8. O sr acredita que a composição mínima para o COGEC proposto seria de 1 (um) oficial especialista em Guerra Eletrônica, 1 (um) oficial especialista em Guerra Cibernética e 1 (um) oficial integrador?
   ( ) Sim
   ( ) Não
   9.

9. Caso tenha respondido "Não" na questão anterior, gostaria que o sr expusesse os motivos ou outra proposta que julgue pertinente.

_____
_____
_____

FECHAMENTO

10. Sugestões ao trabalho:

_____
_____
_____

Obrigado pela participação.