PADECEME

A publicação de atualização dos diplomados da ECEME

Publicação semestral | Nº 01/2020

A DIMENSÃO INFORMACIONAL

Escola de Comando e Estado-Maior do Exército
(Escola Marechal Castello Branco)
v. 15 n. 24 - 01/2020

PADECEME

01/2020
Rio de Janeiro

ISSN 1677-1885

A PADECEME é uma publicação semestral da Divisão de Doutrina da Escola de Comando e Estado-Maior do Exército (ECEME), de natureza acadêmica, sem fins lucrativos, baseada na política de acesso livre à informação.

Endereço e Contato
Praça General Tibúrcio, 125, Praia Vermelha, Rio de Janeiro/RJ, Brasil. - CEP: 22290-270.
Tel: (21) 3873-3825 / Fax: (21) 2275-5895
e-mail: padeceme@eceme.eb.mil.br

Editoração
Divisão de Doutrina da ECEME.

Impressão
Seção de Editoração Eletrônica - SEDEL.

Design gráfico da capa
Divisão de Doutrina da ECEME.

Foto da capa
Montagem com Fotos de: eb.mil.br

Tiragem
400 exemplares (Distribuição Gratuita)
Disponível também em:<www.eceme.eb.mil.br>

Dados Internacionais de Catalogação na Publicação (CIP):

P123 PADECEME. — N. 01- . — Rio de Janeiro: ECEME, 2002- . v. : il.; 23 cm.

Semestral
Publicada dos n.1-14 com o título PADECEME entre os anos de 2002 e 2007, volta a ser publicada com o mesmo título em 2015, dando sequência a sua numeração.
ISSN : 1677-1885

1.DOUTRINA MILITAR. 2. DEFESA. I. Escola de Comando e Estado-Maior do Exército (Brasil).

CDD 355

EDITORIAL

O que, na atualidade, é denominado *dimensão informacional* sempre foi elemento de extrema relevância nas guerras. Obter a informação, produzi-la com fins específicos ou negá-la ao adversário é consideração fundamental para o planejamento e a condução das operações militares.

As primeiras duas décadas do século XXI têm demonstrado o que já se previra ao final do século anterior: com a revolução dos meios tecnológicos computacionais, chegando-se ao advento das mídias sociais e da inteligência artificial, a humanidade vê-se transformada na sua capacidade de pesquisar, produzir, difundir e armazenar informação em grande volume. Vivemos, hoje, a era dos metadados ou metainformação. Essa capacidade amplificada, que antes estava ao alcance apenas do Estado ou das grandes corporações, chegou à palma da mão de cada pessoa. Um indivíduo ou sistema inteligente por ele instruído recebe e dissemina a informação (de qualidade ou não) a milhares ou mesmo milhões de outros indivíduos em curtíssimo tempo! E, acompanhando a *informação fática* e mesmo com maior ênfase, muitas vezes circula a *percepção* sobre ela, moldando-a na produção do que se pode chamar de *pós-verdade*. Esta, por sua vez, pode potencializar a realidade dos fatos, mas, comumente, modifica a verdade, com um propósito definido por interesses de indivíduos ou grupos.

Portanto, o planejamento e a condução de operações militares, mais que nunca, devem ter a dimensão informacional como um dos fatores determinantes da decisão. O combate moderno passa, necessariamente, pela atuação no espectro informacional, em busca de vantagens competitivas sobre o adversário.

A ECEME é uma escola centenária que capacita os futuros líderes estratégicos do Exército e que foi criada para antever o futuro e ser capaz de trabalhar o inédito. Na história do nosso Exército, os oficiais diplomados pela ECEME deram inúmeras provas de capacidade de superar desafios. Talvez, o maior deles tenha sido o planejamento, o preparo e o emprego da Força Expedicionária Brasileira nos campos da Itália. Hoje, o enfrentamento à pandemia COVID-19 torna a exigir o máximo de capacidade dos nossos oficiais do Quadro de Estado-Maior da Ativa (QEMA). E, neste enfrentamento, o saber lidar com a dimensão informacional se torna essencial para que o planejamento e a condução das operações tenham o melhor resultado. Por isso, ficamos honrados por trazer ao nosso leitor a riqueza de conhecimento sobre a dimensão informacional, contida nos artigos desta edição do PADECEME.

Ao final da leitura deste periódico, espero que o caro leitor possa compartilhar da mesma percepção sobre tão relevante tema, expressa no seguinte pensamento: *a vitória tática no campo de batalha somente se traduzirá como vitória estratégica e política se também vencermos no campo da pós-verdade.*

"O saber na defesa da Pátria!"

Rio de Janeiro - RJ, 2 de maio de 2020.

General de Brigada Rodrigo Pereira Vergara
Comandante da ECEME


Escola Marechal Castello Branco
1905
Escola de Estado-Maior

SUMÁRIO

A COMUNICAÇÃO ESTRATÉGICA DO EXÉRCITO E A DIMENSÃO INFORMACIONAL

Gen Div RICHARD FERNANDES NUNES[1]

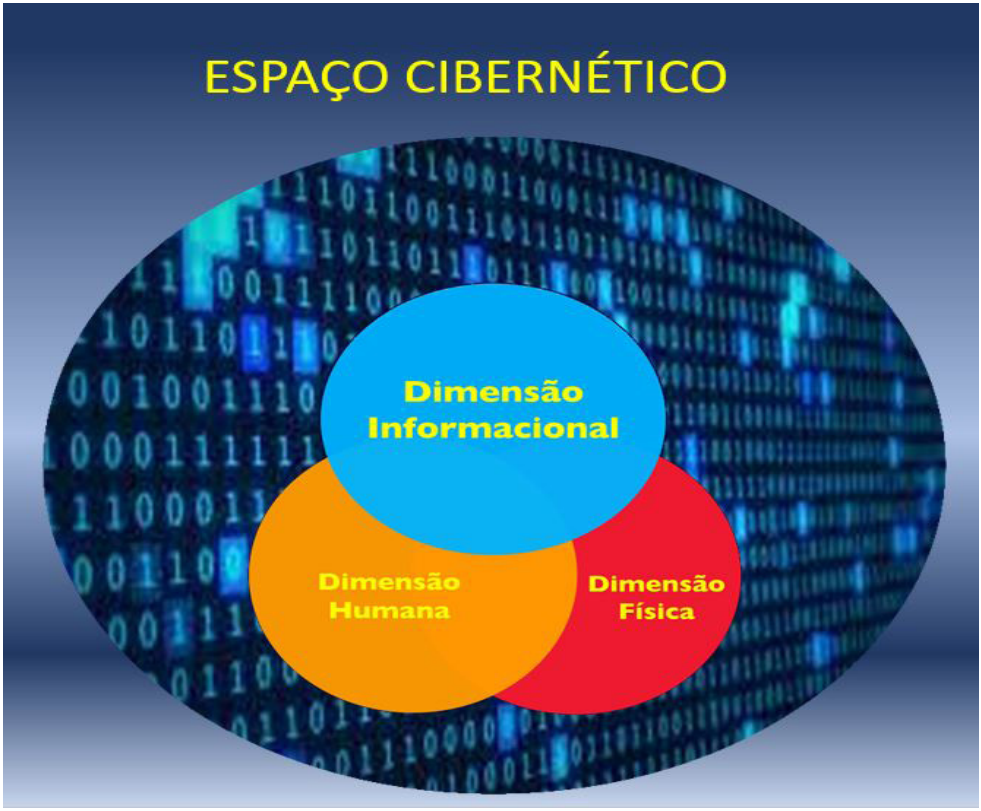
I. INTRODUÇÃO

A **comunicação estratégica**[1] pode ser definida como a comunicação integrada, sincronizada e alinhada com as ações realizadas por uma organização para atingir seus objetivos. Pressupõe a combinação das práticas adotadas no âmbito da **comunicação social** tradicional[2] com **relações institucionais** sistematizadas e com o emprego das **mídias digitais,** aí incluídas as mídias e redes sociais. Tal conceito de comunicação, típica do meio corporativo, é perfeitamente aplicável à comunicação no âmbito do Exército Brasileiro.

A doutrina militar terrestre preconiza que o ambiente operacional onde se desenrolam as ações militares compreende três **dimensões**[3]: a física, de natureza geográfica e material, com ênfase para o terreno, as condições meteorológicas e os equipamentos empregados; a humana, de caráter psicossocial e cultural, pautada pelas interações entre as tropas e populações envolvidas; e a **informacional**, altamente dependente de meios tecnológicos, centrada na elaboração de narrativas que retratem a percepção da realidade. Sobre esta configuração, paira o **espaço cibernético** (Fig. 1), no qual se observa a aceleração, a potencialização e a automação dos mais diversos sistemas e processos, sem perder de vista a intencionalidade humana no fenômeno da comunicação.

1 Chefe do CCOMSEx desde fevereiro de 2019. Comandou a ECEME de setembro de2016 a março de 2018.

Fig. 1 Dimensões do ambiente operacional

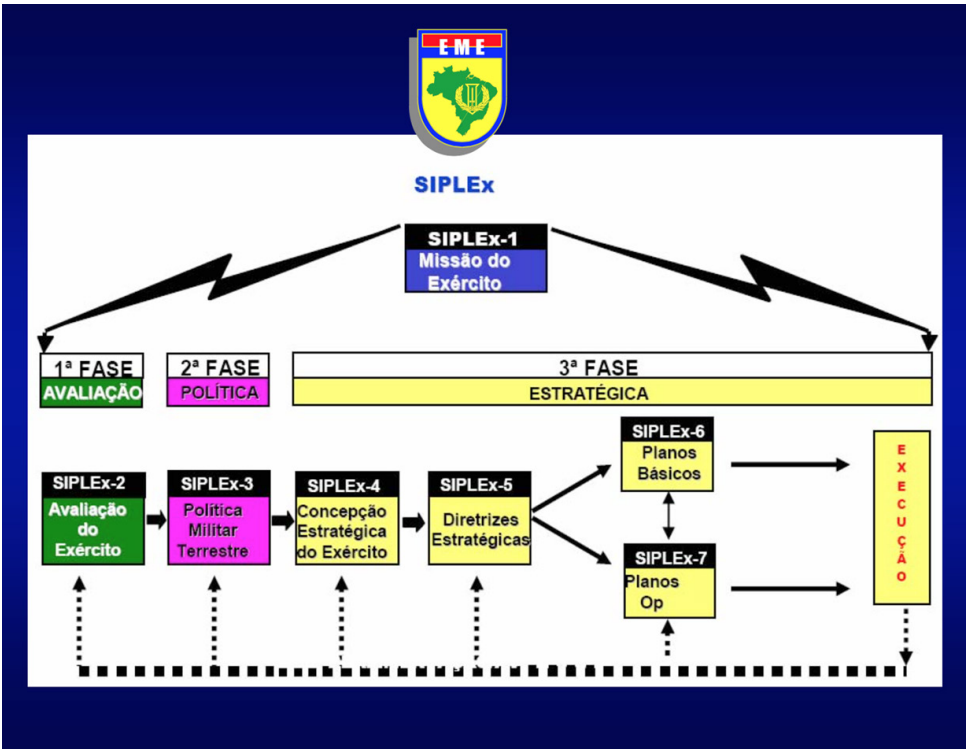


O propósito deste trabalho é analisar o desenvolvimento da comunicação estratégica do Exército Brasileiro em meio à complexidade que caracteriza a dimensão informacional, extrapolando ambos os conceitos de modo a serem aplicados tanto na vertente institucional quanto no âmbito operativo dessa comunicação, considerando-se a crescente relevância das ações realizadas no espaço cibernético.

II. A COMUNICAÇÃO NO EXÉRCITO BRASILEIRO

O Exército Brasileiro explicita, por meio de seu Sistema de Planejamento Estratégico (SIPLEx) (Fig. 2), os objetivos a serem alcançados pela instituição, bem como detalha as condições de realização das ações planejadas. Alinhada com o SIPLEx, a comunicação do Exército adquire feição estratégica, a ser ratificada conforme a capacidade de integração e sincronização que for capaz de obter, seja em relação aos objetivos específicos que lhe competem, seja no apoio à consecução dos demais.

Fig. 2 Esquematização do SIPLEx



O sistema corporativo encarregado da comunicação social do Exército é o SISCOMSEx[4], cujo órgão central é o Centro de Comunicação Social do Exército (CCOMSEx), a quem compete propor os planos e diretrizes e coordenar as ações correspondentes, valendo-se de rede dedicada a esse fim: a RESISCOMSEx[5]. Além dessa atribuição, o CCOMSEx tem sua atuação na vertente institucional ampliada pela missão de ser um dos órgãos de assistência direta e imediata (OADI) ao Comandante do Exército.

O caráter estratégico, eminentemente institucional, permanente e sistemático da comunicação social do Exército não restringe, ao contrário, potencializa, sua participação no ambiente operacional, particularmente no âmbito das operações de informação[6], como uma das capacidades relacionadas à informação (CRI). Neste caso, **a comunicação estratégica mobiliza-se para a atuação operativa**, como ferramenta indispensável para se multiplicar o poder de combate, fortalecer o espírito de corpo e o moral da tropa, na dimensão humana; bem como para se buscar a participação efetiva na elaboração de narrativas a fim de se obter o apoio da opinião pública, centro de gravidade da **dimensão informacional**, condição essencial para o aumento da liberdade de ação.

Em qualquer situação, considerações acerca das atividades no ciberespaço se impõem, devido ao relativamente baixo custo que requerem e à dificuldade de se atribuir responsabilidades de narrativa nesse meio tão propício à ambiguidade, em que é difícil identificar condições de alinhamento aos nossos interesses, e no qual "o inimigo do nosso inimigo não é necessariamente nosso amigo".

Considerando essa gama de responsabilidades, cabe ao CCOMSEx a **missão** precípua de **preservar e fortalecer a imagem do Exército**, condição essencial para que possa atingir seus objetivos a instituição que, ao longo de sua trajetória histórica, tem desfrutado de ilibada reputação e dos mais altos índices de credibilidade junto à sociedade brasileira.

III. A PRESERVAÇÃO DA IMAGEM DO EXÉRCITO

A missão de preservar a imagem do Exército subentende abordagem preventiva e reativa, diante das ameaças potenciais ou concretas que possam afetá-la. Os ativos mais relevantes a se proteger são exatamente os elementos essenciais da reputação e da credibilidade desfrutadas pela Instituição. Assim, os princípios éticos e os valores morais que a sustentam, a cultura organizacional que a caracteriza e a narrativa consolidada de sua trajetória histórica precisam ser permanentemente protegidos contra posicionamentos adversos que, de modo explícito ou dissimulado, possam atingir a imagem da Força e dificultar a consecução de seus objetivos estratégicos.

Nesse contexto, devem ser objeto de redobrada atenção: os estabelecimentos de ensino do Exército e a educação militar por eles proporcionada, reconhecida pela qualidade e pelo culto aos valores centrais da Instituição; a memória dos patronos e de outros vultos e fatos históricos em que a Força Terrestre se notabilizou; a honorabilidade dos comandantes, chefes e diretores em todos os níveis; o respeito aos preceitos da hierarquia e da disciplina; o emprego atual da Força no amplo espectro das operações; bem como as narrativas elaboradas pela Força e difundidas pelo SISCOMSEx, em particular nos diversos ativos digitais do Exército.

Eventuais deficiências observadas no tratamento desses temas podem se converter em vulnerabilidades passíveis de exploração negativa, com reflexos ainda mais expressivos se esta vier a ocorrer no espaço cibernético. A metodologia aplicada na análise de riscos à segurança orgânica é pertinente também nesta área. A exposição inadequada ou a superexposição de assuntos de interesse, por exemplo, constituem riscos ponderáveis a considerar. A falta de alinhamento, de sincronização e de integração da comunicação, ou seja, a perda do seu caráter estratégico, constitui o pior cenário, capaz de caracterizar fragilidade na chamada segurança cibernética social, relacionada ao entendimento e previsão de mudan-

ças influenciadas pela cibernética no comportamento humano e seus resultados sociais, culturais e políticos[7].

As ameaças à imagem do Exército, como quaisquer outras que visem obstar a conquista de seus objetivos estratégicos ou operacionais, podem ser de origem interna ou externa, provenientes de forças oponentes regulares ou irregulares, de organizações não governamentais ou agências diversas, de produtores de mídia ou de atores não estruturados. Os ataques que podem ser desferidos na dimensão informacional visam, em última análise à desinformação, à contraposição de narrativas alternativas, com ou sem fundamento nos fatos, neste caso as chamadas *fake news*, com o propósito deliberado de atingir a imagem da instituição. São comuns os recursos ao emprego de *deep fakes*[8], de *hackers, bots e trolls*[9], de *cyborgs*[10], bem como à manipulação, à distorção, à descontextualização, à falsificação de perfis e de conteúdos.[11]

A resposta adequada à concretização dessas ameaças depende de efetivo monitoramento do espaço cibernético com ferramentas tecnológicas desenvolvidas para a análise de tudo o que circula em meio digital e que possa estar relacionado aos interesses do Exército. Nessa tarefa, a comunicação estratégica, a inteligência e a defesa cibernética precisam atuar absolutamente integradas, de modo a proporcionarem acurado assessoramento à tomada de decisão, daí decorrendo as ações diretas e indiretas a realizar. Para o êxito da missão de preservação da imagem da Força, iniciativa e liderança são atributos fundamentais a serem observados em todos os níveis. Com a velocidade e a abrangência que caracterizam as ações no espaço cibernético, não há tempo a perder para a adoção oportuna das medidas preventivas ou reativas que se fizerem necessárias.

IV. O FORTALECIMENTO DA IMAGEM DO EXÉRCITO

A missão de fortalecer a imagem do Exército tem enfoque proativo, com vistas ao aproveitamento de todas as oportunidades oferecidas ou criadas para a veiculação de mensagens favoráveis, por todos os integrantes do SISCOMSEx. A conquista do apoio da opinião pública confere a legitimidade necessária à obtenção de liberdade de ação para a consecução dos objetivos estratégicos e operacionais da Força.

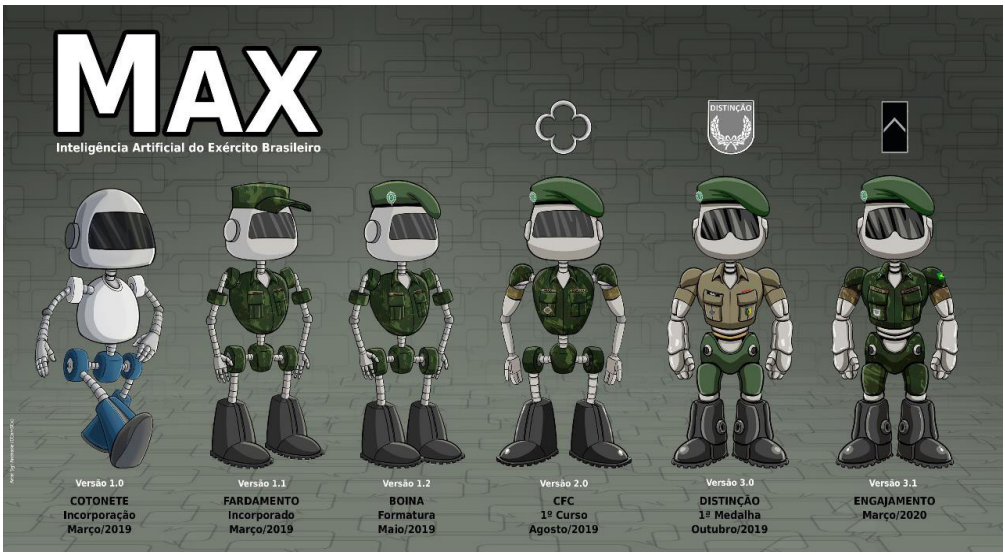
A atitude mais positiva é a difusão e o reforço de narrativas, de modo integrado e sincronizado, acerca dos elementos essenciais da reputação e da credibilidade da Instituição, considerando-se que "tudo comunica!". Neste sentido, todos os veículos disponíveis devem ser mobilizados, com especial atenção para as plataformas digitais. A busca de parcerias com órgãos externos à Força capazes de multiplicar o efeito dessas narrativas é altamente recomendável. Para isso, a sistematização das relações institucionais, inclusive com órgãos de mídia, constitui

componente relevante da comunicação estratégica do Exército.

O emprego alinhado, integrado e sincronizado das mídias digitais no âmbito do SISCOMSEx é impositivo para o êxito na missão. Para isso, foram publicadas as Normas para Criação e Gerenciamento das Mídias Sociais no Âmbito do Exército Brasileiro[12] em 1º de julho de 2019. Tais normas constituem instrumento disciplinador essencial para a comunicação estratégica do Exército, deixando claro o que é permitido e desejável e resguardando a Instituição de eventuais interações prejudiciais às narrativas da Força.

O fortalecimento da imagem do Exército comporta também o emprego de inteligência artificial. Em 1º de março de 2019, foi "incorporado às fileiras do Exército" o Soldado MAX, abreviatura de Módulo Auxiliar de relações públicas e homenagem ao herói brasileiro da 2ª Guerra Mundial[13]. Iniciativa inovadora, esse *chatbot*, cujo algoritmo é desenvolvido pelo Exército, tem demonstrado excepcional capacidade de interação, particularmente com segmentos de público mais jovens interessados em ingressar na Força Terrestre, que podem acompanhar a evolução de seu progresso na "carreira" por meio de sucessivos avatares (Fig. 3) e do incremento em sua responsividade.

Fig. 3 MAX – a inteligência artificial do Exército Brasileiro



Em termos de dimensões do ambiente operacional, todas perpassadas pelo espaço cibernético, não se pode perder a noção de que a atuação de uma força armada está intrinsecamente ligada à geração de fatos reais, nas dimensões física e humana. A dimensão informacional remete a representações virtuais dessa realidade sujeitas a uma série de filtros de caráter multidisciplinar. A História, o

Direito, a Sociologia, a Antropologia, a Psicologia, entre outras disciplinas, além de posicionamentos ideológicos diversos, condicionam a percepção da realidade. Sendo assim, a elaboração de narrativas direcionadas para o fortalecimento da imagem institucional do Exército, bem como da força empregada, precisa levar em consideração esse complexo espectro de áreas do conhecimento.

Na literatura que se tem produzido a respeito da chamada Guerra Híbrida, percebe-se a combinação dessas variáveis dimensionais, de modo integrado e sincronizado às tradicionais formas de combate, impactando o comportamento do público, muitas vezes com narrativas manipuladas no ciberespaço para a obtenção de legitimidade e da consequente liberdade de ação. O Exército tem de estar preparado para esse tipo de conflito e nada mais adequado que adotar a proatividade que resulte no fortalecimento da imagem e na participação efetiva na elaboração de narrativas desejáveis, em tempos de paz ou de conflito armado.

V. CONSIDERAÇÕES FINAIS

Como se pode depreender deste trabalho, a preservação e o fortalecimento da imagem do Exército, nos tempos atuais, indicam a necessidade de uma abordagem mais abrangente que a da comunicação social tradicional, de um redirecionamento para a adoção dos preceitos da comunicação estratégica.

Para isso, há a imperiosa necessidade de atualização dos cursos e estágios que capacitam militares para essas competências e, de modo mais abrangente, dos currículos das escolas de formação, de aperfeiçoamento e de altos estudos, por meio de disciplinas regulares e eletivas. Quanto à tropa, a exemplo do que já se observa em outros exércitos , deve-se incluir conhecimentos sobre o ambiente informacional nos programas de instrução militar relativos à formação individual do combatente, de acordo com a premissa do SISCOMSEx de que cada soldado corresponde a uma mensagem.

Uma instituição com a reputação e a credibilidade do Exército deve boa parte dessa condição ao culto à verdade e à transparência, esta última salvaguardada pelo sigilo que envolve os temas de segurança nacional.

A chamada pós-verdade , que opõe aos fatos o apelo a emoções, sentimentos, crenças e paixões ideológicas, a fim de se criar narrativas alternativas, tão em voga nos dias atuais, não se coaduna com a comunicação estratégica do Exército. Esse tipo de narrativa oportunista não perdura em sociedades democráticas e estruturadas em instituições sólidas. Não pode, entretanto, ser desprezado, devido aos danos que a desinformação pode causar. A vitória, nesse contexto, demanda vigilância constante e permanente disposição para a atuação proativa na dimensão informacional.

Com as possibilidades tecnológicas proporcionadas no espaço cibernético, acelerando, potencializando e automatizando ações informacionais, torna-se ainda mais relevante a observância de sólidos princípios éticos, garantia do caráter regular e permanente do Exército, condizente com a grandeza da missão de defender a Pátria Brasileira.

1 Não há definição consolidada na literatura acerca desse conceito. Entretanto, há consenso de que se trata de ações integradas de comunicação com vistas à conquista dos objetivos organizacionais.

2 Compreende as atividades de Relações Públicas, Assessoria de Imprensa e Divulgação Institucional (Manual de Fundamentos EB20-MF-03.103 Comunicação Social, 2ª Edição, 2017).

3 Manual de Campanha EB70-MC-10.223 Operações, 5ª Edição, 2017.

4 Sistema composto por agências classe A, B, C e Especiais, estruturas de comunicação social distribuídas por todas as organizações militares do Exército (Manual de Fundamentos EB-20-MF-03.103 Comunicação Social, 2ª Edição, 2017).

5 Rede colaborativa pela qual os integrantes do sistema estabelecem as ligações do canal técnico necessárias ao funcionamento do SISCOMSEx (Manual de Fundamentos EB20-MF-03.103 Comunicação Social, 2ª Edição, 2017).

6 Manual de Campanha EB20-MC-10.213 Operações de Informação, 1ª Edição, 2014.

7 Segurança Cibernética Social: um requisito emergente de segurança nacional (Beskow, David e Carley, Kathleen, Military Review, 3º trim 2019).

8 Sincronização de sons e falas com vídeos que originalmente tinham outros áudios.

9 Típicos atuadores no ciberespaço, *hackers* são indivíduos capazes de produzir modificações não autorizadas em sistemas computacionais, *bots* são softwares desenvolvidos para atuar como robôs simulando ações humanas, e *trolls* são agentes perturbadores da edição de conteúdos e das discussões nas redes sociais.

10 Automação moderada por controle humano.

11 The Global Desinformation Order, 2019 Global Inventory of Organized Social Media Manipulation, Oxford Internet Institute (Univ of Oxford)

12 Portaria Nº 196-EME, de 1º jul 2019, publicada no Boletim do Exército Nº 28, de 12 jul 2019.

13 Sargento Max Wolf Filho, morto em combate na região de Montese, na Itália, em 12 abr 45.

14 A Guerra pela Opinião Pública (Royal, Benoît, Bibliex, 2019, p. 55).

15 Dicionário Oxford (https://en.oxforddictionaries.com/definition/post-truth).

FATORES DA DECISÃO (*)

Cel Cav QEMA FLÁVIO ROBERTO BEZERRA MORGADO[1]

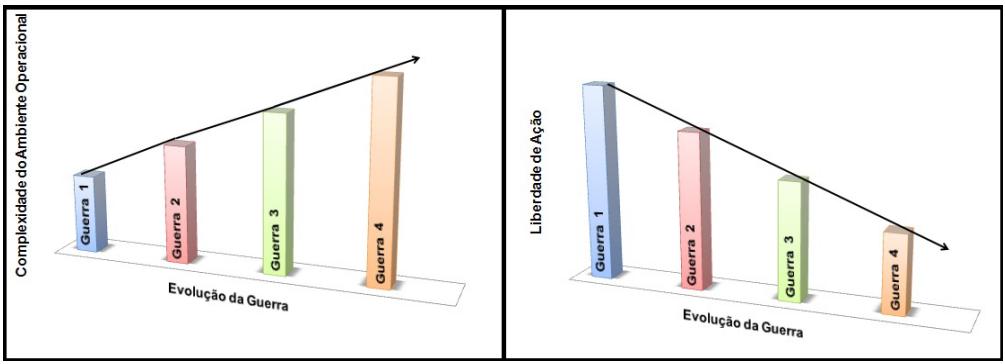
> Tão aceleradas são as mudanças na cena mundial, hoje em dia, que agora as revisões doutrinárias - que costumavam acontecer a cada quarenta ou cinquenta anos - são necessárias de ano em ano ou de dois em dois anos. (Alvin e Heidi Tofler)

O mundo vem passando por sucessivas mudanças em todos os campo do poder, que ocasionam instabilidade no cenário mundial e o aparecimento de conflitos locais e regionais, envolvendo, inclusive, atores não estatais. Houve uma significativa transformação no modo de operar das forças militares, como consequência da evolução e da facilidade de acesso às novas tecnologias, ocasionando a aproximação dos níveis político e tático; a socialização da Internet, disponibilizando, a qualquer cidadão, informações antes reservadas aos Estados; e o aparecimento das redes sociais e a atuação da mídia, provocando a rápida inserção da sociedade no contexto dos conflitos. (Concepção de Transformação do Exército) Alvin e Heidi Tofler, em seu livro Guerra e Antiguerra, analisa a evolução dos conflitos ao longo do tempo, demonstrando o aumento da sua complexidade e consequente diminuição da liberdade de ação dos comandantes durante as operações.

1 O autor é Coronel de Cavalaria e atualmente desempenha a função de Chefe da Divisão de Doutrina da Escola de Comando e Estado-Maior do Exército.

*** Este artigo foi originalmente publicado em 2019 como: MORGADO, Flávio Roberto Bezerra. Fatores da Decisão. Doutrina Militar Terrestre em revista, Julho e Setembro/2019, pág 44 - 47, 2019.**

Figura 1 – Evolução da Guerra



Fonte: Próprio autor

O conflito é um fenômeno social caracterizado pelo choque de vontades, podendo envolver indivíduos, grupos ou nações. Os interesses antagônicos entre diferentes partidos geram situações que podem variar desde uma divergência pacífica até situações de extrema violência, onde se busca a solução dos contenciosos por intermédio da força. Na atualidade, a natureza do conflito, em seus diferentes níveis, tornou-se imprevisível, com atores não estatais competindo, muitas vezes, com estados. (BRASIL, 2014a)

O ambiente operacional moderno apresenta características peculiares, que influenciam de forma marcante a condução das operações militares. Fenômenos atuais como a crescente urbanização, a popularização do acesso aos meios de tecnologia da informação, a ampliação da capacidade de atuação e difusão da mídia, entre outros, conferem um elevado grau de complexidade ao cenário aonde se desenrolam as operações militares. (BRASIL, 2014a)

Tradicionalmente, o foco da análise do ambiente operacional era concentrado na dimensão física, considerando a preponderância dos fatores terreno e condições meteorológicas sobre as operações. As variações no caráter e na natureza do conflito, resultantes das mudanças tecnológicas e sociais, impõem uma visão que também considere as influências das dimensões humana e informacional sobre as operações militares e vice-versa. (BRASIL, 2013a)

Ele é o conjunto de condições e circunstâncias que afetam o espaço onde atuam as forças militares e que interferem na forma como são empregadas, sendo caracterizado pelas dimensões física, humana e informacional. (BRASIL, 2017)

Acrescenta-se de que ele é composto por um somatório de condições, circunstâncias e fatores que afetam o emprego de capacidades e influenciam

as decisões do comandante. A fim de que se possa construir e aprimorar o entendimento do ambiente operacional e do problema militar, é indispensável a disponibilidade de informações completas, detalhadas e oportunas. (BRASIL, 2014b)

Figura 2 – Ambiente Operacional

Fonte: BRASIL, 2017.

O cientista político Samuel P. Huntington, em seu livro O Soldado e o Estado, descreve que a administração da violência é uma das principais características da profissão militar. Esta administração coloca os comandantes militares de frente a diversos problemas, os quais são solucionados após serem analisados através de uma metodologia própria, existente na doutrina militar.

O Exército Brasileiro adota o Processo de Planejamento e Condução das Operações Terrestres como uma metodologia para a solução dos problemas enfrentados durante os conflitos.

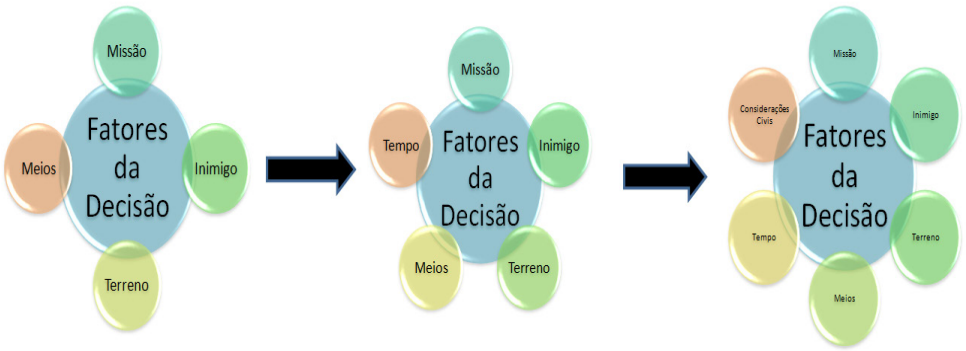
Este processo se constitui no meio segundo o qual os comandantes em todos os níveis desenvolvem o exercício da autoridade visando ao cumprimento de uma missão, além de orientá-los para uma adequada tomada de decisão. (BRASIL,

2014b)

A metodologia concebida para a solução de um problema militar, em qualquer nível, é sustentada pelo estudo de aspectos relevantes que são organizados e orientados por determinados fatores. As partes constitutivas dessa metodologia são os fatores da decisão, isto é, elementos que orientarão o processo decisório. Os principais fatores da decisão são: missão, inimigo, terreno e condições meteorológicas, meios, tempo e considerações civis. (BRASIL, 2017)

Os fatores da decisão descrevem as características de uma área de operações, e são concentrados na análise de como podem afetar o cumprimento da missão. Eles permitem que sejam abordados os aspectos relevantes que alteram o resultado das operações e aprimoram a consciência situacional. (BRASIL, 2014b

Figura 3 – Evolução dos Fatores da Decisão



Fonte: Próprio autor

Os fatores da decisão sofreram atualizações nas últimas décadas dentro da Doutrina Militar Terrestre, como consequência da evolução dos conflitos e do aumento da complexidade do ambiente operacional. Até a década de 90, eles eram constituídos de missão, terreno e condições meteorológicas, inimigo e meios. Na década de 90, o fator tempo passou a ser considerado mais um fator da decisão, assim como o fator considerações civis, a partir da metade da segunda década do século XXI.

O estudo integrado dos fatores da decisão se constitui em uma peça fundamental para que a decisão tomada pelos comandantes em todos os níveis seja a

melhor para o cumprimento da missão num ambiente operacional extremamente complexo como ocorre nos conflitos atualmente.

Ao se analisar o relacionamento dos fatores da decisão com o ambiente operacional, verifica-se que o terreno está diretamente relacionado com a dimensão física e as considerações civis com a dimensão humana, entretanto não se verifica nenhum relacionamento dos fatores da decisão com a dimensão informacional, a qual aumenta, a cada dia, sua importância nos conflitos, de forma exponencial.

O Processo de Integração do Terreno, Inimigo, Condições Meteorológicas e Considerações Civis busca fazer a integração dos fatores da decisão, mas não o realiza na sua plenitude, pois não considera a dimensão informacional, além de não analisar o ambiente operacional como um todo, composto por suas 3 (três) dimensões.

A dimensão informacional abrange os sistemas utilizados para obter, produzir, difundir e atuar sobre a informação. Reveste-se de destacada importância, uma vez que as mudanças sociais estão alicerçadas na elevada capacidade de transmissão, acesso e compartilhamento da informação. (BRASIL, 2017)

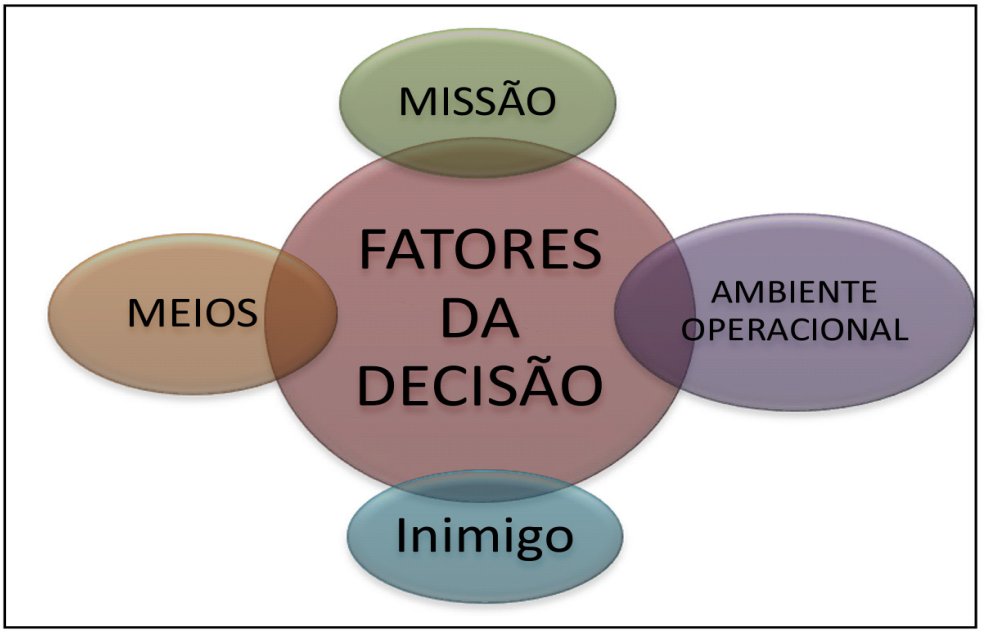
A dimensão física considera a análise do terreno e das condições meteorológicas. A dimensão humana abrange os fatores psicossociais, políticos e econômicos da população local, assim como suas estruturas, seus comportamentos e interesses. Nessa dimensão, o foco é o indivíduo e a sociedade, crescendo de importância a preocupação com a perda de vidas humanas e danos colaterais. (BRASIL, 2017)

Outro ponto a ser destacado é que o estudo do terreno (dimensão física) e das considerações civis (dimensão humana) não está sendo analisado de maneira totalmente integrada, conforme orienta o manual EB70-MC-10.223 Operações, ao caracterizar o ambiente operacional.

Este fato demonstra a necessidade dos fatores da decisão sofrerem uma nova atualização, a fim de serem analisados de uma forma mais integrada, proporcionando melhores condições para que a decisão a ser tomada seja a melhor possível.

Seguindo nesta direção, sugere-se que os fatores da decisão passem a ser constituídos da missão, do ambiente operacional, do inimigo e dos meios. Nesta proposta, o ambiente operacional como fator da decisão permite uma análise mais holística daquilo que circunda a dimensão física e imaterial do campo de batalha, ou seja, empute o estudo integrado do terreno, tempo, condições meteorológicas, considerações civis e a dimensão informacional, além de outros aspectos que se

levantem em casos específicos.



Fonte: Próprio autor

Nos últimos anos o Exército Brasileiro está transformando a Doutrina Militar Terrestre com o objetivo de fornecer as ferramentas necessárias para enfrentar os desafios existentes em um ambiente operacional complexo.

A Doutrina Militar Terrestre baseia-se na permanente atualização, em função da evolução da natureza dos conflitos, resultado das mudanças da sociedade e da evolução tecnológica aplicadas aos assuntos de defesa. As mudanças experimentadas pelas sociedades, com reflexos na forma de fazer política, e o surgimento de nova configuração geopolítica conduzem a horizontes mais incertos e complexos para planejar a Defesa da Pátria, razão de ser das Forças Armadas. Essas mudanças vêm alterando gradativamente as relações de poder, provocando instabilidades e incertezas e suscitando o aparecimento de conflitos locais e regionais com a inserção de novos atores – estatais e não estatais – no contexto dos conflitos. (BRASIL, 2013a)

Este artigo tem como objetivo propor uma discussão sobre a necessidade de atualização dos fatores da decisão, a fim de se melhorar as ferramentas disponíveis para os decisores durante os conflitos na atualidade e contribuir com o aperfeiçoamento da Doutrina Militar Terrestre.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Exército. Estado-Maior do Exército. **EB20-MC-10.301 A Força Terrestre Componente nas Operações**. 1. ed. Brasília, DF, 2014a.

_____. Exército. Estado-Maior do Exército. **Bases para a Transformação da Doutrina Militar Terrestre**. 1. ed. Brasília, DF, 2013a.

_____. Exército. Gabinete do Comandante do Exército. **Concepção de Transformação do Exército**. 1. ed. Brasília, DF, 2013b.

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

_____. Exército. Estado-Maior do Exército. **EB20-MC-10.211 Processo de Planejamento e Condução das Operações Terrestres**. 1. ed. Brasília, DF, 2014b.

HUNTINGTON, Samuel P. **O Soldado e o Estado**. 2.ed. Rio de Janeiro. BIBLIEX, 2016.

TOFFLER, Alvin e Heidi**. Guerra e Anti-Guerra**. 1. ed. Rio de Janeiro. Editora Record, 1993.

O LEVANTAMENTO ESTRATÉGICO DE ÁREA PARA O PLANEJAMENTO DE OPERAÇÕES CIBERNÉTICAS

Ten Cel Com QEMA RONALDO ANDRÉ FURTADO*

1 INTRODUÇÃO

A Guerra Cibernética (G Ciber) é uma nova área do conhecimento militar para onde os conflitos já migraram e onde os seus cenários de emprego são possivelmente os mais prováveis que as Hipóteses de Conflito convencionais. Atualmente, com amplo emprego nas Operações de Informação (Op Info)[1], sendo que a G Ciber também é uma nova Capacidade Relacionada a Informação (CRI)(CARNEIRO, 2012).

Agravando a atual situação, a velocidade no desenvolvimento de novas tecnologias da informação (TI), os procedimentos que podem ser utilizados para esse fim e a possibilidade de ataques serem perpetrados não somente por Estados, mas também por organizações ou, até mesmo, por indivíduos isolados, com as mais diversas motivações e capacidade de agir, aparentemente só tendem a crescer.

Assim, é necessário desenvolver, de forma organizada, coordenada e integrada a capacidade de dissuasão, onde identificar, rastrear e responder a ataques são capacidades fundamentais para preservar a segurança de um Estado, seus serviços essenciais, suas infraestruturas criticas e seus cidadãos. Deixar de desenvolver capacidades nessa área poderá acarretar sérios prejuízos ou danos a Estrutura Militar de Defesa e ao futuro do País (CARNEIRO,2012).

A consolidação de uma metodologia para sistematização da construção LEA[2] que contemple parâmetros da G Ciber, ainda não ocorreu. O presente

1 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 Psicológicas (Op Psico); a Guerra Eletrônica (GE); a Guerra Cibernética (G Ciber);e a Inteligência (Intlg) (EXÉRCITO BRASILEIRO, 2014).

2 **Levantamento Estratégico de Área (LEA)** é a compilação organizada e metódica de conhecimentos determinantes ou condicionantes do Poder Nacional de um determinado país ou do potencial de uma área estratégica ou de atividades humanas. (MINISTÉRIO DA DEFESA, 2011)

artigo propõe fatores que possam ser incluídos na confecção do LEA para poder mitigar essa problemática.

2 CAMPOS DO PODER

Os Objetivos Nacionais são aqueles que a Nação busca satisfazer, em decorrência da identificação de necessidades, interesses e de suas aspirações, em determinada fase de sua evolução histórico-cultural. Sendo assim, o Poder nacional é a capacidade que tem o conjunto de homens e meios que constituem a Nação pra alcançar e manter os Objetivos Nacionais, em conformidade com a Vontade Nacional. Além disso, o Poder Nacional deve ser sempre entendido como um todo, uno e indivisível, sendo os seus fundamentos o Homem, a Terra e as Instituições. Entretanto, para melhor compreender os elementos estruturais podemos estudá-lo segundo suas manifestações, que se processam por intermédio de cinco expressões ou campos do poder, a saber: Política; Econômica; Psicossocial; Militar; Científica e Tecnológica. (ESG, 2019)

No manual de Fundamentos do Poder Nacional (ESG, 2019), em nenhum momento é citado algum item relativo a Cibernética. Conclui-se parcialmente, que os fatores que compõem as expressões do poder são as bases para confecção do LEA. Sendo assim, cabe destacar da importância do estudo da Cibernética que é um tema transversal, perpassando todos os Campos do Poder.

3 LEVANTAMENTO ESTRATÉGICO DE ÁREA

O LEA tem por finalidade levantar todos os dados estratégicos e elementos que determinam ou condicionam o poder e o potencial estratégico de uma determinada área. Consiste, essencialmente, na coleta de dados e informações que facultam o conhecimento da área em seus aspectos positivos e negativos. Trata-se de um trabalho metódico e continuado, realizado desde o tempo de paz. Dessa forma, há necessidade de uma constante atualização das informações obtidas (EXÉRCITO BRASILEIRO, 2001).

Fazendo o levantamento estratégico de uma área operacional, não se deve esquecer da motivação básica da predominância de ações da expressão militar. Entretanto, atualmente existem cinco divisões dos campos do poder, ou seja, econômico, militar, político, psicossocial e científico-tecnológico que não contemplam o advento da G Ciber, que é uma das mais recentes formas de atuação em um conflito no amplo espectro.

A Guerra do futuro se apresenta, intrinsecamente, por ser não convencional e assimétrica, onde recursos limitados aliados a um profundo conhecimento

técnico de poucas pessoas podem gerar um efeito extremamente eficaz em um alvo (CARNEIRO, 2012). Logo, abre-se espaço para concluir parcialmente que se pode propor um novo modelo de auxílio de dados que facilite a padronização de procedimentos por parte dos analistas que produzem o LEA, contemplando o levantamento de fatores que abarquem dados relevantes para a atuação no Setor Cibernético.

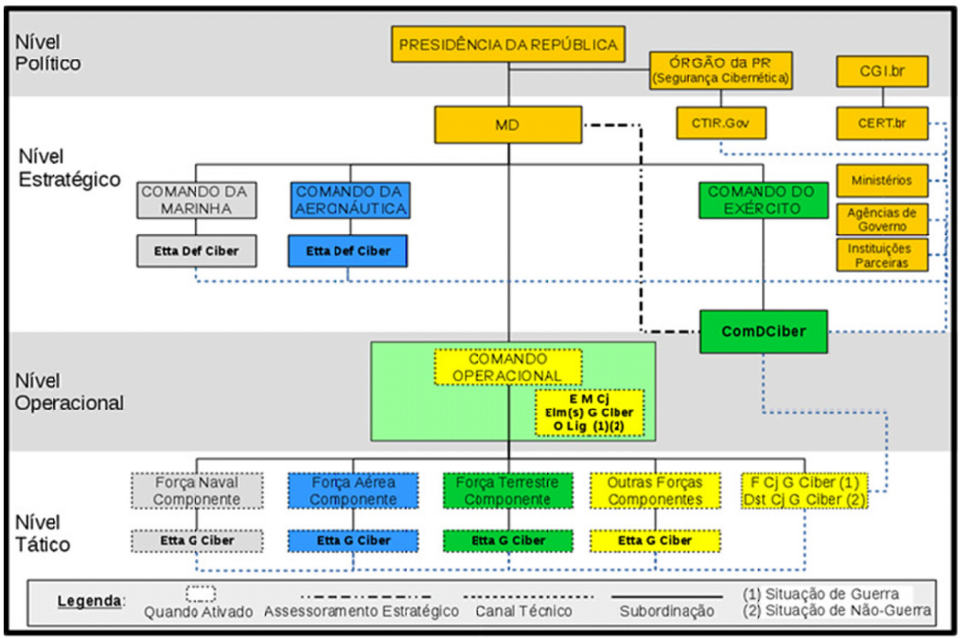
Observa-se que a escassa literatura que trata sobre LEA é pragmática, os relatos são baseados no cotidiano dentro das Instituições que trabalham com cibernética, sem interface entre elas na elaboração de modelos mais abrangentes que apoiem a continuidade de seu estudo, principalmente, no que tange, a integração da G Ciber aos demais Campos do Poder. A equipe de analistas que produz o LEA tem uma rotina particular quanto às medidas de sua confecção, ou seja, o que um analista faz, o outro não replica, ou mesmo verifica se é compatível ou viável com seu caso particular.

Apesar da relevância do tema, por ser algo novo nos Estudos de Defesa, não há nas Forças Armadas, uma agenda de pesquisa que avance nos estudos sobre o tema de cibernética englobando a confecção do LEA. Não existem ferramentas analíticas e outros tipos de insumos para que facilite as autoridades decisoras na condução de Operações envolvendo a Guerra Cibernética. Por isso, o modelo de LEA parece ser uma forma consistente, apesar de original, de introduzir essa temática.

4 ESTRUTURA DE DEFESA CIBERNÉTICA

No nível tático, quando for ativada a Estrutura Militar de Defesa (Etta Mi D), a Força Terrestre Componente (FTC) será apoiada por uma Etta de G Ciber. Essa estrutura engloba os elementos do 1o Batalhão de Guerra Eletrônica (BGE), o Batalhão de Comunicações (B Com), o Batalhão de Comunicações e Guerra Eletrônica (B Com GE), o Batalhão de Inteligência Militar (BIM), a Companhia de Comando e Controle (Cia C2) e as Companhias de Comunicações (Cia Com). Em um momento determinado, de acordo com a missão da FTC, o comando poderá variar a Etta de G Ciber (EXÉRCITO BRASILEIRO, 2017).

No nível Estratégico e Operacional temos a estrutura do Comando de Defesa Cibernética (ComDCiber) que é o órgão central do Sistema Militar de Defesa Cibernética (SMDC). O ComDCiber tem como missão coordenar e integrar os componentes das Forças Singulares visando viabilizar o exercício do Comando e Controle (C2), por meio da proteção dos ativos da informação, além de negar o exercício do C2 ao oponente (EXÉRCITO BRASILEIRO, 2017).



Fonte: EXÉRCITO BRASILEIRO, 2017.

4 CAPACIDADES E TAREFAS DA GUERRA CIBERNÉTICA

A Capacidade é a aptidão requerida a uma força ou organização militar, para que possa cumprir determinada missão ou tarefa. É obtida a partir do desenvolvimento de um conjunto de sete fatores determinantes, inter-relacionados e indissociáveis: doutrina, organização (e processos), adestramento, material (e sistemas), educação, pessoal e infraestrutura com acrônimo (DOAMEPI). (EXÉRCITO, 2014)

As capacidades operativas (CO) da capacidade militar terrestre cibernética são três: a proteção cibernética, o ataque cibernético e a exploração cibernética. Elas realizam ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para superar os Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC3) do oponente e defender os próprios (EXÉRCITO, 2015).

As CO da G Ciber são utilizadas durante a fase de planejamento das Operações Militares, por meio delas os comandantes e seus estados-maiores identificam todas as atividades a cumprir no espaço cibernético. Em seguida, selecionam as tarefas mais adequadas a serem conduzidas e iniciam o detalhamento de como conduzir as ações cibernéticas necessárias ao

cumprimento da missão. Embora, caiba destacar que as Operações conduzidas na dimensão informacional já se valem do LEA produzido pelo Escalão Enquadrante, o presente artigo propõe preencher a lacuna da falta de fatores que possibilitem maximizar o planejamento do emprego dos especialistas em G Ciber.

5 RESULTADO E ANÁLISE

Quanto aos fins, o tipo de investigação escolhido para a realização da pesquisa qualitativa enquadra-se como exploratória. Já no que diz respeito aos meios de investigação, optou-se pela pesquisa de campo, por haver escassez de literatura sobre o tema. A seleção dos sujeitos das entrevistas aconteceu a partir da identificação de especialistas integrantes do Setor Cibernético Brasileiro com no mínimo de 01 (um) ano de experiência nas atividades de exploração, ataque e proteção cibernética. Durante o trabalho de pesquisa, a principal fonte da coleta dados para a análise deste estudo foi um questionário realizado com os integrantes do Setor Cibernético, no qual ouviu-se 30 (trinta) oficiais de diversos postos das três Forças Armadas, além de integrantes de outros órgãos do Governo Federal como Agência Brasileira de Inteligência (ABIN) e Controladoria Geral da União (CGU).

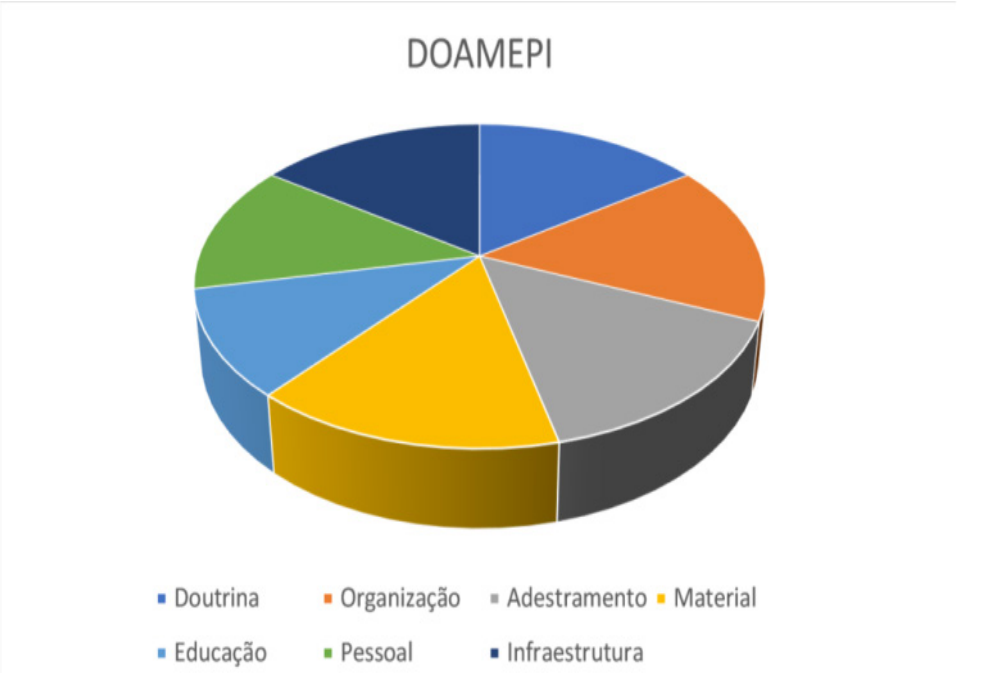
Os participantes foram questionados quanto à percepção das capacidades do inimigo, por meio de um DOAMEPI reverso, ou seja, um DOAMEPI com um intuito de levantar as capacidades que devem ser observadas no oponente com o intuito de serem levantadas no nosso LEA voltado para Operações Cibernéticas.

O questionário foi dividido em 02 (duas) etapas, sendo em uma primeira parte realizada com perguntas abertas focadas em ataque e exploração cibernética, dando a possibilidade do entrevistado escolher o caminho e as dimensões que desejava trilhar. Na segunda parte do questionário que foi focada na parte de proteção cibernética e utilizou-se a perguntas objetivas modeladas na escala Likert[3].

Na primeira parte realizada com perguntas abertas os especialistas indicaram um total de 255 (duzentas e cinquenta e cinco) ideias grupadas nas 07 (sete) áreas do DOAMEPI e distribuídas, quantitativamente, conforme o Gráfico 1. Observa-se abaixo no Gráfico 1: Resultado do Ataque e Exploração Cibernética, uma proporcionalidade das respostas dentro dos 07 (sete) fatores que compõem o DOAMEPI por parte dos sujeitos pesquisados.

3 A **escala Likert** ou **escala de Likert** é um tipo de escala de resposta psicométrica usada em questionários, e é a escala mais usada em pesquisas de opinião. Ao responderem a um questionário baseado nesta escala, os perguntados especificam seu nível de concordância com uma afirmação. O formato típico de um item Likert é: Discordo totalmente, Discordo parcialmente, Indiferente, Concordo parcialmente e Concordo totalmente.

Gráfico 1: Resultado do Ataque e Exploração Cibernética



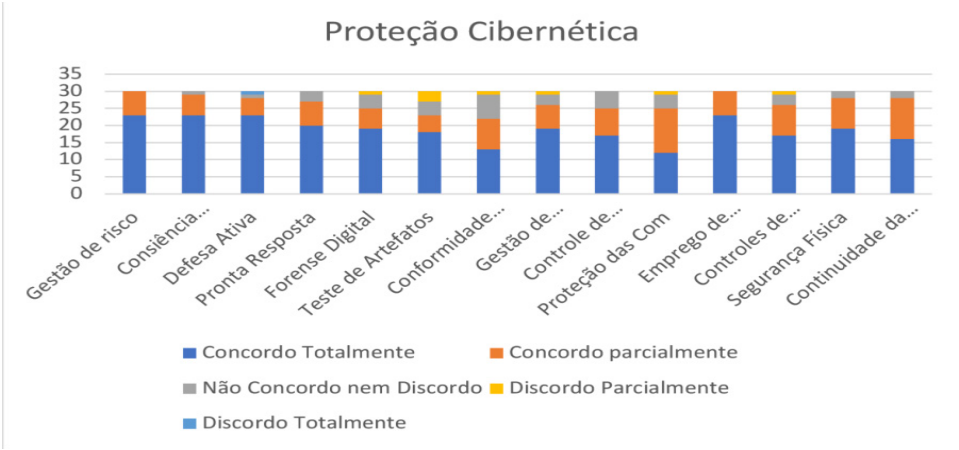
Fonte: Próprio autor, 2019.

Após o trabalho de interpretação e análise das respostas nos critérios de coerência, originalidade e adequabilidade com os assuntos propostos foram modelados 70 (setenta) fatores, conforme consta no Capítulo 6 deste artigo: LEA para Planejamento de Operações Cibernéticas, para complementarem os LEA já produzidos e voltados, exclusivamente, para a Guerra Cibernética.

Na segunda parte do questionário observa-se no Gráfico 2: Resultado da escala Likert que não houve nenhum fator que destacou-se, abruptamente, dos demais na distribuição dos resultados na consolidação das respostas sobre proteção cibernética.

Os 14 (quatorze) itens mensurados no questionário: Gestão de Risco, Consciência Situacional, Defesa ativa, Pronta Resposta, Forense Digital, Teste de Artefatos, Conformidade de SIC, Gestão de Incidentes de Rede, Controle de Acesso, Proteção das Comunicações, Emprego de Criptografia, Implementação de Controle de Segurança, Segurança Física e Gestão de Continuidade da Missão contam no manual Guerra Cibernética (EXÉRCITO BRASILEIRO, 2017).

Gráfico 2: Resultado da escala Likert

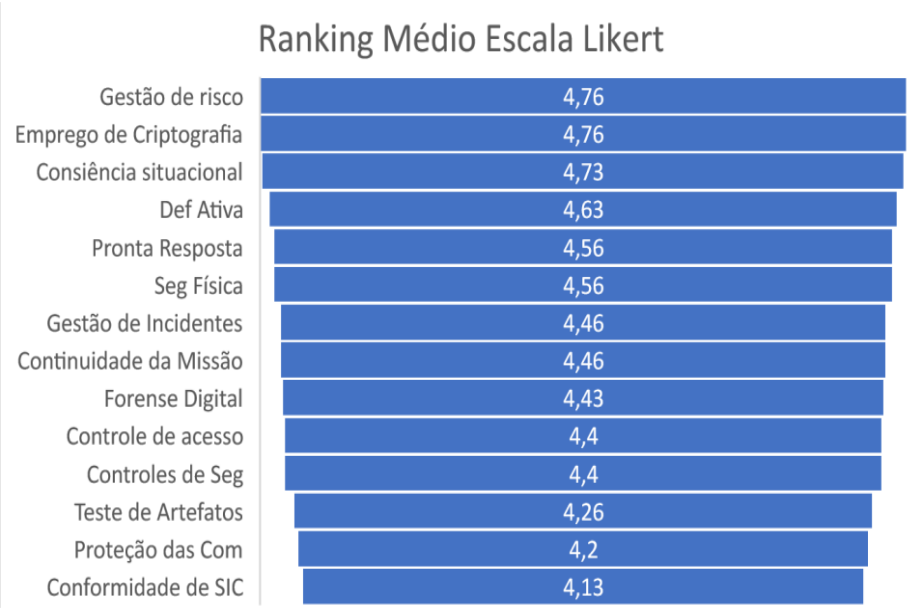


Fonte: Próprio autor, 2019.

Para uma melhor análise dos resultados, na segunda parte, utilizou-se perguntas objetivas para realizar uma abordagem quantitativa de forma a estabelecer um Ranking Médio (RM). O questionário utilizou a escala Likert de que é composta de 5 (cinco) pontos para mensurar o grau de concordância dos sujeitos que responderam ao questionário.

Realizou-se a verificação quanto à concordância ou discordância das questões avaliadas, através da obtenção do RM da pontuação atribuída às respostas, relacionando a frequência das respostas dos respondentes que fizeram tal atribuição, onde os valores menores que 3 são considerados como discordantes e, maiores que 3, como concordantes, considerando uma escala de 5 pontos. O valor exatamente 3 seria considerado "indiferente" ou "sem opinião", sendo o "ponto neutro", equivalente aos casos em que os respondentes deixaram em branco. Para o cálculo do RM utilizou-se o método de análise de escala do tipo Likert apresentado por Malhotra (2001) e utilizado por Tresca e de Rose Jr (2004) e por Cassiano (2005). Os valores consolidados constam do Gráfico 3: Proteção Cibernética.

Gráfico 3: Proteção Cibernética



Fonte: Próprio autor, 2019.

Analisando o Gráfico 3: Proteção Cibernética observa-se que não houve uma grande variação do ranking médio da escala Likert, assim chega-se a conclusão que os especialistas que responderam o questionário pensam que não deva haver uma grande priorização dos meios de proteção cibernética, pois todos itens se complementam e são importantes. Observa-se também, que devido a pró-atividade, os itens pós-ataque cibernético acabam tendo um peso menor na avaliação dos especialistas em relação aos que protegem ao ataque.

Analisando o descrito no Capítulo 6: LEA para Planejamento de Operações Cibernéticas e o Gráfico 3: Proteção Cibernética, deve ser dada atenção na confecção do LEA para a proteção cibernética das Infraestruturas Críticas[4], quando da produção do conhecimento de inteligência. A Portaria nº 2 do Gabinete de Segurança Institucional de 2008 estabeleceu 05 (cinco) áreas como prioritárias: Energia, Transporte, Telecomunicações, Água e Finanças.

4 **Infraestruturas críticas são** as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional.

6 LEA PARA PLANEJAMENTO DE OPERAÇÕES CIBERNÉTICAS

6.1 CAMPOS DO PODER

a) Político

1. Há cumprimento das normas de DICA/DIH e regulamentos internacionais?
2. Organização das agências e organizações civis que podem vir a atuar em proveito do Ini no ambiente assimétrico?
3. Enquadramento dos Órgãos de Segurança de Redes (CERT, CIRT etc)?
4. Exercícios de adestramento envolvendo Defesa, Governo, setor privado (IEC) e academia e qual a participação em exercícios combinados e com quais países?
5. Parcerias internacionais cibernéticas celebradas (especialmente EUA, Rússia, China, Israel e Irã)?
6. Controle das atividades cibernéticas do pessoal especializado fora do ambiente militar?

b) Econômico

1. Relação das empresas privadas que desenvolvem artefatos cibernéticos?
2. Empresas que fornecem serviços e infraestrutura de TI?
3. Quem provê os recursos de rede/ internet e quais as características desses serviços?
4. Vulnerabilidades Cibernéticas nas Infraestruturas Críticas nas áreas de: Água, Energia, Finanças, Telecomunicações e Transporte?

c) Psicossocial

1. Utilização da tabela MITRE ATTACK?
2. Principais lideranças no ambiente informacional em redes sociais e suas características (organização, meios empregados etc)?
3. Cursos de segurança cibernéticas existentes?
4. Programas de capacitação existentes no âmbito da Defesa, junto à academia e de intercâmbio com outros países?
5. Relação entre o material existente e a capacidade o nível de conhecimento dos programas de capacitação para operação dos meios?
6. Quantidade de vagas x elementos capacitados em cibernética por ano?
7. Certificações nacionais e internacionais na área de cibernética?
8. Qual a integração do Setor Cibernético com a acadêmica?
9. Institutos de Capacitação e Pesquisa no Setor Cibernético?
10. Recrutamento de talentos no setor cibernético?

11. Cursos realizados pelos militares e civis (Ciber e C2)?
12. Nível da cultura de segurança cibernética da sociedade?
13. Nível de motivação do pessoal do Setor Cibernético?
14. Valorização profissional dos especialistas em Cibernética?
15. Plano de carreira voltado para especialistas em Cibernética?
16. Dados dos indivíduos vinculados aos ativos de TI alvo, incluindo, informações sobre familiares?
17. Antologias utilizadas pelos indivíduos na área de operações?
18. Autoridades que são suscetíveis a engenharia social?
19. Liderança das Forças Cibernéticas?
20. Senhas e usuários padrões dos sistemas corporativos?

d) Militar

1. Missões, ações, atividades e tarefas previstas na doutrina?
2. Nível de atualização doutrinária e influência advinda de outros países.?
3. Doutrina para atuação coordenada e integrada envolvendo outros Países, Agências, Governo, Setor Privado e Academia?
4. Documentos e informações, ordem de operações e manuais de cibernética? Hipóteses de emprego/ cenário para emprego de ações cibernéticas?
5. *Modus operandi* das ações cibernéticas realizadas anteriormente?
6. Técnicas, táticas e procedimentos (TTP) das ações cibernéticas?
7. Manuais sobre planejamento de operações Cibernética?
8. Estrutura organizacional de Forças Cibernéticas em tempo de paz e após o acionamento da Etta Mil Def?
9. Desdobramento dos meios militares e a ligação com meios civis que podem ser mobilizados?
10. Fluxo da informação, relações de comando e o C2?
11. Efetivo envolvido, regime de trabalho e escala de serviço para a proteção de ativos de TI?
12. Tipos de simuladores e atividades de simulação Cibernética construtiva, virtual e viva realizadas para adestrar e quais indicadores das simulações?
13. Nível de adestramento das frações cibernéticas nas ações de proteção, exploração e ataque cibernético?
14. Operações Singulares e Conjuntas cibernéticas realizadas?
15. Capacidade de mobilização e de integração de material civil para emprego Mil?
16. Recrutamento e mobilização de pessoal especializado na área de cibernética?
17. Nível de preenchimento de cargos de especialistas de cibernética dentro

da estrutura organizacional das Força Armadas?
18. Dotação das Forças Cibernéticas?
19. Perfil dos militares e civis que trabalham no Setor Cibernético?
20. As instalações que possuem ativos de TI possuem controle de acesso
21. Vulnerabilidades existentes nas instalações?
22. Localização dos Centros de Operações Cibernéticas?

e) Científico e Tecnológico

1. Grau de conhecimento técnico dos profissionais responsáveis pela proteção de ativos de TI?
2. Hardware e software voltados para ações ofensivas, fabricantes e versões?
3. Características dos ativos alvo (sistema operacional, versões, fabricante, licenças, localização física, topologia de rede)?
4. Nível de atualização tecnológica do material e a capacidade de interferir sobre sistemas de Forças aliadas?
5. Desenvolvimento de criptografia própria ou de qual país adquiri usualmente?
6. Marca e tipo dos principais ativos de redes (Roteadores, Switches, VOIp e etc)?
7. Sistemas Operacionais utilizados (local, marca, versão etc)?
8. Ferramentas de Segurança utilizadas (local, marca, versão etc)?
9. Equipamentos móveis utilizados (local, marca, versão, frequência)?
10. Servidores corporativos (Email, Banco de Dados, Pagamento, Gestão, etc) e versões, vulnerabilidades conhecidas, IP, etc)?
11. Equipamentos de comutação de rede?
12. Capacidade de desenvolver artefatos cibernéticos?
13. Localizações dos *backbones*, cabos de fibra ótica e cabos submarinos?
14. Infraestrutura de redes celular 3G/4G/5G e de provedores internet banda larga?
15. Sistemas de TI não segregados acessíveis pela internet?
16. Satélites de dados utilizados?
17. Relação de IP dos principais sistemas e ativos de redes?

6 CONCLUSÃO

A importância de se ter um LEA com itens voltados para as Operações Cibernéticas como uma ferramenta de análise em Estudos de Defesa é que ela é uma opção eficaz aos tradicionais métodos de análise de dados que usam os critérios de avaliação empíricos. Atualmente, são muito ligados à experiência

pessoal da autoridade, função, tempo no cargo e treinamento do especialista que executa a avaliação, sendo pouco ligado ao rigor científico ou a outros métodos qualitativos de avaliação.

O estudo do LEA abarcando os campos do poder já é realizado por muito tempo, contudo, devido a Cibernética ser uma nova área do conhecimento, ainda não constam itens que subsidiem o planejamento de Operações que envolvam a Guerra Cibernética. O resultado final do artigo foi elencar 70 (setenta) itens para compor o LEA em Operações Militares, estes itens abarcaram os 05 (cinco) Campos do Poder. Apesar da escassez do tempo para a confecção do artigo e a limitação do universo pesquisado foi possível extrair ideias úteis dos especialistas para guiar os futuros analistas no planejamento de Operações Militares envolvendo a área cibernética.

Por fim, cabe destacar que como a cibernética é uma área estratégica não encontramos na literatura nenhuma menção doutrinária de outros países de como fazer um LEA. Assim, este foi o primeiro passo para que se possa ser aprofundado em trabalhos futuros, principalmente no que tange a como classificar estes itens corretamente dentro dos Campos do Poder.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Gabinete de Segurança Institucional. **Portaria nº 02/2008, de 02 de fevereiro de 2008.** Institui Grupos Técnicos de Segurança de Infra-estruturas Críticas (GTSIC), Brasília-DF, 2008.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas**. MD-30-M-01, Brasília-DF, V.3, 2011.

CARNEIRO, João Marinonio Enke. A Guerra Cibernética: **uma proposta de elementos para formulação doutrinária no Exército Brasileiro**. 2012. Tese (Doutorado) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

CASSIANO, Reinaldo Mesquita. **Estratégias competitivas das empresas produtoras de sementes de soja:** um estudo exploratório no Sul de Mato Grosso. 2005. Mestrado em Administração e Desenvolvimento Organizacional-CNEC/FACECA. Faculdade Cenecista de Varginha. Minas Gerais, 2005.

ESCOLA SUPERIOR DE GUERRA. **Fundamentos do Poder Nacional**. Rio de Janeiro-RJ. 2019.

EXÉRCITO BRASILEIRO. **Estratégia**. C 124-1, EME. Brasília-DF, 3. ed. 2001.

EXÉRCITO BRASILEIRO. **Guerra Cibernética**. EB70-MC-10-232, Comando de Operações Terrestres. Brasília-DF, 2017.

EXÉRCITO BRASILEIRO. Manual de Fundamentos: **Doutrina Militar Terrestre**. EB20-MF-10-102, Comando de Operações Terrestres. Brasília-DF, 2014.

EXÉRCITO BRASILEIRO. **Operações de Informação**. EB70-MC-10-213, Comando de Operações Terrestres. Brasília-DF, 2014.

MALHOTRA, Naresh. **Pesquisa de Marketing: uma orientação aplicada**. Porto Alegre: Bookman, 2001.

TRESCA, Rosemary Pezzetti; DE ROSE JR, Dante. **Estudo comparativo da motivação intrínseca em escolares praticantes e não praticantes de dança**. Disponível em: http://www.ucb.br/mestradoef/rbcm/downloads/a1v8n1.pdf. Acesso em: 09 ago 2019.

EXÉRCITO BRASILEIRO. **Catálogo de Capacidades do Exército**. EB20-C-07-001, Estado-Maior do Exército. Brasília-DF, 2015.

*Artigo realizado a partir do trabalho de conclusão do Curso de Especialização em Planejamento de Guerra Eletrônica e Guerra Cibernética em apoio às Operações do Centro de Instrução de Guerra Eletrônica (CIGE), em 2019. Realizado pelo Ten Cel QEMA Ronaldo André Furtado, Oficial de Comunicações do Exército Brasileiro. Atualmente, é instrutor de C2, GE, Cibernética e Inteligência na Divisão de Doutrina da Escola de Comando e Estado-Maior do Exército.

AS OPERAÇÕES DE INFORMAÇÃO NA OPERAÇÃO DE GARANTIA DA LEI E DA ORDEM POTIGUAR 2

Maj Inf QEMA CARLOS AUGUSTO DA SILVA NÉTO[1]

1 INTRODUÇÃO

No ambiente operacional contemporâneo, as operações militares têm ocorrido cada vez mais em áreas humanizadas, onde a presença da população e o caráter difuso das ameaças dificultam a identificação dos oponentes e favorecem a ocorrência de danos colaterais. Além disso, a presença de novos atores, estatais e não estatais, com poder de influenciar opiniões e de defender interesses diversos torna o ambiente operacional ainda mais complexo.

Doutrinariamente, o ambiente operacional é caracterizado pela existência de três dimensões: a física, a humana e a informacional. A dimensão física considera a preponderância dos fatores terreno e condições meteorológicas sobre as operações. A dimensão humana compreende os elementos relacionados às estruturas sociais, os comportamentos e interesses, normalmente geradores do conflito. A dimensão informacional abrange os sistemas utilizados para obter, produzir, difundir e atuar sobre a informação.

Em uma sociedade cada vez mais dependente da informação, a dimensão informacional do ambiente operacional é de fundamental importância para o planejamento e a condução das operações militares, sendo a percepção estabelecida como válida nas mentes de um ou mais públicos-alvo (narrativa dominante) considerada um acidente capital.

1 O autor foi declarado Aspirante a Oficial de Infantaria pela Academia Militar das Agulhas Negras (AMAN), em 2001. Realizou cursos de Inteligência no Exército Brasileiro e no Exército do Chile e o curso de Manobra para Capitães de Carreira no Exército dos EUA. Foi instrutor do Curso de Infantaria da Escola de Aperfeiçoamento de Oficiais (EsAO) e Assessor Militar do Curso de Aperfeiçoamento de Oficiais do Exército do Suriname. Comandou a Companhia de Comando da 7ª Brigada de Infantaria Motorizada durante a Operação Potiguar 2. Atualmente é instrutor da Escola de Comando e Estado-Maior do Exército (ECEME).

No contexto da dimensão informacional do ambiente operacional, as Operações de Informação (Op Info) consistem na atuação integrada de capacidades relacionadas à informação (CRI), 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 adversárias na dimensão informacional.

Com o incremento do emprego do Exército Brasileiro (EB) em Operações de Garantia da Lei e da Ordem (Op GLO) nos últimos anos e em face da influência da informação no ambiente operacional contemporâneo, torna-se necessário o estudo da aplicação prática das Op Info nas Op GLO.

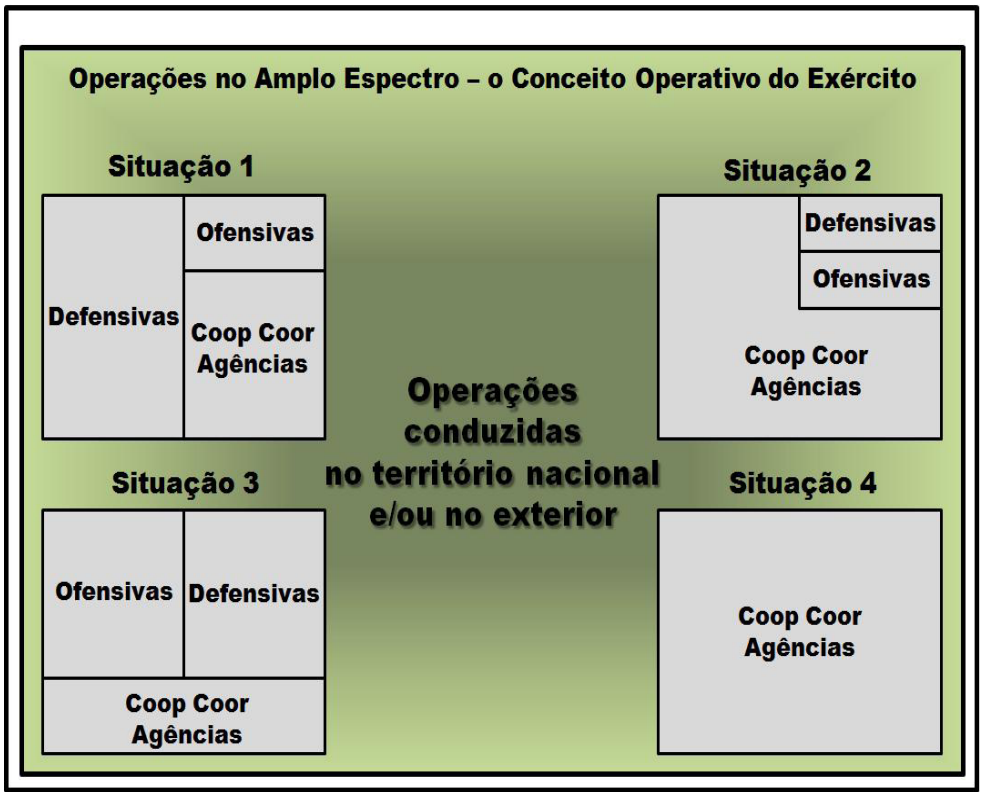
Nos anos de 2016, 2017 e 2018, ocorreram, respectivamente, as Op GLO Potiguar 1, 2 e 3, em virtude da crise no Sistema de Segurança Pública no estado do Rio Grande do Norte (RN). Essas operações tiveram o comando confiado ao comandante (Cmt) da 7ª Brigada de Infantaria Motorizada (7ª Bda Inf Mtz), Grande Unidade do EB, localizada em Natal/RN, e contaram com a participação do EB, da Marinha do Brasil, da Força Aérea Brasileira e de Órgãos de Segurança Pública (OSP).

No contexto das Op Info durante as Op GLO, esse artigo pretende apresentar, sucintamente, como as CRI contribuíram para o cumprimento da missão atribuída à Força Terrestre (F Ter) na Op Potiguar 2.

2 AS OPERAÇÕES DE GARANTIA DA LEI E DA ORDEM

O EB adota o conceito operativo de Operações no Amplo Espectro, que interpreta a atuação dos elementos da F Ter para obter e manter resultados decisivos nas operações, mediante a combinação das operações básicas (operações ofensivas, defensivas e de cooperação e coordenação com agências), simultânea ou sucessivamente, prevenindo ameaças, gerenciando crises e solucionando conflitos armados, em situações de Guerra e de Não Guerra.

Figura 1 – Operações no Amplo Espectro



Fonte: BRASIL, 2019

As Operações de Cooperação e Coordenação com Agências (OCCA) compreendem o apoio prestado por elementos da F Ter, por meio da interação com outras agências, definido em diploma legal, com a finalidade de conciliar interesses e coordenar esforços para a consecução de objetivos ou propósitos convergentes com eficiência, eficácia, efetividade e menores custos e que atendam ao bem comum, evitando a duplicidade de ações, dispersão de recursos e a divergência de soluções.

As Op GLO enquadram-se como uma das OCCA, já que que se destinam a proteger a sociedade, dentro de um contexto de Proteção Integrada.

O Ministério da Defesa (MD) do Brasil define a Op GLO nos seguintes termos:

> A Operação de Garantia da Lei e da Ordem (Op GLO) é uma operação militar determinada pelo Presidente da República e conduzida pelas Forças Armadas de forma episódica, em área previamente estabelecida e por tempo limitado, que tem por objetivo a preservação da ordem

> pública e da incolumidade das pessoas e do patrimônio em situações de esgotamento dos instrumentos para isso previstos no art. 144 da Constituição ou em outras em que se presuma ser possível a perturbação da ordem. (BRASIL, 2014)

As ações e medidas desenvolvidas nas Op GLO podem ser de caráter preventivo ou repressivo. As ações preventivas abrangerão o preparo da tropa em caráter permanente e as atividades de inteligência, de comunicação social e dissuasão. Também se enquadram nesta classificação as ações adotadas frente a uma possível ameaça detectada pela inteligência. As ações repressivas serão desenvolvidas para fazer frente a uma ameaça concretizada, com o intuito de preservar ou restabelecer a ordem pública e a incolumidade das pessoas e do patrimônio.

Dependendo da característica do emprego autorizado na GLO, as seguintes ações podem ser executadas: controlar vias de circulação; desocupar ou proteger as instalações de infraestrutura crítica, garantindo o seu funcionamento; garantir a segurança de autoridades e de comboios; garantir o direito de ir e vir da população; impedir o bloqueio de vias vitais para a circulação de pessoas e cargas; realizar a busca e apreensão de armas, explosivos etc; realizar policiamento ostensivo, estabelecendo patrulhamento a pé e motorizado, dentre outras.

3 AS OPERAÇÕES DE INFORMAÇÃO

Na Doutrina Militar Terrestre (DMT), as Operações Complementares são aquelas que se destinam a ampliar, aperfeiçoar e/ou complementar as operações básicas no amplo espectro, a fim de maximizar a aplicação dos elementos do poder de combate terrestre e, por suas peculiaridades, obter melhores resultados, abrangendo, dentre elas, as Op Info. Dessa forma, as Op Info complementam e contribuem com as Operações de GLO.

Atualmente, as informações disponíveis, aliadas à capacidade de geri-las, determinam a amplitude e a exatidão da consciência situacional, assegurando a decisão adequada e oportuna em qualquer situação de emprego, permitindo que os comandantes possam se antecipar aos oponentes e decidir pelo emprego de meios na medida certa, no momento e local decisivos, proporcionalmente à ameaça.

Em um ambiente operacional em contínua transformação, onde a tecnologia infunde, na área da informação, junto à sociedade, mudanças cada vez mais rápidas, as Op Info passam a ser uma aptidão essencial como instrumento integrador das CRI.

As CRI são aptidões requeridas para afetar a capacidade de oponentes ou

potenciais adversários de orientar, obter, produzir e/ou difundir informações. Permitem maximizar o potencial do comandante de informar audiências amigas e influenciar públicos-alvo (Pub A) adversários, bem como afetar ou obstar o processo de tomada de decisão de potenciais oponentes, ao mesmo tempo em que protege o nosso processo decisório. Visam, ainda, a evitar, impedir ou neutralizar os efeitos das ações adversárias na dimensão informacional, por meio de uma série de atividades, para moldar e assegurar os resultados desejados.

Nesse sentido, as Op Info contribuem para a obtenção da superioridade de informações[2] integrando as CRI, dentre as quais, destacam-se: a Comunicação Social (Com Soc); as Operações Psicológicas (Op Psc); a Guerra Eletrônica (GE); a Guerra Cibernética (G Ciber); e a Inteligência (Intlg).

Nas Op Info, a aplicação isolada de cada CRI ou de recursos a elas relacionados dificilmente conduz a resultados satisfatórios. Somente a atuação integrada e sincronizada desses instrumentos contribui efetivamente para atingir o Estado Final Desejado (EFD)[3] de uma operação.

O entendimento de conceitos básicos das CRI são fundamentais para o entendimento das Op Info. Assim, serão apresentados abaixo, tal como descritos no manual do EB que trata do assunto.

3.1 Comunicação Social

A Com Soc é o processo pelo qual se busca aperfeiçoar o relacionamento entre os seres humanos, como indivíduos, ou como integrantes de um grupo social. Também pode ser entendida como uma série de ações segundo as quais se podem exprimir ideias, sentimentos e informações visando ao estabelecimento de relações e soma de experiências. Cumpre a missão do Exército de manter os públicos (internos e externos) informados, por meio de atividades de Relações Públicas, Informações Públicas e Divulgação Institucional.

2 É traduzida por uma vantagem operativa derivada da habilidade de coletar, processar, disseminar, explorar e proteger um fluxo ininterrupto de informações aos comandantes em todos os níveis, ao mesmo tempo em que se busca tirar proveito das informações do oponente e/ou negar-lhe essas habilidades. É possuir mais e melhores informações do que o adversário sobre o ambiente operacional. Permite o controle da dimensão informacional (espectros eletromagnético, cibernético e outros) por determinado tempo e lugar. Operações de Informação (BRASIL, 2014)
3 Situação, política ou militar, favorável que deve ser alcançada quando a operação estiver finalizada. Operações de Informação (BRASIL, 2014)

Figura 2 – Atividades de Comunicação Social

Fonte: Operações de Informação (2014)

3.2 Operações Psicológicas

As Op Psc são definidas como procedimentos técnico-especializados, aplicáveis de forma sistematizada, de modo a influenciar Pub A a manifestar comportamentos desejáveis, com o intuito final de apoiar a conquista dos objetivos estabelecidos.

As Op Psc constituem uma das principais CRI colocadas à disposição de comandantes de elementos da F Ter para informar e influenciar Pub A neutros e hostis num Teatro de Operações (TO) ou Área de Operações (A Op). Os destacamentos de Op Psc conduzem operações para induzir ou reforçar atitudes e comportamentos favoráveis aos objetivos militares específicos. São, como executores primários da tarefa de informar e influenciar Pub A, responsáveis por desenvolver campanhas de Op Psc, além de analisar, produzir e disseminar produtos. Os especialistas em Op Psc agregam experiência sobre o assunto à estrutura de Op Info, como também assessoram, planejam, analisam mensagens e avaliam ações com efeitos psicológicos reais ou potenciais.

3.3 Guerra Eletrônica

A GE é o conjunto de atividades que visam a desenvolver e assegurar a capacidade de emprego eficiente das emissões eletromagnéticas próprias, ao mesmo tempo em que buscam impedir, dificultar ou tirar proveito das emissões inimigas. É responsável, portanto, por garantir e manter a liberdade de ação no espaço eletromagnético para nossas forças enquanto exploram ou negam essa liberdade aos oponentes. Além de contribuir para influenciar Pub A adversários, a GE está intimamente vinculada às Op Info no que se refere à degradação do processo decisório de potenciais oponentes, ao mesmo tempo em que é utilizada para proteger o nosso. Serve, ainda, desde que devidamente integrada a outras CRI, para evitar, impedir ou neutralizar os efeitos das ações adversárias na dimensão informacional.

3.4 Guerra Cibernética

As Ações Cibernéticas (exploração, ataque e proteção) são o emprego de recursos do espaço cibernético e objetivam: proteger os próprios ativos de informação; explorar e atacar redes do oponente, mantendo a capacidade de interferir no desenrolar das operações militares no espaço de batalha; bem como afetar as condições de normalidade em uma determinada área ou região, atingindo gravemente o funcionamento de estruturas estratégicas e serviços essenciais destinados à população.

As ações cibernéticas visam a negar ou a manipular o oponente ou potencial adversário, por meio do direcionamento de um meio de informação (como um ponto de acesso sem fio na perspectiva física), da mensagem em si (uma mensagem cifrada na perspectiva lógica), ou de uma pessoa virtual (uma identidade "on line" que facilita a comunicação, a tomada de decisão e/ou a influência dos Pub a na perspectiva cognitiva).

3.5 Inteligência

A Intlg é uma capacidade vital para as Op Info. A utilização de conhecimentos de inteligência integrados facilita sobremaneira a compreensão da dimensão informacional. A inteligência envolve um processo integrado de fusão de dados, permeia todo o ciclo do conhecimento (orientação, obtenção, produção e difusão) e gera produtos que irão expor as capacidades e vulnerabilidades de oponentes e de potenciais adversários selecionados. Para tal, utiliza uma variedade de ferramentas para avaliar a dimensão informacional, proporcionando, assim, uma visão ampliada e holística dessa dimensão.

Da análise dos fatores psicossociais da população local do TO/A Op –

incluindo as informações transmitidas por meio de redes físicas – o Sistema de Inteligência pode contribuir, significativamente, com os integradores de CRI e planejadores de Op Info na determinação do efeito adequado para conduzir respostas específicas desejadas.

4 A OPERAÇÃO DE GLO POTIGUAR 2

4.1 O Ambiente Operacional antes do início das ações

As Organizações Criminosas (ORCRIM) do RN envolveram-se no conflito entre o Primeiro Comando da Capital (PCC) e facções regionais, iniciado no Norte do país, deflagrando um conflito no interior do Presídio Estadual de Alcaçuz, onde foram mortos 26 detentos.

Por meio de Agentes Perturbadores da Ordem Pública (APOP), as ORCRIM iniciaram, no dia 18 de janeiro de 2017, uma série de ataques aos meios de transporte e instalações públicas nas cidades de Natal, Parnamirim, Macau, Caicó e Parelhas, gerando uma sensação de insegurança por parte da população dessas cidades.

Os OSP do Estado, policiais civis e militares e agentes penitenciários, foram acionados e atuam no sentido de conter as tentativas de fuga dos presídios e impedir os atos urbanos contra a segurança da população.

Figura 3 – Rebelião no Presídio de Alcaçuz em Natal

Fonte: Operação Potiguar 2 (2017)

Diante da crise, o Governador do Estado do Rio Grande do Norte solicitou, em caráter de urgência, o emprego das Forças Armadas (FA), em razão da insuficiência de meios. Em consequência, o Presidente da República emitiu decreto presidencial autorizando o emprego temporário e episódico de meios das FA, em ações de GLO, no período compreendido entre os dias 20 e 30 de janeiro de 2017, em razão da insuficiência de meios dos órgãos de segurança pública daquele Estado. Posteriormente, mediante novo decreto presidencial, as ações desenvolvidas pelas FA para GLO em Natal foram prorrogadas até 4 de fevereiro de 2017.

4.2 A missão atribuída à Força Terrestre

A missão inicialmente estabelecida pelo Cmt da 7ª Bda Inf Mtz foi:

> Preservar a ordem pública e a incolumidade das pessoas e do patrimônio, na área metropolitana do Município de Natal, no Estado do Rio Grande do Norte, no período de 20 a 30 de janeiro de 2017.

A intenção do Cmt 7ª Bda Inf Mtz era que as tropas empregadas atuassem em conformidade com as regras de engajamento, priorizando a segurança do pessoal e do material, bem como preservando a imagem da Força Terrestre perante a sociedade brasileira.

4.3 O Estado Final Desejado (EFD)

Retorno às condições de normalidade, onde permaneçam preservadas a ordem pública, a incolumidade das pessoas e do patrimônio, mantendo a prioridade à segurança do pessoal militar e do material, bem como preservando a imagem da Força Terrestre perante a sociedade brasileira.

4.4 Ações táticas realizadas

Quadro 1– Ações Táticas na Operação Potiguar 2

Ação Tática	Quantidade
Patrulha a Pé	659
Patrulha Motorizada	1988
Guarda de Área de interesse	259
Ponto de Bloqueio e Controle de Vias Urbanas (PBCVU)	47
Patrulha Blindada	5
Ponto Estático	801
Patrulha Fluvial	12
Escoltas	28
PBCE	20
Reconhecimento	54
Reconhecimento Aéreo	6
TOTAL	3879

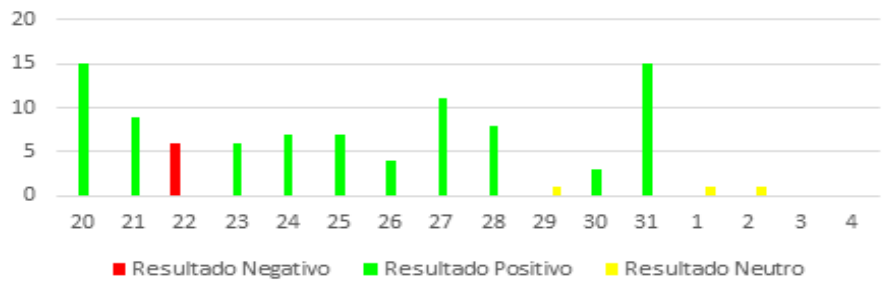
Figura 4 – Ponto de Bloqueio e Controle de Vias Urbanas (PBCVU) em Natal

Fonte: Operação Potiguar 2 (2017)

4.5 O Ambiente Operacional ao término das ações

Foram restabelecidas as condições de normalidade anteriores ao início dos ataques, com a redução de alguns índices específicos de criminalidade, como roubos de automóveis, assaltos a usuários de bancos nas imediações dos estabelecimentos e roubos a transeuntes, assim como a circulação dos meios de transporte.

Gráfico 1 – Circulação dos Meios de Transporte (Frota)



Fonte: Operação Potiguar 2 (2017)

5 CAPACIDADES RELACIONADAS À INFORMAÇÃO NA OPERAÇÃO POTIGUAR 2

Tendo em vista as sugestões e as oportunidades de melhoria levantadas por ocasião da Operação Potiguar 1 e em face da inexistência de especialistas em todas as CRI no âmbito da 7ª Bda Inf Mtz para a condução de Operações de Informação, foi solicitado ao Escalão Superior o apoio de equipes especializadas para a Operação Potiguar 2, que foram disponibilizadas conforme o quadro abaixo:

Quadro 2 – Equipes especializadas em Operação de Informação na Operação Potiguar 2

Capacidade Relacionada à Informação	Efetivo		
	Of	Sgt	
Comunicação Social (Com Soc)	2	1	3
Defesa Cibernética (D Ciber)	1	1	2
Guerra Eletrônica (GE)	2	6	8
Inteligência (Intlg)	1	4	5
Operações Psicológicas (Op Psc)	2	-	2

Fonte: Operação Potiguar 2 (2017)

5.1 Comunicação Social

A Comunicação Social durante a Operação Potiguar 2 foi planejada e conduzida por um oficial superior que veio do Centro de Comunicação Social do Exército (CCOMSEX) para chefiar a Equipe de Comunicação Social, militar que também desempenhou a função de Porta-Voz da Operação.

A missão era apoiar a 7ª Bda Inf Mtz com atividades de comunicação social, a fim de otimizar o relacionamento das FA com a população local, utilizando-se das relações públicas, relações com a mídia e divulgação institucional.

Nesse contexto, de acordo com o planejamento de Comunicação Social, foram estabelecidos os seguintes objetivos:

5.1.1 Antes e durante o emprego

- Conquistar o apoio de colaboradores, formadores de opinião e lideranças nas ações das FA na área de operações;

- Fortalecer o apoio das principais autoridades do Governo do Estado do Rio Grande do Norte às ações das FA;

- Conscientizar as tropas empregadas sobre a importância de não divulgar

informações atinentes à operação que pudessem comprometer o sigilo das mesmas;

- Conscientizar a população sobre a importância da colaboração e apoio às ações das FA na área de operações para o restabelecimento de um ambiente seguro e estável;

- Motivar a população a denunciar as ações e planos das ORCRIM;

- Conscientizar os OSP e a tropa empregada sobre a importância do trabalho integrado entre as FA e os referidos órgãos;

- Conscientizar a população da área de operações que a missão das FA é o restabelecimento de um ambiente de segurança e paz no local;

- Conscientizar a população da área de operações sobre a importância de atender às orientações dos integrantes da Operação Potiguar 2;

- Prevenir e se contrapor à desinformação deliberada na mídia e nas redes sociais;

- Reduzir ou neutralizar os eventuais efeitos da opinião pública contrários às FA;

- Conquistar a superioridade de informações e o domínio da narrativa nos meios de comunicação;

- Fortalecer a credibilidade e imagem positiva das FA na região;

- Reduzir e/ou eliminar a vontade dos integrantes das ORCRIM em prosseguir em suas ações de perturbação da paz social;

- Contribuir, em articulação com a seção de Op Info, para reduzir e/ou eliminar a capacidade de comunicação entre as lideranças da ORCRIM e seus integrantes, assim como para desacreditar os líderes da ORCRIM junto aos seus integrantes;

- Intensificar as medidas de contrainteligência com a finalidade de proteger nosso fluxo de informações, instalações e meios militares;

- Contribuir, em articulação com a seção de Op Info, para aumentar a sensação de segurança na área de operações e desestimular as ORCRIM a praticarem suas ações;

- Realizar a análise de vínculo, por meio das ações de exploração em fontes

abertas dos públicos-alvo prioritários;

- Levantar, nas mídias sociais, possíveis campanhas de desinformação deliberadas com impacto negativo na atuação e na imagem das FA;

- Levantar, nas mídias sociais, possíveis comentários negativos e/ou vazamento de informações relativas à atuação das FA por parte de integrantes da tropa;

- Realizar a análise de vínculo, por meio das ações de exploração em fontes abertas da Capacidade de Inteligência Cibernética dos públicos-alvo prioritários;

- Monitorar sistematicamente o espaço cibernético de interesse, visando manter e/ou ampliar a consciência situacional;

- Acompanhar, nas mídias sociais, a repercussão da atuação das FA na A Op, identificando formadores de opinião e veículos com posição favorável e contrário à ação da tropa;

- Levantar informações relacionadas ao aumento/diminuição da sensação de segurança e tensão na região por parte da população.

5.1.2 Após o emprego

- Potencializar as ideias-força na A Op;

- Conscientizar a população de que a participação das FA foi fundamental para solução da crise;

- Conscientizar a população de que as FA estarão sempre prontas para defender os interesses do Estado e do Povo Brasileiro;

- Contribuir para o fortalecimento dos OSP e a consequente manutenção do clima de estabilidade da região;

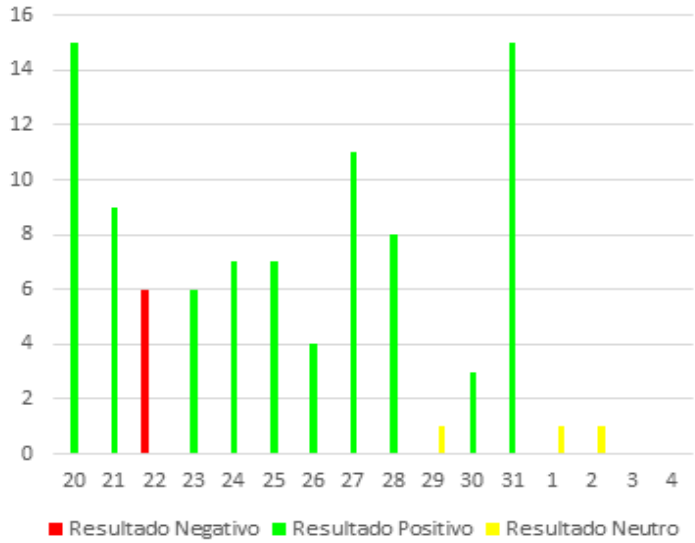
- Manter a credibilidade e imagem positiva das FA na região; e

- Contribuir para que a população aceite a solução adotada para a crise.

Durante a Operação Potiguar 2, a Com Soc, por meio de suas atividades, acompanhou os meios de comunicação, preparou coletivas de imprensa, notas à imprensa e "*media training*", bem como realizou a divulgação institucional, por meio de matérias e produtos, reforçando as ideias-força.

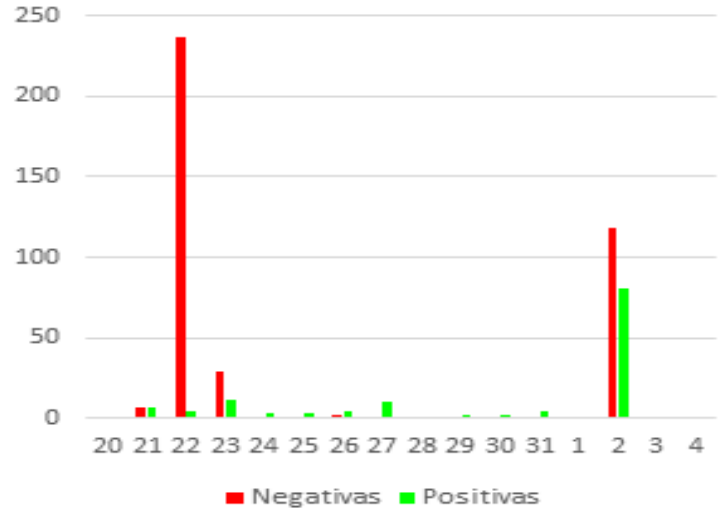
Os gráficos a seguir produzidos pela equipe de Com Soc apresentam indicativos utilizados para o acompanhamento das inserções na mídia ou nas redes sociais de matérias referentes à operação.

Gráfico 2 – Inserções positivas na mídia durante a Operação Potiguar 2



Fonte: Operação Potiguar 2 (2017)

Gráfico 2 – Inserções positivas nas redes sociais durante a Operação Potiguar 2



Fonte: Operação Potiguar 2 (2017)

5.2 Operações Psicológicas

A Operação Potiguar 2 contou com a participação de quatro militares especializados em Operações Psicológicas do 1º Batalhão de Operações de Apoio a Informação (1º BOAI), atual 1º Batalhão de Operações Psicológicas.

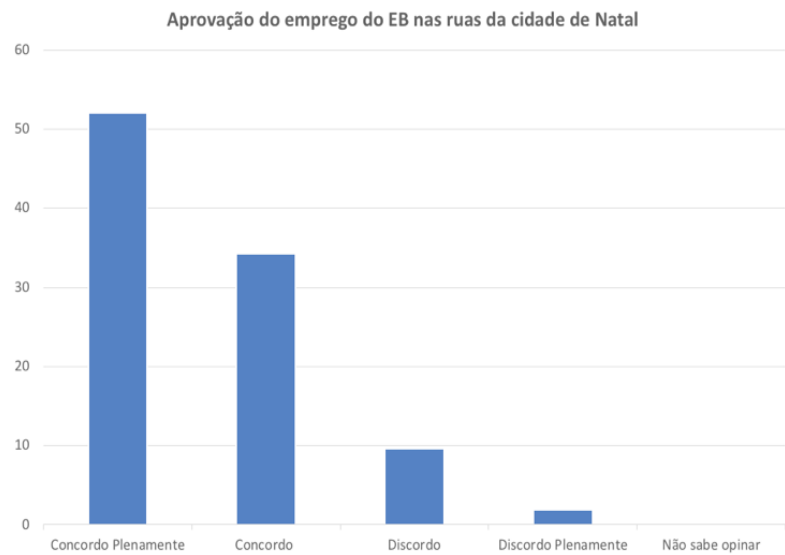
A CRI Operações Psicológicas realizou ações e produtos de operações psicológicas e elaborou pesquisa de opinião em prol da operação.

Situações que poderiam ter comprometido a imagem do EB e a atuação da tropa na operação eram levantados por todas as CRI, permitindo a análise integrada, a proposição e a execução de ações (por CRI ou integradas) que poderiam minimizar possíveis efeitos negativos. Como exemplo, foi observada a produção de vídeo institucional, integrando as CRI Comunicação Social e Operações Psicológicas, para difundir as ações de atuação da tropa.

Nos últimos dias da operação, foi realizada uma pesquisa a fim de realizar um levantamento da percepção da população de Natal/RN relativa à segurança pública, bem como sobre o nível de aprovação da presença do Exército.

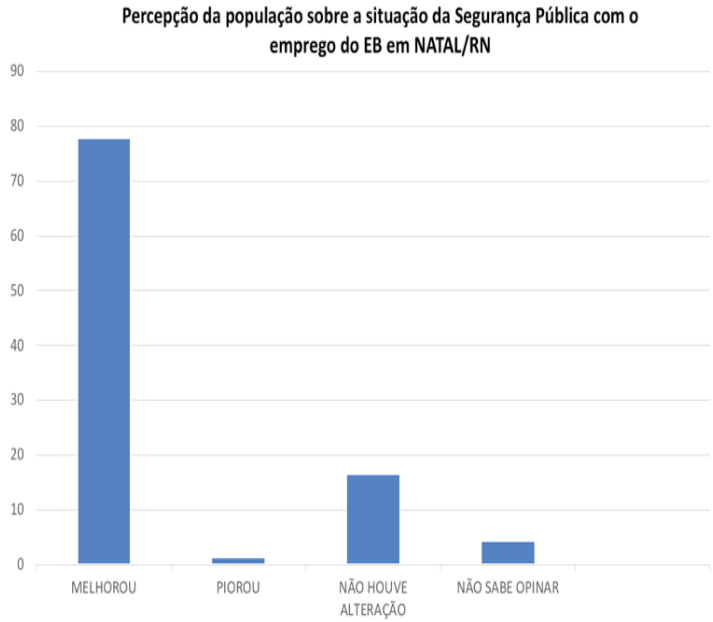
Os dados coletados na pesquisa mostraram que a atuação do EB nas ruas da cidade de Natal em operações de GLO foi aprovada por 86,28% da população. A percepção de aumento na segurança das áreas públicas com a presença do EB nas ruas foi apontada por 77,88% dos entrevistados.

Gráfico 3 – Aprovação do emprego do EB em NATAL/RN



Fonte: Operação Potiguar 2 (2017)

Gráfico 4 – Melhora na segurança pública com o emprego do EB em NATAL/RN



Fonte: Operação Potiguar 2 (2017)

5.3 Inteligência, Guerra Eletrônica e Defesa Cibernética

A seção de inteligência da 7ª Bda Inf Mtz foi reforçada por uma central de inteligência, constituída por militares do Centro de Inteligência do Exército (CIE). Realizou todo o processamento e análise dos dados de inteligência, suporte de contrainteligência (CI) e o estabelecimento de um Centro de Comunicações (C Com) para atender o fluxo de documentos de inteligência.

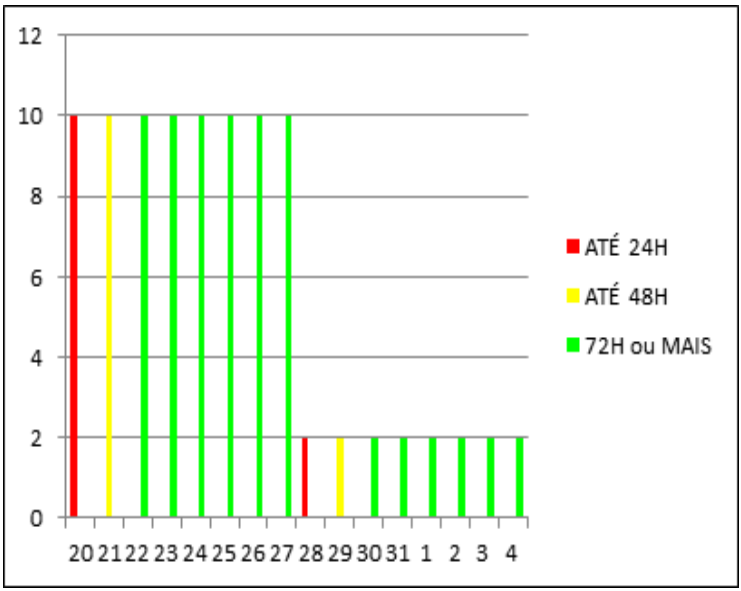
Integrantes do Sistema de Inteligência do Comando Geral da Polícia Militar/RN, do Comando de Polícia Metropolitana (CPM) e do Comando de Polícia do Interior (CPI), bem como, integrantes da Inteligência da Polícia Civil/RN e da Polícia Rodoviária Federal (PRF) participaram das reuniões realizadas pela seção de Inteligência.

As CRI Intlg, GE e D Ciber foram reunidas na central de inteligência para potencializar a produção de conhecimentos, o acompanhamento de fontes abertas, de redes sociais e do espectro eletromagnético, ficando em condições de realizar ações específicas em suas áreas de atuação.

Os conhecimentos de inteligência produzidos pela atuação integrada das CRI Intlg, GE e D Ciber permitiram o acompanhamento das ações das ORCRIM e da evolução do reestabelecimento da situação de normalidade.

O gráfico a seguir apresenta um dos indicativos utilizado para o acompanhamento dos resultados da Operação, no período de 20 Jan 17 a 4 Fev 17.

Gráfico 4 – Anulação das Ações das ORCRIM (tempo desde últimos ataques)



Fonte: Operação Potiguar 2 (2017)

5.4 Pontos fortes relacionados às Operações de Informação

Dentre os pontos fortes observados, destacam-se:
- Ativação de todas as seções previstas para o Estado-Maior (EM) de uma Grande Unidade encarregada de planejar e conduzir Operações Militares no nível tático, permitindo a ligação de cada seção com o Centro de Coordenação de Operações do CMNE, favorecendo a maior integração das atividades das CRI.
- Pronto atendimento pelo Comando de Operações Terrestre (COTER) da solicitação das CRI não existentes na 7ª Bda Inf Mtz. O envio das equipes especializadas foi de vital importância para a execução das tarefas de Op Info.
- Entendimento da importância das Op Info no âmbito da Op GLO por parte dos integrantes do EM/7ª Bda Inf Mtz.
- Inserção de ideias-força sugeridas pelo CCOMSEX.
- Realização do *"VIP Day"*, atividade de reunião de integrantes da mídia (TV, Rádio,

Internet) e outros convidados com o intuito de aproximá-los dos integrantes das FA.

5.5 Oportunidades de Inovação e Melhoria relacionadas às Operações de Informação

Dentre as sugestões e oportunidades de melhoria, destacam-se:
- Necessidade da adequação dos efetivos para o emprego de cada uma das CRI de acordo com a natureza da missão. No caso das Op Psc, para uma missão como a Operação Potiguar 2, é necessário que seja acionado um Oficial de Ligação e um Destacamento de Operações Psicológicas com meios de produção e disseminação. Já no caso da Cibernética, o apoio foi concentrado em atividades de inteligência de fonte humanas.
- A realização de uma videoconferência entre o Oficial de Op Info da operação e os responsáveis pelas CRI, durante a fase de planejamento, seria importante para uma melhor adequação dos meios e apoios empregados.
- Necessidade de um local reservado para as CRI, de modo a não utilizar as mesmas instalações da seção de inteligência da 7ª Bda Inf Mtz.
- Necessidade de manter licitação aprovada para execução de serviços gráficos, de modo a ter rapidez na execução dos produtos de Com Soc e Op Psc.

5.6 Percepção dos oficiais envolvidos com alguma das CRI durante a Operação Potiguar 2

A análise das respostas dos questionários enviados para oficiais que participaram do planejamento e da condução da operação evidenciou que 80% considerou que a CRI em que participou contribuiu para o cumprimento da missão atribuída à Força Terrestre na Operação Potiguar de maneira elevada e que dois oficiais consideraram que a CRI em que participaram contribuiu de maneira suficiente.

Além disso, 90% concordaram plenamente que as Op Info contribuíram para o cumprimento da missão atribuída à Força Terrestre e apenas um oficial concordou parcialmente com a citada assertiva.

Ademais, 80% dos oficiais concordaram que durante a Operação Potiguar 2, os meios (pessoal e material) para o planejamento e execução das Op Info foram adequados e dois oficiais consideraram que não foram adequados.

Na opinião dos oficiais, fruto da formação e do aperfeiçoamento nas Escolas do EB, a capacidade dos militares da Força Terrestre para planejar e executar atividades e tarefas de Op Info durante operações de GLO foi considerada elevada por 25%, suficiente por 33,3% e insuficiente por 41,7%.

6 CONSIDERAÇÕES FINAIS

Este artigo teve por objetivo apresentar como as CRI foram empregadas na Op GLO Potiguar 2.

Em síntese, as CRI facilitaram sobremaneira o cumprimento da missão da 7ª Brigada de Infantaria Motorizada e o atingimento do EFD, contribuindo para o sucesso da operação e para o reestabelecimento da situação de normalidade na Região Metropolitana de Natal.

Considerando a importância da informação no ambiente operacional contemporâneo e as sugestões e oportunidades de melhoria observadas na operação, recomenda-se a necessidade do permanente estudo e do aperfeiçoamento do planejamento e do emprego das Op Info no âmbito do EB, particularmente pelo COTER e pelas Escolas Militares.

Com base na análise das fontes disponíveis e nas percepções de oficiais participantes da operação, recomenda-se, também, o aperfeiçoamento da capacidade de planejar e conduzir as atividades e tarefas de Op Info, durante a realização dos cursos da Escola de Aperfeiçoamento de Oficiais (EsAO) e da Escola de Comando e Estado-Maior do Exército (ECEME), assim como o incremento de estágios setoriais de Op Info nos Comandos Militares de Área (C Mil A).

Por fim, o adequado planejamento e emprego das Op Info será fundamental para o sucesso das operações futuras do EB e contribuirá de forma relevante para os efeitos desejados na dimensão informacional do ambiente operacional.

REFERÊNCIAS

BRASIL. Ministério da Defesa. **Manual de Garantia da Lei e da Ordem** – MD33 – M-10, 2ª Edição, aprovado pela Portaria Normativa Nº 186/MD, de 31 de janeiro de 2014.

_____.Manual de Campanha EB20-MC-10.213 **Operações de Informações**. Brasília-DF, 1ª Edição, 2014, aprovado pela Portaria Nº 008-EME, de 24 de janeiro de 2014.

_____.Nota de Coordenação Doutrinária Nº 02/2015. **Metodologia para o Planejamento das Operações de Informações**. – 3ª SCh EME, 10 AGO 15.

_____. Presidência da República. **Decreto Presidencial autoriza o emprego das Forças Armadas para a Garantia da Lei e da Ordem na Região Metropolitana do Município de Natal, Estado do Rio Grande do Norte**. 19 de janeiro de 2017.

_____. Exército. 7ª Brigada de Infantaria Motorizada. **Operação Potiguar 2** Natal, RN, 2017.

_____. Manual de Fundamentos EB20-MF-10.102 – **Doutrina Militar Terrestre**. Brasília-DF, 2ª Edição, 2019, aprovado pela Portaria Nº 326-EME, de 31 de outubro de 2019.

LINHARES, Marcello Vinicius Mota. **Operação Potiguar 2.** Publicado no EBLOG (BLOG DO EXÉRCITO BRASILEIRO) em 15 de maio de 2017. Disponível em http://eblog.eb.mil.br/index.php/operacao-potiguar. Acessado em 6 de janeiro de 2017.


Escola de Comando e Estado-Maior do Exército
ECEME
O Saber na Defesa da Pátria!

Instruções aos autores

Caso os diplomados queiram participar de nossa publicação, enviando artigos de opinião, resenhas ou mesmo artigos cientifícos, estes deverão ser encaminhados por via digital para os nossos endereços eletrônicos. www.eceme.ensino.eb.br (padeceme@eceme.eb.mil.br)

Os textos devem ser em "Times New Roman 12" espaço simples com termos estrangeiros em itálico. O tamanho sugerido do artigo deve ser de no máximo 4.000 palavras, podendo ter até 3 (três) ilustrações, com resolução de 300 dpi (entre figuras, mapas, imagens, desenhos, fotografias, gravuras, tabelas e gráficos) referidas o mais próximo possível da localização no texto e acompanhadas das respectivas legendas e fontes.

As normas para Referências Bibliográficas e Citações deverão seguir as recomendações da Associação Brasileira de Normas Técnicas (ABNT/NBR 6023 e 10520 respectivamente). As citações deverão ser indicadas no texto pelo sistema de chamada autor-data, sendo sua correlação na lista de referências.

Os autores devem informar, se for o caso, local onde servem (nome da OM, cidade, estado e país) e a mais alta titulação.

ISSN 1677-1885