ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INT MARCO ANTONIO ALTRUDA ARCHANGELO

UM ESTUDO ACERCA DA RELAÇÃO ENTRE A DEFESA CIBERNÉTICA E A FUNÇÃO DE COMBATE LOGÍSTICA

Rio de Janeiro
2019

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INT MARCO ANTONIO ALTRUDA ARCHANGELO

UM ESTUDO ACERCA DA RELAÇÃO ENTRE A DEFESA CIBERNÉTICA E A FUNÇÃO DE COMBATE LOGÍSTICA

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Logística Operacional.

Rio de Janeiro
2019

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **CAP INT MARCO ANTONIO ALTRUDA ARCHANGELO**

Título: **UM ESTUDO ACERCA DA RELAÇÃO ENTRE A DEFESA CIBERNÉTICA E A FUNÇÃO DE COMBATE LOGÍSTICA.**

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, com ênfase em Logística Operacional, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **CHARLES DAVIDSON SOARES BITENCOURT - Maj** Cmt Curso e Presidente da Comissão	
_____ **WAGNER SANTANA DA COSTA - Maj** 1º Membro	
_____ **ANDERSON JOSÉ SOARES DE LIMA - Cap** 2º Membro e Orientador	

_____
MARCO ANTONIO ALTRUDA ARCHANGELO- Cap
Aluno

UM ESTUDO ACERCA DA RELAÇÃO ENTRE A DEFESA CIBERNÉTICA E A FUNÇÃO DE COMBATE LOGÍSTICA

Marco Antonio Altruda Archangelo[*]
Anderson José Soares de Lima[**]

RESUMO
Nas operações militares, apesar de o ambiente cibernético promover inúmeros benefícios para a melhoria da logística, também pode ser considerado como um cenário que traz vulnerabilidades, sendo fundamental uma atuação voltada para a proteção desses dados. Assim sendo, este estudo tem como objetivo geral analisar a possibilidade de integração das ações de defesa cibernética com a logística empregada em operações militares, com fins de proteção da informação e dos dados logísticos. Como metodologia,foram empregadas as pesquisas bibliográfica e documental. Ao final do estudo, foi possível verificar que o apoio logístico envolve todos os níveis de logística militar no amplo espectro e no ambiente interagências, gerando a necessidade de integração com outros Órgãos, pressupondo apoio logístico contínuo e tempestivo, bem como enaltecendo a garantia de segurança dos ciberdados logísticos, pois o seu vazamento pode comprometer totalmente uma operação militar. Restou demonstrado que a guerra cibernética corresponde ao uso ofensivo de informações para explorar e degradar o adversário em uma operação militar. Para mitigar os riscos dessa problemática, verificou-se que o Exército Brasileiro conta com a proteção dos sistemas de informação e de defesa cibernética, que inclui uma defesa ativa e profunda dos sistemas de informação e da capacidade de gerenciamento de crises cibernéticas, negando, assim, o acesso às estruturas das tropas, direcionando-se por um meio de informação ou de uma mensagem em si. Salienta-se que, para que as ações de guerra cibernética possam assegurar a logística nas operações militares, exige-se coordenação central e interlocutores bem identificados, tendo em vista a necessidade de definição de uma organização única e centralizada, responsável pela direção geral do campo e pela gestão operacional da defesa dos sistemas de informação sob a autoridade competente.

Palavras-chave: Guerra cibernética.Defesa cibernética. Função de combatelogística.

ABSTRACT
In military logistical operations, although the cybernetic environment may bring innumerable benefits in improving operations, it can also be considered as ascenario that brings vulnerabilities, being fundamental an action focused on the protection of these data. Thus, this study has the general objective to analyze the possibility of integration of cyber defense planning with the logistics used in military operations for purposes of information protection. Bibliographical and documentary researches were used as methodology. At the end of the study, it was possible to verify that logistical support involves all levels of military logistics in a wide range of tasks, generating the need for integration with the organs, assuming logistical support to other national and/or foreign forces. The study showed that cybernetic war corresponds to the offensive use of information to exploit and degrade the adversary in a military operation. To mitigate the risks of this problematic it was verified that the Brazilian Army counts on the protection of the information systems and of the cyber defense, which includes an active and in-depth defense of information systems and cybersecurity management capacity, thus denying access to troop structures, by means of information medium or a message per se. It should be noted that cyber defense in military logistics operations requires central coordination and well-identified interlocutors, given the need to define a single, centralized organization responsible for the overall direction of the field and operational management of defense of information systems under authority of the Head of the Department of Defense.

Keywords: Cybernetic war. Cybernetic defense.Logisticscombatfunction.

[*] Capitão do Serviço de Intendência. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2009. Especialista em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (AMAN) em 2019.
[**] Capitão do Serviço de Intendência. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2005. Especialista em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (AMAN) em 2014.

1 INTRODUÇÃO

Como nação soberana, o Brasil deve possuir capacidade de se contrapor a ameaças externas de modo compatível com a sua dimensão e as suas aspirações político-estratégicas.

Essa questão envolve toda a cadeia logística,que engloba as atividades relativas à previsão e provisão dos recursos que contribuam com os serviços necessários à execução e atuação conjunta das diversas missões das Forças Armadas e de defesa militar no que se refere à defesa cibernética.

Nesse sentido, a Política Nacional de Defesa (PND) é um documento no qual estão definidas todas as ações e estratégias, no âmbito das Forças Armadas, voltadas para a defesa do território e dos cidadãos brasileiros.

Considerando esse cenário, a defesa cibernética, por meio da guerra cibernética, vem se estabelecendo como atividade fundamental para o êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do comando e controle, por meio da proteção dos ativos de informação, ao mesmo tempo em que permite que esse exercício seja negado ao oponente.

Cabe notar que as estratégias de proteção do espaço cibernético estão intrinsecamente associadas à atividade logística, pois, obrigatoriamente, necessitarão do uso de sistemas de comunicação e controle instalados, a fim de que possam exercer o apoio de forma correta e célere.

A função de combate logística configura uma gama de ações e sistemas que suprem, em apoio e serviços, a condução e a manutenção das operações militares. Tais atividades logísticas abrangem o controle de materiais e recursos humanos que atendam às demandas do Estado, não só pela defesa e manutenção da autonomia, como também no que se refere ao apoio à população.

Em relação àdefesa cibernética, a principal estratégia é o desenvolvimento de tecnologias e doutrinas voltadas para o seu planejamento e a sua execução, as quais contribuam com a segurança do espaço cibernético, tendo como exemplo os conceitos de guerra cibernética em operações como sistema de segurança em ambientes computacionais(BRASIL,2014b).

É importante considerar que as operações militares modernas dependem totalmente do domínio cibernético. Isso porque não podem transcorrer eficazmente

sem redes confiáveis de informação e comunicação, com acesso seguro ao ciberespaço e ao espaço em geral.

Assim sendo, o Exército Brasileiro deve estar empenhado em assegurar que as estratégias sejam mantidas e monitorizadas, para rever regularmente o progresso das medidas tomadas para esse fim. Além disso, precisa avaliar regularmente a abordagem de como os recursos logísticos gerariam saídas necessárias tendo os seus principais sistemas comprometidos por ataques cibernéticos, bem como responder às mudanças nos níveis de ameaças e aos avanços nas tecnologias de segurança (BRASIL,2014c).

Cumpre notar que o setor cibernético nacional envolve a atuação integrada de vários Órgãos,militares e civis, cada um com as suas atribuições específicas. Tais Órgãos devem ser capazes, ainda, de garantir que todos os esforços sejam empreendidos para tornar os sistemas seguros e proteger os dados e as redes contra qualquer ataque ou tentativa de interferência. Daí a necessidade de definir os mais rígidos padrões de segurança cibernética e aplicá-los escrupulosamente, como um pilar da segurança nacional e da garantia da soberania do país (BRASIL,2014b).

1.1 PROBLEMA

Não obstante o ambiente cibernético promover inúmeros benefícios para a melhoria das operações militares, no sentido de maior celeridade e detalhamento das informações, também pode ser considerado como um cenário que traz diversas vulnerabilidades, sendo fundamental o entendimento de que é necessária a segurança cibernética de computadores como um todo, fator que gera o seguinte questionamento: Quais medidas podem ser adotadas para mitigar os impactos de ataques cibernéticos às redes e aos sistemas de comando e controle para garantir a efetividade logística e a continuidade do apoio em operações militares?

1.2 OBJETIVOS

Diante dessa indagação, o objetivo geral do presente artigo é analisar quais medidas podem ser adotadas para mitigar os impactos de ataques cibernéticos às redes e aos sistemas de comando e controle para garantir a continuidade e a disponibilidade do fluxo logístico em operações militares, bem como determinar os conceitos de guerra cibernética que o Exército Brasileiro pode utilizar para proteger informações logísticas no espaço cibernético.

Nesse diapasão, os objetivos específicos resumem-se em:

a) identificar dados relacionados a possíveis ataques inimigos que possam impactar os sistemas das funções logísticas de apoio de material, pessoal e saúde de tropas em operações militares;

b) analisar as vulnerabilidades de defesa cibernética construída, em especial pelo Exército Brasileiro, no âmbito das Forças Armadas;

c) apontarações de guerra cibernética necessárias para evitar as consequências de um ataque cibernético que possam prejudicar a logística militar em geral.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

De uma maneira geral, é possível caracterizar crimes cibernéticos como sendo aqueles cometidos contra a segurança de informações e dados militares, enfatizando-se, neste estudo, as operações militares logísticas, que, de acordo com Silva e Musetti (2003), vêm ocupando posição de destaque na administração de conflitos armados militares ou paramilitares, principalmente nas atividades de mobilização, manutenção da paz, deslocamento, posicionamento e manutenção de tropas, equipamentos, operações conjuntas e suprimentos.

Sabendo-se da importância das atividades logísticas no ambiente operacional e militar, bem comotendo ciência de que as operações militares modernas dependem do domínio cibernético, foca-se, neste estudo, na vulnerabilidade das informações e dos dados militares, considerando que a guerra cibernética faz parte da guerra moderna.

Não se pode negar que, atualmente, a sociedade vem sofrendo mudanças no que se diz respeito à informação e à tecnologia, mais precisamente com a evolução dos recursos de acesso à internet, que interliga milhares de pessoas, facilitando inúmeras situações e possibilitando novas formas de comunicação para a população mundial, que tenta se adaptar às novas realidades. As informações ficam cada vez mais acessíveis a grande parte das pessoas, de maneira mais simples, apresentando taxas enormes de crescimento. Em síntese, a popularização da comunicação por meio da informática vem criando novas maneiras, costumes, grafias, enfim, um universo digital diferente.

Consequentemente, um grande problema vem acompanhado essa situação: o número de casos de crimes virtuais vem crescendo emuma velocidade maior do que a dos crimes convencionais, tornando-se um problema internacional (ARANHA

FILHO, 2002). Esses crimes podem ser classificados como delitos praticados com o uso da internet, configurando uma preocupação para as polícias e os Órgãos de fiscalização e controle, especialmente nos quesitos de materialidade e evidências.

Os crimes virtuais surgiram e se desenvolveram no mesmo passo do surgimento e do avanço dos recursos da internet, e vêm se aprimorando com o passar dos anos, tendo como objetivo, sempre, trazer prejuízos a outros usuários. Também chamados de eletrônicos ou cibernéticos, tais delitos são aqueles cometidos por meio do uso de um espaço cibernético, criado a partir de uma rede mundial, em sua maioria de computadores, conectados à internet, de modo que o agente não necessariamente comete o delito em um território, nem a vítima necessariamente precisa ser abordada fisicamente (MIRANDA, 2013).

Souza (2015) elucida que os crimes cibernéticos apresentam-se como um desafio no âmbito da investigação, inseridos em um processo de mudanças contínuas na sociedade, sendo possível afirmar que abrangem desde a dificuldade das próprias pessoas em saberem se proteger no uso da internet, tornando-se vulneráveis a qualquer ataque, assim como os avanços tecnológicos que facilitam a concretização dos objetivos dos criminosos, os quais podem ser qualquer pessoa, considerando a facilidade que o mundo virtual traz na obtenção de ferramentas para o crime.

Nessa esteira, por meio de ações de guerra cibernética, o Exército Brasileiro é, acima de tudo, responsável pela proteção da nação e pela conduta competente do seu Governo. Essa estratégia reflete tais atributos. Trata-se de um passo ousado e ambicioso para combater as muitas ameaças que o país enfrenta no ciberespaço. Embora todos tenham um papel a desempenhar na gestão e na redução de tais ameaças, o nível estratégico do Governo deve estar ciente da responsabilidade especial de dirigir o esforço nacional necessário.

De uma forma geral, a logística nas operações militares deve ser assegurada para garantir o bom combate. Conforme já salientado, não obstante o ambiente cibernético traga inúmeros benefícios para a melhoria das operações militares, também pode ser considerado como um cenário que traz vulnerabilidades às operações que podem ser acessadas pelo inimigo, sendo fundamental uma atuação voltada para a proteção desses dados.

Desse modo, busca-se, neste artigo, analisar o planejamento de defesa cibernética voltado mais especificamente para a guerra cibernética na logística

empregada em operações militares no Exército Brasileiro com fins de proteção da informação.

O presente estudo possui relevância social, por envolver um assunto referente à segurança nacional, destacando que um ataque cibernético pode comprometer toda a logística de uma operação militar e, consequentemente, a segurança dos atores envolvidos no teatro de operações e, por conseguinte, de toda uma nação.

Ademais, o estudo ainda possui relevância profissional, considerando que pode trazer subsídios para que o Exército Brasileiro atue no ambiente cibernético de forma segura em relação às informações pertinentes a operações logísticas em conflitos armados e operações com a integração e com ações de planejamento de guerra cibernética. Destaca-se, também, a sua relevância acadêmica, já que poderá contribuir para pesquisas futuras sobre o assunto.

2 METODOLOGIA

O presente estudo tem como objeto formal a segurança de ciberdados logísticos em operações militares do Exército Brasileiro.

Como metodologia, foi realizada uma revisão de literatura, com abordagem qualitativa dos dados coletados, o que caracteriza o artigo como um estudo exploratório e descritivo, que buscou compilar o que diferentes autores abordam sobre a segurança da informação no processo de migração de arquivos para a nuvem, chegando a uma proposta de boas práticas de segurança nesse processo.

Gil (2007) explana que, normalmente, o primeiro passo, antes de se iniciar uma pesquisa social, começa quando o pesquisador determina o problema a ser pesquisado, que pode ser qualquer questão não resolvida que constitua objeto de discussão em qualquer área do conhecimento, recebendo, involuntariamente, influências do meio cultural, social e econômico do pesquisador.

Dessa forma, a partir do problema traçado, desenvolveu-se uma pesquisa bibliográfica, utilizando-se como método a revisão sistemática da literatura, que, ainda segundo Gil (2007), é realizada a partir de material já elaborado, constituído, sobretudo, de livros e artigos científicos.

De acordo com Lakatos e Marconi (2001), a pesquisa bibliográfica é composta por oito fases, quais sejam: a) determinação dos objetivos; b) elaboração do plano de trabalho; c) identificação das fontes; d) localização das fontes e

obtenção do material; e) leitura do material; f) tomada de apontamentos; g) confecção de fichas; h) redação do trabalho.

Quanto à abordagem, esta pesquisa pode ser classificada como qualitativa. Para Flick (2004), a pesquisa qualitativa é fundamental no momento de fazer a escolha mais adequada de métodos e teorias oportunas, no reconhecimento e na análise de diferentes perspectivas, nas reflexões do pesquisador a respeito da pesquisa como parte do processo de produção do conhecimento e nas variedades de abordagens de métodos. Roesch (2005) complementa, afirmando que a pesquisa qualitativa é importante porque permite utilizar técnicas e métodos diversos, bem como porque dá prioridade a uma postura investigativa.

Ressalta-se, ainda, que esta pesquisa pode ser classificada como descritiva. Dessa forma, foi realizado um estudo sobre a importância de ações de guerra cibernética que assegurem a veracidade e a tempestividade de ciberdados logísticos em operações militares do Exército Brasileiro, mais especificamente em operações militares no amplo espectro, com características interagências em tempo de guerra e de não guerra.

As informações necessárias para o alcance dos objetivos desta pesquisa, os quais constituíram os orientadores nesse processo de coleta de dados, foram coletadas a partir de documentos oficiais e de outros artigos publicados sobre o assunto.

2.1REVISÃO DE LITERATURA: LOGÍSTICA MILITAR E A VULNERABILIDADE A ATAQUES CIBERNÉTICOS

Em breves palavras, Logística Militar pode ser definida como o movimento dos materiais, equipamentos, armazenamento e pessoal militar de um lugar para outro. É composta de fornecimento, gerenciamento de materiais e distribuição.

Vale observar que o mercado de logística militar é impulsionado pela modernização das instalações de infraestrutura entre as forças de defesa, levando à integração de tecnologias robustas em infraestrutura e logística (MCGINNIS, 1992). Trata-se de um setor crucial para decidir o resultado geral da guerra, com o uso de tecnologias, tornando-se também vulnerável a ataques cibernéticos.

Nesse mesmo sentido, Silva e Musetti (2003) afirmam que a Logística Militar pode ser entendida como uma atividade operacional e estratégica, sendo responsável, na área de combate, por suprir e transportar homens, animais,

alimentos, munição e equipamentos. Dessa forma, configura-se como uma atividade imprescindível para o sucesso das operações em campo de batalha, registrando interdependência com as estratégias e as táticas planejadas.

Cabe destacar, ainda com base em Silva e Musetti (2003), que a logística militar é processada em ambientes dinâmicos e imprevisíveis, requerendo uma combinação de habilidades para o planejamento, considerando os eventos inesperados. Com isso, as tecnologias têm sido importantes aliadas nesse processo de planejamento das operações logísticas; contudo, em contraponto, também têm sido utilizadas como meio de espionagem e ataque, visto que falhas na defesa cibernética podem trazer vulnerabilidades para as informações, dando aos inimigos maior poder de ataque.

Em linhas gerais, uma ameaça pode ser definida como o perigo latente de um evento que causa danos ou a perda de ativos (informações). As ameaças são consideradas externas a qualquer sistema, e, embora seja impossível eliminá-las, é possível estabelecer medidas de proteção que reduzam a possibilidade de sua consumação. Uma vulnerabilidade é uma fraqueza interna de um sistema, que causa a sua exposição a ameaças existentes, as quais podem ser exploradas por um invasor para violar a segurança. As vulnerabilidades são uma consequência de falta de manutenção, de erros de planejamento, de pessoal sem conhecimento adequado de sistemas de informática e, até mesmo, de limitações tecnológicas(FLORÊNCIO FILHO*et al*., 2014).

Portanto, entende-se que as ameaças exploram vulnerabilidades, causando ataques. Então, um ataque é o culminar de uma ameaça. Dessa forma, é essencial fazer uso de recomendações para garantir que a comunicação entre as empresas e a troca de informações sejam feitas com segurança(FLORÊNCIO FILHO*et al*., 2014).

Castells (2010), ao tratar sobre a vulnerabilidade a crimes cibernéticos, afirma que o dinamismo da internet impede que sejam desenvolvidos controles às ameaças criadas aos indivíduos e expõe quais são as características da chamada Sociedade Informacional. No mais, de acordo com Palazzi (2000, p. 54), crime virtual significa:

> Qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados. Essa criminalidade apresenta algumas características, entre elas: transnacionalidade (veiculada virtualmente, todos os países têm acesso e fazem o uso da informação), universalidade (é um fenômeno de massa e não de elite) e ubiquidade (está presente nos setores privados e públicos).

Também conceituando crimes virtuais, Rossini (2004) destaca a sua denominação de delitos informáticos como sendo a de maior amplitude, envolvendo toda e qualquer conduta que guarde relação com os sistemas informáticos, não precisando, necessariamente, que o crime tenha ocorrido na internet para a sua tipificação. Em suas palavras:

> A denominação “delitos informáticos” alcança não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta sem imprescindível “conexão” à Rede Mundial de Computadores, ou qualquer outro ambiente telemático. Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da internet, também seria alcançada pelo que se denominou “delitos informáticos” (ROSSINI, 2004, p. 110).

Nos crimes virtuais, o computador ocupa lugar de destaque e, na maioria dos casos, é o meio utilizado para a prática dos delitos. Pode-se, dizer, portanto, que tal equipamento é o instrumento para a prática do crime virtual. Contudo, o computador pode vir a ser também um alvo, ou, penalmente falando, o objeto danificado de uma vítima.

Como elucida Coutinho (2011), o computador pode ser alvo, ocasião que envolve exemplos de crimes de invasão, instalação de vírus e arquivos maliciosos com o intuito de furtar dados e/ou informações etc. De igual sorte, pode ainda ser o instrumento para o crime, por meio do qual um agente frauda contas correntes ou cartões de crédito e débito, transfere valores ou altera saldos, por exemplo.

É importante acrescentar que a eficácia das operações militares, sobretudo no amplo espectro e interagências, é finalmente baseada no *backup* que a nação fornece com os seus recursos infraestruturais, econômicos e políticos. *Boots-in-the-ground* em situações de combate em tempo real não podem ter sucesso sem um suporte logístico eficiente e tempestivo, sendo totalmente dependentes do ciberespaço. Assim, há uma necessidade tanto de capacidade cibernética ofensiva e exploratória quanto de capacidade defensiva (REIS, 2018).

Tem-se, portanto, como indispensável, o desenvolvimento de políticas de segurança da informação para a organização, identificando as vulnerabilidades, as ameaças e os riscos associados, de modo que os principais ativos de informação estejam devidamente protegidos do acesso indevido de pessoas estranhas à organização e de perda indesejada de dados, sem falar na própria disponibilidade dos equipamentos e serviços.Nesse sentido, para um sistema ser definido como

seguro, ele deve satisfazer os três princípios básicos da segurança da informação, quais sejam a integridade, a confidencialidade e a disponibilidade(BRASIL,2014b).

Não se pode olvidar que a função de combate logística desempenha um papel fundamental no sucesso das operações militares. No entanto, deve ser coerentemente planejada e executada desde o tempo de paz, bem como estar ligada à logística conjunta e nacional.

A função de combate logística compõe um conjunto de ações e tarefas por intermédio de sistemas inter-relacionados para suprir em apoio e serviços, assegurando a liberdade de ação, a amplitude no alcance, na vantagem e na duração das operações, bem como a continuidade no apoio dos elementos em combate (BRASIL, 2014c).

A previsão e a provisão do apoio necessário para a geração, assim como o desdobramento, a sustentação e a reversão de Forças Terrestres em operações, constituem um processo integrado de pessoas,de materiais e, principalmente, de sistemas computacionais e de rede, sincronizado com o planejamento de emprego da Força Terrestre. A logística em nível tático compreende a sincronização de todas as atividades necessárias para sustentar e suprir as operações militares, bem como a sua efetividade e resiliência logística(BRASIL, 2014c).

Segundo o Manual de Campanha Guerra Cibernética EB70-MC-10.232:

> O planejamento de guerra cibernética deve fornecer dados relacionados a possíveis ataques inimigos que possam impactar o suprimento e ressuprimento da tropa. Além disso, o fornecimento de equipamentos e a mobilização de pessoal são alguns exemplos de integração da capacidade cibernética à logística. As capacidades e ativos da informação não providos pela logística do Exército poderão ser contemplados por meio da mobilização(BRASIL, 2017a, p. 4-5).

Para a condução de ações de guerra cibernética, o comandante do teatro de operações, em seu Estado-Maior, e os elementos responsáveis pela guerra cibernéticasão obrigados a ter uma noção plena dos meios físicos do espaço cibernético e da localização precisa de onde os efeitos devem ocorrer. Além disso, essa logística deve ser criteriosamente coordenada, a fim de assegurar que os recursos sejam disponibilizados aos usuários em todos os níveis e escalões de emprego.Isso porque toda rede telemática ativa está sujeita e vulnerável a ataques cibernéticos, mesmo apresentando sistemas robustos de segurança. Ademais, a Logística Militar é impulsionada pela modernização das instalações de infraestrutura entre as Forças de Defesa, levando à integração de tecnologias robustas em

infraestrutura e logística (MCGINNIS, 1992). Trata-se de um setor crucial para decidir o resultado geral da guerracom o uso de tecnologias, tornando-se também vulnerável a ataques cibernéticos(BRASIL,2017a).

Convém esclarecer que, no ano de 2008, foi divulgada a Estratégia Nacional de Defesa (END), visando a abordar questões políticas e institucionais importantes para a defesa nacional.Nela, estão relatadas diretrizes como as seguintes:

> Resguardados os interesses de segurança do Estado quanto ao acesso a informações, serão estimuladas iniciativas conjuntas entre organizações de pesquisa das Forças Armadas, instituições acadêmicas nacionais e empresas privadas brasileiras. O objetivo será fomentar o desenvolvimento de um complexo militar-universitário-empresarial capaz de atuar na fronteira de tecnologias que terão quase sempre utilidade dual, militar e civil. [...] Para o atendimento eficaz das Hipóteses de Emprego, as Forças Armadas deverão estar organizadas e articuladas de maneira a facilitar a realização de operações conjuntas e singulares, adequadas às características peculiares das operações de cada uma das áreas estratégicas. [...] O instrumento principal, por meio do qual as Forças desenvolverão sua flexibilidade tática e estratégica, será o trabalho coordenado entre as Forças, a fim de tirar proveito da dialética da concentração e desconcentração. Portanto, as Forças, como regra, definirão suas orientações operacionais em conjunto, privilegiando essa visão conjunta como forma de aprofundar suas capacidades e rejeitarão qualquer tentativa de definir orientação operacional isolada (BRASIL, 2008, p. 37-48).

Não menos importante,é imprescindível observar que o Departamento de Ciência e Tecnologia (DCT) publicou um documento caracterizando as vulnerabilidades e os riscos existentes nos sistemas corporativos do Exército Brasileiro:

> Em estudo recente conduzido por este ODS [Órgão de Direção Setorial] constatou-se que diversos sistemas de uso corporativo no Exército, relativos à gestão de pessoal e financeira, são vulneráveis a acessos por pessoas não autorizadas utilizando apenas técnicas e ferramentas livremente disponíveis na Internet. Alguns desses sistemas são operados pelo SERPRO [Serviço Federal de Processamento de Dados] e atendem a toda a administração pública federal. Nesses sistemas, verificou-se que é possível, no mínimo, a obtenção de informações confidenciais ou sensíveis. De forma análoga aos sistemas corporativos em uso no Exército, e pela experiência das vulnerabilidades encontradas em estudos semelhantes conduzidos pelo Departamento de Defesa norte-americano, acredita-se que diversos sistemas de comando e controle da infraestrutura crítica nacional sejam vulneráveis a operações de guerra cibernética (BRASIL, 2004, sem paginação).

É conveniente notar que o Exército Brasileiro avançou muito em se tratando de base doutrinária acerca de defesa cibernética e, mais especificamente, sobre guerra cibernética, entretanto, ainda se faz necessário o fomento de estudos que apontem para diretrizes consolidadas e que possam ser eficazmente empregadas nas operações militares, principalmente no sentido de proteger os ciberdados e as

informações acerca da cadeia logística que coordena o fluxo logístico de operações em qualquer espectro.Não se trata somente de aquisições de tecnologia de ponta e de uma infinidade de equipamentos de última geração, mas também de investimentos em pesquisa sobre a guerra cibernética em operações militares e troca de experiências tecnológicas com outras potências.

No mais, cumpre esclarecer que, no Brasil, crime digital é o fato consistente na prática de ilícito contra uma pessoa ou sociedade, mediante o uso da internet, passível de enquadramento nas leis penais brasileiras, para fins de punição efetiva, ou seja, o delito sai do virtual e entra na realidade de todos (CARDOSO, 2015). A sua tipificação penal é um incansável objeto de estudo por parte dos grandes penalistas, juristas e doutrinadores.

De maneira geral, conforme assevera Silva (2013, p. 21):

> Os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódioe descriminação, escárnio religioso, difusão de pornografia infantil, terror infantil, terrorismo, entre outros.

Assim, um ataque cibernético pode estar em um computador individual, um sistema, uma rede ou um servidor. Mas a ameaça não ocorre apenas pela internet. Existem muitos dispositivos e ferramentas de *software* para obter acesso físico a um sistema ou banco de dados. A maioria dos criminosos cibernéticos cobre habilmente os seus rastros para escapar da detecção e da prisão, e um fator favorável a esses delinquentes é que a maioria das leis de segurança cibernética é de âmbito nacional, ao passo que a internet não se limita a fronteiras políticas ou geográficas nacionais. Além disso, os países não concordam uns com os outros no que tange à segurança cibernética e à privacidade (REIS, 2018).

Vale destacar que o Brasil está amadurecendo e evoluindo quanto à sua atuação para conter os ataques virtuais e as ações de guerra cibernética. Segundo Carneiro (2012),o Ministério da Defesa classifica as ações no ciberespaço em três níveis. O Nível Político é chamado de Segurança da Informação e Comunicações (SIC), o qual abrange um conceito acima do ciberespaço, conhecido como *cyber security*, que corresponde à participação de todas as agências do Governo Federal e de bases nacionais de infraestrutura crítica dos setores público e privado. O Nível Estratégico corresponde à defesa cibernética, com as ações realizadas pelo Ministério da Defesa em coordenação com outros Ministérios. No Nível Operacional

e Tático, as ações são chamadas de guerra cibernética, sendo dependentes de cada uma das Forças Armadas.

Agostini (2014) comenta que a atuação do Exército Brasileiro tem se sobressaído frente à das demais Forças Armadas por sua dedicação e pelos avanços na formação especializada de suas equipes e no desenvolvimento de soluções de alto nível tecnológico. Não se pode negar que o ciberespaço oferece muitas possibilidades para os seus usuários, tanto para fins benéficos quanto como verdadeiras armas de guerra. Por isso, é fundamental que as Forças Armadas invistam não apenas em treinamento com armas e estratégias de guerra, mas, especialmente, em inteligência e capacidade técnica para lidar com a cibernética.

A cooperação interagências em nível nacional e internacional é um fator fundamental para a eficácia da logística voltada a operações militares e ao combate aos crimes virtuais no Brasil. Nesse diapasão, a missão de conduzir operações contra ameaças cibernéticas apresenta uma ideia nova do ponto de vista da doutrina, com conceitos de defesa, exploração e ataque à rede de computadores (guerra cibernética),considerando a quebra de barreiras geográficas trazida pelas tecnologias da informação, podendo ser solicitada quando o provedor responsável pelo serviço de onde foi praticado o crime virtual for localizado no exterior, não contando com subsidiária dentro do país. Caso exista subsidiária, como é o caso de Facebook, Google, Microsoft e Twitter, por exemplo, não há necessidade de cooperação internacional, sendo os criminosos submetidos à jurisdição brasileira (BRASIL, 2017c).

Frente a todo o exposto, cabe considerar que, de vários atores com motivações variadas, os ataques contra os sistemas de informação tornaram-se uma grande ameaça, cuja recente multiplicação demonstra a realidade, e diante da qual uma proteção fixa já não é suficiente (GONÇALVES, 2002). De acordo com Cruz Júnior (2013, p.9):

> Defesa cibernética diz respeito ao conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. Segurança cibernética refere-se à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos

> públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da administração pública federal.

A passagem de uma estratégia de defesa passiva para uma estratégia ativa de defesa em profundidade, combinando sistemas de proteção intrínsecos, acompanhamento permanente, resposta rápida e ação ofensiva, requer um forte pulso governamental e uma mudança de pensamento (BARBOSA, 2019).

A *expertise* do Estado na segurança dos sistemas de informação deve ser fortemente desenvolvida, mantida e disseminada para os agentes econômicos, particularmente os operadores de rede. A natureza imediata e quase imprevisível dos ataques também requer capacidade de gestão de crise e pós-crise, assegurando a continuidade dos negócios e possibilitando a acusação e a repressão dos agressores.

Além disso, como o ciberespaço transformou-se em um novo campo de ação no qual já estão ocorrendo operações militares, o Brasil terá que desenvolver uma capacidade de lutar nesse espaço. É imprescindível que a cadeia de defesa cibernética esteja presente em todas as entidades e atividades dos Ministérios e das Forças Armadas. A organização adotada deve, portanto, ser desdobrada nas entidades elementares, a fim de garantir a plena continuidade da ação no mais profundo dos sistemas, com uma reatividade correspondente à velocidade dos ataques (BRASIL,2014b).

A doutrina de defesa cibernética destina-se, sobretudo, às autoridades militares e civis do Ministério da Defesa, encarregadas dos principais mandamentos ou responsabilidades de gestão.

Pretende-se ser a referência a partir da qual cada agência departamental deve definir e estabelecer uma estrutura de defesa cibernética e uma organização permanente para a defesa dos sistemas de informação (BRASIL, 2014b). Com base no conceito de defesa cibernética, que lembra os elementos essenciais, sua finalidade é:

a) formalizar as funções e os meios necessários para a defesa cibernética – dispor dos recursos e dos meios, conhecer e antecipar, prevenir, intervir e restabelecer os princípios e os métodos segundo os quais se realiza a defesa dos sistemas de informação (ciclo do combate à informática defensiva e forças a serem implementadas);

b) organizar e distribuir responsabilidades de defesa cibernética dentro do Ministério, no que se refere a relações com parceiros nacionais e relações com parceiros estrangeiros.

Em resumo, o ciberespaço surge como um novo espaço de confronto militar, que deve ser apreendido de acordo com uma abordagem operacional em vigor, em todos os ambientes de ação (Terra, Ar, Mar, Espaço). E a guerra cibernética, como forma de proteção, complementa – dentro de uma nova capacidade global da cibersegurança– a abordagem clássica à segurança dos sistemas de informação, em benefício da eficácia militar.

3 RESULTADOS E DISCUSSÕES

A função de combate logística desempenha um papel relevante no sucesso das operações militares, devendo ser planejada em tempo de paz e sincronizada com todas as ações a serem desenvolvidas, além de ser meticulosamente coordenada para que os recursos sejam disponibilizados aos usuários em todos os níveis (BRASIL, 2014b).

O planejamento logístico sincronizado tem o objetivo de manter prontidão operativa, aumentando o poder de combate da força apoiada no espaço da batalha, abrangendo o espaço cibernético, sendo que a capacidade de mobilização militar é um fator que deve ser considerado nos planejamentos logísticos, na medida em que é preciso ter elasticidade na função de poder de combate. Com isso, é preciso enquadrar as unidades de combate para proteção, quando necessário (BRASIL, 2018b).

Vale destacar que todo o planejamento, a coordenação e a execução da logística militar têm como elo de cadeia a Força Operacional, sendo a sua organização realizada considerando os seguintes fatores:

> a) a ameaça visualizada no planejamento operacional; b) as dimensões da área de responsabilidade; c) a quantidade de G Cmdo, GU e U a serem empregadas; d) a disponibilidade de recursos logísticos disponibilizados pelo C Op; e) as necessidades logísticas para cada fase das operações planejadas; f) a necessidade de contratação e/ou mobilização de meios civis; g) a possibilidade de o oponente atuar nos eixos de transporte e nas estruturas logísticas desdobradas na ZC; h) a possibilidade de danos colaterais à população civil, decorrentes de prováveis ações do oponente sobre as instalações logísticas; e i) a disponibilidade de recursos de TIC e de C2 (BRASIL, 2014b, p. 7).

Nesse contexto, faz-se importante mencionar a Base Logística Conjunta (Ba Log Cj), que consiste em um agrupamento temporário para a realização do apoio logístico às Forças Operacionais, organizada com vistas a explorar ao máximo as capacidades logísticas das organizações e dos sistemas informatizados que a compõem.

Para melhorar as ações logísticas, pode ainda ser instituída a Base Logística Terrestre (BLT), de acordo com as distâncias de apoio e a natureza e o valor da força a sustentar. A Figura 1 apresenta um exemplo de desdobramento da BLT.

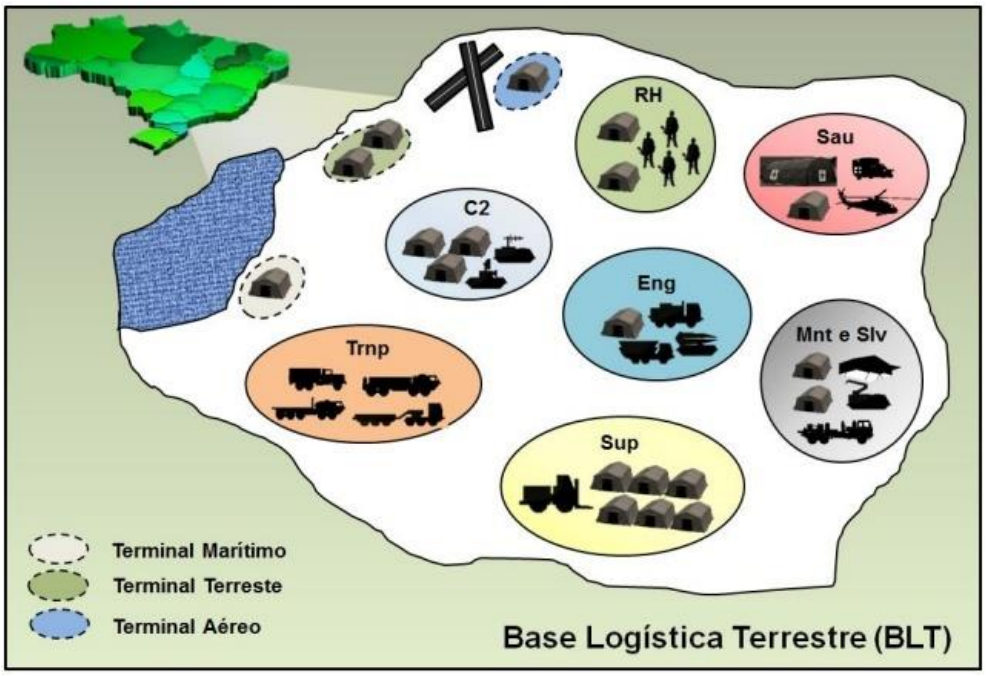

FIGURA 1 - Exemplo de BLT[1]
Fonte: MINISTÉRIO DA DEFESA, 2014

Em campo de combate, o Exército também conta com uma Base Logística de Brigada (BLB), que é organizada de forma modular e fundamentada para proporcionar certo grau de autonomia à Força Operacional apoiada. Cumpre acrescentar, ainda, a existência o Destacamento Logístico (Dst Log), que consiste em uma estrutura flexível, modular e adaptada às necessidades logísticas do elemento apoiado, tendo como objetivo proporcionar apoio logístico cerrado e contínuo (BRASIL, 2014b).

[1] A Figura 1 apresenta um exemplo dos módulos dos Grupos Funcionais Suprimento (Sup), Manutenção (Mnt), Transporte (Trnp), Recursos Humanos (RH), Saúde (Sau), Engenharia (Eng) e Salvamento (Slv), oriundos de um Gpt Log, desdobrados em uma BLT. Para a sua composição, podem ser utilizados recursos recebidos da Região Militar (RM) e dos Grupamentos de Engenharia (GptEng), para a ampliação da capacidade de apoio nas áreas de RH, Sau e Eng.

Importante observar que, dentre os aspectos do ambiente operacional que devem ser considerados na definição das capacidades das Forças Militares, cabem ser citados:

> A proliferação das novas tecnologias em materiais de emprego militar, permitindo que indivíduos ou grupos não estatais disponham desses meios e os utilizem como arma; o emprego dos meios cibernéticos, informacionais e sociais como instrumentos de guerra, fragilizando as fronteiras geográficas; a utilização da informação como arma, afetando diretamente o poder de combate dos beligerantes (BRASIL, 2018b, p. 2).

A proteção de recursos e informações logísticas é dimensionada conforme o gerenciamento do risco logístico, tendo em vista a necessidade de se manter a continuidade do apoio logístico, posto que o crescente emprego de recursos deTecnologia da Informação e Comunicação(TIC) nas tarefas de apoio logístico exige a aplicação de medidas de proteção desses sistemas, em face das ameaças cibernéticas, para que seja possível mitigar as vulnerabilidades e o risco de comprometer o fluxo das informações da cadeia logística (BRASIL, 2018b).

Compreende, a guerra cibernética, o uso ofensivo e defensivo de informação e sistemas de informação para negar, corromper ou destruir a capacidade do adversário em um contexto de operação militar, bem como ações que envolvem ferramentas de TIC para tirar proveito dos Sistemas de Tecnologia da Informação para o comando e controle do oponente (BRASIL,2017c).

No Brasil, em consonância com a atribuição da função da autoridade nacional para a defesa dos sistemas de informação, a defesa dos sistemas genéricos de informação e comunicação do Ministério da Defesa e dos sistemas específicos das Forças Armadas foi confiada às Forças Armadas.

De acordo com Agostini (2014), o Exército Brasileiro vem se destacando na execução desse plano estratégico, conduzindo as políticas, os debates públicos e os projetos do setor cibernético para o país, além de ter sido fundamental na segurança dos eventos mundiais realizados em território nacional, como a Conferência Rio+20, a Copa das Confederações e a Copa do Mundo.

Em 2014, o Chefe do Estado-Maior do Exército, General Joaquim Silva e Luna, aprovou o Manual de Campanha EB20-MC-10.204 LOGÍSTICA, 3ª edição, que estabelece as diretrizes e os protocolos para os setores responsáveis pela logística das ações das Forças Armadas (BRASIL, 2014c). A Logística, segundo o documento, “[...] deve ser capaz de prever e prover o apoio em materiais e serviços

necessários para assegurar a essa força liberdade de ação, amplitude do alcance operativo e capacidade de durar na ação" (BRASIL, 2014c, prefácio).

No item "Proteção dos Recursos Logísticos", a preocupação com o ciberespaço aparece descrita da seguinte forma:

> 6.4.6 O crescente emprego de recursos de TIC nas tarefas de apoio logístico requer medidas de proteção desses sistemas, em face das ameaças cibernéticas, visando a mitigar as vulnerabilidades e o risco de comprometimento do fluxo das informações da cadeia logística (BRASIL, 2014c, p. 6).

No âmbito das Forças Armadas, o Exército Brasileiro, em parceria com o Serviço Federal de Processamento de Dados (SERPRO), construiu o Centro de Defesa Cibernética (CDCiber), voltado para o desenvolvimento de um complexo militar-universitário empresarial, capaz de atuar na fronteira de tecnologias que terão quase sempre utilidade dual, militar e civil (CENTRO DE DEFESA CIBERNÉTICA, 2014).

Para se adaptar a essas novas ameaças, é imprescindível ter uma visão compartilhada e um projeto geral, dentro do Ministério da Defesa, acerca do que a defesa cibernética envolve. Isso possibilitará estabelecer, dentro da defesa, um entendimento comum e uma garantia de maior eficiência, bem como ter uma referência indispensável às interações com os atores nacionais e internacionais do campo.

No quesito da Logística, a Estratégia Nacional de Defesa, publicada em 2008 e revisada em 2012, privilegia a aceleração da integração entre as Forças Armadas no âmbito de tecnologia industrial básica, logística e mobilização, comando e controle, e operações conjuntas. Nesse sentido:

> 1) O Ministério da Defesa, por intermédio da SEPRO, ficará encarregado de formular e dirigir a política de obtenção de produtos de defesa.
> 2) O Ministério da Defesa, por intermédio da SEPRO, ficará encarregado da coordenação dos processos de certificação, de metrologia, de normatização e de fomento industrial.
> 3) O Ministério da Defesa incentivará, junto às esferas do Governo federal, a ampliação e a compatibilização da infraestrutura logística terrestre, portuária, aquaviária, aeroespacial, aeroportuária e de telemática, visando os interesses da defesa (BRASIL, 2008, p. 131).

O Governo assumiu o espaço cibernético como um dos setores estratégicos mais importantes para a defesa do país, e decidiu investir em capacitação para a utilização do ciberespaço de forma industrial, educativa e militar. O Plano de Defesa define como prioridade as tecnologias de comunicação entre as Forças Armadas, visando à atuação em rede.

As ações de guerra cibernética têm como escopo negar o acesso virtual às estruturas de TIC das tropas do Exército por parte do oponente ou na tentativa de manipulá-lo (BRASIL, 2017a). Para a função de combate logística, o espaço cibernético deve se guiar por princípios da defesa cibernética, quais sejam princípio do efeito, princípio da dissimulação, princípio da rastreabilidade e princípio da adaptabilidade (BRASIL, 2014b).

No entender deMandarino (2009), a guerra cibernética consiste em atacar a informação no ciberespaço, utilizando diversas formas de ação, do terrorismo à destruição da infraestrutura total da informação, causando assimetria de poder econômico, capacidade militar e estrutura organizacional de uma nação. Essas ações obtêm vantagens civis ou militares. Portanto, a modernização dos sistemas militares traz vulnerabilidades que permitem ações que podem atrapalhar as redes de computadores para os sistemas de armas. Ela afeta aqueles que precisam sincronizar ações no tempo e no espaço, afetando a liderança e a capacidade de tomar decisões em diferentes níveis.

Desse modo, é necessária uma doutrina cibernética alinhada em todos os níveis, englobando os diversos atores envolvidos em Segurança da Informação e Comunicações no Governo Federal, com o objetivo de atuar como Estado-nação, a fim de facilitar e garantir a sua disponibilidade, integridade, confidencialidade e autenticidade.

O plano diretor de capacidade identifica, dimensiona e avalia o que faz parte da função de cibersegurança transversal, com a melhor compreensão do seu impacto potencial, descrevendo as ações necessárias para as funções específicas dos sistemas de informação a serem colocadas na segurança cibernética. A definição de objetivos de capacidade pelos operadores deve incluir: recursos de segurança cibernética específicos dos programas de armas, que devem ser tidos em conta nos envelopes dos programas de armas em causa;e segurança cibernética necessária para os sistemas de informação existentes, que se destinam a ser levados em consideração nos envelopes dos operadores de quem é a responsabilidade. Nesse diapasão, um elo fraco pode comprometer toda a cadeia de cibersegurança, devido a uma vulnerabilidade que permite que um invasor contorne a defesa.

Destaca-se que quanto mais desenvolvido for um sistema, mais ele é vulnerável às ações cibernéticas, e o oponente deve possuir mais condições de se

defender dos ataques cibernéticos conforme o seu grau de desenvolvimento tecnológico. Com isso, a utilização de ações de guerra cibernética garantindo a segurança de dados logísticos no ambiente operacional e tático deve ser empregada para obter o efeito desejado(BRASIL, 2014b).

Na Logística Militar, a proteção cibernética deve desenvolver ações para neutralizar ataques cibernéticos contra os dispositivos computacionais militares, incrementando ações de segurança, defesa e guerra cibernética em uma situação de conflito. Em nível tático, as ações cibernéticas ficam a cargo das Forças Componentes, com os seus elementos de guerra cibernética quando ativados.

É fundamental que o CDCiber mantenha um canal técnico com os Órgãos de Inteligência das Forças Armadas no âmbito do Sistema de Inteligência de Defesa (SINDE) para a difusão de dados obtidos por meio da fonte cibernética. Devem os níveis de alerta cibernéticos ser usados em situações em que haja probabilidade de se concretizar uma ameaça cibernética no espaço militar.

Além disso, deve o CDCiberproduzir conhecimento exclusivo da fonte cibernética e empregar conhecimento de outras fontes para que haja um melhor desempenho das suas funções (BRASIL, 2014b).

O Ministério da Defesa deve ser capaz de operar com segurança em um ambiente cada vez mais digital e garantir compromissos operacionais, não obstante os possíveis ataques aos sistemas. Para isso, conta com a proteção dos sistemas de informação e da defesa cibernética, que inclui uma defesa ativa e profunda dos sistemas de informação e da capacidade de gerenciamento de crises cibernéticas.

Os efeitos de um incidente ou ataque, com o risco de disseminação rápida e de contágio a outros sistemas, requerem o estabelecimento de um dispositivo reativo, essencial para o controle da defesa cibernética e a condução de intervenções de controle.

As consequências do insucesso, da corrupção ou do encerramento de um sistema sobre o funcionamento do Departamento de Defesa e a conduta de compromissos operacionais exigem uma estreita cooperação entre a cadeia de comando das operações de ciberdefesa e o Ministério da Defesa. Finalmente, a evolução rápida e constante do campo, a sua dualidade intrínseca, juntamente com a partilha das mesmas ameaças, tanto com parceiros quanto com o Governo e a sociedade civil, exigem uma coordenação central, organização e interlocutores bem identificados.

Essas necessidades orientaram a definição de uma organização única e centralizada, responsável pela direção geral do campo e pela gestão operacional da defesa dos sistemas de informação sob a autoridade do Chefe do Departamento de Defesa.

4 CONSIDERAÇÕES FINAIS

Diante de todo o exposto neste estudo, pode-se concluir que, se não existir um sistema de segurança cibernética robusto, a logística em qualquer tipo de operação militar fica totalmente comprometida.

Desse modo, considerando o cenário atual, nenhum tipo de operação militar consegue ser executado eficazmente, se não houver uma proteção do espaço cibernético voltada para as suas informações logísticas.

Frisa-se, assim, como conclusão, que a defesa cibernética, por intermédio da guerra cibernética, é de suma importância para proteger os ciberdados logísticos em qualquer tipo de operação militar.

Analisando as diretrizes estratégicas do Plano Nacional de Defesa do Brasil, bem como o extenso arcabouço documental de operações de guerra cibernética no âmbito do Exército Brasileiro, observa-se que o nível estratégico tem necessidades fundamentais de coordenação.

A Inteligência do Exército Brasileiro apresenta os mesmos poderes de coordenação do nível político, além de ter que centralizar os seus esforços para alcançar uma melhor interoperabilidade entre as Forças e a sinergia de seus meios.

A defesa cibernética precisa aumentar a coordenação não apenas entre as Forças Armadas, mas também para outras agências, por meio dos elos sincronizados entre os seus sistemas de comando e controle. No entanto, a condução das ações deve sempre ser realizada pelo Ministério da Defesa, devido à sua capacidade de integrar outras habilidades relacionadas à defesa nacional. Assim, o referido Ministério torna-se o único elo entre os Níveis Político e Operacional.

O ciberespaço tornou os recursos de aprendizagem aptos a proporcionar um terreno de destruição, pois, com as suas habilidades de invasão,tentam causar danos a diversos Órgãos, agências reguladoras, iniciativa privada de uma forma geral, e também ao Exército Brasileiro.

Ao final do estudo, foi possível verificar que o apoio logístico em operações no amplo espectro atual, envolvendo atividades interagências, é muito complexo e exige integração, coordenação e sincronização no comando e controle dos diversos Órgãos.

Constatou-se, também, que o espaço cibernético nessas operações militares é bastante vulnerável, tendo em vista o crescente avanço das habilidades dos invasores.

No mais, o estudo demonstrou, ainda, que a guerra cibernética corresponde ao uso de informações para explorar e degradar o adversário, buscando mitigar os riscos dessa problemática, sendo fundamental para assegurar a eficiência e a continuidade do apoio logístico nessas operações militares, pois, se o inimigo conseguir invadir, distorcer, danificar ou manipular qualquer sistema de comando e controle relativo à logística, toda a operação militar estará totalmente comprometida. Vidas serão colocadas em risco e as consequências são incomensuráveis.

Os ciberdados logísticos devem contar com proteção dos sistemas de informação e da defesa cibernética, que inclui uma defesa ativa e profunda dos sistemas de informação e da capacidade de gerenciamento de crises cibernéticas, negando, assim, o acesso às informações e aos dados das atividades das tropas, direcionando-se por um meio de informação ou de uma mensagem em si.

Por derradeiro, é importante mencionar que o presente estudo foi limitado pelo acesso às informações como possíveis ataques a dados e informações logísticas nas operações militares, bem como a maiores detalhes sobre como o processo de guerra cibernética é realizado, por serem informações sigilosas, dados os riscos que poderiam ocorrer ao se deixar os invasores terem contato com tais informações, comprometendo toda uma estrutura logística de conflito armado em tempos de guerra e de não guerra.

Cabe notar que, dentre as principais dificuldades da Logística do Exército Brasileiro, estão: a identificação da origem dos ataques cibernéticos; a quase impossibilidade de se manter a invulnerabilidade de seus próprios sistemas de computação; os obstáculos em identificar e recrutar material humano especializado; a vulnerabilidade a ataques de ações assimétricas; e, finalmente, uma grande dificuldade em monitorar os avanços tecnológicos.

Houve, sim, melhorias ao longo do tempo e aprendizados com as experiências dos grandes eventos. Mas ainda é necessário investir mais em

educação, capacitação e melhoramento das habilidades técnicas em recursos humanos.

Destaca-se, ainda, após a conclusão deste trabalho, que a pesquisa científica acerca da segurança das informações logísticas nas operações militares deve ser fomentada e estimulada para que as doutrinas a esse respeito se consolidem, bem como deve ser estimulada a busca,nos bancos acadêmicos, de uma maior interação e interoperabilidade entre as Forças Armadas e diversos Órgãos, por intermédio de discussões, palestras e estudos que agreguem conhecimento sobre o tema.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE DIREITO DO ESTADO. **Comentários ao Marco Civil da Internet**: Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: ABDET, 2014.

AGOSTINI, Marcos Tocchetto. **A cibernética sob a ótica do fenômeno da guerra e da agenda de segurança**. 2014. Monografia (Bacharelado em Relações Internacionais) – Universidade Federal de Santa Catarina, Florianópolis, 2014.

ARANHA FILHO, Adalberto José Q. T. de Camargo. Crimes na internet e a legislação vigente. **Revista Literária de Direito**, São Paulo, v.9, n.44, p. 23-25, out./dez. 2002.

BARBOSA, Daniel Cunha. Defesa em profundidade: como aplicar essa estratégia de defesa de redes em qualquer ambiente. **WeLiveSecurity**, [*S.l.*], 2019. Disponível em: https://www.welivesecurity.com/br/2019/02/04/defesa-em-profundidade-como-aplicar-essa-estrategia-de-defesa-de-redes-em-qualquer-ambiente/. Acesso: 20 jul. 2019.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 10 jul. 2019.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 jul. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, [2018a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 jul. 2019.

BRASIL. Ministério da Defesa. Exército Brasileiro.**Doutrina Militar de Defesa Cibernética**. Brasília, DF: Exército Brasileiro,2014b.

BRASIL. Ministério da Defesa. Exército Brasileiro.**Estratégia Nacional de Defesa**. Brasília, DF: Exército Brasileiro,2008. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 15 jul. 2019.

BRASIL. Ministério da Defesa. Exército Brasileiro.**Manual de Campanha**: Logística. 3. ed. Brasília, DF: Exército Brasileiro,2014c.

BRASIL. Ministério da Defesa. Exército Brasileiro.**Manual de Campanha**: Logística Militar Terrestre. Brasília, DF: Exército Brasileiro, 2018b.

BRASIL. Ministério da Defesa. Exército Brasileiro.**Manual de Campanha**: Operações. 5. ed.Brasília, DF: Exército Brasileiro,2017a.

BRASIL. Ministério da Defesa. Exército Brasileiro. Secretaria de Ciência e Tecnologia. **Memória nº 010-A/4-04-SCT, de 08 de abril de 2004**. Guerra Cibernética e Segurança da Informação. Brasília, DF: Exército Brasileiro, 2004.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão. **Roteiro de atuação**: crimes cibernéticos. Brasília, DF: MPF/2ªCCR, 2017b.

BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017c.

CARDOSO**,**Fabio Fettuccia.O combate à criminalidade cibernética no Brasil: parâmetros objetivos de tipicidade. **JusBrasil**, [*S.l.*], 2015.Disponível em: https://fabiofettuccia.jusbrasil.com.br/artigos/180688749/o-combate-a-criminalidade-cibernetica-no-brasil-parametros-objetivos-de-tipicidade. Acessoem: 2 jul. 2019.

CASTELLS, Manuel. **The rise of the network society**. Malden: Wiley-Blackwell, 2010.

CENTRO DE DEFESA CIBERNÉTICA. CDCIBER: perspectivas em face da espionagem eletrônica. *In*: CURSO DE EXTENSÃO EM DEFESA NACIONAL, 8., 2014, Belém. **Anais** [...]. Belém: UNAMA, 2014.

COUTINHO, Isadora Caroline Coelho. Pedofilia na era digital. **Âmbito Jurídico**, Rio Grande, XIV, n. 91, ago. 2011. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10082. Acesso em: 12 jul. 2019.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

CRUZ JÚNIOR, Samuel de César. A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual.**Texto para Discussão do IPEA**, Brasília, DF, n. 1805, jul. 2013. Disponível em: http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1850.pdf. Acesso em: 15 ago. 2019.

FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO. **Cartilha de proteção de dados pessoais**. São Paulo: FIESP, 2019.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

FLICK, Uwe. **Uma introdução à pesquisa qualitativa**. Porto Alegre: Artmed, 2004.

FLORÊNCIO FILHO, Marco Aurélio *et al*. **Marco civil da internet**: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014.

GIDDENS, Anthony. **Sociologia**. 4. ed. Porto Alegre: Artmed, 2005.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

GONÇALVES, Júlio César. **O gerenciamento da informação e sua segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico**. 2002. Dissertação (Mestrado em Administração) – Faculdade de Economia, Contabilidade e Administração, Universidade de Taubaté,Taubaté, 2002.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2001.

MANDARINO Jr, Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético**. 2009. Monografia (Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações)– Universidade de Brasília,Brasília, DF, 2009.

McGINNIS, Michael A. Military logistics.**International Journal of Physical Distribution & Logistics Management**, Bradford, v.22, n.2, p. 22-32, abr. 1992.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via internet.**Charlie Oscar Tango**, [*S.l.*], 2013. Disponível em: http://www.charlieoscartango.com.br/cot-diversos-artigobaeta.html. Acesso em: 3 jul. 2019.

PALAZZI, Pablo Andrés.**Delitosinformáticos**. Buenos Aires: Ad Hoc, 2000.

REIS, Flavio Américo dos. Military logistics in natural disasters: the use of the NATO response force in assistance to the Pakistan earthquake relief efforts. **Contexto Internacional**, Rio de Janeiro, v.40, n.1, p.73-96, 2018.

ROESCH, Sylvia Maria Azevedo. **Projetos de estágio e de pesquisa em administração**. 3. ed. São Paulo: Atlas, 2005.

ROSA, Fabrízio. **Crimes de informática**. Campinas: Bookseller, 2005.

ROSSINI, Augusto. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SILVA, Carlos Alberto Vicente da; MUSETTI, Marcel Andreotti. Logísticas militar e empresarial: uma abordagem reflexiva. **Revista de Administração - RAUSP**, São Paulo, v. 38, n. 4, p. 343-354, 2003.

SILVA, Welder Cassimiro da.**A ausência de segurança jurídica na legislação brasileira mediante aos crimes cibernéticos**. 2013. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Fundação Universidade Federal de Rondônia, Cacoal, 2013.

SOUZA, Larissa Anne de Moraes. A dificuldade da repressão aos crimes virtuais. **Interm@s**, [*S.l.*], v. 30, n. 30, p. 1281-1677, 2015.