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.

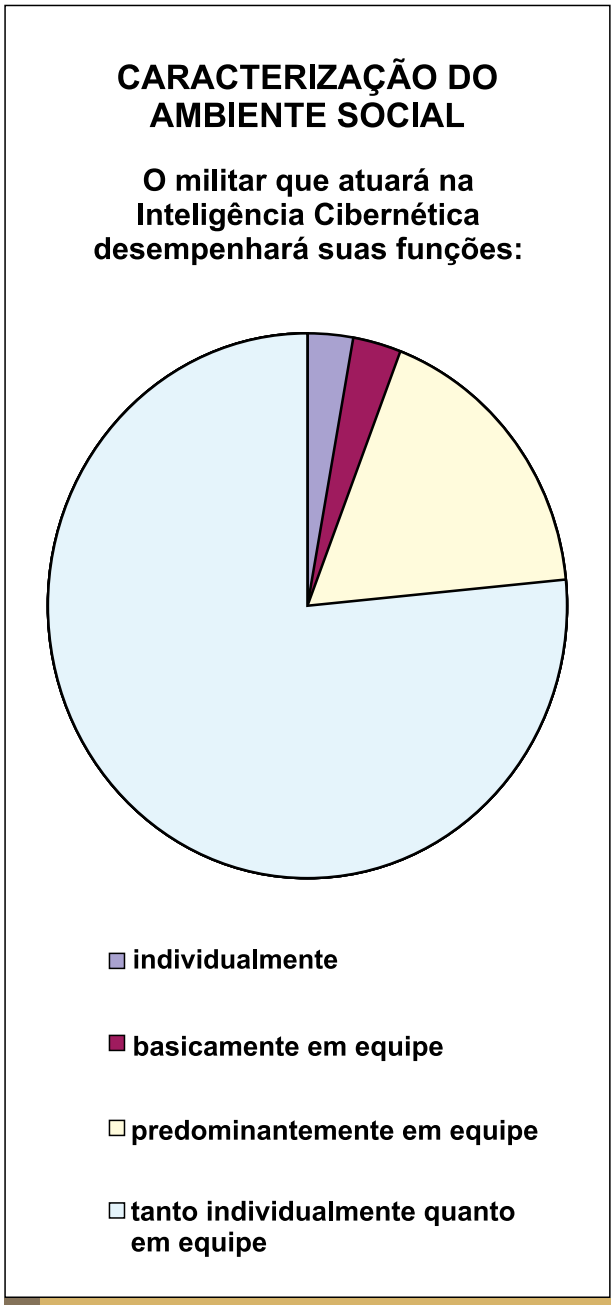

Gráfico 1 - Caracterização do ambiente social
Fonte: Autores

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

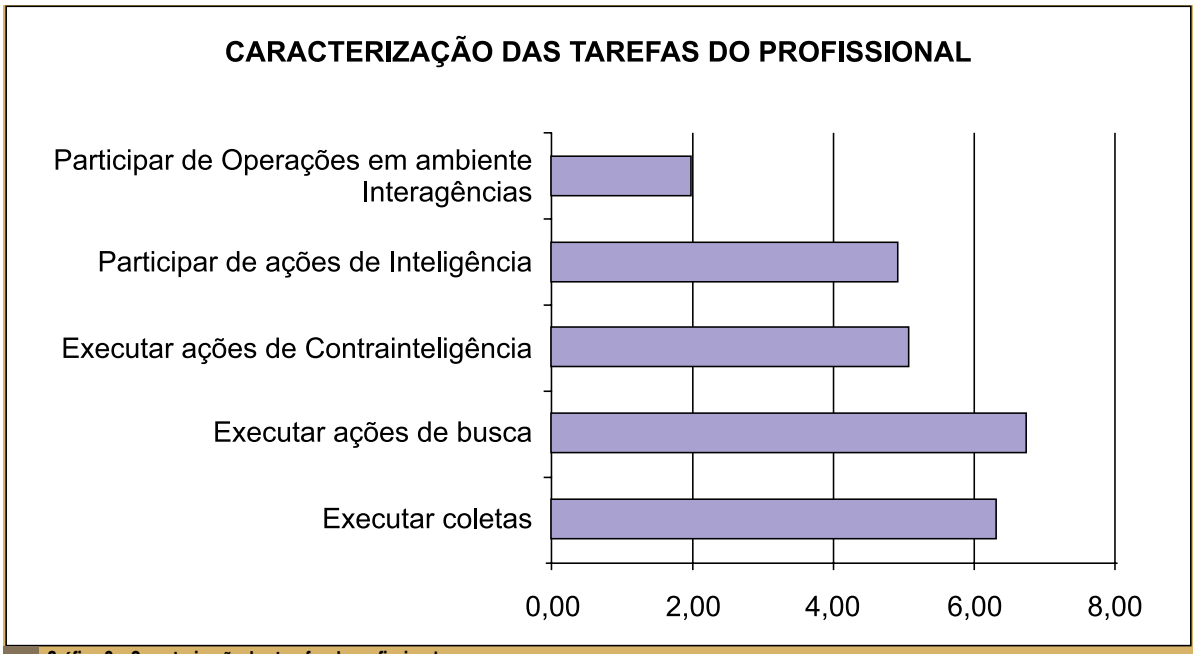

Gráfico 2 - Caracterização das tarefas do profissional
Fonte: autores

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.