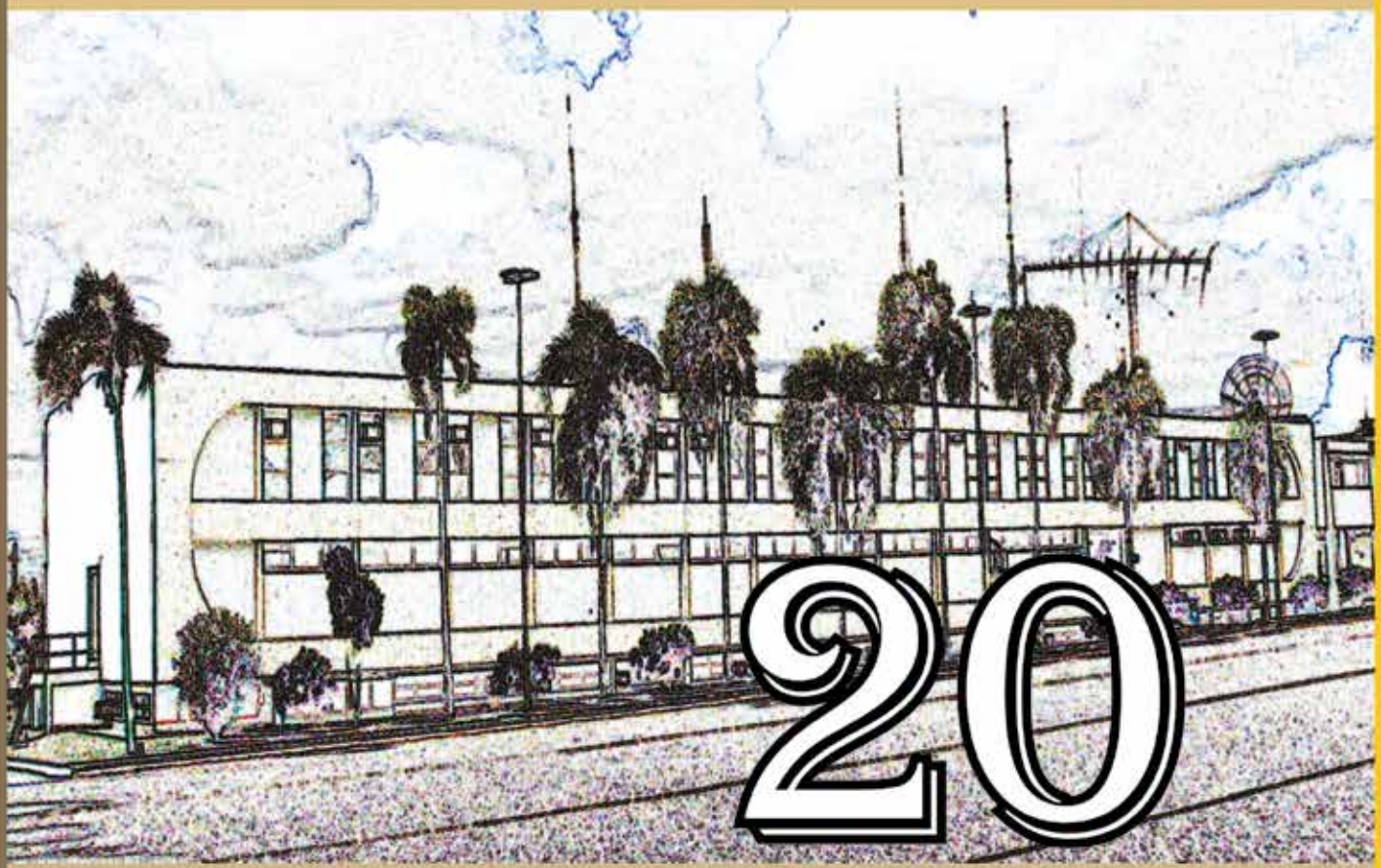
A Lucerna

Escola de Inteligência Militar do Exército



Há duas décadas especializando recursos humanos para a Inteligência Militar.

ISSN 2316 - 364X

A Lucerna

ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO
Cel Art Adilson Carlos **Katibe** - Comandante

Comissão Editorial da Revista "A LUCERNA"
Cel Art Adilson Carlos **Katibe**
Cel Cav Marcus Antonio Ferreira **Pereira**
Ten Cel Eng Alex Murilo de **Freitas**
Ten Cel Inf André Luiz **Velozo**
Ten Cel Cav **Vagner** Knopp de Carvalho
Ten Cel Inf Marcelo Barbosa Lima **Gasse**
Maj Art Carlos **Gustavo** Monteiro
Maj Cav Leandro **Maronês** Peçanha
Maj MB Vinícius José **Negrini** Soares
Maj Art David Vieira de **Matos Júnior**
Maj Int **Aliomar** Nazareno Pinheiro Junior

Capa
1º Sgt Cav André Luiz de **Oliveira**

Elaboração Gráfica
1º Sgt Cav **Aurenide** José dos Santos

Diagramação
Jheison Henrique

Revisão
Cel Art Adilson Carlos **Katibe**
Ten Cel Cav **Vagner** Knopp de Carvalho

Catalogação bibliográfica internacional, normalização e editoração
Biblioteca do Colégio Militar de Brasília

Disponível em: http://www.esimex.ensino.eb.br

Contatos
Av. Duque de Caxias, S/Nr - SMU
Cep: 70630-000 - Brasília-DF
E-mail: esimex@solsi.eb.mil.br
Tiragem desta edição: 300 (trezentos) exemplares

Impressão
Cidade Gráfica e Editora - Brasília-DF

Dados Internacionais de Catalogação na Publicação (CIP)

A LUCERNA / ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO. ANO III NR 5 - EDIÇÃO ESPECIAL (JUL 2014). BRASÍLIA: CIDADE, 2014.

48P.

ISSN 2316-364X

1. INTELIGÊNCIA MILITAR 2. EXÉRCITO BRASILEIRO 3. ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO

CDU: 355.40(81)

Sumário

Editorial

A Escola de Inteligência Militar do Exército (EsIMEx) tem a honra e a satisfação em apresentar a edição especial da Revista "A Lucerna", comemorativa aos vinte anos de criação da Escola.

Nessas duas décadas de existência, tivemos o privilégio de especializar mais de 3600 (três mil e seiscentos) militares do Exército, das Forças Singulares, de Nações Amigas, policiais e bombeiros militares e integrantes de organizações civis pertencentes ao poder público.

Na presente edição, a comissão editorial da EsIMEx conferiu um enfoque comemorativo à Revista, porém, não deixou de selecionar os trabalhos produzidos pelos discentes desta Escola, com maior relevância para a divulgação doutrinária da Atividade de Inteligência Militar.

O primeiro artigo reveste-se de caráter histórico, onde o intuito foi o de permitir ao leitor conhecer o processo de criação e consolidação da EsIMEx como um Estabelecimento de Ensino de referência na especialização de recursos humanos em Inteligência Militar, tanto na vertente humana, quanto na tecnológica.

No segundo, aproveitamos esta edição especial para divulgar o "Projeto Nova Escola" que irá permitir a ampliação, reestruturação e modernização da estrutura organizacional e física da EsIMEx, para oferecer melhores condições ao desenvolvimento do processo de ensino-aprendizagem, impostos pela evolução doutrinária da Atividade de Inteligência.

No artigo subsequente, os autores, embasados por suas experiências profissionais e por um profundo trabalho de pesquisa, nos levam a refletir sobre o perfil desejável do militar para a exploração da Inteligência na fonte cibernética, identificando as habilidades adequadas para a obtenção e a análise de dados oriundos do complexo e difuso espaço cibernético.

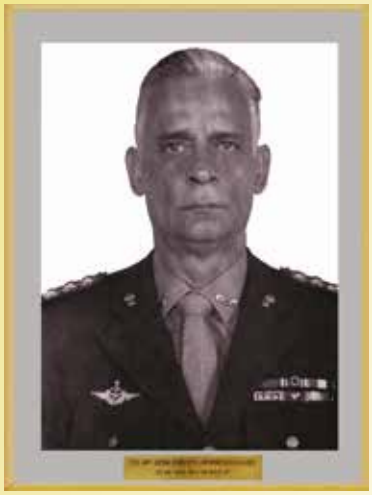
O quarto artigo trata de um estudo de caso sobre a função de combate Inteligência e a sua interrelação com as capacidades relacionadas às Operações de Informação, ambientando este estudo na Operação Humaitá, desencadeada na área do Comando Militar da Amazônia, entre dezembro de 2013 e fevereiro de 2014.

Por fim, não poderia deixar de registrar nosso reconhecimento e gratidão aos autores dos artigos desta edição pela valiosa contribuição para a difusão do trabalho realizado pela Escola, bem como para a evolução da Doutrina de Inteligência.

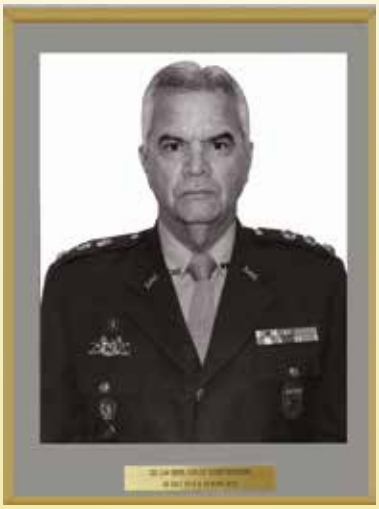
Boa leitura!

Adilson Carlos **Katibe** - Coronel
Comandante e Diretor de Ensino da EsIMEx

Galeria dos Ex-Comandantes



Homenagem da Escola de Inteligência Militar do Exército aos antigos Comandantes por sua dedicação, contribuição e comprometimento em duas décadas de ensino de Inteligência Militar no Exército Brasileiro.



A Escola de Inteligência Militar do Exército

Foto 1 - Vista frontal da EsIMEx

1. O PROCESSO DE IMPLANTAÇÃO

A Escola de Inteligência Militar do Exército (EsIMEx), único Estabelecimento de Ensino de Inteligência das Forças Armadas do Brasil, foi criada pela Portaria Ministerial Nr 034–EME–RES, de 13 de junho de 1994, passando a funcionar em 1º de julho do mesmo ano, subordinada ao Estado-Maior do Exército (EME).

A EsIMEx surgiu num momento de transição da conjuntura nacional em que ocorria a extinção do Serviço Nacional de Informações e a transformação da Escola Nacional de Informações (EsNI) em Centro de Formação de Recursos Humanos (CeFARH), que não mais contemplava o ensino de Inteligência em Operações Militares.

No início de seu funcionamento, em 1994, a Escola realizou, em caráter emergencial, a primeira capacitação de recursos humanos especializados em Inteligência Militar, por intermédio do curso especial para Oficiais e Sargentos. Na mesma época ultimava-se a elaboração de currículos, planos de disciplinas e perfis profissiográficos, conforme as normas do Sistema de Ensino do Exército. Assim, já no início de 1995, funcionaram os Cursos Básico e Intermediário para Oficiais.

A partir de 1º de agosto de 1995, por questões relacionadas a sua administração e atividade–fim, a Escola passou à subordinação direta do Centro de Inteligência do Exército (CIE).

Foto 2 - Vista da entrada principal

Para efeitos de orientação pedagógica, a EsIMEx é vinculada ao Departamento de Educação e Cultura do Exército (DECEx), por intermédio da Diretoria de Educação Técnica Militar (DETMil).

A Escola nasceu como um estabelecimento de ensino de grau superior e médio, de **especialização**, na Linha de Ensino Militar Bélico, destinado a:

- especializar oficiais e graduados, habilitando-os ao desempenho de funções previstas nos Quadros de Cargos (QC) e Quadros de Cargos Previstos (QCP) das Organizações Militares (OM) integrantes do Sistema de Inteligência do Exército (SIEx);
- realizar pesquisas na área de sua competência, se necessário, com a participação de instituições congêneres; e
- contribuir com o Estado-Maior do Exército (EME) para o desenvolvimento da Doutrina de Inteligência Militar da Força Terrestre, na área de sua competência.

O Curso Básico de Inteligência para Sargentos, o Estágio de Inteligência Militar para Oficiais e o Estágio para as Forças Especiais passaram a funcionar em 1996, objetivando formar "massa crítica", que atendesse, de imediato, aos setores mais carentes de recursos humanos especializados do Sistema de Inteligência do Exército.

A criação do Curso Avançado de Inteligência para Oficiais, no ano de 1997, permitiu a especialização de oficiais superiores, capacitando-os ao desempenho

Foto 3 - Instrução em Sala de Aula

de cargos e funções de analista e chefe de Agências de Inteligência. Nesse ano, a Escola passou, também, a cooperar na especialização de recursos humanos das Forças Singulares, das Polícias Militares e de militares oriundos de Exércitos de países amigos, com os quais o Exército Brasileiro mantém intercâmbio de Inteligência.

Os avanços tecnológicos aliados ao rápido desenvolvimento doutrinário percebido no início do século XXI contribuiu para a EsIMEx reorientar o ensino da Inteligência Militar. Nesse contexto, foi realizado, em 2004, o primeiro Curso de Inteligência de Imagem para Sargentos com o objetivo de dar o primeiro passo no domínio dessa fonte de inteligência. Com isso, o SIEx passou a contar com elementos especializados na produção de conhecimentos utilizando sofisticados softwares para tratamento e interpretação de imagens, permitindo assim, o domínio de uma nova dimensão de elevado valor no ambiente operacional.

No ano de 2005, ainda dentro da conjuntura de ampliação da capacidade de especialização de recursos humanos, foram iniciadas mais duas novas especializações: o Curso de Inteligência de Imagens para Oficiais e o Curso Avançado de Inteligência para Subtenentes e Sargentos, o que permitiu ao SIEx ampliar a disponibilidade de militares com especialização em Inteligência Militar. No ano de 2012, aconteceu a última atualização nos Cursos ministrados pela EsIMEx, com o acréscimo de 2 (dois) novos Cursos, o de Inteligência do Sinal para

Foto 4 - Estágio para órgãos civis

Oficiais e o de Sargentos. Esses Cursos representam uma solução inovadora no âmbito do Exército, pois foram concebidos para funcionar em dois Estabelecimentos de Ensino distintos, cabendo à EsIMEx os assuntos curriculares de Inteligência Militar e ao Centro de Instrução de Guerra Eletrônica (CIGE) a docência de assuntos relativos à exploração e ao domínio do espectro eletromagnético.

2. RECONHECIMENTO INSTITUCIONAL

A trajetória marcada pela seriedade de propósitos e pelo trabalho profícuo de especialização de recursos humanos na Atividade de Inteligência Militar permitiu o reconhecimento da EsIMEx, no âmbito do Exército Brasileiro e por outras instituições militares e civis, com a outorga de condecorações a este Estabelecimento de Ensino. O Estandarte Histórico da Escola, no ano de 2005, foi agraciado com as Insígnias de Bandeira da Medalha do Pacificador e da Medalha Marechal Trompowsky.

Cabe destacar, no ano de 2006, a concessão ao Estandarte Histórico da Escola da Insígnia de Bandeira da Medalha da Ordem do Mérito do Ministério Público Militar, como reconhecimento pelos relevantes serviços prestados na especialização de promotores da justiça militar de todo o País.

Foto 5 - Entrega da Insígnia de Bandeira da Medalha Marechal Trompowsky

A mais elevada distinção honorífica do Exército Brasileiro, a Insígnia de Bandeira da Ordem do Mérito Militar condecorou o Estandarte Histórico da EsIMEx, no ano de 2012, como reconhecimento pelos bons serviços prestados por esse Estabelecimento de Ensino no diuturno esforço para especializar militares e civis para o desempenho de funções no Sistema de Inteligência nas respectivas Instituições.

Foto 6 - Entrega da Insígnia de Bandeira da Medalha Ordem do Mérito do Ministério Público Militar

3. O ENSINO DE INTELIGÊNCIA

A proposta pedagógica da EsIMEx está orientada pela legislação normativa da DETMil e o disposto pelo DECEx, integrando aspectos de várias linhas pedagógicas, a cultura e a tradição didática do Ensino Militar.

A EsIMEx programa suas atividades letivas inserindo os conteúdos a serem trabalhados dentro de uma temática de cunho prático, próxima da realidade a ser vivenciada pelo concluinte em suas ações futuras no desempenho de seus cargos ou funções no âmbito da Força.

A Escola propõe um trabalho baseado nas diferenças individuais e na consideração das peculiaridades de cada discente, mas preocupando-se em desenvolver as habilidades de trabalho em equipe e de relação interpessoal, inerentes à Atividade de Inteligência Militar. O ensino proposto segue a linha "doutrina - diálogo - experimentação - compreensão" e busca a participação baseada na relação direta da teoria com a prática por parte do discente.

Foto 7 - Exercício de Inteligência nas Operações Militares

É tarefa primordial da Escola a difusão de conteúdos contextualizados e de aplicação inerentemente prática, portanto indissociáveis da realidade da Atividade de Inteligência. A Escola atende às diretrizes e necessidades do Sistema de Inteligência do Exército (SIEx), seu principal cliente, isto é, possui conteúdos curriculares apropriados e coerentes com as peculiaridades do Sistema.

A evolução acelerada das conjunturas nacional e internacional, como decorrência do avanço da ciência e da tecnologia, de novos aspectos do relacionamento humano e das peculiaridades da Atividade de Inteligência Militar, são fatores determinantes para que a Escola constantemente reveja a pertinência da carga horária e das disciplinas dos currículos em vigor, adote estratégias educacionais que favoreçam o autoaperfeiçoamento, desenvolva nos discentes mecanismos de adaptação e estabeleça técnicas e procedimentos que permitam a rápida atualização da prática educacional.

A implantação do ensino baseado no desenvolvimento das competências individuais e do grupo sempre foram objetivos delineados em todos os planejamentos educacionais da EsIMEx, visando a preparar o aluno, sendo ele militar ou civil, para o desempenho da função e a ocupação de cargos nos respectivos Sistemas de Inteligência. Conhecimentos, habilidades, atitudes, princípios, valores e experiências formam o cerne do ensino da Escola.

Foto 8 - Exercício de Inteligência nas Operações Militares

O incremento na utilização da tecnologia da informação, como importante meio de apoio à produção do Conhecimento, no aprimoramento do emprego das técnicas operacionais e dos equipamentos empregados na Atividade de Inteligência, condiciona este Estabelecimento de Ensino a fornecer ao discente a capacitação técnica necessária à utilização dos meios computacionais no âmbito de sua especialização, contribuindo, assim, para o melhor desempenho funcional nos cargos previstos na estrutura do SIEx.

O fenômeno da globalização implica em domínio de diferentes idiomas, culturas e conhecimentos de outras doutrinas. Neste sentido, a EsIMEx desenvolve no discente a capacidade para interagir e conhecer a Atividade de Inteligência de outros exércitos, por meio da participação de oficiais e praças de Nações Amigas nos cursos regulares, permitindo, assim, a escola ampliar o seu quadro de referência.

A consecução de todos os objetivos anteriores exige um relacionamento estreito da Inteligência Militar com a comunidade de Inteligência alocada nas diversas esferas do poder do Estado Brasileiro. Para tanto, a EsIMEx adota estratégias e instrumentos para aprofundar esse relacionamento com a oferta de estágios e palestras para civis e militares.

Foto 9 - Intercâmbio com militares de Nação Amiga

Dessa forma, a EsIMEx contabiliza 3.660 (três mil, seiscentos e sessenta) discentes especializados na Atividade de Inteligência, desde a sua criação até o mês de julho do corrente ano. Nesse contexto, foram contemplados com especializações deste Estabelecimento de Ensino militares das Forças Armadas, das Nações Amigas e das Forças Auxiliares, bem como, autoridades e personalidades civis, sendo que o maior percentual de especializados pertence ao Exército Brasileiro.

Foto 10 - Formatura de conclusão de curso

4. CONCLUSÃO

Concluindo, cabe destacar que o foco do processo ensino-aprendizagem da EsIMEx está centrado em priorizar a qualidade das práticas pedagógicas em consonância com as novas demandas da Era do Conhecimento, no culto à legalidade, às tradições, à ética, à memória e aos valores morais, culturais e históricos da Atividade de Inteligência Militar e do Exército Brasileiro, de modo a capacitar recursos humanos para a atividade que é considerada o apanágio dos nobres e que se confiada a outros desmorona.

Projeto Nova Escola

Foto 11 - Fachada da Nova Escola

1. ASPECTOS CONJUNTURAIS

O ambiente operacional mais complexo e difuso, onde o elevado componente de incerteza agrava o processo de identificação de oportunidades e ameaças no espaço de batalha, implica na adaptação ou na criação de novas estruturas e na especialização de recursos humanos, capazes de operar em ambientes de elevada complexidade, utilizando materiais de emprego militar (MEM) dotados de novas tecnologias e capacidades.

A Atividade de Inteligência, nesse contexto, também é afetada, visto que os avanços tecnológicos e as interações globalizadas ampliam a dificuldade de definição das ameaças, bem como, o controle das atividades e o acompanhamento da evolução das intenções e ideologias das forças adversas. Tais premissas exigem homens com novas capacidades de obter, processar e analisar dados, visando a produzir conhecimentos objetivos e oportunos para assessorar um decisor.

As crescentes demandas por informação no âmbito da Força Terrestre requerem constante aperfeiçoamento do pessoal da Inteligência. O imperativo tecnológico da atividade exige, ainda, as adequações necessárias à salvaguarda e à produção do conhecimento de inteligência em resposta às diversas ameaças ao Sistema Exército.

O rápido processo de transformação da Força Terrestre, como resultado imediato do Decreto Nr 6703, de 18 de dezembro de 2008, que aprovou a Estratégia Nacional de Defesa (END) desencadeou uma dinâmica de evolução doutrinária e de disponibilização de novos materiais de emprego militar para a execução da Atividade de Inteligência Militar.

A edição da END, aliada ao processo de transformação do Exército e concomi-

tante com a atual evolução doutrinária, impõe novos desafios para a execução da Atividade de Inteligência, que impactam diretamente no processo de capacitação de recursos humanos habilitados a atuar num ambiente operacional complexo com ameaças multifacetadas.

A END expressa, também, a necessidade de que os **recursos humanos** sejam **capacitados em análise e técnicas** de **monitoramento/controle,** fazendo de cada combatente, um sensor capaz de obter dados, que comporão os conhecimentos de inteligência destinados a assessorar os Comandantes em qualquer nível.

Nessa mesma direção de transformação, o Comandante do Exército Brasileiro enfatiza em sua Diretriz 2011–2014, que o Sistema de Inteligência do Exército é essencial, em operações ou no cotidiano da Instituição, ao contribuir para a consecução de diversos objetivos da Política Militar Terrestre (PMT) e ao permear outras atividades. O Sistema deverá iniciar ou prosseguir as seguintes ações:

- aperfeiçoar o Sistema de Inteligência do Exército, **modernizando sua estrutura e capacitação dos recursos humanos;** e
- aperfeiçoar a Doutrina de Inteligência, em sintonia com os Sistemas de Doutrina, Operacional e de Educação e Cultura da Força.

De acordo com os aspectos levantados, tanto na END, como na Diretriz do Comandante da Força, verifica-se a necessidade de se aumentar a capacitação dos quadros que trabalham na Atividade de Inteligência, tanto em qualidade quanto em quantidade, de modo que existam recursos humanos devidamente aptos a atender à criação de Unidades e Subunidades de Inteligência, à operação de novos materiais de emprego militar (MEM) e à nova concepção doutrinária de Inteligência (função de combate Inteligência) do Exército Brasileiro.

Nesse sentido de transformação da Força Terrestre, o Estado-Maior do Exército (EME) aprovou a Diretriz de Implantação do Projeto LUCERNA, no mês de maio do corrente ano, com o intuito de dotar o Exército Brasileiro de uma nova estrutura para o Sistema de Inteligência do Exército (SIEx), com vistas a impactar os processo de apoio à decisão, pela integração das estruturas de análise de Inteligência às estruturas de obtenção de dados de diversas fontes.

O Projeto LUCERNA elenca como objetivos, no que concerne ao ensino da Atividade de Inteligência Militar e que impactam diretamente na concepção futura da Escola, os seguintes aspectos:

- capacitar, qualificar e treinar o pessoal para as novas Organizações Militares (OM) de Inteligência Militar, por intermédio da Escola de Inteligência Militar do Exército (EsIMEx);
- atualizar e aprimorar o ensino da Disciplina de Inteligência Militar nos Estabelecimentos de Ensino;
- ampliar, reestruturar e modernizar a estrutura organizacional e física

da Escola de Inteligência Militar do Exército; e

- aperfeiçoar a doutrina da Atividade de Inteligência, criando mecanismos e definindo procedimentos que norteiem a experimentação doutrinária e a execução da Atividade de Inteligência em tempo de paz e em operações militares (guerra e não-guerra).

Diante dessa necessidade, a Escola de Inteligência Militar do Exército (EsIMEx) vem realizando uma autoavaliação para normatizar os cursos existentes de acordo com a evolução doutrinária e dos materiais de emprego militar, bem como, propor a criação de novos cursos, que atendam a novos cargos e funções existentes no Sistema de Inteligência do Exército.

2. PROJETO NOVA ESCOLA

O Projeto Nova Escola tem por objetivo subsidiar a reestruturação e a modernização da estrutura organizacional e física da Escola de Inteligência Militar do Exército (EsIMEx), visando a proporcionar um incremento qualitativo na capacitação de recursos humanos para atender aos aperfeiçoamentos no processo de ensino-aprendizagem exigidos pela evolução doutrinária da Atividade de Inteligência.

No conjunto de todo o processo de evolução doutrinária da Força, ressalta-se a criação, em 2013, do Núcleo do Batalhão de Inteligência Militar (BIM), no Comando Militar do Oeste (CMO), onde foram criados novos cargos e onde estão sendo alocados materiais de emprego militar específicos para a execução da Atividade de

Foto 12 - Entrega do Projeto Arquitetônico

Inteligência em Operações Militares num Ambiente Operacional de Amplo Espectro. Com isso, se faz necessário que a Escola de Inteligência seja dimensionada e adequada para atender a essa nova conjuntura.

Consonante a todo o processo de rápida transformação, será efetuada a construção da Nova Escola, que irá fornecer, a partir do final de 2016, melhores condições para a execução da atividade docente e estará perfeitamente colimada com as Diretrizes do Departamento de Educação e Cultura do Exército (DECEx) para a implantação do Ensino por competências.

Foto 13 - Saguão principal da Nova Escola

Nesse quadro de mudanças, torna-se imprescindível a atualização do escopo da EsIMEx com a construção da nova Escola, bem como, a revisão dos currículos e o aumento do corpo docente para qualificar, de acordo com as necessidades do SIEx, maior efetivo de oficiais e graduados aptos a responderem por suas atribuições funcionais nos diversos segmentos da atividade de Inteligência.

Para adequar-se à nova realidade e atender às demandas do SIEx, a especialização na área de Inteligência necessita ser ajustada para que os oficiais, subtenentes e sargentos recebam instruções voltadas ao desenvolvimento de competências necessárias para atuar no mundo da "Era do Conhecimento", no qual a Atividade de Inteligência exige algumas características como as seguintes: inteligência apoiada por meios de Tecnologia da Informação (TI), análise não linear (sistemas complexos), análise estruturada e holística, integração sistêmica e capacidade de coleta e

análise de grande quantidade de dados e informação.

Diante disso, a construção das novas instalações da EsIMEx irá contribuir para a ampliação, quantitativa e qualitativa, da capacidade de especialização dos recursos humanos para o Sistema de Inteligência do Exército (SIEx).

De acordo com o projeto, a nova Escola contará com novas salas de aula com a capacidade de especializar o dobro de alunos por curso, auditório próprio, alojamentos em condições de acomodar quatro vezes mais alunos que atualmente, bem como, novos materiais de emprego militar para atender às demandas do SIEx na presente conjuntura.

Foto 14 - Novas salas de aula

3. CONCLUSÃO

Portanto, a construção da estrutura física da nova Escola, até o final do ano de 2016, permitirá a EsIMEx contar com instalações adequadas para acomodar o seu corpo docente e discente, em excelentes condições, facilitando assim, a condução da especialização dos Recursos Humanos para o desempenho de funções no Sistema de Inteligência do Exército.

O Perfil do Militar de Inteligência Cibernética

Marcel Francisco de Souza **Mota** [1]

Claubert Santos de Rezende[2]

Marco Aurélio Gonçalves[3]

Abstract

The objective of this research is to make about the most appropriate profile of the military who will work with the cyber source on the Intelligence activity. It discusses the attributes of the affective area, skills and abilities necessary for the military to act on the cyber environment, inferring about their influence on the intelligence activity.

At first, it reviews the concept of Military Intelligence and covers various aspects of Cyber War, commenting several international events that demonstrate the power of cyberattacks. Then, it discusses what would be the Cyber Intelligence, a concept not yet consolidated in the Ministry of Defence or in the Brazilian Army, and the use of cyber source in Intelligence activity. Furthermore, it discusses the roles that soldiers can perform using the cyber source, to analyze finally the responses collected from a questionnaire distributed to people in various Military Organizations, directly involved in this issue. Finally, it consolidates the various aspects addressed, concluding with a proposed military profile facing the exploitation cyber source.

Keywords: Military Intelligence. Cyber Intelligence. Cyber War. Cyber Source.

Resumo

O objetivo desta pesquisa é elaborar um perfil para os militares que trabalharão com a fonte cibernética na atividade de Inteligência. A pesquisa aborda os atributos da área afetiva (AAA), competências e habilidades necessárias para que o militar atue no ambiente cibernético, inferindo acerca da sua influência sobre a Atividade de Inteligência.

Em um primeiro momento, revisa o conceito de Inteligência Militar e aborda

1 Oficial do Quadro Complementar de Oficiais do Exército Brasileiro - Informática - Escola de Administração do Exército (EsFCEx); Graduado como Tecnólogo em Processamento de Dados - Universidade do Vale do Rio dos Sinos (UNISINOS); Especialista em Sistemas de Informação e Telemática - Universidade Federal do Rio Grande do Sul (UFRGS); Especialista em Aplicações Complementares às Ciências Militares - Escola de Administração do Exército (EsAEx); e Especialista em Conhecimentos Militares - Escola de Aperfeiçoamento de Oficiais (EsAO).

2 Oficial de Infantaria do Exército Brasileiro - Academia Militar das Agulhas Negras (AMAN); Bacharel em Ciência da Computação - Centro Universitário do Triângulo (UNITRI); Especialista em Criptografia e Segurança em Redes - Universidade Federal Fluminense (UFF); e Especialista em Operações Militares - Escola de Aperfeiçoamento de Oficiais (EsAO).

3 Oficial do Corpo de Bombeiros Militar do Estado de Santa Catarina - Academia da Polícia Militar de Santa Catarina; Bacharel em Segurança Pública - Academia de Polícia Militar de Santa Catarina; Bacharel em Direito - Universidade do Sul de Santa Catarina (UNISUL); Especialista em Direito Público - Universidade do Vale do Itajaí (UNIVALI); e Mestre em Administração Empresarial - Universidade do Sul de Santa Catarina (UNISUL).

diversos aspectos da Guerra Cibernética, comentando alguns eventos internacionais que demonstram o poder dos ciberataques. Em seguida, discorre sobre o que seria a Inteligência Cibernética, um conceito ainda não consolidado no Ministério da Defesa ou mesmo no Exército Brasileiro, e sobre o uso da fonte cibernética na Atividade de Inteligência Militar. Posteriormente, trata sobre as funções em que militares podem desempenhar no uso da fonte cibernética para, finalmente, analisar as respostas coletadas em um questionário distribuído a militares de diversas Organizações Militares, envolvidos diretamente no assunto em pauta. Por fim, consolida os diversos aspectos abordados, concluindo com uma proposta de perfil do militar voltado para a exploração da fonte cibernética.

Palavras-chave: Inteligência Militar. Inteligência Cibernética. Guerra Cibernética. Fonte Cibernética.

1. INTRODUÇÃO

O tema Inteligência Cibernética, apesar da relevância e importância, possui poucas referências bibliográficas sobre o assunto. Diante dessa realidade, muitas são as iniciativas realizadas para seu estudo, devido ao aumento e diversificação das ações criminosas e terroristas no espaço cibernético.

A necessidade de tratar o assunto com urgência levou governos do mundo todo a priorizar este espaço e, por conseguinte, a defesa cibernética passou a ser considerada questão de segurança nacional.

Como exemplo, pode ser citada a iniciativa do governo americano, em 2010, na gestão do Presidente Barack Obama, de lançar uma cartilha de Segurança Cibernética (*Cybersecurity*) e de criar o Comando Cibernético nas Forças Armadas dos Estados Unidos (WENDT, 2011).

No Brasil, os primeiros passos foram dados com a Política de Defesa Nacional - PDN (2005), a qual cita que é "essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de Tecnologia da Informação e Comunicação (TIC) ou permitam seu pronto restabelecimento". Por sua vez, a edição Estratégia Nacional de Defesa - END (2008) estabeleceu o setor cibernético como uma das prioridades, devendo para isso "desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos nos níveis operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas", além de "estruturar a produção de conhecimento oriundo da fonte cibernética".

Outro exemplo da preocupação do Governo Brasileiro com a segurança cibernética, o Livro Branco de Defesa Nacional (2012) caracteriza que: "a proteção do espaço cibernético abrange um grande número de áreas, como a capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal".

O Ministério da Defesa (MD), por sua vez, definiu em suas diretrizes na Política Cibernética de Defesa (2012), mais especificamente no "Objetivo Nr II - capacitar e gerir talentos humanos necessários à condução das atividades do setor cibernético

no âmbito do MD", o que segue transcrito:

a) definir os perfis do pessoal necessário para a condução das atividades do setor cibernético;

b) criar cargos e funções específicos e mobiliá-los com pessoal especializado para atender às necessidades do setor cibernético;

c) estabelecer critérios e controlar a mobilização e desmobilização de pessoal para a atividade de Defesa Cibernética;

d) identificar, cadastrar e selecionar o pessoal com competências ou habilidades, existente nos ambientes interno e externo das Forças Armadas, para integrar o Sistema Militar de Defesa Cibernética (SMDC);

e) capacitar, de forma continuada, pessoal para atuar no setor cibernético, sob a orientação do órgão central do SMDC, aproveitando estruturas existentes;

f) viabilizar a participação de pessoal envolvido com o setor cibernético em cursos, estágios, congressos, seminários, simpósios e outras atividades similares relacionadas no Brasil e no exterior; (Política Cibernética de Defesa, 2012)

.....

A "Guerra Cibernética"[4] é uma realidade, comprovada por meio de diversos ataques amplamente divulgados, como, por exemplo, a sabotagem da Internet na Estônia, em 2007, e o caso do *worm*[5] *Stuxnet*, em 2010, implantado no sistema de controle das centrífugas de enriquecimento de urânio do Irã (MACHADO, 2011).

O Governo Brasileiro avançou no reconhecimento da necessidade de proteção de seu "Espaço Cibernético", por meio da Portaria GSI nº 45, de 8 de setembro de 2009, que diz em seu Art. 2º: "Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas".

Segundo Mandarino Junior (2009), Diretor-Geral do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR):

> "A atividade de inteligência exerce papel fundamental nos ambientes de Segurança, Defesa e Guerra Cibernética. Ela é essencial na busca de informações, empregando todas as fontes disponíveis, para identificar e prevenir ameaças cibernéticas e proporcionar respostas adequadas, com oportunidade."

Com o crescimento exponencial da utilização da internet e dos meios de TIC, surgiu a necessidade de explorar mais profundamente o "Espaço Cibernético", inserindo-o como mais uma fonte para a produção do conhecimento. Dessa demanda nasceu a Inteligência Cibernética.

Todavia, ainda existem lacunas conceituais na área da Inteligência Cibernética, principalmente na definição do perfil e das competências dos militares que atuam nesse setor.

4 De acordo com o MD-30-M-01 - Doutrina de Operações Conjuntas do Ministério da Defesa, Guerra Cibernética é definida como o "conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informação para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil".

5 Programa que, explorando deficiências de segurança de hosts, logrou propagar-se de forma autônoma na Internet na década de 80" (INFOPEDIA, 2013).

Considerando que atualmente uma das necessidades proeminentes é a definição dos perfis das pessoas que atuarão na área de Inteligência Cibernética, faz-se necessário realizar trabalhos com o objetivo de suprir essa lacuna. Como óbice a essa iniciativa, existe a carência de literatura específica.

Com características próprias, a exploração da Fonte Cibernética constitui um novo desafio para a Atividade de Inteligência, demandando a inserção de conhecimentos adicionais na área de TIC na formação dos profissionais dessa área.

Considerando que o ambiente operacional da Inteligência Cibernética será o "Espaço Cibernético", um campo ainda bastante desconhecido para muitos, surge o seguinte questionamento: qual deve ser o perfil dos militares que irão atuar nesse espaço?

2. REVISÃO DA LITERATURA E FUNDAMENTOS

Para que se possa ter uma ideia concreta da situação atual da "Guerra Cibernética", tema ainda pouco conhecido, faz-se necessário expor ações já evidenciadas em diversos conflitos recentes e identificar o papel exercido pela Atividade de Inteligência dentro desse contexto. Somente com a compreensão desse universo, poder-se-á verificar quais serão os elementos envolvidos com a Atividade de Inteligência utilizando a fonte cibernética e qual(is) será(ão) o(s) perfil(is) desejado(s) para esses elementos.

Para isso, também deve ser considerado o que disse Branco (2012), um dos mais famosos *hackers*[6] do Brasil e organizador da *Hackers to Hackers Conference* (H2HC), durante o III Seminário de Defesa Cibernética ocorrido em Brasília, em 2012, "*hackers* competentes são pessoas especiais, e para selecionar pessoas especiais não se pode usar processos de seleção comuns".

2.1. Guerra Cibernética

A guerra cibernética, ou ciberguerra (*cyberwar*), é o confronto promovido sem o uso clássico de armas físicas, mas virtualmente, pelo uso da Internet e de meios eletrônicos, dentro do ciberespaço, para promover ataques com os mais diversos objetivos no mundo real, sejam políticos, econômicos ou militares (BEZERRA, 2009; CIBERGUERRA, 2013).

A ciberguerra pode ocorrer de forma autônoma (independente) ou simultânea (paralela) a um conflito armado. Quando autônomos, esses confrontos normalmente são unilaterais, visto que o alvo do ataque só detecta que foi vitimado quando seus sistemas já se encontram comprometidos. Na maioria das vezes, os atores dentro deste cenário atuam anonimamente, o que é possibilitado pelas características da própria Internet (GUEDES *et al*, 2012; MACHADO, 2011).

Os agentes podem ser estatais ou não-estatais. Os primeiros são organismos institucionais de um Estado constituído, como organizações, centros e agências de

6 "Pessoa que viola a segurança de sistemas informáticos; [...]" (INFOPEDIA, 2013).

governo. Os não-estatais são pessoas ou organizações contratadas pelo Estado para atuar no ciberespaço, com objetivos definidos. Esta ação governamental visa isentar sua iniciativa e ocultar suas intenções (CIBERGUERRA, 2013).

O ambiente operacional é o ciberespaço ou "Espaço Cibernético" (E Ciber). A Nota de Coordenação Doutrinária NCD 04/2013 - C Dout - Fundamentos da Inteligência Militar Terrestre conceitua esse ambiente como "o espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas ou são armazenadas".

Os ataques nesse novo ambiente operacional são promovidos por meio de negação de serviços ou de intrusões ilícitas a computadores ou redes, no intuito de implantar dispositivos maliciosos, normalmente visando destruir ou comprometer algum equipamento (sabotagem), ou apropriar-se indevidamente de informações (espionagem). Em geral, os potenciais alvos são infraestruturas críticas de funcionamento de um país, como o serviço financeiro, de segurança, de saúde, de transportes, ou redes de telefonia, energia elétrica, gás e água.

Do ponto de vista militar, as redes de computadores, fundamentais para o tráfego de informações e para o comando e controle das operações, são sistemas críticos e tornam-se alvos por demais sensíveis.

A guerra cibernética passou a ser considerada uma das principais ameaças à segurança nacional, superando até mesmo ameaças terroristas. Os ataques cibernéticos tornaram-se preocupação dos governos de diversos países, que têm aumentado o investimento no setor. Claramente, as maiores economias do mundo saíram na frente na proteção de seus sistemas digitais, pois o desenvolvimento tecnológico está intrinsecamente relacionado à prosperidade econômica. Estados Unidos, Coréia do Sul, Grã Bretanha, China, Irã, Rússia, estão entre os países que tomaram a iniciativa (BEZERRA, 2009).

No Brasil não foi diferente. Em 2010, foi criado o Centro de Defesa Cibernética (CD Ciber), com a responsabilidade de coordenar e integrar as atividades de defesa cibernética no âmbito do MD, conforme preconiza a END (CARNEIRO, 2013; END, 2008; Portaria nº 3.405-MD, 2012). Porém, existem ainda muitas questões legais a serem debatidas, principalmente em foro internacional, como assuntos relativos às discussões técnicas e jurídicas neste setor.

Alguns eventos internacionais que demonstraram o crescimento do poder dos ciberataques e provaram a necessidade de as nações preocuparem-se mais com segurança cibernética:

- **os ataques à Estônia**: País tecnológico, altamente dependente da Internet, foi alvo de ciberataques durante três semanas do mês de abril de 2007, vitimando *sites* do governo, de bancos, de jornais e de emissoras de televisão. Mesmo havendo controvérsias, a ação foi creditada a *hackers* russos, em retaliação à retirada de uma estátua de um soldado soviético do centro de Tallinn, a capital da Estônia;

- **Guerra na Ossétia do Sul**: conflito que opôs forças separatistas ossetas, apoiadas pela Rússia, contra a Geórgia, por questões territoriais. Historicamente, foi o primeiro conflito em que a ciberguerra ocorreu paralelamente com as ações militares no terreno;

- **os ataques chineses aos Estados Unidos**: empresas do ramo de Tecnologia da Informação dos EUA foram vítimas de ataques de *hackers* chineses, em janeiro de 2010, entre elas a Microsoft e a Google, sendo esta última o principal alvo. O objetivo dos ataques era o monitoramento de mensagens eletrônicas de ativistas de direitos humanos contrários ao governo chinês e o acesso a informações sobre investigações realizadas pelo governo dos Estados Unidos. A China, por sua vez, negou todas as acusações e defendeu sua política de censura;

- **caso *Stuxnet***: em 2010, o sistema industrial conhecido como Supervisory Control and Data Acquisition[7] (SCADA), da empresa alemã Siemens, que controla as centrífugas de enriquecimento de urânio do Irã, foi vitimado pela ação do *worm Stuxnet*, comprometendo o programa nuclear daquele País. O vírus demonstrou a potencialidade de uma ciberarma quando aplicada com objetivos políticos e militares; e

- **espionagem americana (Programa *PRISM*)**: em maio de 2013, o ex-analista de inteligência americano Edward Snowden tornou público detalhes de vários programas altamente confidenciais de vigilância eletrônica do Governo dos Estados Unidos. A revelação deu detalhes do projeto de monitoramento global, denominado *PRISM*, que monitorou comunicações e tráfego de informações na Internet e conversas telefônicas de cidadãos americanos e de outros países. Essa atuação pode ser considerada como um caso de obtenção de dados para a produção de Inteligência oriunda da fonte cibernética.

Segundo Chade (2013), Hamadoun Touré, Secretário-Geral da União Internacional de Telecomunicações (UIT), declarou em Genebra, na Suíça, que "o mundo já vive uma guerra cibernética e a prática de espionagem na rede é algo generalizado entre os governos", ou seja, não deveria mais haver surpresa diante das denúncias de espionagem.

2.2. Inteligência Cibernética

O conceito de Inteligência Cibernética não está consolidado no Ministério da Defesa ou mesmo no Exército Brasileiro. É provável que esse termo nem venha a ser utilizado dentro da reformulação da Doutrina de Inteligência que está sendo realizada pelo Exército Brasileiro. A NCD 04/2013 - C Dout - Fundamentos da Inteligência Militar Terrestre não cita o termo Inteligência Cibernética em nenhum momento, mas apenas a Fonte Cibernética, sendo definida como "[...] obtenção de dados, protegidos ou não, obtidos no E Ciber".

7 Sistemas de Supervisão e Aquisição de Dados - Tradução do Autor

Apesar dessa tendência, o termo ainda está sendo utilizado pelo Exército Brasileiro como cognome[8] de um dos projetos estruturantes do setor estratégico cibernético, sob coordenação do Exército Brasileiro, denominado "Estrutura para a produção do conhecimento oriundo da Fonte Cibernética (Projeto Inteligência Cibernética)".

Pesquisando a literatura disponível, não somente é possível encontrar diversas definições para o termo Inteligência Cibernética, como também diferentes significados.

Por exemplo, Coleman (2011) define Inteligência Cibernética como "todas as ações e atividades realizadas por ou em nome de uma organização, concebidas e utilizadas para identificar, rastrear, medir e monitorar informações de ameaças digitais, dados e conhecimentos sobre as operações de um adversário".

Já Marcelino (2013) conceitua como "nada mais que a própria atividade de Inteligência de Estado e/ou Operacional voltada para os meios eletrônicos", enquanto Wendt (2011) afirma que a Inteligência Cibernética tem "o objetivo de subsidiar decisões governamentais ou não nas ações preventivas de segurança no mundo virtual e de repressão aos delitos ocorridos".

Essas e outras várias definições mostram que o termo Inteligência Cibernética não está sendo usado somente para a Inteligência de Estado, mas também no meio civil, tanto no Brasil quanto no exterior, onde as empresas mostram-se muito preocupadas com a espionagem e sabotagem industrial, dentre outras ações no Espaço Cibernético.

A procura por profissionais na área de Inteligência Cibernética pode ser facilmente verificada na Internet. No *site* de procura de empregos INDEED (http://www.indeed.com), nos Estados Unidos da América (EUA) foi possível encontrar 997 vagas ofertadas para o cargo de *Cyber Intelligence Analyst* (Analista de Inteligência Cibernética) ou semelhante (dados de 9 de agosto de 2013).

Em outro *site* de oferta de empregos, o USAJOBS (https://www.usajobs.gov/GetJob/ViewDetails/348847300), foi achado um anúncio para o desempenho da função de *Senior Cyber Intelligence Analyst*[9] (Analista Sênior de Inteligência Cibernética). O salário proposto era de US$ 105.211,00 a US$ 155.500,00 por ano, e entre suas atribuições estava "realizar pesquisas e análises relacionadas às ameaças cibernéticas no setor financeiro a fim de produzir, editar e supervisionar a elaboração de produtos de Inteligência Cibernética sobre questões de importância nacional que afetam o sistema financeiro dos EUA".

No *site* de busca de empregos, da empresa americana CGI (http://jobs.cgi.com/job/Ft-Meade-Cyber-Intelligence-Analyst-Job-AL/2027412/?feedId=4&utm_source=Indeed), foi encontrado uma vaga para *Cyber Intelligence Analyst* (Analista de Inteligência Cibernética) no Comando Cibernético dos

8 Epíteto, apelido (www.dicionarioinformal.com.br). (acesso em 26 ago 2013)

9 Cargo direcionado ao trabalho no Department of the Treasury, semelhante ao Ministério da Fazenda Brasileiro (dados de 9 de agosto de 2013).

Estados Unidos (*U.S. Army Cyber Command* - USCYBERCOM), em *Fort Meade*, Estado de *Maryland*, sede da NSA.

O *site* define, ainda, aspectos julgados necessários para assumir o cargo de Analista de Inteligência Cibernética (tradução nossa):

> Principais Deveres e Responsabilidades:
>
> - realizar pesquisas e avaliar a Inteligência Cibernética de todas as fontes para desenvolver uma análise aprofundada e uma avaliação sobre as ameaças às redes críticas e infraestruturas críticas.
> - realizar análise, coordenação e interação complexas de Inteligência Cibernética, por meio de uma ampla gama de atividades conjuntas e interagências.
> - trabalhar em estreita colaboração com outros profissionais técnicos, forenses e de gestão de incidentes, para desenvolver uma melhor compreensão das intenções, objetivos e atividades de atores em ameaças cibernéticas.
> - analisar eventos de rede para determinar o impacto sobre as operações atuais e realizar pesquisas em todas as fontes para determinar a capacidade de aconselhamento e intenção.
> - preparar avaliações e perfis de ameaças cibernéticas em eventos atuais, com base em pesquisas em fontes de informações classificadas e abertas.
> - correlacionar dados sobre ameaças a partir de várias fontes.
> - desenvolver e manter procedimentos analíticos para atender mudanças de exigências.
> - coletar dados usando uma combinação de métodos de inteligência padrão e processos de negócios.
> - produzir artigos de alta qualidade, apresentações, recomendações e conclusões para funcionários seniores de inteligência do governo dos EUA e de operações de rede.
>
> Conhecimentos, habilidades, capacidades e competências necessárias:
>
> - credenciamento ultrassecreto ativo e elegibilidade para Polígrafo de Contrainteligência.
> - experiência em aplicação da Garantia da Informação e dos conceitos, práticas e ferramentas de Defesa de Redes de Computador.
> - conhecimento profundo de segurança da informação e de segurança cibernética.
> - capacidade para transmitir complexa informação técnica e de programação, muitas vezes verbalmente e em atualizações visuais, relatórios de situação e instruções.
> - capacidade de trabalhar de forma independente.
> - habilidade para escrita e apresentações.
> - capacidade para trabalhar bem em equipe.
>
> (tradução dos autores).

Além da oferta de empregos, também foi possível encontrar ofertas de serviços na área de Inteligência Cibernética. A empresa brasileira APURA *Cyber Intelligence Services*, por exemplo, oferece em seu *site* (http://www.apuratrustedservices.com/apura/apura-cyber-intelligence-services/) os seguintes serviços de Inteligência:

> ***InstaIntel* - Consciência Situacional sobre Ameaças Cibernéticas Regionais**. Tome decisões acertadas e trabalhe na mitigação de riscos que realmente importam para sua organização com inteligência objetiva, proativa e contextualizada com o Brasil e a região que o cerca. Priorize as ameaças que causam mais

perdas, conheça as ameaças que afetam outras organizações do mesmo mercado, conheça as ameaças globais e a implicação na realidade do Brasil. Deixe de gerenciar segurança e passe a mitigar e gerenciar riscos. Este tipo de inteligência é entregue na forma de "*feeds*" de diversas categorias.

***DeepIntel* - Pesquisa de Inteligência sobre Ameaças Cibernéticas.** Coleta abrangente de dados em fontes abertas (*Open Source Intelligence* - OSINT) **e não abertas**, **(grifo nosso)** análise e produção de relatórios de inteligência com alta relevância para sua organização. Consideramos a análise negativa, discutindo exaustivamente elementos dos dados coletados que não apóiem ou pareçam contradizer padrões.

Essa diversidade de definições também leva a uma dualidade na interpretação do termo. Em alguns momentos, o termo Inteligência Cibernética é usado como a "produção de conhecimentos de inteligência com dados oriundos da fonte cibernética" e, em outras oportunidades, como a "produção de conhecimentos de inteligência para serem usados no contexto de operações ou da proteção cibernética". No primeiro caso, os dados oriundos da fonte cibernética são utilizados integrados com outras fontes (humanas, sinais e imagens) para a produção de conhecimentos de inteligência, enquanto que no segundo caso os conhecimentos de inteligência produzidos são utilizados diretamente para uso em operações no ambiente cibernético.

O contexto utilizado será o primeiro, ou seja, a Inteligência Cibernética será tratada sendo a "atividade de obtenção de dados, protegidos ou não, no espaço (ou fonte) cibernético, com o objetivo de produção de conhecimentos de inteligência".

No Exército Brasileiro, a Inteligência Cibernética não somente está ligada à Inteligência Militar como está nela inserida. A fonte cibernética está classificada como a quarta fonte na NCD 04/2013 - C Dout - Fundamentos da Inteligência Militar Terrestre, além das fontes de humanas, sinais e imagens.

3. USO DA FONTE CIBERNÉTICA NA ATIVIDADE DE INTELIGÊNCIA

O uso da fonte cibernética na atividade de inteligência já está previsto na Política Cibernética de Defesa (MD31-P-02) (2012, p. 13-20):

DOS OBJETIVOS

2.1. Objetivos

São objetivos da Política Cibernética de Defesa: [...]

colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR); [...]

DAS DIRETRIZES

3.1. Definição

3.2.3. Diretrizes atinentes ao Objetivo Nº III - colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o SINDE e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o GSI/PR:

adequar a doutrina de Inteligência de modo a

> inserir a fonte cibernética no contexto da integração de fontes de dados visando à produção de conhecimento;
>
> criar estruturas de Inteligência Cibernética, conforme a necessidade dos órgãos centrais de Inteligência das FA e do SMDC, para aplicar métodos científicos e sistemáticos, buscando extrair e analisar dados oriundos da fonte cibernética, produzindo conhecimento de interesse; [...]

3.1. Funções, Habilidades e Competências

Em setembro de 2012, foi realizado na EsIMEx o 1º Simpósio de Inteligência Cibernética, que reuniu palestrantes e participantes das Forças Armadas e de diversas organizações governamentais e acadêmicas, como a Agência Brasileira de Inteligência (ABIN), as Polícias Federal, Militar e Civil, a Universidade de Brasília (UnB), dentre outras.

Um dos eventos desse Simpósio foi a realização de uma sala temática com o título "Recursos Humanos para a Inteligência Cibernética". Uma das conclusões obtidas foi de que a fonte cibernética na atividade de Inteligência será utilizada por dois tipos de profissionais: o **agente** e o **analista**. Essa conclusão, mesmo não estando consolidada no âmbito do Ministério da Defesa ou mesmo no Exército, é coerente com artigos e publicações encontrados sobre o assunto.

3.1.1. Agente de Inteligência

O agente de inteligência é o elemento especializado responsável pela obtenção de dados. Esse procedimento dar-se-ia por meio de ações de busca, que são atividades planejadas e executadas com esse intuito. Para tanto, necessita de pessoal especializado e o emprego de técnicas específicas. Algumas dessas podem ser adaptadas para utilização no Espaço Cibernético. Boa parte desse conjunto de conhecimentos pode ser encontrada na ementa do Curso de Guerra Cibernética para Oficiais, conduzido pelo Centro de Instrução de Guerra Eletrônica.

Uma vez que o trabalho no ambiente cibernético utiliza intensamente os meios de TI, para que o agente possa atuar de maneira eficiente nesse ambiente, também serão necessários conhecimentos específicos em algumas áreas da Ciência da Computação.

Apresenta-se a seguir uma sugestão de repertório de conhecimentos, baseada nas ementas dos cursos de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG) (http://www.dcc.ufmg.br/dcc/images/ementas_computacao.pdf), da Universidade Federal do Pará (UFPA) - (http://www.ufpa.br/informatica/interna.php?page=estrutura) e do curso de Análise Forense Computacional da empresa CLAVIS, especializada em soluções e treinamentos de Segurança da Informação, como Segurança em Aplicações *Web*, Teste de Invasão e Análise de Risco (http://www.clavis.com.br/curso/forense_computacional/), adaptadas pelos autores (acessadas em 27 ago 2013):

a) **Sistemas Operacionais:** tipos e estrutura dos sistemas operacionais; processos e *threads*; sincronização e comunicação entre processos; alocação de recursos e *deadlocks*; gerência do processador; gerência de memória; sistemas de arquivo; gerenciamento de entrada e saída; sistemas operacionais de tempo real; e virtualização.

b) **Redes de Computadores:** topologias físicas e topologias lógicas; dispositivos de redes; cabeamento e infraestrutura; modelo de referência OSI e TCP/IP; camadas da arquitetura de rede TCP/IP; protocolos e suas funções; endereçamento; roteamento; tipos de redes (LAN, MAN, WAN, etc); e redes sem fio.

c) **Segurança de Redes e Sistemas:** controle de acesso físico e lógico; gerência de riscos; plano de continuidade de negócio; tratamento de incidentes e de problemas; categorias de ataques e proteções de redes e sistemas; monitoramento de redes; criptografia, autenticação, assinatura e certificação digital; *firewalls*; auditoria de redes e sistemas; e política de segurança da informação e comunicações.

d) **Linguagens de Programação:** linguagens de alto e baixo nível; algoritmos; representação de dados; testes e depuração; modularização e recursão; métodos de ordenação e de busca; acesso a arquivos; orientação a objetos; máquinas virtuais e *garbage collectors*; uso de componentes; programação por camadas; persistência de dados; programação e processamento paralelo; sistemas distribuídos; processos e sincronização entre processos; e programação com memória compartilhada.

e) **Análise Forense Computacional:** processo investigativo; legislação vigente nacional e internacional; funcionamento e abstrações de sistemas de arquivos; recuperação de dados e *backup*; dados, informações e evidências (persistência dos dados; ordem de volatilidade; aquisição, duplicação e preservação); esteganografia; captura e análise de tráfego de rede (coleta passiva e ativa; análise de logs; análise de pacotes; e tunelamentos); análise de dispositivos móveis; análise de artefatos dinâmica e estática (técnicas de confinamento; monitoramento de chamadas de sistema e de bibliotecas; e proteções contra engenharia reversa).

3.1.2. Analista de Inteligência

O analista de inteligência é o profissional que, mediante processo mental elaborado, realiza a produção de conhecimentos após a reunião de dados e conhecimentos de diferentes fontes (Manual MD35-G-01 - Glossário das Forças Armadas, 2007). Brennen (2008) vai um pouco além e escreve o seguinte (tradução dos autores):

> A formação de analistas cibernéticos será complexa, misturando: matemática, operações de computadores e redes em nível de componentes de hardware e software, computação forense, teoria militar geral, conhecimento de infraestrutura e indústrias críticas, operações ofensivas e defensivas, inteligência estratégica e compreensão das práticas de tecnologia da informação estrangeiras, entre outros conhecimentos e habilidades diversas.

Essa proposta apresentada por Brennen (2008) extrapola o que é pensado atualmente pela doutrina do Exército Brasileiro, que prevê uma atuação menos técnica e complexa.

Mesmo sem uma especialização específica, os analistas de Inteligência já utilizam exaustivamente a Internet - que representa uma grande parcela da fonte cibernética - em suas pesquisas em fontes abertas.

Como a função de um Analista de Inteligência Cibernética contempla também a análise de dados obtidos dessa fonte, uma sugestão seria o acréscimo de disciplinas específicas nos Cursos Avançado e Intermediário de Inteligência para Oficiais da EsIMEx, principalmente no que se refere à navegação segura em ambiente *web*.

O acréscimo de disciplinas específicas para trabalhos na fonte cibernética permitirá que o Analista de Inteligência, hoje formado pelos cursos da EsIMEx, execute esse tipo de tarefa, evitando a criação de uma nova função e um curso específico para isso, alinhando-se ao que consta na Nota de Coordenação Doutrinária - NCD 04/2013 - C Dout - Fundamentos da Inteligência Militar Terrestre:

> O Ciclo de Inteligência não se altera com esse incremento e tampouco será necessário qualificar novos tipos de analistas para lidar com ele. Entretanto é evidente que os analistas devem estar preparados - se possível especializados - para processar os dados oriundos de fontes tecnológicas e orientar os técnicos que irão processar tais dados. A Inteligência, portanto, continua a ser uma disciplina única, apesar da ampliação de seu campo de atuação. (NCD-04/2013-C Dout, pág 15).

3.2. Critérios para a Seleção do Pessoal

Para a seleção de militares que irão atuar com a fonte cibernética na Atividade de Inteligência, a abordagem conceitual exposta até o momento indica que os critérios previstos para a seleção de pessoal no SIEx são perfeitamente aplicáveis, desde que no processo seletivo sejam acrescidos os conhecimentos técnicos específicos descritos no item 3.1 - Funções, Habilidades e Competências.

No que tange ao processo de desligamento desses militares do sistema, cabe ressaltar que são elementos detentores de conhecimentos sensíveis e dominam técnicas complexas para operar no ambiente cibernético, exigindo um processo de desmobilização coerente com as normas em vigor.

4. RESULTADOS E DISCUSSÕES

No intuito de subsidiar o trabalho, foi elaborado um questionário com o objetivo de coletar dados e responder algumas questões relativas aos problemas elencados.

Para a presente pesquisa foi definida como população alvo, militares integrantes das seguintes organizações do Exército: Departamento de Ciência e Tecnologia (DCT); Centro de Inteligência do Exército (CIE); Centro de Defesa Cibernética (CDCiber); Centro Integrado de Telemática do Exército (CITEx); Centro de Instrução de Guerra Eletrônica (CIGE); e Escola de Inteligência Militar do Exército (EsIMEx). A pesquisa também contemplou o universo dos concludentes do Curso de Guerra Cibernética para Oficiais, realizado no ano de 2012.

A população levantada para a presente pesquisa foi de 45 (quarenta e cinco) militares, que preenchem o requisito de estar trabalhando ou ter trabalhado nas organizações militares acima elencadas.

Dos 45 (quarenta e cinco) militares que receberam o questionário, 34 (trinta e quatro) responderam de forma integral, o que resultou nos dados apresentados na sequência.

4.1. Caracterização do Ambiente Social

Na caracterização do ambiente social, os dados coletados nos questionários deixam claro que o militar que atuará na Inteligência Cibernética desempenhará suas funções tanto individualmente quanto em equipe, perfazendo um total de 76,5% dos dados coletados neste sentido.

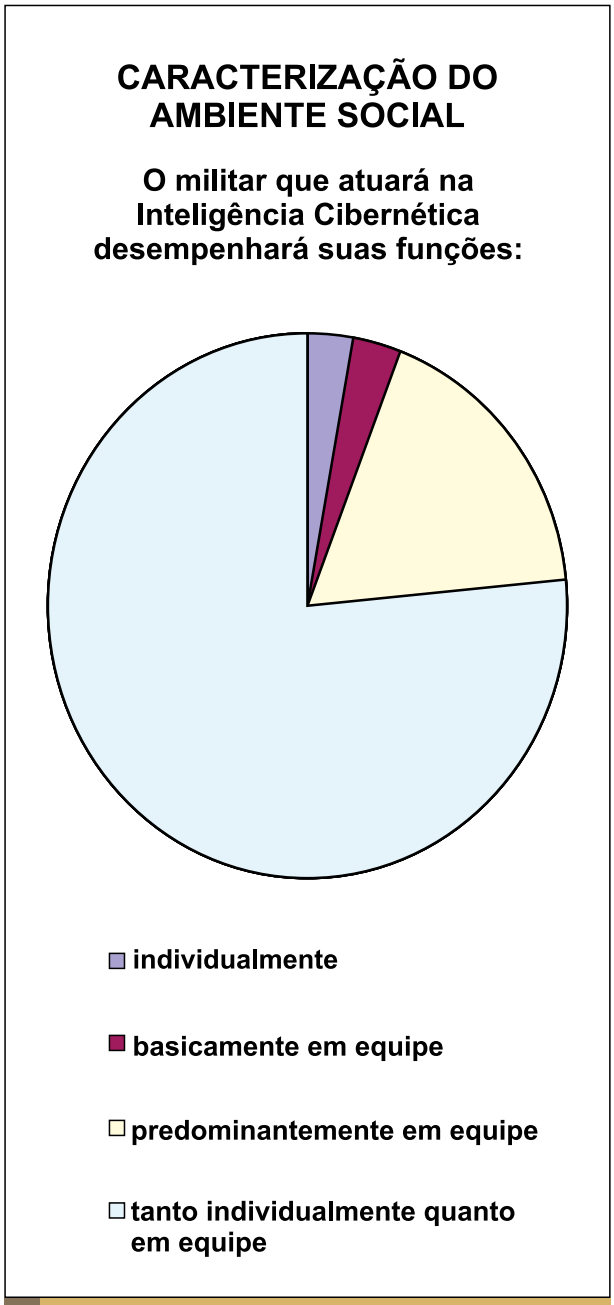


Gráfico 1 - Caracterização do ambiente social
Fonte: Autores

4.2. Requisitos Pessoais

No levantamento das características pessoais que devem compor o perfil profissiográfico do militar vocacionado a atuar no ambiente cibernético, a população em estudo elencou como requisitos considerados **indispensáveis** a "integridade", a "lealdade", a "discrição" e a "honestidade".

Como requisito pessoal **necessário**, o item mais destacado foi o "equilíbrio emocional" como um dos principais atributos a serem evidenciados pelo militar que atuará no ambiente cibernético. Os demais itens não obtiveram uma pontuação significativa que os destacasse.

No requisito pessoal **recomendável**, o item que obteve maior pontuação foi "resistência", não sendo significativo o resultado obtido pelos demais itens.

Finalmente, o item apontado no requisito pessoal como **desnecessário** foi a "persuasão".

4.3. Caracterização das Tarefas do Profissional

No estudo das tarefas que serão executadas pelo militar que irá desempenhar funções ligadas a exploração da fonte cibernética, a que apresentou maior indicação por parte dos entrevistados foi "executar coletas", com 16 (dezesseis) indicações no grau de importância 1 - "mais importante", seguido da tarefa "executar ações de busca", que foi indicada por 9 (nove) entrevistados no grau de importância 1 - "mais importante'. Entretanto, ao se analisar o resultado final, pode-se observar que a tarefa

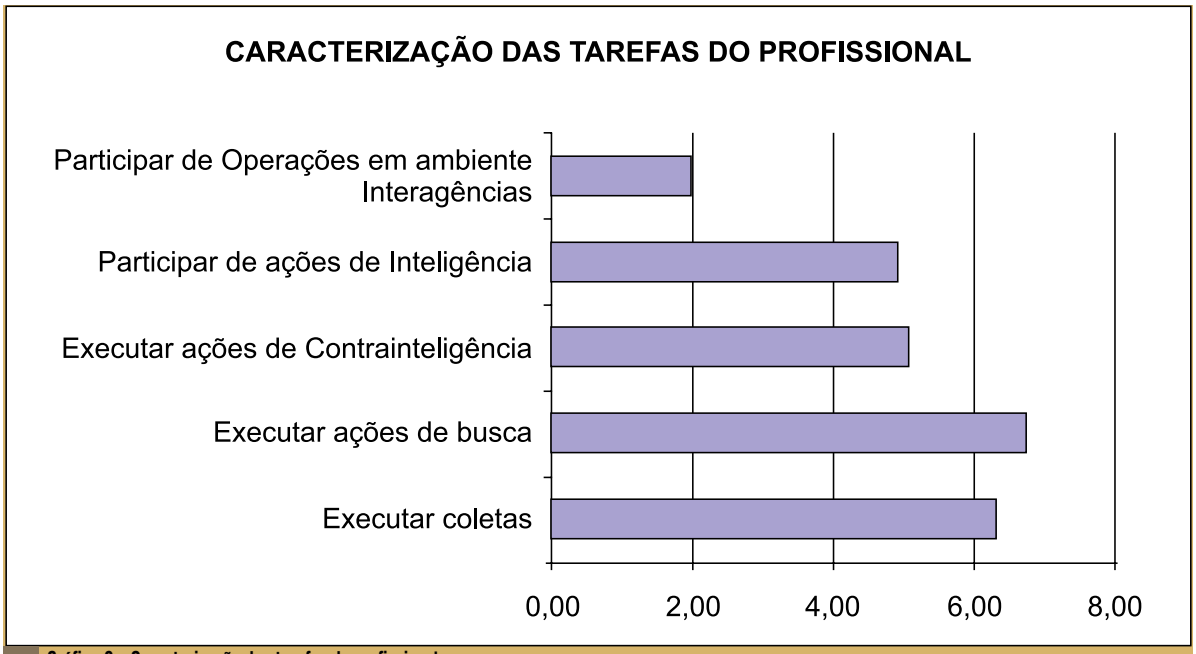


Gráfico 2 - Caracterização das tarefas do profissional
Fonte: autores

de maior importância a ser desenvolvida pelo militar é "executar ações de busca".

Diante dos resultados obtidos pela pesquisa com profissionais que labutam no ambiente cibernético, observa-se que o profissional para explorar ou realizar análise para a produção do conhecimento de inteligência sobre as ameaças e oportunidades nesse ambiente deverá possuir características peculiares no campo cognitivo, afetivo e psicomotor, que lhe facultarão a capacidade de operar materiais e empregar técnicas específicas para a obtenção de dados para a produção de inteligência oriunda desse ambiente operacional.

5. CONCLUSÕES E SUGESTÕES

O objetivo deste trabalho foi identificar os perfis mais adequados para os militares que trabalharão com a fonte cibernética na Atividade de Inteligência, analisando os atributos da área afetiva (AAA), as competências e as habilidades que serão necessárias para que o militar atue no ambiente cibernético, inferindo acerca da sua influência sobre a Atividade de Inteligência.

O trabalho baseou-se na pesquisa em diversas fontes bibliográficas, na Internet e na análise de questionário elaborado pelos autores e distribuído a militares com conhecimento na área da Segurança da Informação.

A pesquisa focou a importância da exploração da fonte cibernética para a Atividade de Inteligência e constatou a necessidade da criação de cargos e funções em duas áreas específicas, ou seja, uma de agente de Inteligência Cibernética, para a obtenção de dados negados e pesquisas especializadas em fontes abertas e, outra de analista da fonte cibernética, para a produção do conhecimento.

Concluiu-se que o agente deve atuar em ações de busca na fonte cibernética (ex-

ploração cibernética) e em coletas especiais, realizadas pela utilização de ferramentas e técnicas especializadas[10] para pesquisas aprofundadas e seletivas de dados em fontes abertas.

Cabe destacar que o trabalho do agente de Inteligência Cibernética diferencia-se do elemento especializado em guerra cibernética, pois este último realiza ainda as ações de proteção e ataque naquele ambiente (MD30-M-01 - Doutrina de Operações Conjuntas - Volumes 1).

Assim como um Analista de Inteligência de Imagens obtém frações significativas para produzir conhecimentos na análise de uma fotografia aérea, o Analista da Fonte Cibernética deve realizar a produção de conhecimentos por meio da análise de dados oriundos daquela fonte, normalmente não inteligíveis para um analista comum. Cita-se, como exemplo:

- análise de cabeçalhos de *e-mails*, um artefato comum do qual se pode extrair informações valiosas, desde que possuindo a capacidade técnica para tal; e

- análise de *logs* diversos, como de eventos do sistema operacional, de rede de dados, de segurança de sistemas, entre outros.

Em um segundo momento, baseado nas respostas obtidas por meio do questionário distribuído, concluiu-se que, para o trabalho de Inteligência utilizando a fonte cibernética, são atributos indispensáveis aos militares a "integridade", a "lealdade", a "discrição" e a "honestidade". Da mesma forma, foi considerado como atributo necessário o "equilíbrio emocional", como recomendável a "resistência" e como desnecessário o atributo "persuasão".

Os atributos estudados estão relacionados à Atividade de Inteligência oriunda da fonte cibernética como um todo e não de forma isolada, ou seja, enquadram-se tanto para o agente quanto para o analista. Para isso, deve haver uma pesquisa técnico-pedagógica especializada mais aprofundada para fins de elaboração do perfil profissiográfico e do relatório de análise ocupacional de cada um desses atores.

Em relação às competências e às habilidades para exercer as funções identificadas na Atividade de Inteligência utilizando a fonte cibernética, concluiu-se ainda, que são indispensáveis conhecimentos específicos nas seguintes áreas da Ciência da Computação: Sistemas Operacionais; Redes de Computadores; Segurança de Redes e Sistemas; Linguagens de Programação; e Análise Forense Computacional.

Com referência ao ambiente social, infere-se que o militar que atuará na Inteligência Cibernética deverá desempenhar suas funções tanto individualmente quanto em equipe. Essa conclusão é corroborada pelas demandas de profissionais que tenham este perfil no mercado de emprego dos EUA.

Para a seleção de militares que irão atuar com a fonte cibernética na Atividade

10 Como exemplo de técnica especializada pode-se citar o *Google Hacking*, que envolve o uso de operadores avançados no motor de busca do *Google* para localizar sequências específicas de texto dentro de resultados de pesquisa (OLIVEIRA, 2011).

de Inteligência, o estudo indica que os critérios previstos para a seleção de pessoal para o SIEx são perfeitamente aplicáveis, desde que no processo seletivo seja considerado, como pré-requisito, que os candidatos possuam os conhecimentos técnicos específicos anteriormente descritos.

Sugere-se uma revisão das Funções de Inteligência previstas nas normas existentes para a seleção de pessoal para o SIEx, incluindo as novas funções de Inteligência relacionadas nesta pesquisa.

Para que sejam supridas as demandas recentes da necessidade de um Analista da fonte cibernética, propõem-se as seguintes linhas de ação:

- Linha de Ação 1: criação de um Curso ou Estágio de Analista de Inteligência da Fonte Cibernética, para militares não possuidores de cursos de Inteligência, mas possuidores de conhecimentos técnicos na área de TIC; e

- Linha de Ação 2: criação de um Curso ou Estágio de Análise de Inteligência da Fonte Cibernética, visando prover aos analistas possuidores dos Cursos Avançado ou Intermediário de Inteligência, conhecimentos necessários para análise de dados técnicos oriundos da fonte cibernética, formas de navegação segura e sigilosa em ambiente *web*, além de medidas de contrainteligência cibernéticas.

Para a criação de cursos e estágios no Exército Brasileiro são necessários diversos estudos e a elaboração de documentos, como Perfil Profissiográfico, Documento de Currículo, Plano de Disciplinas (PLADIS), Relatório de Análise Ocupacional e Catálogo de Cargos e Atribuições.

Como esse processo demanda certo tempo, propõe-se, como linha de ação alternativa, o acréscimo de disciplinas nos cursos já existentes (Cursos Avançado e Intermediário de Inteligência para Oficiais), visando a completar os conhecimentos técnicos considerados indispensáveis.

Para que o militar desempenhe o cargo ou função de Agente de Inteligência Cibernética, sugerem-se:

- Linha de Ação 1: a criação de um Curso ou Estágio de Agente (ou Operador) Cibernético, para militares não possuidores do Curso Básico de Inteligência, mas possuidores de conhecimentos técnicos na área de TIC; e

- Linha de Ação 2: a criação de um Curso ou Estágio de Busca na Fonte Cibernética, visando prover aos militares possuidores do Curso Básico de Inteligência conhecimentos necessários para ações de busca e coletas especializadas na fonte cibernética.

Algumas questões não puderam ser respondidas neste trabalho, como o levantamento dos atributos psicomotores indispensáveis e os desejáveis para que se possa atuar na exploração da fonte cibernética

Concluindo, cabe salientar a relevância no cenário internacional dos temas ligados ao domínio e exploração do ambiente cibernético o que avulta a importância e a premência para a implementação das ações propostas nesse artigo que, de certa forma, contribuirão para o desenvolvimento de capacidades no profissional de inteligência para operar na complexa e difusa dimensão cibernética.

REFERÊNCIAS

BEZERRA, Marcelo. **Cyberwar**. São Paulo, SP, 4 ago. 2009. Disponível em: <http://segdigital.blogspot.com.br/2009/08/cyberwar.html>. Acesso em: 7 ago. 2013.

BRANCO, Rodrigo Rubira. In: **III Seminário de Defesa Cibernética**. Brasília, DF: Centro de Inteligência do Exército (CIE), 2012.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional (LBDN)**. Brasília, DF, 2012.

_____. _____. **MD30-M-01: Doutrina de Operações Conjuntas / Volumes 1, 2 e 3**. Portaria Normativa nº 3.810/MD, de 8 de dezembro de 2011. 1. ed. Brasília, DF, 2011.

_____. _____. **MD31-P-02: Política Cibernética de Defesa**. Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012. Brasília, DF, 2012.

_____. _____. **MD35-G-01: Glossário das Forças Armadas**. Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007. 4. ed. Brasília, DF, 2007.

_____. _____. Portaria nº 3.405-MD, de 21 de dezembro de 2012: **Atribui ao Centro de Defesa Cibernética (CDCiber) a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa**. Brasília, DF, 2012.

_____. Estado-Maior do Exército. Exército Brasileiro. **NCD 04/2013-C Dout.__: Fundamentos da Inteligência Militar Terrestre**. 1. ed. Brasília, DF, 2013.

_____. _____. _____. Portaria nº 005-DEP, de 24 de janeiro de 2008: **Glossário de Termos e Expressões de Educação e de Cultura**. Rio de Janeiro, RJ, 2008.

_____. _____. _____. Portaria nº 012-DEP, de 12 de maio de 1998: **Conceituação dos Atributos da Área Afetiva, para uso pelos Órgãos e Estabelecimentos de Ensino subordinados, coordenados ou vinculados técnico-pedagogicamente ao Departamento**. Rio de Janeiro, RJ, 1998.

_____. Presidência da República. **Decreto nº 5.484, de 30 de junho de 2005**: Aprova a Política de Defesa Nacional (PDN) e dá outras providências. Brasília, DF, 2005.

_____. _____. **Decreto nº 6.703, de 18 de dezembro de 2008**: Aprova a Estratégia Nacional de Defesa (END) e dá outras providências. Brasília, DF, 2008.

_____. _____. _____. _____. **Portaria nº 45-GSI, de 8 de setembro de 2009**: Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Brasília, DF, 2009.

BRENNEN, Jonh E. **Intelligence Support to Cyber Operations**. 2008. Disponível em: <http://innovative-analytics.com/docs/IntelligenceSupportCyberOperations.pdf>. Acesso em: 3 ago. 2013.

CARNEIRO, João Marinonio Enke. **Os setores estratégicos da END - O Setor Cibernético**. Palestra proferida na Universidade Federal de Mato Grosso do Sul (UFMS). In: CURSO DE EXTENSÃO DE DEFESA NACIONAL, VII, 2013. Campo Grande/MS, 6 jun. 2013. Disponível em: <http://www.defesa.gov.br/projetosweb/cedn/arquivos/palestras-junho-2013/os-setores-estrategicos-da-end-cibernetico.pdf>. Acesso em: 8 ago. 2013.

CHADE, Jamil. **Guerra cibernética e espionagem são disseminadas, diz agência da ONU**. Genebra, Suíça, 2013. Disponível em: <http://www.estadao.com.br/noticias/internacional,guerra-cibernetica-e-espionagem-sao-disseminadas-diz-agencia-da-onu,1053701,0.htm>. Acesso em: 7 ago. 2013.

CIBERGUERRA. In: **Infoescola, Navegando e Aprendendo**, 2013. Disponível em: <http://www.infoescola.com/informatica/ciberguerra/ >. Acesso em: 11 set. 2013.

COLEMAN, Kevin. **Cyber superiority requires intelligence edge**. 2011. Disponível em: <http://defensesystems.com/articles/2011/05/03/digital-conflict-cyber-intelligence-capabilities.aspx>. Acesso em: 3 ago. 2013.

GUEDES, Sylvio; BRASIL, Thâmara; TEIXEIRA, João Carlos (Ed.). Inimigos invisíveis. **Em Discussão!**: Revista de audiências públicas do Senado Federal, Brasília, DF, n. 10, p.38-39, mar. 2012. Disponível em: <http://www.senado.gov.br/NOTICIAS/JORNAL/EMDISCUSSAO/upload/201201%20-%20marco/pdf/em%20discuss% C3%A3o!_marco_2012_internet.pdf> . Acesso em: 7 ago. 2013.

INFOPEDIA. In: **Infopédia Encicopédia e Dicionários Porto Editora**. 2013. Disponível em: <http://www.infopedia.pt/lingua-portuguesa/hacker;jsessionid=iCAeJbt1uEip4S1hQrT1ew>. Acesso em: 11 set. 2013.

MACHADO, André. **Cresce número de ciberataques em que tecnologia e Internet são usadas como armas em guerras**. 2011. Disponível em: <http://oglobo.globo.com/tecnologia/cresce-numero-de-ciberataques-em-que-tecnologia-internet-sao-usadas-como-armas-em-guerras-2901730>. Acesso em: 16 mai. 2013.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**: Centro de Gestão e Estudos Estratégicos (CGEE), Brasília, DF, v. 14, n. 29, p. 21-46, jul./dez. 2009.

MARCELINO, Ítalo Adriano. **Inteligência Cibernética: você sabe o que é?** 2013. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34328&sid=15>. Acesso em: 28 jul. 2013.

OLIVEIRA, Maria. **O que é Google Hacking?** 2011. Disponível em: <http://blog.inurl.com.br/2011/01/o-que-e-google-hacking.html >. Acesso em 08 set. 2013.

RODRIGUES, Auro de Jesus. **Metodologia Científica**. São Paulo, SP: Avercamp, 2006.

WENDT, Emerson. Ciberguerra, Inteligência Cibernética e Segurança Virtual: alguns aspectos. **Revista Brasileira de Inteligência**: Agência Brasileira de Inteligência, Brasília, DF , n. 6, p. 15-26. abr. 2011.

O Emprego da Inteligência em Apoio as Operações de Informação - Estudo de Caso da Operação Humaitá

Paulo **César Pasini**[1]
Marcelo **Ferraz** dos Reis[2]

ABSTRACT

This paper presents a study case on the role of combat intelligence and its interrelation with the capabilities related to information (CRI), Support Operations Information (IOS) and Public Relation during HUMAITÁ Operation. The employment of intelligence in Military Operations is one of the activities contained in the Brazilian Army. It is, usually performed in military operations involving the operations of land forces against an opponent fully defined military doctrine. However, Brazilian Army has been increasing its participation interagency operations and subsidiary support operations shares or logistics cooperation which, in turn, show the importance of using all available CRI to facilitate the identification of threats and opportunities. Considering the recent technological and doctrinal advances of Land Forces and the increasing of using of talk about radios, telephones, tablets and many other devices to access social media by population, grows the importance of this work in order to highlighting the relevance of the interrelationship of intelligence, CRI, IOS and Public Relation in the context of the Information Operations. Finally, it shows how the Intelligence maximizes combat power of the Commander of all levels, especially the tactical level, for better understanding of the operating environment. At last, it concludes that the Information Operations should be employed to ensure the domain of Informational Environment by Military Forces and integration capabilities seeking synergy of efforts in the field of information.

Keywords: Intelligence, Capabilities Related to Information (CRI), Information Operations, Knowledge production and integration of CRI.

1 Oficial de Comunicações do Exército Brasileiro - Academia Militar das Agulhas Negras (AMAN); Mestre em Operações Militares - Escola de Aperfeiçoamento de Oficiais (EsAO); e Pós-graduado em Ciências Militares - Escola de Comando e Estado-Maior do Exército (ECEME).

2 Oficial de Comunicações do Exército Brasileiro - Academia Militar das Agulhas Negras (AMAN); Mestre em Operações Militares - Escola de Aperfeiçoamento de Oficiais (EsAO); e Pós-graduado em Ciências Militares - Escola de Comando e Estado-Maior do Exército (ECEME).

RESUMO

Este trabalho apresenta um estudo de caso sobre a função de combate Inteligência e a sua interrelação com as Capacidades Relacionadas à Informação (CRI) Operações de Apoio a Informação (OAI) e Comunicação Social (Com Soc) durante a Operação HUMAITÁ. O emprego da Inteligência nas Operações Militares é uma das atividades que constam da doutrina militar do Exército Brasileiro (EB), normalmente executado nas operações militares que envolvam a atuação da Força Terrestre contra um oponente plenamente definido. Entretanto, o EB está participando, cada vez mais, de operações interagências e operações de suporte a ações subsidiárias ou à cooperação logística que, por sua vez, denotam a importância da utilização de todas as CRI disponíveis para facilitarem a identificação das ameaças e oportunidades. Ao considerar-se os recentes avanços tecnológicos e doutrinários da Força Terrestre e a utilização cada vez maior de rádios *talk about*, aparelhos telefônicos, *tablets* e de diversos outros equipamentos de acessos a mídias sociais pela população, cresce de importância o presente trabalho, a fim de se destacar a importância da interrelação da Inteligência, das CRI, OAI e Com Soc no contexto das Operações de Informação (Op Info). Finalmente, constata-se que a Inteligência maximiza o poder de combate do comandante de qualquer nível, com destaque no nível tático, para a melhor compreensão do ambiente operacional. Conclui-se, também, que as Operações de Informação devem ser empregadas para garantir às forças militares o domínio do Ambiente Informacional e a integração de capacidades buscando sinergia de esforços no domínio da informação.

Palavras-chave: Inteligência, Capacidades Relacionadas à Informação (CRI), Operações de Informação, Produção do conhecimento e Integração das CRI.

1. INTRODUÇÃO

A Era da Informação e do Conhecimento permitiu que a digitalização atingisse todos os campos de poder de uma Nação, facilitando o surgimento de oportunidades para a implementação de sinergias entre todas as esferas envolvidas. Essa busca de iniciativas políticas, estratégicas e operacionais de integração decorre da complexidade dos sistemas que se proliferaram nos vários setores e da combinação das telecomunicações com a informática, o que aumentou substancialmente a velocidade com que a informação é produzida, disponibilizada e armazenada.

A conjuntura acima descrita, facilitada pela globalização, permitiu que todos os países direcionassem a condução e o emprego de suas Forças Armadas (FA) para obterem a informação decisiva no momento adequado, de modo a alcançar vantagem sobre o adversário. Essa mudança de perspectiva dos conflitos armados decorre do contínuo aumento de grupos transnacionais e/ou insurgentes, os quais, com ou sem apoio político e material de outros atores globais, ampliaram o caráter difuso das ameaças a serem enfrentadas com o emprego de Forças de Defesa e Segurança. (BRASIL, 2014, p. 2-1)

Os ministérios e/ou departamentos de defesa foram influenciados a elaborarem planejamentos de emprego conjunto de suas FA com as diversas agências e órgãos de todas as esferas, visando preservar ao máximo as vidas dos efetivos militares e civis presentes na Área de Operações (A Op). Nesse complexo cenário de integração sincronizada de combinações dos diversos tipos de sensores com capacidades e métodos específicos de comprometer os atributos da segurança da informação que estejam baseadas em qualquer sistema, quer seja ele um meio físico (documento, local-alvo em um ambiente, foto e outros), informatizado, de telecomunicações ou no próprio homem, deu origem as Operações de Informação (Op Info). Isso significa que as Op Info atuam sobre os campos cognitivo, informacional e físico da informação do oponente. (BRASIL, 2006, p. 41)

As Op Info visam afetar diretamente a disponibilidade, integridade, confidencialidade e autenticidade (MANDARINO, 2010, p. 50), atuando sobre os processos e os sistemas dos meios anteriormente elencados, podendo, em alguns casos, quando bem focalizadas e devidamente coordenadas, impedir o conflito armado. Além disso, as Op Info fornecem opções estratégicas ao nível político e alternativas operacionais e/ou táticas aos comandantes protegendo as forças amigas e os respectivos processos e sistemas de tomada de decisão dos elementos da Força Terrestre (F Ter) de um Teatro de Operações/Área de Operações (TO/A Op), quando ativado(a) (BRASIL, 2014c, p. 3-1).

A evolução da doutrina de Op Info passou a ocorrer em diversos Estados, como no Brasil, nos Estados Unidos da América (EUA) e no continente europeu. Concomitantemente a reformulação doutrinária, eles passaram a adotar também uma doutrina de Op Interagências visando conciliar interesses e coordenar esforços para a consecução de objetivos comuns, a fim de evitar a duplicidade de ações e a dispersão de recursos em áreas divergentes pelos diversos órgãos empregados (BRASIL, 2013, p. 1-2). Esta nova realidade está gerando constante aperfeiçoamento na relação de poder entre os Estados, principalmente agora, com o emprego das FA em ambientes que contam cada vez mais com a presença da população civil, o que reduz a possibilidade de identificar o oponente e requer o emprego de novas capacidades de combate para reduzir os efeitos colaterais.

Nesse espectro de integração de Operações de Informação e Operações Interagências, esse trabalho realiza um estudo de caso sobre a Operação HUMAITÁ, realizada pela 17ª Brigada de Infantaria de Selva (17ª Bda Inf Sl), Porto Velho/RO, no período compreendido entre 24 de dezembro de 2013 e 13 de fevereiro de 2014.

O Exército Brasileiro (EB), por intermédio da 17ª Bda Inf Sl, recebeu a missão de prover o apoio a Órgãos de Segurança Pública (OSP), sob o enfoque de Operação de Suporte (BRASIL, 2007, p. 181) com atribuições subsidiárias de assistência militar a Operação HUMAITÁ, deflagrada com o objetivo de cumprimento a cinco mandados de prisão temporária de indígenas da

etnia "Tenharim", que habitam o território localizado entre os quilômetros 100 e 150 da BR-230, a Rodovia Transamazônica (POLÍCIA FEDERAL, 2014). O apoio foi realizado em prol das investigações da Polícia Federal (PF), Polícia Rodoviária Federal (PRF), Força Nacional de Segurança Pública (FNSP) e Polícia Militar do Estado do Amazonas (PMAM), por ocasião das investigações sobre o desaparecimento de três civis, no dia 16 de dezembro de 2013, na altura da aldeia "Taboca" (km 125, da BR 230). O crime teve repercussão nacional no final do dezembro de 2013 e provocou manifestações da comunidade não-indígena contra os índios desta tribo, culminando com a destruição de carros e instalações da Fundação Nacional do Índio (FUNAI) em Humaitá/AM. Essas manifestações foram decorrentes da população da cidade ter ficado inconformada com a demora do início das investigações e, assim, ter promovido incêndio e depredação do patrimônio público naquela cidade, na noite de 25 de dezembro de 2013.

Essa operação reuniu tropas do EB, agências federais e estaduais, equipe interministerial da Presidência da República (PR), dentre outros atores, como a população não-indígena e a população indígena. Diante desse quadro de atores tão diverso, percebe-se a importância do emprego das capacidades relacionadas ao domínio da informação, com especial destaque para a atividade de Inteligência, ferramenta fundamental para a condução da narrativa nos quatro níveis (político, estratégico, operacional e tático), visando assessorar a aquisição de consciência situacional pelo Comandante da Brigada.

Esse artigo está delimitado na realização de um estudo de caso sobre o emprego da Inteligência durante a Operação HUMAITÁ, no período de 24 de dezembro de 2013 a 13 de fevereiro de 2014, sob a ótica das Operações de Informação.

O objetivo geral deste trabalho é analisar as oportunidades (capacidades e limitações) surgidas para o emprego das Capacidades Relacionadas à Informação, durante essa Op, e a sua difusão oportuna pela função de combate Inteligência.

2. DESENVOLVIMENTO

2.1. Pressupostos Teóricos

O manual Doutrina Militar Terrestre, dentro do assunto das principais implicações para o emprego da Força Terrestre, aborda que:

> "As Operações de Informação (Op Info) consistem em um trabalho metodológico e integrado de capacidades relacionadas à informação, em conjunto com outros vetores, para informar e influenciar grupos e indivíduos, bem como afetar o ciclo decisório de oponentes, ao mesmo tempo protegendo o nosso. Além disso, visam a evitar, impedir ou neutralizar os efeitos das ações oponentes na Dimensão Informacional." (BRASIL, 2014a, p. 7-3)

O Manual Operações menciona que a informação, na Era do Conhecimento, influencia o comportamento dos atores envolvidos nos conflitos, ou seja: a mídia, os atores civis não-combatentes, os grupos e organizações presentes em áreas conflagra-

das, o público de massa – nacional e internacional – e os dirigentes e líderes em todos os níveis. Dessa forma, os Comandantes (Cmt) de todos os níveis devem empregar as Op Info para identificar a interferência da dimensão informacional no ambiente operacional, conforme apresentado na Figura 1.

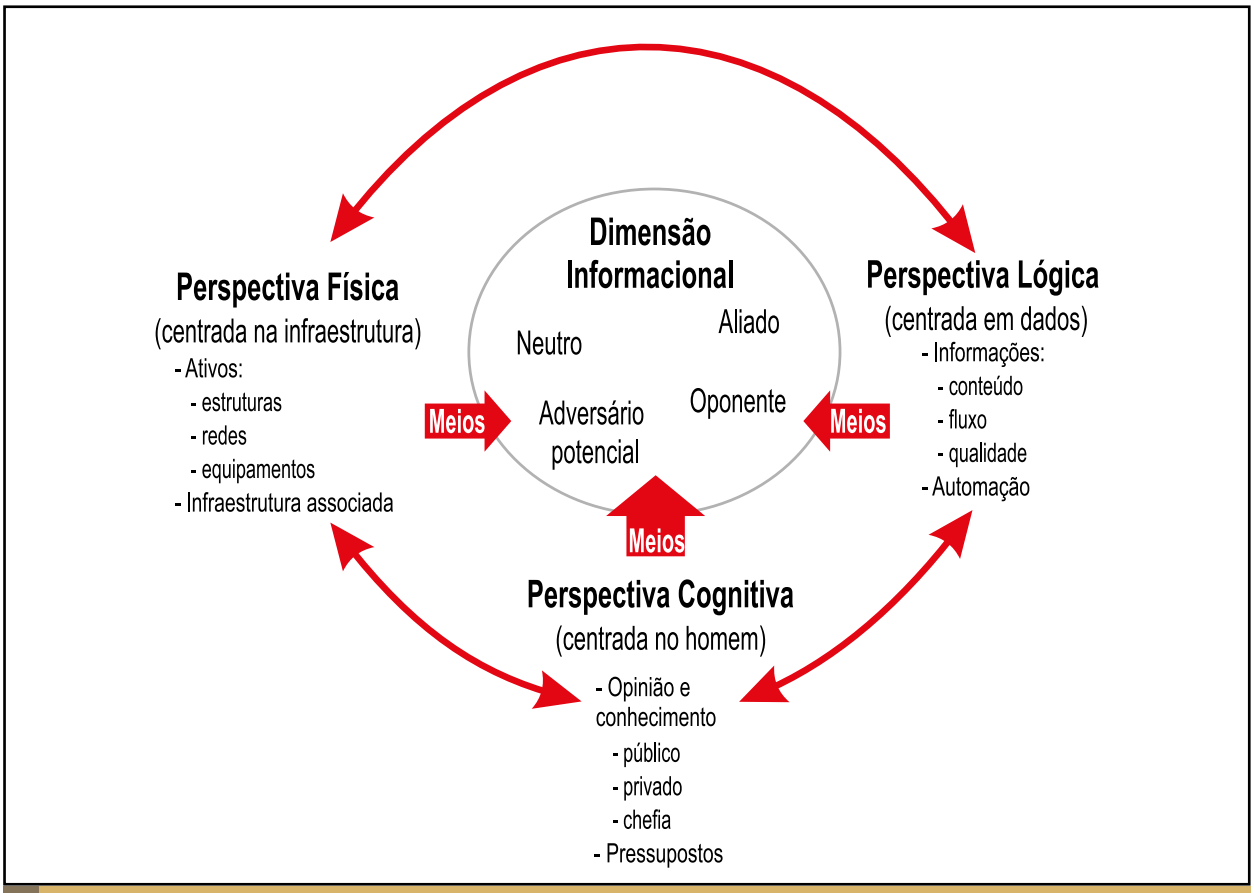


Figura 1: A Dimensão Informacional do Ambiente Operacional
Fonte: BRASIL, 2014b, p. 6-9

Nesse sentido, o Manual de Operações de Informação, descreve as Capacidades Relacionadas à Informação (CRI) como "aptidões requeridas para afetar a capacidade de oponentes ou potenciais adversários de orientar, obter, produzir e/ou difundir informações, em qualquer uma das três perspectivas da dimensão informacional (física, cognitiva ou lógica)". (BRASIL, 2014c, p. 2-7) Além disso, menciona que os oponentes podem utilizar as CRI para obter vantagens na dimensão informacional, as quais possibilitam, ainda, maximizar o potencial do comandante de influenciar públicos-alvo adversários, afetando ou obstando o processo de tomada de decisão dos oponentes. Portanto, devem ser levadas em consideração no planejamento, preparação e execução das operações militares, a serem realizadas. Para que o Cmt possa considerar isso, ele descreve que as Op Info

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

No intuito de inserir a Inteligência nas Op Info o manual Operações são apresentadas as seguintes definições

> "Inteligência é o conjunto de atividades, tarefas e sistemas inter-relacionados empregados para assegurar a compreensão sobre o ambiente operacional, as ameaças (atuais e potenciais), os oponentes, o terreno e as considerações civis. Com base nas diretrizes do comandante, executa as tarefas associadas às operações de Inteligência, Vigilância, Aquisição de Alvos (e ameaças) e Reconhecimento". (BRASIL, 2014b, p. 3-21)

> "As Op Info consistem na atuação, metodologicamente integrada, de capacidades relacionadas à informação, em conjunto com outros vetores, para informar e influenciar grupos e indivíduos, bem como afetar o ciclo decisório de oponentes, ao mesmo tempo protegendo o nosso." (BRASIL, 2014b, p. 6-9)

A IP 30-1 divide a atividade de Inteligência em dois ramos: Inteligência (Intlg) e Contrainteligência (C Intlg). Especifica a Inteligência como o ramo que abrange a atividade especializada, que é exercida permanentemente. Tem o objetivo de produzir conhecimentos de interesse do comandante de todos os níveis, sobre o terreno, inimigo e as condições meteorológicas, proporcionando as melhores condições para a tomada de decisões.

Diante do exposto, pode-se concluir parcialmente que os novos recursos tecnológicos e de sistemas acessíveis à sociedade passaram a exercer influência direta no planejamento e na condução das operações militares, alterando, significativamente, as capacidades militares. Diante disso, a Inteligência tem papel preponderante dentro das Op Info para identificar lacunas e prioridades de informação como parte do processo de planejamento e condução das operações terrestres, identificando e coordenando as Necessidades de Inteligência (NI) para permitir uma melhor compreensão do ambiente operacional no apoio ao planejamento e a condução das Op.

2.2. A Operação HUMAITÁ

No escopo da Operação HUMAITÁ, a principal missão imposta à 17ª Bda Inf Sl foi de prestar apoio logístico às ações da Polícia Federal (PF), Polícia Rodoviária Federal (PRF) e da Força Nacional de Segurança Pública (FNSP), as quais constituíram uma Força Tarefa (FT) de investigação. O efetivo conjunto empregado por essa FT, pelo EB e pela Polícia Militar do Amazonas (PMAM), apesar de variar constantemente, chegou a cerca de 500 (quinhentos) integrantes por dia. Os efetivos estavam distribuídos na cidade de Humaitá/AM, Santo Antônio do Matupi/AM e ao longo da BR-230 (Rodovia Transamazônica).

O 54º Batalhão de Infantaria de Selva (54º BIS) sediado na cidade de Humaitá/AM, foi a principal base de apoio para as operações desenvolvidas pela FT. O relacionamento com os segmentos da população da região ficou facilitado, em virtude da

presença e interação positivas do Batalhão com a comunidade local.

Embora a principal missão do EB fosse prover o apoio logístico para as agências, o Cmt da 17ª Bda Inf Sl foi constantemente solicitado por autoridades locais sobre uma maior participação das tropas na Operação. Além disso, o Comandante Militar de um Teatro de Operações deve possuir, em todas as oportunidades, a consciência situacional para decidir com maior probabilidade de acerto. Assim, na Op HUMAITÁ a Inteligência atuou de forma a prover ao Comandante da Brigada com os conhecimentos necessários para atender suas necessidades de conhecer, bem como, a integração dos mesmos com as demais CRI para atender às demandas surgidas ao longo da Operação.

Esta Operação foi determinada pela Presidente da República (PR) e o Ministério da Justiça (MJ) ficou encarregado de conduzir as investigações. O Ministério da Defesa (MD) expediu a Diretriz Ministerial e o Comando de Operações Terrestres (COTER) emanou a Diretriz de Planejamento Operacional Militar (DPOM), de modo a fornecer o amparo necessário para o desencadeamento da Operação HUMAITÁ, em virtude das manifestações de populares que buscavam o início das investigações do desaparecimento de três civis, próximo à aldeia "Taboca", na altura do km 125 da BR-230. Por diversas vezes, antes de localizarem os corpos, surgiram boatos difundidos por populares que diziam tê-los achado e convocando pessoas para manifestações, bem como, para a invasão de aldeias indígenas. Nesse contexto, ainda coube à PF a incumbência de investigar as depredações ao patrimônio público, ocorridos durante os protestos na cidade de Humaitá/AM, no dia 25 de dezembro de 2013, quando cerca de duas mil pessoas ocuparam as ruas daquela cidade, requerendo o início das investigações.

A população não-indígena cobrava maior atuação e rapidez nas investigações conduzidas pelos órgãos federais. Parte deste público agia de forma agressiva em relação aos indígenas, chegando a invadir algumas aldeias situadas as margens da BR-230. Estes públicos, que representavam ameaças à ordem pública e ao desenrolar da Operação HUMAITÁ, foram acompanhados pela Inteligência. Outra parte, familiares e pessoas ligadas aos desaparecidos, buscavam as respostas para o ocorrido e a localização dos desaparecidos.

As mídias sociais, como o "Facebook", e programas de mensagens, como o "Whatsapp", foram largamente utilizados pela população local, constituindo-se em ameaças e, dessa forma, em possíveis objetivos para as estruturas de Inteligência voltadas para a exploração da fonte cibernética. O clima de instabilidade na região permaneceu durante toda a investigação, requerendo maior atuação das Forças de Segurança na prevenção e identificação das fontes de distúrbio, servindo de oportunidade de obtenção de dados por parte da Inteligência. Isso exigiu monitoramento constante, de modo a antecipar as possíveis ações agressivas, por parte de indígenas e não-indígenas insatisfeitos.

Por sua vez, os indígenas estavam receosos de irem à cidade de Humaitá/AM, temendo a reação de alguns populares. Evitavam ir ao comércio, permanecendo nas aldeias. Para viabilizar o auxílio aos indígenas, foi providenciado o transporte dos mesmos até a cidade, a cargo do 54º BIS. Houve, também, a entrega de cestas de alimentos, bem como, o atendimento de saúde, diretamente nas aldeias, permitindo garantir a segurança e o apoio logístico aos indígenas em suas aldeias.

A Inteligência, valendo-se de colaboradores na região, levantou que os indígenas da aldeia "Tenharim-Marmelo" ameaçavam o bloqueio da BR 230 (Rodovia Transamazônica), mediante a queima de pontes existentes naquela rodovia. Esta ameaça requereu atenção especial, de modo a permitir o andamento das investigações, uma vez que a BR 230 é a única ligação entre as aldeias.

O Cmt da 17ª Bda Inf Sl permaneceu na Área de Operações, na maior parte do tempo. De posse dos dados levantados e utilizados na produção do conhecimento pela Inteligência, permitiu exercer a liderança estratégica nas reuniões que participou com autoridades locais, familiares dos desaparecidos, de coordenação da missão e com as lideranças indígenas, nas aldeias. Além disso, o Cmt Bda pode assessorar, com oportunidade, o Comandante Militar da Amazônia (Cmt Mil Amz), por ter o domínio integral das informações.

Da mesma forma, o Cmt Mil Amz esteve por vários dias no terreno, acompanhando os trabalhos realizados. Em virtude disso, foi convidado pela Presidente da República (PR) a participar de uma reunião no Palácio do Planalto, em Brasília/DF, para tratar da referida Operação.

Após esta reunião, o Governo Federal enviou representantes do Ministério do Meio Ambiente e Recursos Naturais Renováveis (MMA), do Ministério do Desenvolvimento Sustentável e Combate à Fome (MDS), do Ministério do Desenvolvimento Agrário (MDA) e da Secretaria Especial da Presidência da República (SE/PR). Participaram de diversas reuniões com diferentes públicos e visitas a diferentes etnias, elencando ações a serem realizadas para o desenvolvimento sustentável da região, onde mais uma vez os conhecimentos de Inteligência foram essenciais para a compreensão do Ambiente Operacional por parte das agências estatais.

Ficou latente a diferença de interesses entre as etnias, durante a ida da comitiva às aldeias. Nas reuniões realizadas na aldeia "Marmelo", representantes das etnias "Tenharim" e "Jiahoi", mostravam-se apreensivos, exigindo o retorno da cobrança do pedágio na BR-230 ou de uma compensação financeira vitalícia, para toda a aldeia. Por outro lado, lideranças da etnia "Parintintin", na aldeia "Traíra", mostraram-se contrários à referida cobrança e seus anseios estavam ligados ao desenvolvimento sustentável de sua Terra Indígena (TI).

Mereceu destaque, também, o fato de que os indígenas mais jovens, na aldeia "Marmelo", filmavam as reuniões, entre as autoridades e as lideranças indígenas,

com modernos *smartphones*. Foi percebida, também, a presença de integrantes do Conselho Indigenista Missionário (CIMI) e de repórteres estrangeiros. Todos esses atores, como se observa, buscavam o domínio da informação.

Com o andamento das investigações, a PF cumpriu mandado de prisão de cinco indígenas da etnia "Tenharim". Dentre eles, dois filhos de Ivan Tenharim, cacique da aldeia "Taboca", um professor municipal e um agente de saúde federal, acusados de participar da morte dos três desaparecidos. Cerca de quatro dias depois destas prisões, no dia 3 de fevereiro de 2014, foi encontrado o local onde foram enterrados os desaparecidos, próximo da aldeia "Taboca".

Por intermédio do emprego pontual dos meios da função de combate Inteligência, pode-se cumprir uma das metas estabelecidas pela PF em um dos inquéritos instaurados, onde buscava-se solucionar o desaparecimento dos três civis. Apesar de ser um pleito dos familiares e de parte da população local, a prisão de suspeitos e a identificação dos corpos não pacificou a região. Problemas de toda a ordem permanecem e os ressentimentos continuam. Estas ameaças continuam a ser monitoradas pela Inteligência, de modo a produzir os conhecimentos oportunamente, facilitando a tomada de decisão dos Comandantes em todos os níveis.

Desta forma, conclui-se parcialmente que acompanhar a conjuntura num ambiente de tensão e interesses difusos e com ausência de diversos segmentos do Poder Público Federal, é um desafio para a função de combate Inteligência e um ambiente rico para as Operações de Informação.

2.3. O Papel da Inteligência nas Operações de Informação e sua Integração com a Comunicação Social e Operações de Apoio a Informação

O acompanhamento das ações na região do conflito foi feita de maneira sistemática e contínua, por parte da função de combate Inteligência. A cobrança irregular do pedágio por parte dos indígenas da aldeia "Marmelo" teve início, em meados do ano de 2006, na altura do km 130 da BR 230. Os conhecimentos de Inteligência, desde então, já indicavam o descontentamento por parte da população local com a situação.

Outros fatos relevantes, que antecederam o desencadeamento da Operação HUMAITÁ, também foram obtidos pela função de combate Inteligência. A morte do Cacique Ivan Tenharim, em 3 de dezembro de 2013, e a divulgação de um texto na *internet*, por parte do Coordenador Regional da Fundação Nacional do Índio (FUNAI), em Humaitá/AM, no dia 6 daquele mês, foram os fatos que desencadearam a questão. Este último, em especial, teve repercussão negativa na região, ocasionando a exoneração daquele coordenador, em 10 de janeiro de 2014.

Os conhecimentos de Inteligência disponíveis permitiram antecipar o protesto dos familiares dos três desaparecidos, cobrando o início das investigações por parte das autoridades, e a consequente interdi-

ção da balsa que liga Humaitá/AM a Santo Antônio do Matupi/AM, no dia 24 de dezembro de 2013. O mesmo ocorreu com os desdobramentos nos dias posteriores, sendo esses: as depredações e incêndios na cidade de Humaitá/AM, levadas a efeito por manifestantes radicais; a fuga de indígenas para o aquartelamento do 54º Batalhão de Infantaria de Selva, pois estavam temerosos de serem mortos pelos manifestantes; a concentração de pessoas e veículos na altura do km 150 da BR 230, oriundos das cidades de Santo Antônio do Matupi/AM e Apuí/AM; e a queima de postos de pedágio na aldeia "Marmelo", por parte desses manifestantes. Tudo isto, permitindo que a OM da localidade de Humaitá/AM adotasse as medidas necessárias para atender as demandas da crise instalada.

Paralelamente a isso, foi percebida a insatisfação por parte da população não-indígena, da região, pelo fato de as autoridades dedicarem maior atenção com a população indígena que estava acolhida nas instalações do 54º BIS, do que com os anseios dos primeiros.

A insatisfação da população não-indígena permaneceu constante ao longo de todo o período considerado. As reivindicações variavam desde a celeridade nas investigações, conduzidas pela PF, até a maior atenção para a região, por parte das autoridades locais e federais. As redes sociais eram utilizadas para a disseminação de boatos, como a localização dos corpos dos desaparecidos e convocação para outras manifestações, o que requereu a atenção devida da Inteligência no monitoramento desses meios.

A prisão, em 30 de janeiro de 2014, de cinco indígenas acusados de participação no homicídio e a ocultação dos corpos dos três desaparecidos, em 3 de fevereiro deste ano, próximo à aldeia "Taboca", serviram para abrandar as expectativas da população local.

Todos estes levantamentos foram feitos com oportunidade pela Inteligência, contribuindo para o emprego adequado, por parte do Comandante da 17ª Bda Inf Sl, nas ações de outras Capacidades Relacionadas à Inteligência (CRI), como as Operações de Apoio a Informação (OAI) e a Comunicação Social (Com Soc). Estas tinham condições de serem empregadas a todo instante, quer fosse para informar e esclarecer os públicos-alvo envolvidos na Operação HUMAITÁ, quer fosse para direcionar as ações para o fortalecimento da imagem do EB.

As OAI tiveram campo fértil para conduzir suas ações e, assim, contribuírem para a obtenção da superioridade da informação e apoiar a conquista de objetivos estabelecidos. A identificação das ameaças e das vulnerabilidades pela Inteligência possibilitou a execução de planos para atender às demandas surgidas ao longo da Operação HUMAITÁ.

Uma das principais ameaças identificadas foi a insatisfação da população local com a demora nas investigações da FT e com possíveis privilégios à população indígena. Constatada pelo acompanhamento sistemático das mídias sociais e *blogs*, também foi percebida por entrevistas a populares.

A tensão na região potencializou a importância da atuação de OAI para mostrar à população local que não houve favorecimento a indígenas ou a não-indígenas, e que a atuação do EB e da FT foi pautada pelo cumprimento aos dispositivos legais e pela missão imposta, sem beneficiamento unilateral. Em decorrência disso, foi estimulada a interlocução das autoridades com os cidadãos, ampliando o relacionamento com a imprensa e as lideranças locais, de modo a reduzir o ambiente de instabilidade na região. Foram implementadas, ainda, ações de OAI para reaproximar a população da cidade de Humaitá do 54º BIS, como, por exemplo, uma tocata da banda de música, daquela Organização Militar (OM), na praça principal da cidade.

Diante dos fatos que estavam ocorrendo, surgiram algumas necessidades de coordenação adicionais com os órgãos e agências participantes da Operação, em especial com a FT responsável pela investigação. Foi necessário um maior compartilhamento dos conhecimentos de Inteligência de ambas as Instituições, de modo a aumentar o grau de confiabilidade entre os envolvidos, colaborando para a implementação do banco de dados de Inteligência constantemente atualizado. Implementaram-se melhorias nas reuniões de coordenação para a solução dos problemas apresentados. No entanto, cabe um aprofundamento no tema para extrair as lições aprendidas e aplicar esses ensinamentos em futuras Operações Interagências.

O emprego adequado da função de combate Inteligência permitiu que o Comandante da Brigada possuísse os conhecimentos necessários sobre as ameaças e as oportunidades que foram explorados pela equipe de Com Soc, do Centro de Comunicação Social do Exército (CComSEx). A equipe permaneceu na região, por cerca de dez dias, participando da Operação HUMAITÁ, propiciando uma melhor divulgação dos produtos e acompanhamento das ações, e possibilitando uma sensibilização eficiente e eficaz aos diversos públicos trabalhados.

O compartilhamento dos conhecimentos de Inteligência com a equipe de Comunicação Social viabilizou a publicação de notas de esclarecimento com os meios de imprensa local com oportunidade e seriedade. Facilitou, ainda, os contatos com os jornalistas na região, evitando a transmissão de informações divergentes e incorretas, sobre as ações das Instituições envolvidas na Operação.

Houve, também, a possibilidade de realizar *midia training* com as autoridades, antes dos seus pronunciamentos nos órgãos de imprensa e entrevistas, baseada nos conhecimentos de Inteligência disponíveis. Desta forma, a Com Soc teve sua capacidade de esclarecer e informar a população local sobre as atividades desenvolvidas potencializada, durante o período em que permaneceu na A Op.

Conclui-se parcialmente que, o aumento da rapidez na tomada de decisão, pelo Cmt, só foi possível em virtude da integração da Inteligência com outras CRI, principalmente as OAI e Com Soc, permitindo maior sinergia para identificar ame-

aças e oportunidades, bem como, obter superioridade da informação no Ambiente Operacional.

3. CONCLUSÕES E SUGESTÕES

A compreensão adequada do Ambiente Operacional atual evidencia o fato de que a resolução de futuros conflitos envolverá, cada vez mais, uma coordenação estreita entre todos os campos do poder e a integração de capacidades relacionadas ao domínio da informação, para a obtenção da superioridade da informação.

Essa integração visa proteger e defender os Sistemas de Informação, assegurando a sua disponibilidade, integridade, autenticidade e a confidencialidade. Com isso, cresce de importância a incorporação das Op Info nas estratégias e doutrinas militares convencionais.

A tendência de aumento dos conflitos assimétricos em ambientes urbanos e complexos gera a necessidade de dispor de forças flexíveis capazes de operar em qualquer tipo de ambiente operacional. A Operação HUMAITÁ permitiu o emprego de elementos especializados de Inteligência para o levantamento de dados e para a produção e difusão de conhecimentos, com oportunidade. Ainda que a missão principal imposta à 17ª Bda Inf Sl fosse o apoio logístico às Instituições responsáveis pelas investigações acerca do desaparecimento de três civis, era imperioso que o Comandante da Brigada tivesse a consciência situacional necessária ao acompanhamento das ações.

Neste contexto, a presença de equipes com capacidades relacionadas à informação foi fundamental para a condução das ações por parte do Comandante dessa GU. A Inteligência fez o acompanhamento sistemático e oportuno dos acontecimentos, e as OAI e a Com Soc, de posse desses levantamentos, executaram ações para subsidiar a Operação em curso.

O trabalho realizado pelos meios da função de combate Inteligência em presença começou antes do desencadeamento da Operação. Os dados foram trabalhados com objetividade e amplitude, possibilitando a produção de conhecimentos precisos e oportunos para a melhor tomada de decisão por parte do Comandante da 17ª Bda Inf Sl. Durante todo o período, o trabalho de Inteligência permitiu a antecipação das ações e o conhecimento do *modus operandi* dos públicos-alvo que estavam na região.

Os conhecimentos de inteligência difundidos oportunamente às equipes de OAI e de Com Soc serviram de base para a correta avaliação dos públicos-alvo envolvidos e do que estava ocorrendo na região, colaborando para o arrefecimento da beligerância entre os atores. Dessa forma, a Inteligência, integrada as OAI e Com Soc, forneceu excelentes respostas operacionais e táticas ao comandante da GU. Embora as equipes de OAI e Com Soc tenham permanecido por um curto período na A Op, tiveram importante participação nas ações desenvolvidas durante a operação para complementar a atuação dos militares componentes da estrutura de inteligência da GU e dos demais órgãos presente nessa Op Interagências.

Finalmente, é possível concluir que o domínio da informação é o insumo básico do processo decisório e que, por conta de uma série de fatores atuais, ela está diretamente sujeita às dimensões que compõem o Ambiente Operacional. Na Op HUMAITÁ, pôde-se constatar que o emprego da função de combate Inteligência com antecedência na A Op garantiu às Forças uma elevada fidelidade na aquisição de objetivos, na identificação das ameaças e oportunidades na Área de Operações, facilitando o Comando e Controle. Além disso, a interrelação dessa capacidade com as CRI, Operações de Apoio a Informação e Comunicação Social ensejou o entendimento de que com essas capacidades integradas e coordenadas, atuando em qualquer ambiente operacional, será possível aumentar a superioridade militar de informações.

Dessa forma, as Operações de Informação devem se constituir em instrumento do Comando para permitir a obtenção do resultado necessário e desejado sobre os objetivos, diminuindo o risco à Força e minimizando os efeitos colaterais sobre civis, infraestruturas críticas e instalações existentes no ambiente.

REFERÊNCIAS

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

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **MD 35-G-01 Glossário das Forças Armadas**. 1ª ed. Brasília, DF: 2007.

_____. Ministério da Defesa. **EB 20-MC-10.201 Operações em Ambiente Interagências**. 1ª ed. Brasília, DF: 2013.

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **EB 20-MF-10.102 Doutrina Militar Terrestre**. 1ª ed. Brasília, DF: 2014a.

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **EB 20-MF-10.103 Operações**. 4ª ed. Brasília, DF: 2014b.

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **EB 20-MF-10.213 Operações de Informação**. 1ª ed. Brasília, DF: 2014c.

_____. Exército. Comandante do Exército. Portaria nº 008, de 29 de abril de 2005: **Aprova a Diretriz para a Integração de Dados Oriundos das Diversas Fontes para Produção do Conhecimento de Inteligência Militar.** Brasília, DF, 2005.

_____. Ministério da Defesa. Portaria Normativa nº 447, de 05 de abril de 2005: **Dispõe Sobre a Política Normativa de Meteorologia de Defesa.**

_____. Exército. Estado-Maior. **IP 30-1: A Atividade de Inteligência Militar -2ª Parte: A Inteligência Nas Operações Militares**. 1. ed. Brasília, DF, 1999.

EUA. Department of the Army. **FM 100-3 INFORMATION OPERATIONS**. Washington, DC, 1996.

MANDARINO Jr, Raphael**. Segurança e Defesa do Espaço Cibernético Brasileiro**. Recife: Cubzac, 2010a.

_____. **Livro Verde de Segurança Cibernética no Brasil.** Brasília, DF: GSIPR/SE/DSIC, 2010b

POLÍCIA FEDERAL, Comunicação Social da PF em Rondônia . "**Nota à Imprensa – Operação Humaitá**". 31 de janeiro de 2014. Disponível em: http://odescortinardaamazonia.blogspot.com.br/2014/01/nota-imprensa-operacao-humaita.html. Acesso em 25 ABR 14.

"A Inteligência é um apanágio dos nobres. Confiada a outros, desmorona."

Walther Nicolai

Novas instalações da EsIMEx

" O FUTURO COMEÇA AQUI!"

ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO

EsIMEx

BRASIL

"Antes de tudo, INTELIGÊNCIA!"