ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP ART JOFFRE FERREIRA ABDALLA

DOMÍNIO DO ESPAÇO CIBERNÉRTICO POR UM PAÍS: UMA ANÁLISE DA PRESENÇA DO EXÉRCITO BRASILEIRO NO DOMÍNIO CIBERNÉTICO

Rio de Janeiro
2020

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP ART JOFFRE FERREIRA ABDALLA

O DOMÍNIO DO ESPAÇO CIBERNÉRTICO POR UM PAÍS: UMA ANÁLISE DA PRESENÇA DO EXÉRCITO BRASILEIRO NO DOMÍNIO CIBERNÉTICO

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

Rio de Janeiro
2020

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 Art JOFFRE FERREIRA ABDALLA**

Título: **O DOMÍNIO DO ESPAÇO CIBERNÉRTICO POR UM PAÍS: UMA ANÁLISE DA PRESENÇA DO EXÉRCITO BRASILEIRO NO DOMÍNIO CIBERNÉTICO**

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

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **RENATO MACEDO BIONE DA SILVA - Maj** Cmt Curso e Presidente da Comissão	
_____ **BRUNO VINÍCIUS SILVA VITAL - Cap** 1º Membro	
_____ **JOSÉ RODOLFO BARBOSA ANELLI - Cap** 2º Membro e Orientador	

_____
JOFFRE FERREIRA ABDALLA – Cap
Aluno

O DOMÍNIO DO ESPAÇO CIBERNÉRTICO POR UM PAÍS: UMA ANÁLISE DA PRESENÇA DO EXÉRCITO BRASILEIRO NO DOMÍNIO CIBERNÉTICO

Joffre Ferreira Abdalla*
José Rodolfo Barbosa Anelli**

RESUMO

A rede de dados surgiu a partir da integração das telecomunicações com os meios computacionais. Esta rede é a base da sociedade atual para a circulação de informações de serviços, indústrias e até mesmo de informações restritas aos Estados e as suas Forças Armadas. Neste ambiente em que circulam as informações, analisa-se a importância de um Estado soberano ser capaz de se proteger contra possíveis invasões e, desta forma, garantir o domínio do espaço cibernético nacional, a segurança da informação, bem como das infraestruturas críticas nacionais que dela dependem. Alinhado a isso, em sua Estratégia Nacional de Defesa (END) o Brasil prevê o desenvolvimento do setor cibernético como fundamental para a defesa nacional, o qual fica a cargo do Ministério da Defesa. Para tanto, foi delegado ao Exército Brasileiro a gestão da Defesa Cibernética. Destarte, este trabalho analisa a presença do Exército Brasileiro no espaço cibernético à luz de sua estrutura, doutrina e capacidades essenciais para garantir este domínio nacional através da Defesa Cibernética.

Palavras-chave: Espaço cibernético. Defesa Cibernética. Guerra Cibernética.

ABSTRACT

The data network emerged from the integration of telecommunications with computational media. This network is the basis of today's society for the circulation of information on services, industries and even restricted information from States and their Armed Forces. In that environment in which information circulates, we analyze the importance of a sovereign state being able to protect itself against possible invasions. This way, it guarantees the domination of the national cyberspace and the security of information and the national critical infrastructures that depend on it. Aligned to this, Brazil foresees in its National Strategy Defense, in Portuguese *Estratégia Nacional de Defesa* (END) and the development of the cyber sector as fundamental for national defense, under the responsibility of the Ministry of Defense. In order to achieve that purpose, the management of Cyber Defense was delegated to the Brazilian Army. Thus, this paper analyzes the presence of the Brazilian Army in cyber space in the light of its structure, doctrine and essential capabilities to guarantee this national domination through Cyber Defense

Keywords: Cyberspace, Cyber Defense, Brazilian Army, Cyberwar.

* Capitão da Arma de Artilharia. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2010.

** Capitão da Arma de Artilharia. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2008. Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (ESAO) em 2018.

1 INTRODUÇÃO

Nos últimos tempos ocorreram mudanças em todos os segmentos da sociedade que modificaram comportamentos ante a nova realidade.

Com a evolução constante dos meios de Tecnologia da Informação e Comunicação (TIC) no século XXI (2001 – dias atuais), a sociedade alterou rapidamente seus hábitos, migrando muitas de suas atividades do mundo físico para um ambiente virtual, no qual é possível se comunicar com alcance global e instantâneo, comercializar, estudar e descansar. Assim surgiu o espaço cibernético.

Como extrato da sociedade, no campo da Defesa não foi diferente. Materiais bélicos foram modernizados com as TICs para que as nações que adquirissem estes meios inovadores aperfeiçoassem suas operações militares e, assim, obtivessem vantagem operacional e estratégica.

Diante deste panorama de evolução tecnológica e visando a proteção de sua soberania, o estado brasileiro definiu, através da Estratégia Nacional de Defesa (END), em dezembro de 2008, três setores como essenciais para a Defesa Nacional, a cargo do Ministério da Defesa (MD): o espacial, o cibernético e o nuclear. Em 2009, a Diretriz Ministerial/MD nº 14 estabeleceu providências para o cumprimento da END relativas a estes setores estratégicos, delegando as responsabilidades as suas Forças Armadas.

Assim, a coordenação e a integração do setor espacial ficaram a cargo da Força Aérea Brasileira (FAB). A Marinha do Brasil (MB) ficou responsável pelo setor nuclear e ao Exército Brasileiro (EB) coube as atividades do setor cibernético.

Desta forma, para viabilizar a END o MD executa em nível estratégico a Defesa Cibernética, esta que é uma atividade integrada das Forças Armadas e liderada pelo EB com a intenção de resguardar os interesses da Defesa Nacional relativos ao espaço cibernético.

1.2 PROBLEMA

Neste contexto de atuação no espaço cibernético surgiu o Quinto Domínio Operacional, situado em um espaço virtual composto por dispositivos computacionais conectados em rede ou não, onde as informações digitais transitam,

são processadas e/ou armazenadas: o Espaço Cibernético (BRASIL, 2014a). De forma complementar, Da Silva (2014, p. 195) afirma que:

> Cada vez mais computadores, seus equipamentos de interconexão, sistemas de comando, controle, comunicações e informação (C^3I) e sistemas de apoio à decisão compõem o espaço cibernético militar, em que a informação é o objetivo maior. Dessa forma, esse espaço se tornou fundamental na guerra, em decorrência da grande importância militar dos computadores e de suas redes para a circulação de ordens ou informações.

Decorrente da necessidade de atuação no espaço cibernético para obtenção de vantagens entre as nações, surgiu a Guerra Cibernética, definida por Júnior, Villar-Lopes e Freitas (2017, p. 32) como “[...] uma modalidade beligerante de uso e atuação predominantes do ambiente cibernético para obter informações privilegiadas e/ou desestabilizar sistemas computadorizados de um país”.

Desta forma, observa-se que as Nações entendem o domínio cibernético como fonte de informações estratégicas para o campo da inteligência e como um ambiente para a realização de operações militares de caráter preparatório, complementar ou até mesmo decisivo. Para que isto ocorra, é necessário que um Estado-Nação tenha vantagem da atuação sobre o espaço cibernético de outra Nação. Naturalmente, esta vantagem só é possível se houver o domínio deste campo.

Diante disso, depara-se com a seguinte problemática: Como o Exército Brasileiro está inserido no setor cibernético para garantir o domínio do espaço cibernético nacional?

1.3 OBJETIVOS

O objetivo geral deste estudo consiste em responder a problemática supracitada de modo que consiga esclarecer, doutrinariamente, como o Exército Brasileiro está inserido no setor cibernético para garantir o domínio do espaço cibernético nacional.

Para substanciar esta resposta e consequentemente atingir o objetivo geral, foram traçados os seguintes objetivos específicos:

a) esclarecer conceitos e percepções a cerca do tema guerra cibernética;

b) esclarecer a organização do Exército Brasileiro no setor cibernético;

c) analisar os princípios, as possibilidades e as limitações das operações no espaço cibernético adotadas pelo EB;

d) esclarecer a definição de domínio do Espaço Cibernético.

1.4 JUSTIFICATIVAS E CONTRIBUIÇÕES

Como citado anteriormente, a END estabeleceu o ramo cibernético como um dos três setores essenciais para a Defesa Nacional. Em consonância com esta importância e com suas atribuições no setor cibernético, em 2015 o Exército Brasileiro inaugurou dois núcleos de Defesa cibernética. Na ocasião, o Gen Div Carvalho, então Chefe do Centro de Defesa Cibernética do Exército (CDCiber), afirmou ao noticiário do Exército que a Defesa Cibernética integra e coordena um campo em constante transformação e que não pode abrir mão do conhecimento e da prática.

Contudo, os aspectos da defesa e da guerra cibernética ainda são pouco disseminados em ambiente militar, onde a guerra de fricção inserida nos domínios operacionais terrestre, marítimo e aéreo é assunto preponderante.

Desta forma, o estudo visa nivelar o conhecimento a respeito da influência do domínio operacional cibernético na geopolítica contemporânea, assim como explorar a atuação do Exército Brasileiro neste ambiente. Concomitantemente, promover uma discussão oportuna e de grande valia para a Defesa Nacional e, assim, contribuir para a ambientação e difusão do assunto entre os integrantes das Forças Armadas brasileiras, isso devido a relevância do assunto para manutenção da soberania do país.

2 METODOLOGIA

Para obter subsídios que permitissem formular uma possível resposta para o problema elencado, o delineamento metodológico deste estudo baseou-se em um pesquisa bibliográfica com adoção da coleta de dados, leitura analítica, fichamento das fontes e, por fim, discussão dos resultados encontrados.

Quanto à forma de abordagem do problema, utilizou-se principalmente os conceitos de pesquisa **qualitativa,** apresentando o resultado através de análises, de

modo que fosse possível vincular o discurso teórico da pesquisa - baseada em publicações doutrinárias – com a realidade da geopolítica registrada em bibliografias reconhecidas.

Quanto ao objetivo geral foi empregada a modalidade **exploratória** tendo em vista a necessidade de difundir conceitos acerca do tema, e assim, através de respostas parciais, chegar à resolução do problema-chave pesquisado.

2.1 REVISÃO DE LITERATURA

Inicialmente foram consultados manuais doutrinários, artigos científicos e publicações periódicas para que se fosse possível nivelar o conhecimento teórico acerca do assunto espaço cibernético.

Em seguida, para desenvolver o tema delimitado, buscou-se o Aparato Legal para atuação do Exército Brasileiro no espaço cibernético. Para isto foi utilizada toda legislação vigente publicada pelo estado brasileiro, composta, dentre outros, pela Constituição Federal de 1988, pela Política Nacional de Defesa (PND), pela Estratégia Nacional de Defesa (END), pelo Livro Branco de Defesa Nacional e pela Estratégia Nacional de Segurança Cibernética (Decreto 10.222).

Os manuais militares que tratam sobre a doutrina de Defesa Cibernética foram examinados a fim de desenvolver a análise dos princípios de emprego, possibilidades e limitações das ações cibernéticas.

Por fim, foram analisados artigos científicos e publicações periódicas com intuito de obter esclarecimentos e parâmetros para mensurar a presença do Exército Brasileiro em prol do domínio cibernético nacional.

a. Critérios de inclusão:

- Publicações em língua portuguesa e inglesa, reconhecidas e tomadas como referência pela comunidade de segurança cibernética ou associadas a instituições reconhecidas pela qualidade do trabalho produzido;

- Estudos e periódicos que retratam como ocorreram as ações cibernéticas nos últimos impasses geopolíticos;

- Estudos qualitativos sobre as características do espaço cibernético.

b. Critérios de exclusão:

- Publicações sem referências conhecidas ou publicadas em locais sem credibilidade quanto a veracidade dos trabalhos, como sites de comunidades abertas, como a *Wikipedia*;

- Publicações cujo tema principal seja relacionado exclusivamente à descrição tecnológica e/ou aos equipamentos militares com finalidade diferente da consciência situacional.

2.2 COLETA DE DADOS

Durante a coleta de dados, buscou-se encontrar subsídios para atingir o objetivo geral deste trabalho através da resposta ao problema-chave: Como o Exército Brasileiro está inserido no setor cibernético para garantir o domínio do espaço cibernético nacional?

Entretanto, para isso se fez necessário operacionalizar o problema através da definição de parâmetros que permitissem mensurar a resposta. O primeiro parâmetro consistiu em esclarecer a organização do Exército Brasileiro no setor cibernético. O segundo foi analisar os princípios, as possibilidades e as limitações das operações no ciberespaço adotadas pelo EB. O terceiro consistiu em esclarecer a definição de domínio do espaço cibernético.

3 RESULTADOS E DISCUSSÃO

Neste capítulo apresenta-se os resultados obtidos através da revisão de literatura, esta que foi delineada de forma a atingir os objetivos específicos e os parâmetros definidos. Em seguida, realiza-se uma discussão dos resultados, passos realizados com vistas a atingir o objetivo geral deste trabalho.

3.1 CONCEITOS ACERCA DO ESPAÇO CIBERNÉTICO

Durante a realização da pesquisa foi percebida a necessidade de esclarecer alguns conceitos acerca do assunto em questão:

a) **Rede de computadores** – Também conhecida por rede de dados, é um conjunto de dispositivos computacionais capazes de se comunicar para a troca

informações que gera o compartilhamento de arquivos digitais ou de dispositivos físicos.

De modo resumido, pode-se dizer que uma rede que tem sua comunicação limitada somente aos seus próprios dispositivos interligados é uma **rede interna**. Entretanto, uma rede ligada a várias outras redes é definida como **rede externa** ou internet;

b) **Dado, informação e conhecimento** – Os dados são os ativos que circulam na rede de computadores para gerar a comunicação entre os dispositivos conectados, circulação que ocorre através de pulsos elétricos binários (0 e 1). Para que tenham algum significado, devem ser processados pelos dispositivos computacionais (traduzidos e estruturados). Assim, o dado é transformado em uma informação útil à comunicação humana. O conhecimento é a interpretação e a consequente aplicação da informação pelo homem;

c) **Espaço Cibernético** – O tema em pesquisa está enquadrado no espaço cibernético, que pode ser entendido como um ambiente virtual composto por dispositivos computacionais conectados ou não em rede, por onde as informações digitais transitam, são processadas e/ou armazenadas (BRASIL, 2015b). Cabe ressaltar que devido à amplitude global deste tema, na literatura este espaço virtual também é comumente identificado como *Cyberspace* ou ciberespaço;

d) **Guerra Cibernética** – Pode ser entendida como uma modalidade beligerante de atuação no ciberespaço para obter informações privilegiadas e/ou desestabilizar sistemas computadorizados de um país e, ainda, influenciar no campo de batalha físico (JÚNIOR; VILLAR-LOPES; FREITAS, 2017);

e) **Infraestruturas Críticas** – Podem ser quaisquer instalações, serviços, bens e sistemas que, se tiverem seu funcionamento afetado por interrupção ou destruição, provocarão sério impacto social, econômico e político (BRASIL, 2008).

Atualmente, as infraestruturas críticas, como serviços bancários e sistemas energéticos, tem se ligado à rede a fim de modernizar e de facilitar seus funcionamentos. Contudo, esta facilidade também aumentou a vulnerabilidade dessas infraestruturas devido à maior possibilidade de sabotagem dos serviços através da instalação remota de códigos maliciosos através da internet, como as bombas lógicas;

f) **Bomba lógica –** Segundo Clarke (2010, p. 254), é “uma aplicação de *software* ou uma sequência de instruções que desligam um sistema ou rede e/ou apagam todos os dados ou *softwares* da rede”;

g) **Hacktivismo –** é uma forma de protesto *on-line* em que seus praticantes, os *hacktivistas,* afetam sistemas de informação na internet ao mesmo tempo em que deixam manifestações no sistema invadido de modo a dar visibilidade aos ideais que defendem.

3.2 LEGISLAÇÃO DE AMPARO PARA ATUAÇÃO DO EXÉRCITO BRASILEIRO NO ESPAÇO CIBERNÉTICO

Primeiramente cabe destacar que a atuação das Forças Armadas é amparada pela Constituição Federal de 1988, que prevê, dentre outros, seu emprego para a manutenção da soberania nacional. Já a Estratégia Nacional de Defesa (END), aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, é o vínculo entre a política de soberania nacional e as Forças Armadas como instrumento legal para resguardar essa soberania.

Em síntese, a END trata de questões políticas e institucionais decisivas à defesa do país, de problemas propriamente militares, além de definir que as Forças Armadas são responsáveis pela consecução dos interesses de Estado da Defesa Nacional. Desta forma, como mencionado anteriormente, três setores foram definidos como essenciais para a Defesa Nacional a cargo do Ministério da Defesa (MD): o espacial, o cibernético e o nuclear (BRASIL, 2012).

Em 2009, como consequência da publicação da END, a Diretriz Ministerial/MD nº 14 estabeleceu providências para o cumprimento das estratégias relativas a estes setores essenciais, delegando as responsabilidades as suas Forças Armadas. Assim, a coordenação e a integração do setor espacial ficaram a cargo da Força Aérea Brasileira (FAB). À Marinha do Brasil (MB) coube a responsabilidade sobre o setor nuclear e ao Exército Brasileiro (EB) coube as atividades do setor cibernético.

O setor Cibernético foi dividido em dois campos distintos: a Segurança Cibernética, a cargo da Presidência da República, e a Defesa Cibernética, a cargo do MD através das Forças Armadas (BRASIL, 2014a). Sendo assim, pode-se dividir

a atuação no Espaço Cibernético em três níveis no tocante à Defesa Cibernética: estatégico, operacional e tático (ver Figura 1).

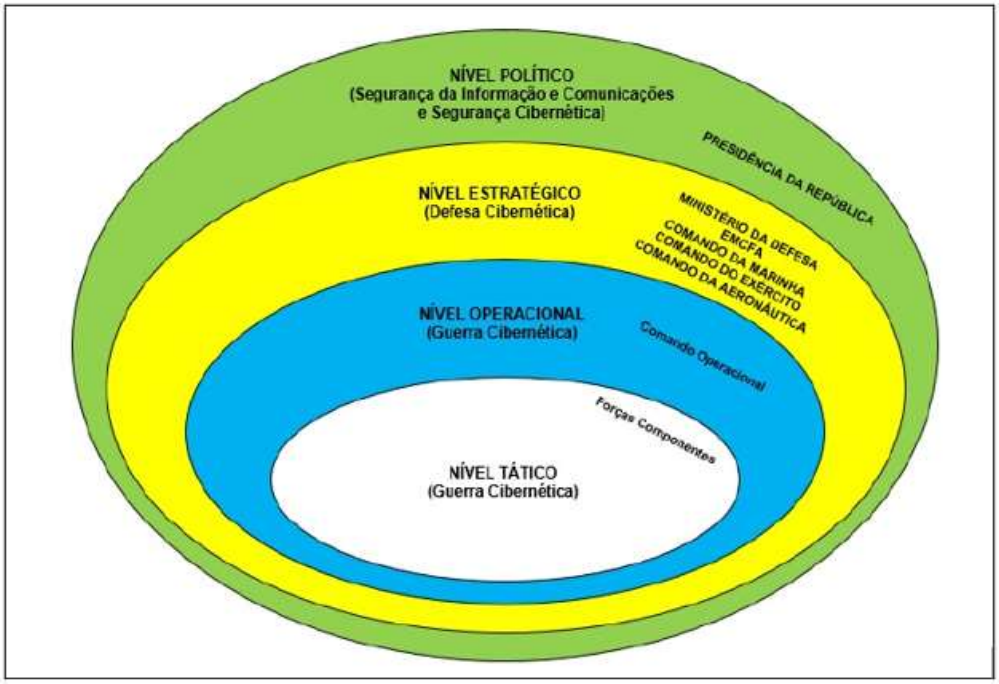

FIGURA 1 – Níveis de organização do setor cibernético brasileiro
Fonte: (BRASIL, 2014a, p. 17/36)

Desta forma, em nível estratégico o MD executa a Defesa Cibernética, uma atividade integrada das Forças Armadas e liderada pelo EB. Esta atividade adota uma abordagem de cunho militar composta por ações realizadas no espaço cibernético com o intuito de proteger os sistemas de informação de interesse da Defesa Nacional. Visa, ainda, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (BRASIL, 2017, p. 2-2). Quando o nível de decisão for o operacional ou o tático, as ações cibernéticas são definidas como Guerra Cibernética (BRASIL, 2014a, p. 26/36).

Cabe complementar que toda esta estrutura estratégica de Defesa Cibernética insere-se em um nível político através da Estratégia Nacional de Segurança Cibernética, que integra a Política Nacional de Segurança da Informação, a cargo do Gabinete de Segurança Institucional da Presidência da República (BRASIL, 2020).

3.3 ORGANIZAÇÃO DO EXÉRCITO BRASILEIRO NO SETOR CIBERNÉTICO

Com intuito de colocar em prática a END, em 2010 o setor cibernético foi inserido na estrutura do Exército Brasileiro através da criação do Centro de Defesa Cibernética (CDCiber), órgão que ficou encarregado de coordenar e de integrar as ações no espaço cibernético em proveito das operações militares.

O CDCiber estava diretamente subordinado ao Departamento de Ciência e Tecnologia (DCT), Orgão de Direção Setorial (ODS), que tem a finalidade de orientar, normatizar e supervisionar a pesquisa, o desenvolvimento e a implementação das bases física e lógica da Defesa Cibernética do Exército, dentre outras missões relacionadas aos meios de Tecnologia da Informação e Comunicações (TIC) (EXÉRCITO BRASILEIRO; DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA, s.a)[3].

Entretanto, para atuar no domínio operacional cibernético, o CDCiber não se ateve apenas a atividades operacionais no ciberespaço. Houve também a necessidade de executar a capacitação de recursos humanos, além do desenvolvimento de doutrina para orientar as ações cibernéticas de ataque e de exploração da rede oponente, bem como da proteção de seus ativos.

Diante desse amplo escopo de atividades, em 2014 o MD decidiu implantar o Comando de Defesa Cibernética (ComDCiber) como elemento central e integrador das Forças Armadas, e a Escola Nacional de Defesa Cibernética (ENaDCiber) como elemento de capacitação dos recursos humanos, para integrar os militares das Forças Armadas e, assim, ampliar as capacidades de Defesa Cibernética nacionais (ver Figura 2).

Em 2017, diante da crescente importância do setor cibernético e visando ampliar suas estruturas e capacidades, o Exército decidiu transformar o Projeto de Defesa Cibernética em Programa Estratégico do Exército (ver Figura 3).

[3] Site do Departamento de Ciência e Tecnologia do Exército Brasileiro. Disponível em: <http://www.dct.eb.mil.br/index.php/historia>.

FIGURA 2 – Organização do Exército Brasileiro no setor cibernético nacional
Fonte: Palestra do Comando de Defesa Cibernética, 2018

FIGURA 3 – Organizações Militares do Exército envolvidas no Projeto Estratégico de Defesa Cibernética
Fonte: Palestra do Comando de Defesa Cibernética, 2018

3.4 SISTEMA MILITAR DE DEFESA CIBERNÉTICA

Como mencionado anteriormente, a Defesa Cibernética é um dos componentes da Defesa Nacional a cargo das Forças Armadas. Contudo, devido ao intenso envolvimento da sociedade no espaço cibernético, se fez necessário um

sistema colaborativo que integrasse este vetor cibernético do MD aos vários setores nacionais de interesse do espectro cibernético.

Diante da integração do setor cibernético das Forças Armadas com a comunidade acadêmica, com setores públicos e privados e com a base industrial de defesa, surgiu o Sistema Militar de Defesa Cibernética (SMDC) com o objetivo de realizar atividades de defesa no Espaço Cibernético (ver Figura 4). Assim, assegura, de forma conjunta, o seu uso efetivo pelas Forças Armadas, bem como coordena e integra a proteção das infraestruturas críticas da Informação de interesse da Defesa Nacional, definidas pelo MD.

FIGURA 4 – Integração do setor cibernético brasileiro
Fonte: Palestra do Comando de Defesa Cibernética, 2018

O órgão central do SMDC é o CDCiber, que atua sob orientação e supervisão do MD. Ele mantém canais técnicos para coordenação e integração com os órgãos envolvidos em atividades de Defesa Cibernética, bem como com os órgãos centrais de inteligência para a difusão e obtenção dos dados oriundos de fonte cibernéticas (BRASIL, 2014a).

3.5 NÍVEIS DE ALERTA CIBERNÉTICO

A Defesa Cibernética é uma atividade diária em operações militares ou em situação de normalidade institucional. No âmbito da Defesa Nacional visa garantir a capacidade de atuação em rede, a interoperabilidade e a proteção dos sistemas e ativos de informação relativos ao Ministério da Defesa.

Consequentemente, para garantir a integridade de sua rede, o Ministério adota níveis de alerta relativos à possibilidade de ameaças no espaço cibernético de seu interesse. Esses níveis estão associados às lições aprendidas de exercícios simulados ou ataques cibernéticos reais, conforme a Figura 5 abaixo (BRASIL, 2014a):

Nível de Alerta		Significado / Interpretação (*)
Cor	Nome	
Branco	Baixo	– Aplicável quando as ameaças cibernéticas percebidas não afetam o Espaço Cibernético de interesse do MD e das FA. – Situação normal ou rotineira, considerando o histórico. – Probabilidade de concretização de ameaças cibernéticas baixa, considerando o histórico.
Azul	Moderado	– Aplicável quando as ameaças cibernéticas percebidas afetam o Espaço Cibernético de interesse do MD e das FA, sem comprometer as infraestruturas críticas da Informação. – Probabilidade de concretização de ameaças cibernéticas entre baixa e média, considerando o histórico.
Amarelo	Médio	– Aplicável quando ações cibernéticas hostis afetam o Espaço Cibernético de interesse, sem comprometer as infraestruturas críticas da informação. – Aplicável quando houver a percepção de ameaças cibernéticas contra as infraestruturas críticas da informação. – Probabilidade da concretização de ameaças cibernéticas entre média e alta, considerando o histórico.
Laranja	Alto	– Aplicável quando as ações cibernéticas hostis degradam alguma Infraestrutura Crítica da Informação. – Probabilidade de concretização de ameaças cibernéticas entre média e alta, considerando o histórico. – Infraestrutura Crítica da Informação atingida, porém com possibilidade de restabelecimento das condições de segurança ou dos serviços em tempos aceitáveis para o cumprimento da missão. – Infraestrutura Crítica da Informação atingida com impacto entre médio e alto, considerando o histórico.
Vermelho	Muito Alto	– Aplicável quando ações cibernéticas hostis exploram ou negam a disponibilidade das infraestruturas críticas da informação. – Probabilidade de concretização de ameaças cibernéticas muito alta, considerando o histórico. – Infraestrutura Crítica da Informação atingida com impacto alto ou superior, considerando o histórico. – Infraestrutura Crítica da Informação atingida, com possibilidade de restabelecimento da condição de segurança ou dos serviços em tempos além dos aceitáveis para o cumprimento da missão.

FIGURA 5 – Quadro dos níveis de alerta adotados pelo Ministério da Defesa
Fonte: (BRASIL, 2014a, p. 27-36)

Dentre os diversos grandes eventos dos quais o CDCiber participou da segurança do espaço cibernético (Figura 6), pode-se mencionar os Jogos Olímpicos do Rio 2016 como uma ocasião em que o nível de alerta cibernético poderia ter

evoluído momentaneamente, embora não tenha ocorrido nenhum pronunciamento oficial a respeito,

Por se tratar de um evento de dimensões internacionais, incidentes cibernéticos praticados por *hacktivistas* e terroristas eram iminentes. Diante disto, foi desencadeada a Operação JO, na qual o sistema de Defesa Cibernético atuou de modo conjunto com órgãos nacionais e internacionais para garantir a integridade das informações da competição que circulavam no espaço cibernético.

FIGURA 6 - Alguns dos grandes eventos em que o CDCiber esteve presente
Fonte: Palestra do Comando de Defesa Cibernética, 2018

Segundo consta em matéria do site G1, durante o evento as redes de apoio da competição sofreram uma média de três incidentes cibernéticos por hora. Diante disso, analisando a conjuntura do grande evento e o fluxo de ameaças cibernéticas neste ambiente, deduz-se que o estado de alerta foi elevado acima do nível baixo, denominado nível branco, que condiz com uma situação rotineira.

Dessarte, levando-se em consideração a consciência situacional, o histórico das edições anteriores, o clima de manifestações e o terrorismo internacionais contra algumas nações que participavam desta edição, existia a probabilidade de concretização de incidentes cibernéticos nos sistemas informacionais dos Jogos Olímpicos Rio 2016 (ver Figura 7).

Entretanto, diante do cenário descrito, os incidentes cibernéticos não comprometeram o funcionamento dos sistemas e, consequentemente, foi garantido

o pleno funcionamento da organização dos jogos que factualmente estava dependente do espaço cibernético.

O êxito contra tais ameaças durante a Operação JO ocorreu devido ao trabalho do sistema de Defesa Cibernética do MD integrado com os demais sistemas públicos e privados envolvidos na proteção do ciberespaço do evento.

FIGURA 7 – Aplicação dos níveis de alerta pelo CDCiber durante as Olimpíadas Rio 2016
Fonte: Palestra do Comando de Defesa Cibernética, 2016

3.6 PRINCÍPIOS, POSSIBILIDADES E LIMITAÇÕES DAS OPERAÇÕES NO ESPAÇO CIBERNÉTICO

A aplicação da Defesa Cibernética pelas Forças Armadas é pautada por princípios, possibilidades e limitações. Estas pautas são essenciais para a escolha das estratégias militares a serem adotadas no domínio operacional cibernético, bem como para definir as linhas de ação a serem executadas nos níveis operacionais e táticos das operações militares através da atividade de guerra cibernética.

Desta forma, este item esclarece a atuação do Exército Brasileiro no setor cibernético em prol das operações militares.

3.6.1 Princípios de emprego

O emprego da guerra cibernética não se adapta exatamente aos mesmos princípios tradicionais da guerra terrestre quanto ao objetivo, a ofensiva, a massa, a economia de força, as manobras, a unidade do comando, a segurança, a surpresa e a simplicidade. Este novo domínio operacional possui uma gama de aplicações que lhe contestam alguns princípios de emprego específicos (DA SILVA, 2014).

Segundo a doutrina de guerra cibernética do Exército Brasileiro, sua metodologia de emprego adota os seguintes princípios:

> 2.3.3. **Princípio do Efeito** - as ações no Espaço Cibernético devem produzir efeitos que se traduzam em vantagem estratégica, operacional ou tática que afetem que afetem o mundo real, mesmo que esses efeitos não sejam cinéticos;
> 2.3.4. **Princípio da Dissimulação** - medidas ativas devem ser adotadas para se dissimular no Espaço Cibernético, dificultando a rastreabilidade das ações cibernéticas ofensivas e exploratórias levadas a efeito contra os sistemas de tecnologia da informação e de comunicações do oponente. Objetiva-se, assim, mascarar a autoria e o ponto de origem destas ações;
> 2.4.5. **Princípio da Rastreabilidade** - medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra os sistemas de tecnologia da informação e de comunicações amigos. Quase sempre, as ações adotadas no Espaço Cibernético envolvem a movimentação ou a manipulação de dados, as quais podem ser registradas nos sistemas de TIC;
> 2.3.6. **Princípio da Adaptabilidade** - consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do Espaço Cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis (BRASIL, 2014a, p. 20-36).

Cabe observar que os princípios de emprego da guerra cibernética supracitados são semelhantes nas doutrinas das Forças Armadas de diversos países, contudo, podem haver divergências conforme a óptica de utilização das ações cibernéticas em prol de objetivos políticos ou estratégicos específicos das Nações.

3.6.2 Possibilidades da guerra cibernética

As principais possibilidades mencionadas pelo manual de Guerra Cibernética do Exército Brasileiro são:

> a) atuar no espaço cibernético, por meio de ações ofensivas, defensivas e exploratórias;
> b) cooperar na produção do conhecimento de inteligência por meio dos dados obtidos da fonte cibernética;
> c) atingir sistemas de informação de um oponente sem limitação de alcance físico e exposição de tropa;
> d) cooperar com a segurança cibernética, inclusive de órgãos externos ao MD, mediante solicitação ou no contexto de uma operação;
> e) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da guerra cibernética;
> f) facilitar a obtenção da surpresa, com base na exploração das vulnerabilidades dos sistemas de informação do oponente;
> g) realizar ações contra oponentes com poder de combate superior; e
> h) realizar ações com custos significativamente menores do que aqueles envolvidos nas operações militares nos demais domínios (BRASIL, 2017, p. 2-5).

Doutrinariamente, as possibilidades supracitadas são fundamentais para a manutenção de Comando e Controle (C2) e devem ser almejadas nas ações cibernéticas de modo geral, pois asseguram vantagens nas Operações Militares, como a ampliação da consciência situacional do campo de batalha e a capacidade para interferir no processo decisório do inimigo.

3.6.3 Limitações da guerra cibernética

Segundo Carneiro (2012, p. 123), as limitações encontradas no domínio operacional cibernético e aplicáveis tanto à defesa quanto à guerra cibernética são:

> a) restrita capacidade de identificação da origem e atribuição de responsabilidades por ataques cibernéticos;
> b) restrita eficácia das ações cibernéticas defensivas, devido à existência de vulnerabilidades nos sistemas computacionais;
> c) restrita capacidade de gestão de pessoas, particularmente no que concerne à identificação, seleção, capacitação e retenção de talentos;
> d) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e
> e) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação.

Durante o processo decisório de Operações Militares, tais limitações devem ser encaradas pelo comando como potenciais vulnerabilidades a serem reduzidas no ambiente cibernético de modo que a sua exploração pelo oponente seja dificultada ou negada. Por outro lado, as mesmas limitações citadas devem ser apontadas como ponto de gravidade e de vantagem a ser buscado para o êxito nas ações de ataque e exploração do ambiente cibernético inimigo.

3.7 DOMÍNIO DO ESPAÇO CIBERNÉTICO

Antes de abordar o conceito de domínio do espaço cibernético, se faz fundamental entender conceitos doutrinários anteriores ou outros mais abrangentes, tal como a concepção de guerra da informação, na qual as atividades cibernéticas inserem-se.

Na década de 80, a inserção massiva da tecnologia da informação nos campos de batalha, como sensores e computadores, provocou o desenvolvimento da doutrina de Comando e Controle (DA SILVA, 2006).

Basicamente, o processo de comando e controle é o conjunto de equipamentos e sistemas de informação e comunicações, procedimentos e pessoal essenciais para que o comandante ou decisor possa planejar e controlar as ações da tropa por meio da consciência situacional. Tal consciência consiste na percepção precisa e atualizada do ambiente operacional em que transcorre a operação militar (BRASIL, 2015c).

Com a adoção de tal doutrina, surgiu a ideia de superioridade do comando e controle: aquele que adquire, através das informações, a consciência situacional mais rápida, tem a vantagem de atuar e modificar o ambiente operacional antes do adversário, tornando inofensivas as ações oponentes.

Após a Guerra do Golfo em 1991, desenvolveu-se a doutrina de Guerra da Informação como resultado da adaptação dos princípios do comando e controle aos novos ambientes operacionais imersos em meios de Tecnologia da Informação e Comunicações (TIC) (DA SILVA, 2006).

De acordo com Souza (2003), a guerra da informação abrange as ações realizadas para obter o seu domínio, atuando contra processos, sistemas de informação e redes de computadores oponentes, bem como defendendo estes recursos das suas Forças inseridas no ambiente operacional.

Neste contexto, o domínio da informação é o grau de superioridade que permite ao seu detentor usar os sistemas para obter uma vantagem operacional e controlar a situação, enquanto nega estas capacidades ao adversário (SOUZA, 2003).

Em conformidade, o Manual de Operações de Informação do Exército Brasileiro prevê a guerra cibernética como uma das cinco Capacidades Relacionadas à Informação (CRI) necessárias para afetar a capacidade oponente de

orientar, obter, produzir e/ou difundir informações em qualquer uma das três perspectivas da dimensão informacional (física, cognitiva ou lógica) (BRASIL, 2014b, p. 3-1).

Cabe ressaltar que os ataques cibernéticos contra sistemas conectados em rede podem gerar os mesmos efeitos que a destruição de uma instalação física de comando e controle por meio de vetores cinéticos, como os fogos de artilharia. Isto ocorre uma vez que ambos visam prejudicar a capacidade de comando e controle do adversário através da interferência no fluxo de informações. Estes efeitos justificam a previsão do vetor cibernético como CRI.

Atualmente, é correto afirmar que o ambiente cibernético das redes de transmissão de dados é o principal vetor de circulação de informações governamentais ostensivas ou sigilosas. É por meio destas redes que circulam as decisões políticas e estratégicas, bem como as ordens das operações militares. Todas estas informações digitais são capazes de influenciar instantaneamente a geopolítica mundial.

Consequentemente, a segurança do espaço cibernético nacional tornou-se fundamental para a soberania das nações. Dentre outras garantias, visa a circulação das informações sem interceptação ou interferência de outros atores, o que garante a privacidade das informações de seus cidadãos e de empresas, a continuidade da prestação de serviços, além do sigilo das políticas e estratégias governamentais.

A interceptação de informações privadas de personalidades públicas, como o vazamento de *e-mails*, pode trazer sérios danos profissionais ou à imagem do indivíduo. No nível empresarial, a interferência na trafegabilidade de dados pode acarretar em roubo de dados confidenciais de clientes, como dados bancários, a negação de serviços digitais em seus *sites* comerciais, bem como a paralisação de suas estruturas físicas. Tais ações podem gerar prejuízos financeiros, além da perda de credibilidade das empresas.

Por sua vez, no cenário interno o vazamento de informações governamentais pode acarretar em instabilidade política, renúncia à cargos e manifestações populares. Já no âmbito externo, o vazamento de políticas e estratégias, como negociações secretas, podem gerar quebra de acordos internacionais, embargos econômicos e até mesmo a declaração de guerras ou intervenções militares.

Por sua vez, o conceito de domínio do espaço cibernético é mais abrangente. Diante de um cenário de conflito, visa ações de ataque e de exploração

a redes de sistemas informacionais de um espaço cibernético alvo, além de ações de proteção de seus próprios ativos de informação contra investidas oponentes.

As ações de ataque compreendem a interrupção, a negação e a degradação de informações ou de sistemas computacionais ligados em redes de dados (BRASIL, 2014a). Um exemplo destas ações poderia ser a interrupção de serviços de infraestruturas críticas automatizadas, que são altamente dependentes das redes para circulação de comandos de funcionamento.

Em uma situação hipotética de conflito, Clarke (2015) menciona o sistema elétrico norte-americano como um alvo compensador, pois sua degradação iria comprometer muitos outros sistemas das Forças Armadas e da sociedade estadunidense.

As ações de exploração cibernética consistem na busca e na coleta de conhecimento sobre o sistema informacional alvo do oponente no que diz respeito ao seu funcionamento, à proteção e às vulnerabilidades, de modo que possa assegurar uma correta consciência situacional durante o planejamento e a execução do ataque a esse alvo (BRASIL, 2014a). Nesta fase, é fundamental a observação do princípio da dissimulação a fim de evitar o rastreamento e a identificação do invasor no sistema, pois do contrário, as vulnerabilidades levantadas serão corrigidas e os mandantes da ação serão sancionados.

Clarke (2015) aborda que o ataque pode ser preparado durante a fase de exploração com a adição de bombas lógica e de códigos maliciosos de *backdooors* (facilitadores de invasão).

Por fim, as ações de proteção, que tem caráter permanente devem neutralizar ataques e explorações oponentes contra sistemas cibernéticos amigos, a fim de garantir a plena utilização do espaço cibernético, em especial do sistema de comando e controle das operações militares (BRASIL, 2014a).

Cabe adicionar que, segundo Clarke (2015), para o domínio de um espaço cibernético, é preferível um sistema de proteção permanente e altamente capacitado a um sistema de ataque cibernético sofisticado, pois um país pode ser surpreendido por um ataque inicial e ter esta capacidade ofensiva anulada. Como exemplo, menciona que China e Coreia do Norte são capazes de lançar ataques cibernéticos e, se necessário, limitar suas conexões na internet, o que minimizaria a eficácia de um ataque de retaliação.

Para Clarke (2015), outro fator influente neste domínio é o grau de dependência cibernética, que representa a quantidade de sistemas de um país que são controlados ciberneticamente. Uma nação que possui muitos sistemas ligados à internet fica mais vulnerável porque cada sistema torna-se um alvo de ataques durante um conflito cibernético, principalmente se for uma infraestrutura crítica, cujo os danos e interrupção dos serviços podem gerar resultados significativos no desenrolar do conflito.

3.8 ANÁLISE DA PRESENÇA DO EXÉRCITO BRASILEIRO NO SETOR CIBERNÉTICO

Neste capítulo foi analisada a presença do Exército Brasileiro no setor cibernético nacional através de tópicos que expuseram conceitos acerca do tema, a legislação vigente para amparar a atividade militar no setor, a organização e a estrutura do EB para execução das atividades cibernéticas, os princípios, as possibilidades e as limitações de emprego.

Na abordagem sobre a legislação vigente, foi esclarecido que a atividade de defesa cibernética possui amparo constitucional para emprego a cargo das Forças Armadas, pois enquadra-se como um dos componentes da Defesa Nacional e sua estratégia. Foi percebido também que o Estado compreende a importância do setor diante da conjuntura geopolítica atual, pois constantemente fez publicações que buscaram garantir a consecução de seus interesses no ciberespaço.

Em complemento, foi analisada a organização e a estrutura do Exército Brasileiro, responsável pela coordenação da Defesa Cibernética. Além disto, foi identificado o esforço constante de aperfeiçoamento de suas estruturas, de maneira que conseguisse aprimorar suas capacidades cibernéticas e assim proporcionar o exercício adequado no ciberespaço sob responsabilidade do Ministério da Defesa.

Destarte, pôde-se coletar dados para esclarecer a organização e a estrutura do EB no setor, suas possibilidades e limitações no emprego da doutrina de defesa cibernética, além de conceituar a ideia de domínio do ciberespaço. Tais esclarecimentos responderam aos parâmetros estipulados e fundamentaram a resposta do problema principal deste trabalho.

O Exército Brasileiro insere-se no setor através da execução e da coordenação das atividades de Defesa Cibernética sob responsabilidade do

Ministério da Defesa. Para cumprir tal objetivo, sua organização funcional e suas infraestruturas foram ampliadas. De forma complementar, existe a previsão de aumento das capacidades através da implantação do setor no Programa Estratégico do Exército.

A luz da doutrina em vigor, o EB adota os princípios adequados em suas operações, além de prever a atuação conjunta com outros sistemas públicos e privados em prol da otimização do sistema de Defesa Cibernética.

Conclui-se que o EB insere-se no setor cibernético de modo permanente, com estruturas cada vez mais adequadas e eficientes. Estas constatações certificam-se pelo êxito das operações cibernéticas executadas durante os grandes eventos desenvolvidos no Brasil.

4 CONSIDERAÇÕES FINAIS

A concepção deste trabalho ocorreu em um contexto no qual as características do combate moderno direcionam à utilização cada vez maior dos meios de Tecnologia da Informação e Comunicação (TIC) como ferramentas de obtenção de dados. Estes últimos são fundamentais para o desenvolvimento do Comando e Controle e do domínio da informação nos conflitos de amplo espectro.

De modo congruente, os meios computacionais em rede estão inseridos neste ambiente de consciência situacional baseada nos meios tecnológicos. Em que pese a exploração do ambiente cibernético para a obtenção de dados ocorrer, ainda que de modo incipiente.

Diante disto, vislumbrou-se que uma análise da presença do Exército Brasileiro (EB) – instrumento para a soberania nacional – no domínio cibernético seria uma oportunidade a ser explorada, e assim chegou-se ao objetivo principal deste trabalho, responder à seguinte questão: **Como o Exército Brasileiro está inserido no setor cibernético para garantir o domínio do espaço cibernético nacional?**

Para atingir este objetivo foi realizada uma pesquisa bibliográfica em fontes de consulta nacionais e internacionais relativas ao assunto. Desta forma foi possível apontar os principais conceitos acerca do tema no que tange à organização e à doutrina.

Salienta-se que a principal dificuldade encontrada para o desenvolvimento do trabalho foi a escassez de fontes de consulta acerca do emprego EB no Espaço Cibernético.

Para responder a pergunta-chave do trabalho em sua plenitude, foi essencial o estabelecimento de parâmetros que permitissem mensurar a resposta, tais como esclarecer a organização do Exército Brasileiro no setor cibernético; analisar os princípios, as possibilidades e as limitações das operações no ciberespaço adotadas pelo EB e esclarecer a definição de domínio do espaço cibernético.

Por intermédio destes instrumentos, durante a pesquisa bibliográfica foi possível identificar a prioridade que o setor cibernético recebeu na END. Também foi constatada a preocupação rotineira em proteger o espaço cibernético nacional, esta que foi resolvida através de um sistema integrado que atua em prol da integridade das informações críticas do Estado Nacional.

Neste aspecto, foi observado que no âmbito do Ministério da Defesa (MD), o EB executa a coordenação e a integração fundamentais entre os órgãos envolvidos na proteção das infraestruturas críticas de informação. Igualmente, foi percebida a crescente ampliação da organização institucional e das capacidades profissionais referentes ao setor cibernético no âmbito do MD, sempre lideradas pelo EB. Esta constatação é importante, pois ainda existiam dúvidas doutrinárias e operacionais quanto ao que seriam tarefas da Defesa Cibernética no cenário nacional.

Como resultado da pesquisa, foi obtida a resposta ao problema-chave do estudo: O Exército Brasileiro está inserido de modo central na Defesa Cibernética para garantir o domínio deste espaço nacional. Fruto disso, tem alcançado a ampliação de suas capacidades e destacado sua presença no cenário geopolítico atual em virtude de sua eficiência nas operações executadas durantes os grandes eventos brasileiros.

Conclui-se ainda que esta pesquisa atendeu ao pretendido nos objetivos, alinhado com as justificativas apresentadas na introdução do trabalho. Destarte, ampliou a compreensão sobre a atividade cibernética sob responsabilidade do Exército Brasileiro.

Durante o desenvolvimento do trabalho, surgiram oportunidades para explorar mais amiúde o nível operacional e tático da defesa cibernética, ou seja, a guerra cibernética. Contudo, coloca-se esta temática como sugestão para trabalhos futuros.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm>. Acesso em: 15 maio. 2020.

_____. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, Brasília, DF, 6 fev. 2020. Seção 1, p. 6.

_____. Gabinete de Segurança Institucional. Portaria nº 2, de 8 de fevereiro de 2008. Institui Grupos Técnicos de Segurança de Infra-estruturas Críticas (GTSIC) e dá outras providências. **Diário Oficial da União**, Brasília, DF, 11 fev. 2008. Seção 1, p. 1.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF, 2012. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/end.pdf>. Acesso em: 02 maio 2020.

_____. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, DF, 2012.

_____. Ministério da Defesa. **Política Nacional de Defesa.** Brasília, DF, 2012.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD30-M-01: Doutrina de Operações Conjuntas**. Brasília, DF, v. 1, 2011.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M-03: Doutrina Para o Sistema Militar de Comando e Controle**. 3. ed. Brasília, DF, 2015a.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M-08: Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014a.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD35-G-01**: **Glossário das Forças Armadas**. 5. ed. Brasília, DF, 2015b.

_____. Ministério da Defesa. Estado-Maior do Exército. **EB20-MC-10.213: Operações de Informação**. Brasília, DF, 2014b.

_____. Ministério da Defesa. Estado-Maior do Exército. **EB20-MF-10.205: Comando e Controle**. Brasília, DF, 2015c.

_____. Ministério da Defesa. Estado-Maior do Exército. **EB70-MC-10.232: Guerra Cibernética.** Brasília, DF, 2017.

CARNEIRO, João M. E. **A Guerra Cibernética:** uma proposta de elementos para formulação doutrinária do Exército Brasileiro. 2012. 204 f. Tese (Doutorado em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

CENTRO DE DEFESA CIBERNÉTICA (Brasil). Equipes de tratamento e resposta a incidentes em redes computacionais In: OFICÍNA TÉCNICA DO CTIR GOV , 2018, Brasília, DF. **Palestras...** Brasília, DF: Palácio do Planalto, 2018.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito. ed. Kindle. Rio de Janeiro: Brasport, 2015.

DA SILVA, Gilmar Pereira. **Guerra Cibernética:** Preparo e Emprego do Exército. 2006. 48 F. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2006.

DA SILVA, Júlio Cezar Barreto Leite. Guerra Cibernética: A guerra no Quinto Domínio, conceituação e princípios. **Revista Escola de Guerra Naval**, Rio de Janeiro, v. 20, n. 1, p. 193-211, jan./jun. 2014.

EXÉRCITO, **Defesa Cibernética entra em nova fase.** Disponível em: <http://www.eb.mil.br/web/midia-impressa/noticiario-do-exercito/-/asset_publisher/IZ4bX6gegOtX/content/defesa-cibernetica-entra-em-nova-fase>. Acesso em 08 ago 2020.

EXÉRCITO, **Missão do DCT**. Disponível em: <http://www.dct.eb.mil.br/index.php/historia>. Acesso em 08 ago 2020.

EXÉRCITO, **Liberdade de ação no espaço cibernético**. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica>. Acesso em 10 maio 2020.

EXÉRCITO; DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA DO EXÉRCITO BRASILEIRO. **Missão.** Disponível em: <http://www.dct.eb.mil.br/index.php/historia>. Acesso em: jul. 2020.

FÓRUM BRASILEIRO DE CSIRTs, 2014-2019, São Paulo. **Anais...** São Paulo. 2019.

G1, **Olimpíada Rio 2016 teve quase 3 incidentes cibernéticos por hora.** Disponível em: <https://g1.globo.com/tecnologia/noticia/olimpiada-rio-2016-teve-quase-3-incidentes-ciberneticos-por-hora.ghtml>. Acesso em: 10 set 2020.

HUREL, Louise Marie; LOBATO, Luisa Cruz. Uma estratégia para a governança da segurança cibernética no Brasil. **Instituto Igarapé - Nota Estratégica,** Rio de

Janeiro, n. 30, set. 2018. 32 p.

JÚNIOR, Augusto; VILAR-LOPES, Gills; FREITAS, Marco. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. **Revista Carta Internacional**, Belo Horizonte, MG, v. 12, n. 3, p. 30-53, 2017.

UNITED STATES. Department of Defense. **DOD Dictionary of Military and Associated Terms.** Washington, D.C., 2020.