ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

Cap QCO Claudio Gomes Pio

A DEFESA CIBERNÉTICA NAS OPERAÇÕES CONJUNTAS: Identificando áreas de atuação, atribuições e atores.

Rio de Janeiro
2016

Cap QCO CLAUDIO GOMES PIO

A DEFESA CIBERNÉTICA NAS OPERAÇÕES CONJUNTAS: Identificando áreas de atuação, atribuições e atores.

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares
.

Orientador: Cap QCO Maxli Barroso Campos

Rio de Janeiro
2016

Cap QCO CLAUDIO GOMES PIO

A DEFESA CIBERNÉTICA NAS OPERAÇÕES CONJUNTAS: Identificando áreas de atuação, atribuições e atores.

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares
.

Aprovado em

COMISSÃO DE AVALIAÇÃO

_____
ANDERSON BARROS **TORRES** – Maj – Presidente
Escola de Formação Complementar do Exército

_____
MAXLI BARROSO **CAMPOS** – Cap – Membro
Escola de Formação Complementar do Exército

RESUMO

Com o crescente desenvolvimento tecnológico, algumas infraestruturas de informação pública, privada e militar, tornaram-se ponto crítico para a garantia da Soberania Nacional. Ao mesmo tempo, em que os conflitos armados deixaram de ser exclusivamente convencionais, passando a ser limitados, sem estimativa de duração, sendo ameaças imprevisíveis, fluidas e difusas. Nesse contexto, surge a necessidade das Formas Armadas atuarem em conjunto, buscando versatilidade, mobilidade e flexibilidade no enfrentamento do oponente. Assim, a Guerra Cibernética ingressa no ambiente de batalha com objetivo principal de proteger a infraestrutura da informação das forças amigas. Apesar dos esforços envolvidos na gestão da Defesa Cibernética, garantir a segurança contra investidas dos oponentes, é algo difícil de ser alcançado, pois, essa segurança envolve investimentos e envolvimento das mais diversas organizações do país. Este trabalho tem como objetivo, relatar o envolvimento da Defesa e da Guerra Cibernética nas Operações Conjuntas. Será realizado um estudo dos principais documentos que normatizam o emprego da Cibernética nas Operações Conjuntas. Conclui-se que a Guerra Cibernética atua em diversas frentes nas Operações Conjuntas, como: provendo proteção da própria infraestrutura de informação, explorando o inimigo em busca de informações e realizando ataques com os mais diversos fins, com o intuito de combater o oponente.

Palavras-chave: Segurança Cibernética, Defesa Cibernética, Guerra Cibernética, Doutrina, Operações de Informação.

ABSTRACT

With increasing technological development, some infrastructures of information public, private and military, have become critical to ensuring national sovereignty. At the same time, in which armed conflicts are no longer entirely conventional, but should be limited, without estimate duration, with unpredictable, fluid and diffuse threats. In this context, the need arises for the Armed Forms act together seeking versatility, mobility and flexibility in facing the opponent. Thus, Cybernetics War enters the battlefield environment with the main purpose to protect the information infrastructure of friendly forces. Despite the efforts involved in the management of Cyber Defense, to ensure security against attacks by opponents, it is something difficult to achieve, because this involves security investments and involvement of various organizations in the country. This study aims, report the involvement of Defense and Cyber Wars Joint Operations, a study of the main documents that regulate the use of cybernetics in the Joint Operations will be conducted. It is concluded that cybernetics War acts on several fronts in the Joint Operations, such as providing protection of their own information infrastructure, by exploiting the enemy in search of information and carrying out attacks with the most diverse purposes, in order to combat the opponent.

Keywords: Cybernetics Security, Cyber Defence, Cyber War, Doctrine, Information Operations.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Os conflitos militares atuais tendem a ser convencionais ou não, sem estimativa de duração, limitados, são ameaças imprevisíveis, fluidas e difusas (BRASIL, 2011a). Caracterizados pelo intenso uso de tecnologias, pela mídia no ambiente operacional, presença de civis, velocidade e letalidade seletiva, utilização de aeronaves remotamente tripuladas e pela capacidade de operar no espeço cibernético. Tornando os conflitos armados cada vez mais complexos, diferentemente dos combates tradicionais, exigindo das Forças Armadas capacidade de atuar de forma conjunta com versatilidade, mobilidade e flexibilidade (BRASIL, 2011a). Nesse contexto, existe o Estado-Maior Conjunto das Forças Armadas subordinado ao Ministério da Defesa, que tem como finalidade planejar e controlar no nível estratégico as Operações Conjuntas.

A área Cibernética passou a fazer parte das atividades militares, quando alguns países perceberam que, se suas infraestruturas críticas fossem afetadas pela ação Cibernética, a Segurança Nacional ficaria comprometida. Em 2011, os Estados Unidos da América, anunciou a sua Estratégia Internacional para o Espaço Cibernético, com o objetivo de proteger seus ativos críticos de informação de ataques indesejáveis, como também, explorar e atacar os oponentes, quando necessário (JUNIOR, 2013).

Com a crescente automatização dos processos industriais, administrativos e comerciais, as infraestruturas de Tecnologias da Informação tornaram-se ponto crítico na maioria das instituições ou organizações públicas, privadas ou militares. A proteção das principais infraestruturas críticas do país passou a ser vital para a manutenção da Soberania Nacional. Assim sendo, e observando a iniciativa americana, o governo brasileiro adicionou na Estratégia Nacional de Defesa (BRASIL, 2012b), a Defesa Cibernética, que tem entre os principais objetivos: capacitar recursos humanos, apoiar o desenvolvimento da indústria nacional de tecnologia e proteger as infraestruturas críticas de informação de interesse do país.

O desenvolvimento dos trabalhos para implantação da Defesa Cibernética, pelo Ministério da Defesa, culminou na criação do Centro de Defesa Cibernética e em 2015, na criação do Núcleo do Comando de Defesa Cibernética e no Núcleo da Escola Nacional de Defesa Cibernética, conforme Martins et al (2016). Nas Operações Conjuntas o Centro de Defesa Cibernética passa ao controle do Estado-Maior

Conjunto das Forças Armadas. E destacamentos de Guerra Cibernética podem ser formados para cada nível de Comando das Operações. Esses destacamentos atuam em diferentes áreas como em atividades de exploração de ameaças, riscos e vulnerabilidades das estruturas de informações internas e dos oponentes. Em proteção das infraestruturas críticas de informação militar e civil das forças amigas, como também atacando o inimigo, buscando comprometer, confundir e destruir a sua estrutura de Comando e Controle e de informações, de acordo com Brasil (2014c).

O Centro de Defesa Cibernética mantém uma estrutura de permanente integração com outros órgãos público e privado, nacional e internacional, com o objetivo de compartilhar aprendizados e trabalhar em cooperação, conforme Martins et al (2016). O Comando de Defesa Cibernética que é órgão coordenador das ações de Defesa Cibernética no âmbito do Ministério da Defesa, participa como órgão operacional das estratégias de atuação em conjunto das Forças Armadas, que por meio do Centro de Defesa Cibernética, ao longo dos últimos anos, vem criando e aplicando nas Operações Conjuntas, a doutrina militar da área de Cibernética, que precisa ser amplamente conhecida dos militares da Marinha, Exército e Aeronáutica, com o intuito de tornar efetiva nossa participação neste novo domínio de guerra.

Neste sentido, o presente trabalho tem por objetivo apresentar a atuação do Sistema de Defesa Cibernética nas Operações Conjuntas, identificando áreas de atuação, atribuições e os atores envolvidos.

O presente trabalho será desenvolvido da seguinte forma: no primeiro capitulo será feita uma abordagem sobre o conceito de Ciberespaço e Guerra Cibernética. No segundo, será feito um estudo sobre a Guerra Cibernética no cenário atual, no terceiro, no cenário futuro. O quarto, abordará o desenvolvimento da Defesa Cibernética no Brasil, o próximo falará sobre a Defesa Cibernética nas Operações Conjuntas e o último apesentará algumas Discursões e Resultados obtidos.

1.1 PROBLEMA

A necessidade de proteger as infraestruturas críticas nacionais de Tecnologia da Informação, forçaram o governo brasileiro a implementar e aperfeiçoar, Políticas de Segurança e Defesa Cibernéticas. A atual revolução tecnológica ascendeu o Ciberespaço a uma nova dimensão nos assuntos referentes à Defesa. Que utiliza a

Tecnologia da Informação, no estabelecimento de uma efetividade decisiva nas operações, tornando-se um novo vetor de combate.

A Guerra Cibernética é uma atividade recente, mas com relevante papel nas Operações Militares, como nas Operações Conjuntas, onde tem participação em várias Funções de Combate. Nesse contexto, verifica-se a necessidade de realizar um estudo sobre o Sistema de Defesa Cibernética nas Operações Conjuntas, identificando as áreas de atuação, as atribuições e os atores envolvidos?

1.2 OBJETIVOS

O presente estudo pretende integrar os conceitos básicos e informações científicas relevantes e atualizadas, a fim de apresentar a atuação do Sistema de Defesa Cibernética nas Operações Conjuntas, identificando áreas de atuação, atribuições e os atores envolvidos.

Com a finalidade de delimitar e alcançar o desfecho esperado para este objetivo, levantou-se objetivos específicos que irão conduzir na consecução do objetivo deste estudo, os quais são transcritos abaixo:

a) definir e caracterizar o Espaço Cibernético ou Ciberespaço;
b) apresentar os riscos e ameaças presentes no Ciberespaço;
c) apresentar acontecimentos que deram origem ao conceito atual de Guerra Cibernética;
d) apresentar a importância a Guerra Cibernética no atual cenário mundial;
e) apresentar as perspectivas sobre as guerras no futuro;
f) apresentar as Políticas e Estratégias de Segurança e Defesa Cibernéticas no Brasil e no mundo;
g) definir e abordar a estrutura da Defesa Cibernética no âmbito do Ministério da Defesa;
h) apresentar as principais estruturas operacionais e táticas da Guerra Cibernética;
i) apresentar os principais componentes do Sistema de Defesa Cibernética;

j) identificar as áreas de atuação do Sistema de Defesa Cibernética nas Operações Conjuntas, as atribuições e os atores envolvidas.

1.3 – QUESTÕES DE ESTUDO

Na analise do questionamento apresentado, algumas questões podem ser formuladas:

a. O que é o Ciberespaço?
b. Qual a origem do Ciberespaço?
c. Quais são as Políticas Nacionais de Segurança e Defesa Cibernéticas?
d. O que é Guerra Cibernética?
e. Como surgiu a Guerra Cibernética?
f. Quais fatores influenciaram para o Brasil e os outros países implantarem projetos de Guerra Cibernética?
g. O que é Operação Conjunta?
h. Quem compõe e qual a finalidade do Estado Maior Conjunto das Forças Armadas?
i. O que é o Centro de Defesa Cibernética?
j. Qual a importância da Guerra Cibernética para as Forças Armadas?
k. Quem são os integrantes das Operações Conjuntas?
l. Quais são as áreas do Sistema de Defesa Cibernética das Operações Conjuntas, as atribuições e atores envolvidos?

1.4 METODOLOGIA

O presente trabalho será desenvolvido através de pesquisa bibliográfica a manuais doutrinários, livros, revistas científicas, sites, portarias, leis, normas e trabalhos científicos.

1.4.1 Objeto Formal de Estudo

O presente trabalho visa realizar um estudo bibliográfico sobre a utilização da Guerra Cibernética nas Operações Conjuntas, identificando as áreas de integração com a atividade Cibernética, quando e sobre as ordens de quem deve atuar, quais conhecimentos produzir e onde aplicá-los, o que será defendido e de que forma. Para responder a estes questionamentos serão abordados conceitos básicos sobre a Guerra Cibernética, levantando características do cenário Cibernético atual e futuro, nacional e internacional, buscando entender o processo de implantação da Defesa Cibernética no Brasil e por último será realizado um estudo das Operações Conjuntas, identificando os papeis a ser desempenhados pela Defesa Cibernética.

1.4.2 Delineamento da Pesquisa

O delineamento do presente trabalho ocorrerá através do levantamento e escolha bibliográfica, leitura, fichamento, argumentação e conclusão crítica.

1.4.2.1 Procedimentos para a revisão de Literatura

Para cumprir o objetivo de levantar informações e estruturar um modelo teórico de análise, será realizada um estudo da bibliografia da seguinte forma:

a. Fontes de busca

   i. Livros;
   ii. Artigos Científicos;
   iii. Monografias, dissertações e teses;
   iv. Sites de Noticias; e
   v. Manuais Doutrinários no Portal de Doutrina do Exército.

b. Estratégia de busca para as bases de dados eletrônicas

Os materiais de consulta bibliográfica serão procurados por meio dos sites de busca como o google. Para otimizar as buscas, alguns termos serão utilizados co-

mo: “Cibernética”, “Guerra Cibernética”, “Ciberespaço”, “Politica de Segurança”, “Politica de Defesa” e “Estratégia de Defesa”.

c. Critérios de inclusão

i. Estudos publicados em português;
ii. Estudos publicados em inglês;
iii. Materiais de autor reconhecido; e
iv. Informações relevantes em Jornais, revistas e TV.

d. Critérios de exclusão

i. Fontes duvidosas; e
ii. Materiais que não esteja relacionado com a Segurança e Defesa Cibernética e Operações Conjuntas.

1.4.2.2 Procedimentos Metodológicos

O presente trabalho caracteriza-se quanto à natureza, como sendo uma pesquisa aplicada, que visa contribuir para a melhoria da situação analisada no problema em estudo, utilizando o método dedutivo para a tomada de conclusões sobre o conteúdo analisado. Será realizada uma pesquisa bibliográfica, com uma leitura exploratória do material utilizado.

1.5 JUSTIFICATIVA

Após as investidas bem sucedidas de alguns ataques Cibernéticos, como os realizados contra o Irã, Estônia e Geórgia (JÚNIOR, 2013), as nações do globo passaram adotar medidas defensivas e ofensivas contra ataques Cibernéticos, que na maioria dos casos, são disseminados na rede mundial de computadores de forma anônima. Essas atitudes de guerra, que exigem planos políticos, estratégicos, operacionais e táticos, transformou o Ciberespaço em um novo ambiente de batalha.

Diante desse novo cenário, onde as nações estão se preparando para proteger suas infraestruturas críticas de informação. O Brasil tem desenvolvido Politicas

de Segurança e de Defesa Cibernética e através do Ministério da Defesa, busca desenvolver tecnologias próprias para minimizar a dependência de tecnologias estrangeiras, necessárias ao funcionamento do ambiente Cibernético Nacional, capacitar pessoal, proteger infraestruturas críticas de informação e combater no Ciberespaço.

Nas Operações Conjuntas, as atividades Cibernéticas executam tarefas de proteção das suas infraestruturas críticas de informação, exploração e ataque das infraestruturas inimigas. Nesse contexto, este trabalho analisará os componentes do Sistema de Defesa Cibernética nas Operações Conjuntas buscando identificar as áreas de atuação, bem como atribuições e atores envolvidos.

2 DESENVOLVIMENTO

2.1 O CIBERESPAÇO E A GUERRA CIBERNÉTICA

Em um livro intitulado, “Cibernética”, Nobert Wiener em 1948, (WIENER, 1954), introduz o termo “Cibernética” e afirma que a compreensão da sociedade só pode ser realizada através do estudo das facilidades de comunicação e de troca mensagens. No futuro, a comunicação entre os homens e as maquinas e entre as máquinas e as máquinas serão cada vez mais importantes. Desenvolve uma teoria da comunicação e do controle, mostrando como o homem se relaciona com o meio que o circunda, trocando informações e tentando se ajustar. Define que informação é o conteúdo que o homem permuta com o mundo exterior ao buscar o seu ajuste ao meio em que vive e que a complexidade da vida moderna acelerou a troca de informações do homem com esse mesmo meio circundante. Defende que a comunicação e o controle, mesmo pertencendo à vida exterior ao homem faz parte da essência da sua vida interior.

> O propósito da cibernética é de desenvolver uma linguagem e técnicas que nos capacitem, de fato, a haver-nos com o problema do controle e comunicação em geral, e a descobrir o repertório de técnicas e ideias adequadas para classificar as manifestações específicas sob a rubrica de certos conceitos (WIENER, 1954).

A Doutrina Militar de Defesa Cibernética, Brasil (2014c), define Cibernética como à comunicação e o controle do uso das redes de computadores, dos computa-

dores, dos sistemas computacionais e de comunicações e suas interações entre si. No âmbito da defesa militar são incluídos na estrutura Cibernética: os recursos de Tecnologia da Informação e Comunicações que compõem o Sistema Militar de Comando e Controle, os sistemas administrativos ligados às atividades operacionais e os sistemas de armas e vigilância.

Gibson (1984) criou a designação de “Ciberespaço” em sua obra de ficção científica chamado de *Neuromancer*. Diz que o ciberespaço é a simulação do espaço real, além disso, ele é composto por toda estrutura física necessária para que os personagens possam interagir entre si, em um ambiente totalmente novo, compartilhando intensas aventuras, que devido ao seu realismo e envolvimento vão afetar as suas vidas particulares. O comentador Silvio Alexandre afirma que:

> Para Gibson, o conceito de ciberespaço é o de "uma alucinação consensual que pode ser experimentada diariamente pelos usuários através de softwares especiais... Uma representação gráfica de dados retirados dos bancos de todos os computadores do sistema humano. Uma complexidade impensável... Linhas de luz que abrangem o universo não-espacial da mente, nebulosas e constelações infindáveis de dados... É também realidade virtual" (GIBSON, 1984).

Em Brasil (2014c), o Ciberespaço ou Espaço Cibernético é o espaço virtual, formado por ativos computacionais que podem estar conectados a rede ou não, onde informações digitais circulam, são processadas e/ou armazenadas.

Martins et. al (2016) definem Cibersegurança ou Segurança Cibernética como a proteção de redes, de dados e sistemas no Ciberespaço. O Crime Cibernético ou Cibercrime limita-se a ações que são proibidas por lei, através do uso da internet. Nem todo Cibercrime é considerado uma ameaça ao estado. A Guerra Cibernética ou Ciberguerra é o confronto através de meios de informática e de eletrônica, usando a internet, com o objetivo de atacar estruturas críticas do interesse público como: os serviços financeiros, a saúde, as redes de transportes, energia elétrica, água e gás. A Ciberdefesa ou Defesa Cibernética são ações empregadas para prevenção e reação de ataques cibernéticos a áreas críticas de um país.

A Segurança Cibernética é a proteção e a garantia da utilização dos ativos estratégicos de informação, que compõem as infraestruturas críticas nacionais, como as de redes de dados, computadores e sistemas informatizados. Abrangendo a interação com órgãos públicos e privados envolvidos com o funcionamento de suas estruturas tecnológicas e informacionais críticas nacionais, especialmente os órgãos

da administração pública federal. Defesa Cibernética é o conjunto de ações ofensivas, defensivas e exploratórias, na área militar, com planejamento estratégico em nível nacional, coordenado e integrado pelo Ministério da Defesa, realizadas no Espaço Cibernético, com a finalidade de proteger os sistemas de interesse da Defesa Nacional, obter dados para a produção de conhecimentos de inteligência e causar prejuízos aos sistemas de informações dos oponentes. Brasil (2014c), (MARTINS et al, 2016), (JÚNIOR, 2013).

Observa-se que a Segurança Cibernética e a Defesa Cibernética têm como objetivos: garantir a disponibilidade, a confidencialidade, a autenticidades e a integridade dos ativos ou meios de informações, que por sua vez, são indispensáveis para que os órgãos, as entidades, a sociedade e o estado alcancem seus objetivos (JÙNIOR, 2013).

2.2 A GUERRRA CIBERNÉTICA NO CENÁRIO ATUAL

De acordo com Ruivo (2014), o mundo está vivendo uma Guerra de Quarta Geração, em que o surgimento de novas tecnologias e de atores não-estatais, permitem que inimigos belicamente inferiores possam enfrentar o Estado. A Guerra de Primeira Geração, com início em 1648, no Tratado de Paz de Westphalia e termino em 1860, teve como característica principal de emprego, o “Princípio de Massa”, em que o objetivo era concentrar o maior poder de combate no local e momento decisivo da guerra, eram batalhas formais, ordenadas e estruturadas, em linhas e colunas, com distinção clara entre militares e civis, uso de uniformes e teve seu auge com as guerras napoleônicas.

A Segunda Geração foi entre 1860 e à Primeira Guerra Mundial, caracterizada pelo uso do poder de fogo em massa, em sua maioria, através da artilharia indireta, a artilharia conquista e a infantaria ocupa. O comandante era como um maestro na sincronização do poder de fogo, havia uma metodização da guerra em detrimento da criatividade e iniciativa do combatente. Com o surgimento dos blindados e da aviação, a guerra entra em um novo estágio, a Guerra de Terceira Geração, conhecida como guerra de manobra, que tem como características: a surpresa, a velocidade, a inteligência e o posicionamento. Diferentemente da batalha de atrito direto, a guerra de manobra, buscava obter uma situação vantajosa, desgastando o inimigo

com mudanças táticas, compreensão da situação do inimigo, dando liberdade para os subordinados adaptar seus planejamentos na busca de vantagens sobre o oponente. O mais importante era os objetivos e não o método ou o processo.

Atualmente, as guerras são classificadas em quatro tipos, conforme Ruivo (2014):

1. A Guerra Convencional ou Regular – caracterizada pelos conflitos entre Estados, combatidas entre exércitos organizados e com nítida separação entre civis e militares.
2. A Guerra de Destruição em Massa – Após a segunda guerra, as armas de destruição em massa, passaram a ser a grande ameaça para a humanidade, no entanto, uma guerra com armas desse tipo, atualmente perece ser improvável.
3. As Guerras Irregulares – são guerras locais como: resistências, guerrilhas e insurreição. Esse tipo de guerra não distingue civil de militar, sem campos de batalha e uniformes.
4. Guerras Assimétricas – podem ser classificadas como Guerras Irregulares em escala mundial e se instaurou após os atentados de 11 de setembro de 2001.

As Guerras Assimétricas formam denominadas de Guerras de Quarta Geração, a qual, Liang e Xiagsui chamaram de “Guerra além dos Limites”, que está voltada para a destruição dos meios internos de sustentação do inimigo, sem ter que abatê-lo fisicamente.

A Guerra de Quarta Geração necessita de um sistema de comando extremamente flexível e intenso trabalho de inteligência. Contém conhecimentos e habilidades de gerações anteriores, exige que os comandantes tenham conhecimento detalhado da guerra que irá enfrentar. De acordo com Liang e Xiagsui, essas guerras podem se manifestar de varias formas, como por exemplo: Guerra Cibernética, Econômica, Psicológica, Biológica, Eletrônica, Química, Radiológica, Nuclear e Bacteriológica ou Virótica (RUIVO, 2014).

Com relação à Guerra Cibernética, atualmente, diversos países se envolveram em ataques cibernéticos, principalmente os Estados Unidos e a China, visto que esses países estão sempre entre os acusados e os acusadores de roubo de informações, ataques e invasões de redes. Outros países considerados coadjuvantes

nos conflitos cibernéticos foram a Estônia, Israel, Irã e Geórgia, em alguns casos foram vítimas de ataques e em outros agiram com o apoio das principais potências (JÙNIOR, 2013).

2.2.1 - Guerra Cibernética e os Estados Unidos da América

Em 2011, os Estados Unidos anunciaram o lançamento da Estratégia Internacional Norte-Americana para o Espaço Cibernético. Foi o primeiro documento a traçar e tornar pública uma posição estratégica e operacional no Espaço Cibernético, tornando-se um marco mundial (JÚNIOR, 2013). Logo após os Estados Unidos tornar público seus planos para o ambiente virtual, outros países começaram a desenvolver seus próprios planejamentos estratégicos, como a Rússia que em 2012, publica um documento sobre as atividades das suas Forças Armadas no Espaço Cibernético.

De acordo com Júnior (2013), a National Security Agency (NSA) é a responsável por todas as questões de segurança Cibernética dos Estados Unidos e faz parte da estrutura do Departamento de Defesa (DoD). A NSA é responsável pela segurança da Tecnologia da Informação e Comunicações dos órgãos federais do governo dos EUA. É responsável por apoiar os outros órgãos do governo em produtos e serviços relacionados ao Espaço Cibernético. A figura 1 apresenta a estrutura do Departamento de Defesa Norte-Americano.

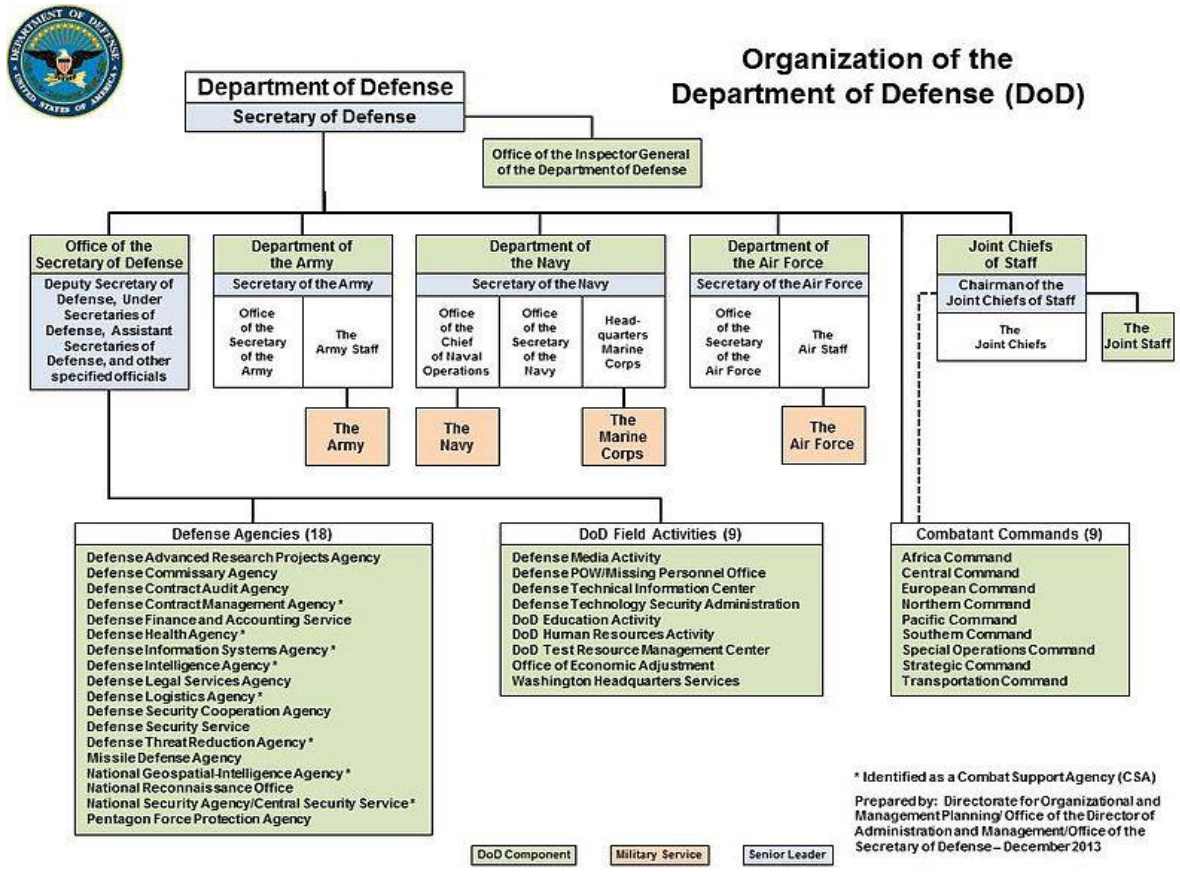

Fig 1. Organização do Departamento de Defesa dos Estados Unidos. Fonte: Júnior (2013).

Os Estados Unidos possuem dezesseis agencias e escritórios responsáveis pelas atividades de inteligência para preservar a segurança nacional. Essas agências coletam informações das mais diversas áreas, como por exemplo, a militar, o terrorismo, a política e o hacketivismo. Em 2009 foi criado o U.S. Cyber Command (USCyberComm), órgão responsável pela coordenação das ações de prevenção e Defesa Cibernética dos Estados Unidos (JÚNIOR, 2013). O cenário mundial da criação do Cyber Command foi os ataques ocorridos na Estônia e na Geórgia em 2007 e 2008, respectivamente, em que a houve a intervenção da Organização do Tratado do Atlântico Norte (OTAN) para defender as redes dos países atacados. Esses ataques, no qual, havia suspeita de envolvimento Russo, causaram a interrupção dos sistemas bancários e de comunicação por vários dias (MARTINS, et al, 2016).

O USCyberComm foi criado para interagir com as forças militares, e com outros órgãos da comunidade de inteligência. É uma subunidade das Forças Armadas subordinada ao Comando Estratégico Norte-Americano. O comandante da NSA é também diretor do USCyberComm e chefe da Central de Segurança, devido o obje-

tivo de alinhar as politicas de Segurança e Defesa Cibernética. O USCyberComm é considerado uma peça do sistema de proteção (JUNIOR, 2013).

A Estratégia Internacional para o Espaço Cibernético (UNITED STATES, 2011) criada em 2011, destaca a importância da Cibernética para o desenvolvimento da humanidade e condiciona os benefícios das Tecnologias da Informação e Comunicações a um ambiente seguro e confiável. Defende, ainda, a liberdade de expressão e associação, privacidade e o livre fluxo de informações. Reforça a importância da capacitação humana, respeito à propriedade privada, abertura comercial, promoção dos direitos universais e da parceria entre países, sociedade, setor privado e usuários na execução da Estratégia Internacional.

O referido documento também assegura que o direito de defesa poderá, ou não, ser pelas vias diplomáticas, podendo ser utilizadas forças militares em retaliação. Deixando claro que as ações Cibernéticas não se limitam ao ambiente virtual, podendo tomar proporções como qualquer ataque militar inimigo. No ambiente nacional, serão tomadas medidas para garantir a segurança e a estabilidade das redes internas, mesmo que para isso medidas coercitivas devam ser tomadas contra o setor privado, para garantir a proteção das redes dados. O documento enfatiza que a Segurança e a Defesa Cibernética dependem muito mais da capacitação humana do que de equipamentos e produtos, valorizando assim, a capacitação humana e a difusão de conhecimentos (UNITED STATES, 2011).

Em documento vazado por Edward Snowden os Esatdos Unidos cria uma diretiva secreta sobre Defesa Cibernética chamada de “Offensive Cyber Effect Operations” (OCEO) Operações Cibernéticas Ofensivas. As OCEO devem fazer uma analise dos alvos selecionados pelos Estados Unidos como sendo de importância nacional, verificando a efetividade da utilização da ofensiva Cibernética em relação a outros meios do poder nacional, deve ser estabelecida e mantida, pelo governo, capacidades para que a OCEO seja integrada a capacidades ofensivas. As capacidades das OCEO estão alinhadas com os objetivos nacionais dos Estados Unidos, podendo agir sem advertir ou fornecer pouca advertência ao oponente ou alvos, podendo causar efeitos insignificantes como também muito danoso. Caso as ferramentas ou o acesso a um determinado alvo não esteja disponível, esse tipo de ofensiva pode demandar tempo e esforço (MARTINS, et al, 2016).

As Operações ofensivas das OCEO requerem o desenvolvimento e implementação de hardwares e softwares para a criação de Ciberarmas, que podem ex-

plorar vulnerabilidades, passando a colecioná-las. No entanto, esse tipo de atividade, pode gerar uma grave crise desconfiança na comunidade internacional, já que na produção de determinados equipamentos ou softwares, vulnerabilidades podem ser colocadas de forma proposital, a fim de coletar informações e realizar ataques. Esse tipo de desconfiança atingiu empresas americanas após as revelações de Snowden. Inclusive soou como alerta para as autoridades brasileiras, para produzir suas próprias tecnologias sensíveis.

Outro aspecto das ações americanas diz respeito à vigilância em massa, no qual, as empresas ou governos passam a coletar informações da sociedade ou de grupos específicos, com o objetivo de cruzar essas informações, na busca de ameaças. Por outro lado, esse tipo de atividade fere o direito de privacidade dos cidadãos, além de colocar em risco a segurança da nação, pois, as informações armazenadas para análise, podem ser extraviadas e utilizada para outros fins (MARTINS, et al, 2016).

2.2.2 – A Guerra Cibernética e a Rússia

Logo após os Estados Unidos anunciar os seus planos relativos à Defesa Cibernética, a Rússia publicou um documento semelhante ao Norte-Americano, com praticamente as mesmas garantias fundamentais, mas diferenciando por apresentar metas e princípios mais voltados a realidade Russa, conforme RÚSSIA (2011). Valorizando o Estado de direito e os princípios de legalidade, reconhece a complexidade que envolve a Cibernética e entende a importância da cooperação e interação com outros países, principalmente na área de proteção.

O documento busca a erradicação de fatores que possam gerar conflitos e não menciona ações ofensivas por parte dos Russos no Espaço Cibernético. Caso ocorram conflitos, devem ser buscadas soluções diplomáticas com base no direito internacional, mas não descarta a possibilidade da força militar contra um possível conflito Cibernético, no princípio do direito da autodefesa. O documento não retrata a estrutura organizacional da sua Segurança e Defesa Cibernética (RÚSSIA, 2011).

2.2.3 A Guerra Cibernética e a Índia

A Índia não possui uma estratégia oficial, mas é possível encontrar alguns documentos preliminares com princípios para o setor. Não possui órgãos relacionados à Defesa Cibernética. Cada órgão é responsável por conduzir ações de acordo com a necessidade de cada um. Alguns documentos abordam a necessidade de integração entre setor público e privado, e interação com outros países, para poder alcançar níveis toleráveis de Segurança Cibernética (JÚNIOR, 2013).

Abordam que as soluções Cibernéticas devem estar além das tecnologias tradicionais, deve haver integração de informações de múltiplas fontes e monitoramento integral dos ativos que necessitam de proteção, garantir capacitação e recursos adequados para lidar com situações de risco, reconhece o investimento em pessoal e nos processos, em conjunto com as melhores soluções de tecnologias disponíveis.

2.3 A GUERRA CIBERNÉTICA NO CENÁRIO FUTURO

Liang e Xiagsui (1999) afirmam que os Estados Unidos da América definiram as quatro formas de guerra possíveis de ocorrer no futuro: Guerra Cibernética, Guerra de Precisão, Operações Combinadas e “Military Operations Other Than War (MOOTW)”. Explica que com exceção das Operações Combinadas, as outras formas de guerra podem ser consideradas como o resultado de um pensamento militar e cita:

> O General Gordon R. Sullivan, ex-Chefe do Estado-Maior do Exercito norte-americano, sustenta que a guerra cibernética será a forma básica de uma guerra futura, e em função desta percepção, desenvolveu uma força militar com o maior nível de informatização possível, tanto no âmbito das Forcas Armadas norte-americanas, quanto em âmbito mundial. Ele ainda propôs o conceito de guerra de precisão, baseado na previsão de que “haverá uma guinada nos fundamentos básicos da guerra do futuro, no sentido de sistemas e processos digitais e os ataques invisíveis à longa distancia”. Para os norte-americanos, é possível que o advento de novas armas e sistemas de alta tecnologia, tais como: as armas de precisão, o Sistema de Posicionamento Global (GPS), os sistemas C4I e os aviões invisíveis pouparão os seus soldados pesadelos da guerra de atrição (LIANG e XIAGSUI, 1999).

Em fevereiro de 2011, autoridades de Inteligência dos Estados Unidos mostraram preocupações sobre a vulnerabilidade que os Estados Unidos enfrentariam

numa possível ameaça de Guerra Cibernética. Situação que então diretor da CIA, Leon Panetta, afirmou que “representa o futuro campo de batalha” e que “o próximo Pearl Harbor poderia muito bem ser um ataque cibernético” (RYAN, 2011).

2.4 – O DESENVOLVIMENTO DA DEFESA CIBERNÉTICA NO BRASIL

2.4.1 A Segurança Cibernética

As ações de Segurança Cibernética do governo federal são tratadas pelo Departamento de Segurança da Informação e Comunicações (DSIC), pelo Gabinete de Segurança Institucional da Presidência da Republica (GSI). A Defesa Cibernética, pelo Centro de Defesa Cibernética (CDCiber), que faz parte do Exército Brasileiro, subordinado ao Ministério da Defesa.

O Conselho de Defesa Nacional (CDN), assessora o Presidente da Republica nas questões de Segurança e Defesa Cibernética. Na Constituição Federal de 1988, o seu art. 91, afirma que o CDN é um órgão de consulta do Presidente da Republica nos quesitos de soberania nacional e defesa do estado democrático de direito. É um órgão de estado com a sua secretária executiva exercida pelo ministro do Gabinete de Segurança Institucional (JÙNIOR, 2013).

A Câmara de Relações Exteriores e Defesa Nacional (Creden), assessora o Presidente da Republica nos assuntos relacionados às relações exteriores e defesa nacional, sua presidência é exercida pelo ministro-chefe do Gabinete de Segurança Institucional. O Instituto Nacional de Tecnologia da Informação (ITI) é uma autarquia subordinada à Casa Civil que tem como finalidade manter o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileiras (ICP/Brasil).

O GSI coordena os assuntos estratégicos que afetam a segurança do Estado e da sociedade, como a segurança da informação e comunicações, segurança das infraestruturas críticas nacionais e Segurança Cibernética no âmbito da administração pública. O GSI é composto por cinco órgãos, listados abaixo (JÚNIOR, 2013):

1. Comitê Gestor de Segurança da Informação (CGSI) – tem como função assessorar o Conselho de Defesa Nacional sobre as diretrizes da Politica de Segurança da Informação na Administração Pública Federal;

2. Secretária de Acompanhamento e Estudos Institucionais (SAEI) – coordena a realização de estudos sobre assuntos relativos à segurança institucional e tratar temas referentes ao gerenciamento de crises;
3. Agência Brasileira de Inteligência (ABIN) – tem como função coordenar as ações do Sistema Brasileiro de Inteligência, produzir e salvaguardar conhecimentos sensíveis.
4. Departamento de Segurança da Informação e Comunicações (DSIC) – tem a atribuição de gerenciar a segurança da Informação e Comunicações no âmbito da Administração Pública Federal;
5. Rede Nacional de Segurança da Informação e Criptografia (RENASIC) – é uma rede virtual de troca de informações sobre a Segurança da Informação e Criptografia.

O GSI através de seus órgãos como a ABIN exerce atividades de prevenção como a repressão de possíveis ataques pelas redes de computadores. No entanto, as ações ofensivas de combate são realizadas pelo CDCiber vinculado ao Ministério da Defesa.

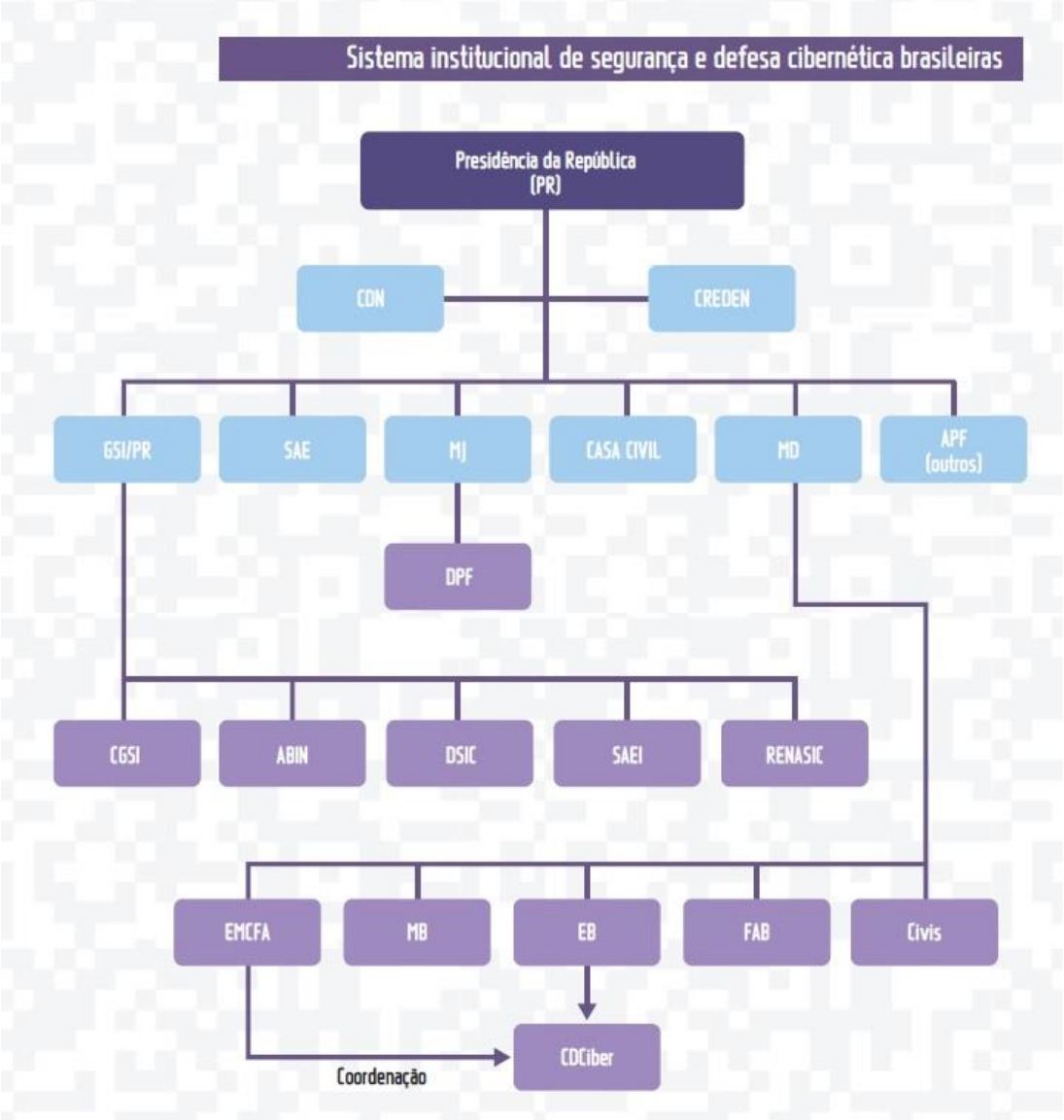

Fig. 2. Sistema Institucional de Segurança e Defesa Cibernética Brasileira. Fonte: Martins, et al (2016).

Existem outros órgãos que atuam na área de Segurança Cibernética Nacional como a Polícia Federal, o Ministério da Justiça, o Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança, o Serviço Federal de Processamento de Dados entre outros. Além dos órgãos estatais, órgãos não-estatais também cuidam da Segurança Cibernética no Brasil. Os não-estatais vão desde administradores de redes até empresas privadas, dentre os não-estatais destacam-se o CERT.br, subordinado ao Comitê Gestor da Internet no Brasil (CGI.br). Já os principais órgãos estatais que atuam na Segurança das redes e dos Sistemas são: A Polícia Federal, a ABIN e o CDCiber, além de Delegacias Especializadas, Secretária de Segurança Pública Estaduais e Polícia Civil. (MARTINS et al, 2016).

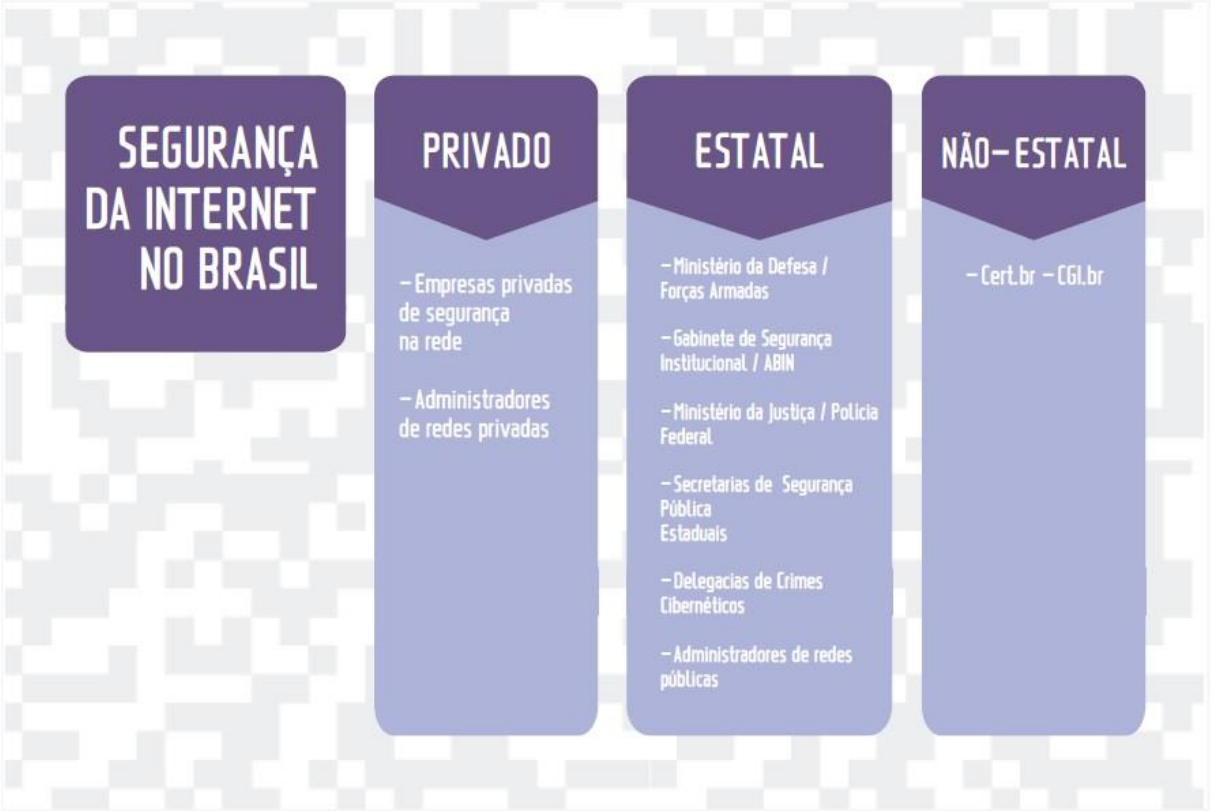

Fig. 3 Segurança da Internet no Brasil. Fonte: Martins, et al (2016).

O CERT.br é o Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil que tem responsabilidade de tratar incidentes de segurança no nível nacional. Detectando e reunindo estatísticas sobre os ataques e incidentes de Segurança na internet e a partir destes dados criar e disseminar materiais educativos sobre a segurança na internet. Ainda, dar suporte ao processo de recuperação e análise de sistemas comprometidos e de ataques, também contribui com outros órgãos no desenvolvimento de boas práticas e cooperação em Segurança nas redes. Assim, o CERT.br atua diretamente na Segurança Cibernética da rede Brasileira.

2.4.2 A Defesa Cibernética

Enquanto o Gabinete de Segurança Institucional gerência os assuntos sobre segurança, o Ministério da Defesa, através do Exército Brasileiro, controla as ações de Defesa Cibernética. O livro verde da Segurança Cibernética interpreta que o escopo de atuação da Segurança Cibernética compreende aspectos e atitudes tanto de prevenção como de repressão (Martins et al, 2016).

A Política Nacional de Defesa (BRASIL, 2012e) é o documento que estabelece os objetivos e orientações para o preparo e emprego das forcas militares e civis, nas questões de Defesa Nacional. É o planejamento de mais alto nível nas ações de defesa, coordenado pelo Ministério da Defesa. A Política Nacional de Defesa define que a Segurança "*é a condição que permite ao País preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais*". E a Defesa Nacional como "*o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas*".

A Política Nacional de Defesa afirma que os objetivos da defesa são inseparáveis dos objetivos de desenvolvimento do país. Sustenta que o domínio de tecnologias sensíveis, principalmente nos setores estratégicos: nucleares, espaciais e cibernéticos, são essenciais para a autonomia e o desenvolvimento nacional. Os avanços tecnológicos nas áreas de Tecnologia da Informação, sensoriamento remoto, satélites e outros, aperfeiçoaram os sistemas administrativos e militares, em países que investiram muitos recursos financeiros na defesa. Esses avanços criaram vulnerabilidades que podem ser exploradas, sendo essencial o investimento nacional no desenvolvimento de tecnologias avançadas para superar essas vulnerabilidades.

Com a intenção de preservar os interesses e a soberania do país, a Política Nacional de Defesa buscou estruturar a Defesa Nacional de forma alinhada com a Política e a Estratégia do Nacional. Nesse contexto foram criados os Objetivos Nacionais de Defesa, que entre eles estão:

> Manter Forças Armadas modernas, integradas, adestradas e balanceadas, e com crescente profissionalização, operando de forma conjunta e adequadamente desdobradas no território nacional; desenvolver a indústria nacional de defesa, orientada para a obtenção da autonomia e tecnologias indispensáveis. (BRASIL, 2012e).

A Política Nacional de Defesa estabelece algumas orientações que devem ser observadas para execução dos Objetivos Nacionais de Defesa enfatizando o setor cibernético:

> Os setores espacial, cibernético e nuclear são estratégicos para a Defesa do País; devem, portanto, ser fortalecidos; Para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar

> procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento. (BRASIL, 2012e).

A Estratégia Nacional de Defesa (BRASIL, 2012b) é inseparável da estratégia Nacional de Desenvolvimento, que entre os princípios de um projeto forte de defesa está à independência da capacitação tecnológica, principalmente nos setores nuclear, espacial e cibernético, enfocando que o domínio de tecnologias sensíveis é essencial para a independência do desenvolvimento e defesa do país. A Estratégia Nacional de Defesa define as diretrizes que devem ser observadas quanto ao desenvolvimento da cibernética:

> Fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear. Esse fortalecimento assegurará o atendimento ao conceito de flexibilidade. Como decorrência de sua própria natureza, esses setores transcendem a divisão entre desenvolvimento e defesa, entre o civil e o militar. Os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio País não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço. [...] (BRASIL, 2012b).

Na Estratégia Nacional de Defesa os setores estratégicos, o espacial, o nuclear e o cibernético são tratados separadamente especificando detalhes de seu desenvolvimento. O setor cibernético desenvolverá capacitações abrangendo usos educacionais, militares e industriais, priorizando as tecnologias de comunicação, assegurando que os integrantes das Forças Armadas possam atuar em rede. Algumas prioridades são: o fortalecimento do Centro de Defesa Cibernética; aperfeiçoar a Segurança da Informação e Comunicações; incentivar a pesquisa científica nacional e internacional para o setor cibernético; utilizar computação de alto desempenho para criar sistemas computacionais no setor cibernético; desenvolver tecnologias que aperfeiçoem a segurança cibernética do país; capacitar, preparar e empregar os poderes cibernéticos estratégicos e operacionais das operações conjuntas; organizar a produção de conhecimentos cibernéticos; e apoiar o desenvolvimento tecnológico de ações cibernéticas.

O livro Branco de Defesa (BRASIL, 2012c) aborda que a proteção do espaço cibernético não abrange apenas, proteger seus próprios ativos e a capacidade de atuação em rede, mas também, outras áreas, como a pesquisa científica, a doutrina, o preparo e emprego operacional, a gestão de pessoal, a capacitação e a inteligência.

A criação do Setor Cibernético tem como finalidade manter: integridade, autenticidade, confidencialidade e disponibilidade das informações que são armazenadas, processadas e que trafegam nas redes. O desenvolvimento da cibernética é um projeto de longo prazo, que abrange a área operacional, a ciência e a tecnologia. O setor Cibernético é coordenado pelo Exército que já avançou significativamente no desenvolvimento de soluções de alto nível tecnológico e na capacitação de pessoal. Sendo que algumas premissas foram desenvolvidas para o projeto como "*contemplar multidisciplinaridade e dualidade das aplicações; fomentar a base industrial de defesa; induzir a indústria nacional a produzir sistemas inovadores; e produzir componentes críticos nacionais*" (BRASIL, 2012c).

O Centro de Defesa Cibernética do Exército é o órgão de integração da Defesa Cibernética, que interage com as outras organizações governamentais de Segurança da Informação e entre outras atividades, busca: *"a melhoria da capacitação dos recursos humanos; a atualização doutrinária; o fortalecimento da segurança; a respostas a incidentes de redes; a incorporação de lições aprendidas; e a proteção contra ataques cibernéticos*". (BRASIL, 2012c).

Em 2012 foi criada a Política Cibernética de Defesa que tem como finalidade, orientar, para o nível estratégico, as atividades de Defesa Cibernética, e para nível operacional e tático, as ações de Guerra Cibernética, no âmbito do Ministério da Defesa, buscando alcançar seus objetivos. São objetivos da Política Cibernética de Defesa (BRASIL, 2012d):

1. Assegurar que as Forças Armadas façam o uso efetivo do espaço cibernético e dificultar ou impedir a sua utilização em desacordo com os interesses da Defesa Nacional;
2. produzir e capacitar recursos humanos para suprir as necessidades das atividades do Setor de Defesa Cibernético;
3. apoiar na produção de conhecimentos de Inteligência, de origem cibernética, úteis para o Sistema de Inteligência de Defesa e para os órgãos de governo federal envolvidos com a SIC e Segurança Cibernética;
4. criar e manter atualizada a doutrina de emprego do Setor Cibernético;
5. desenvolver medidas que contribuam para a Gestão da SIC no âmbito do MD;

6. adequar as estruturas de Comunicações e Tecnologia da Informação das Forças Armadas e desenvolver pesquisa para atender às necessidades do Setor Cibernético;
7. estabelecer os princípios básicos para direcionar a criação de legislações e normas específicas para o Setor Cibernético;
8. interagir com os esforços de mobilização nacional e militar para garantir a capacidade operacional e dissuasória do Setor Cibernético; e
9. contribuir para a segurança da infraestrutura de informação da Administração Pública Federal.

O Brasil, ainda não possui uma Estratégia Nacional para a Defesa Cibernética que estabeleça suas próprias diretrizes (JÙNIOR, 2013). Após a criação do Comando Militar de Defesa Cibernética dos Estados Unidos USCyberComm, o Brasil sentiu a necessidade de se atualizar ao cenário internacional e incorporar a atividade militar, a doutrina da Defesa Cibernética. Essa iniciativa brasileira antecedeu as denúncias de Edward Snowden. Em 2010, coube ao exército criar o Núcleo de Defesa Cibernética (NuCDCiber), com o objetivo de desenvolver o Centro de Defesa Cibernética, coordenar e executar um projeto sobre a área Cibernética, planejar e executar a Segurança Cibernética, coordenar a Rede Nacional de Segurança da Informação e Criptografia e outras responsabilidades (MARTINS et al, 2016).

Em 2012, foi inaugurado o Centro de Defesa Cibernética (CDCiber), vinculado ao Ministério da Defesa, que teve um incentivo em investimentos e reestruturação após as denúncias de Snowden, como a criação da Escola Nacional de Defesa Cibernética, que teve seu projeto iniciado em 2015, com o Instituto de Defesa Cibernética (IDCiber), vinculado a UnB e a implementação do Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber). Este teve como objetivo a criação de cursos de ensino a distância, buscando desvincular o CDCiber da capacitação de pessoal, deixando-o apenas com a atuação em operações de Guerra Cibernética. O IDCiber tem como objetivo cooperar na Rede Nacional de Excelência em Segurança da Informação e Criptografia (RENASIC) e fazer interface com as bibliotecas digitais de interesse.

Nesse mesmo período foi criado o Núcleo do Comando de Defesa Cibernética (NuComDCiber), órgão coordenador da Defesa e Guerra Cibernética no âmbito do Ministério da Defesa. Tanto o NuENaDCiber quanto o NuComCDCiber são subordi-

nados ao CDCiber, que contam com militares da três forças, com o objetivo de integrar atividades para Operações Conjuntas. A portaria 2.777/MD de 27 de outubro e 2014 que criou os núcleos citados, enfatiza a implantação e consolidação do desenvolvimento do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, o apoio à pesquisa e ao desenvolvimento de produtos de defesa cibernética, e por último a criação do Observatório de Defesa Cibernética, conforme Martins et al (2016).

A Defesa Cibernética Brasileira está dividida em quatro níveis de decisão (MARTINS et al, 2016):

1. O Plano Político – é desenvolvido pelo Gabinete de Segurança Institucional e engloba toda a Administração Pública Federal, sendo assessorado pela Casa Civil da Presidência da Republica, ABIN, Câmara das Relações Exteriores (CREDEN), ANATEL, Departamento da Policia Federal, CGI-.br, GSI, SERPRO, Departamento de Segurança da Informação e Comunicações (DSIC) e Conselho de Defesa Nacional;
2. O Plano Estratégico – é desenvolvido pelo Ministério da Defesa e assessorado pelos comandantes do Exército, Marinha e Aeronáutica e do Conselho Militar de Defesa (CMiD).
3. O Plano Operacional e Tático – fica a cargo de cada das Forças Armadas, Marinha, Exército e Aeronáutica. Em Operações Conjuntas, o CDCiber organiza destacamentos militares para atuar nos níveis operacionais e táticos. Atua na centralização das cooperações externas e internas na ótica Cibernética, além de cultivar as relações entre a defesa nacional e a área da Segurança da Informação.

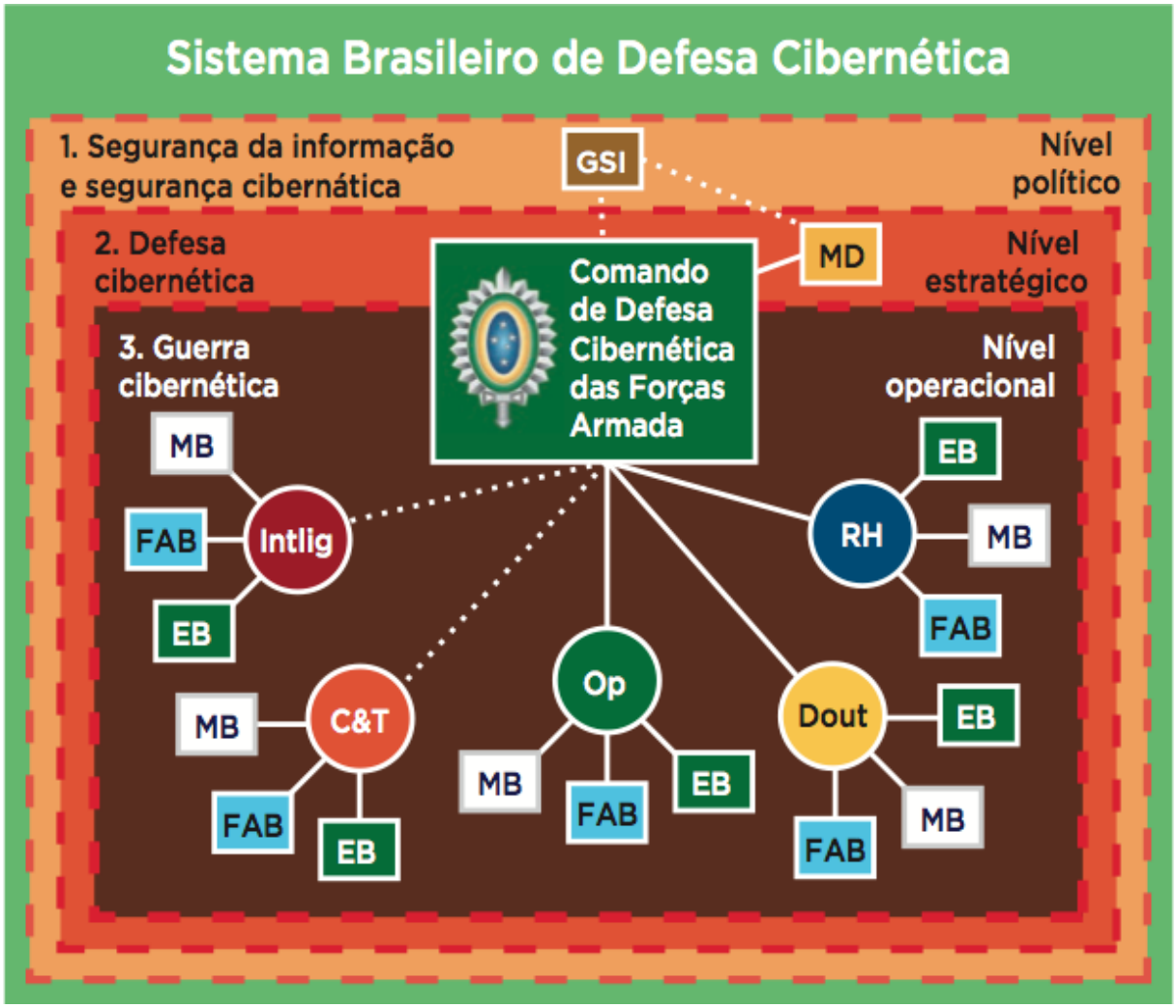

Fig. 4 Sistema Brasileiro de Defesa Cibernética. Fonte: http://defesacibernetica.ime.eb.br/

A Rede Nacional de Segurança da Informação e Criptografia (RENASIC), criada em 2008, apesar de ser coordenada pelo CDCiber é uma entidade de intercâmbio entre entidades privadas e governamentais, instituições nacionais e internacionais e universidades. Sua finalidade é realizar estudos, análises e desenvolvimento de infraestruturas, que incluem (Martins et al, 2016):

> Instrumentação física e lógica para análise de ataques secundários (side-channel atacks), suas respectivas contramedidas; ferramentas para a avaliação dos algoritmos de criptografia; ambientes de avaliação para hardware e software criptográficos; e ferramentas para avaliação dos esquemas de defesa cibernética e forense computacional.

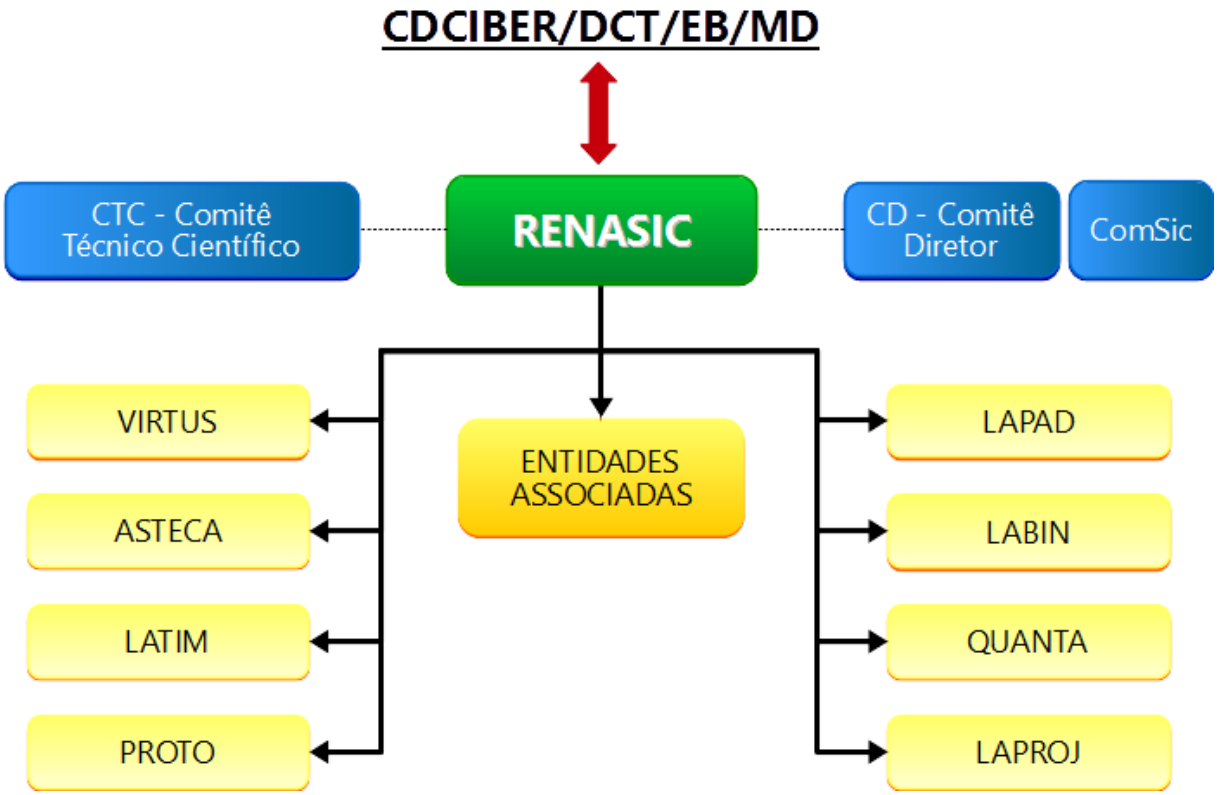

Fig. 5 Estrutura da RENASIC. Fonte: http://www.renasic.org.br/institucional

De acordo com a Doutrina Militar de Defesa Cibernética (BRASIL, 2014c), a Defesa Cibernética possui três tipos de ações:

1. ataque – compreende a negação, a interrupção, a destruição ou corrupção de informações ou sistemas alheio;
2. proteção – compreende a neutralização e mitigação de ataques inimigos;
3. exploração – abrange a obtenção e coleta de informações de interesse sobre o inimigo.

O Ministério de Defesa é o responsável por estabelecer os níveis de alerta cibernético nas atividades diárias e na proteção de grandes eventos. Existem cinco níveis: Branco - Baixo, Azul - Moderado, Amarelo - Médio, Laranja - Alto, Vermelho - Muito Alto. No nível Baixo, as ameaças não afetam os interesses do Ministério da Defesa. No nível Muito Alto, as forças hostis afetam as infraestruturas críticas de informação com grande impacto. (MARTINS et al, 2016).

Nivel 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.

Fig. 6 Níveis de Alerta de ameaça Cibernética. Fonte: Martins et al. (2016)

2.5 – A DEFESA CIBERNÉTICA NAS OPERAÇÕES CONJUNTAS

2.5.1 – Operações Conjuntas

Em épocas passadas as guerras eram simples e permitiam a ação de uma única Força Armada, para que a vitória fosse alcançada. A liderança do Comandante, a superioridade de efetivos e a bravura da tropa eram preponderantes para o sucesso na batalha. No entanto, estudos das últimas guerras e conflitos mostram que as grandes vitórias resultaram das ações integradas das Forças Armadas, Exército, Marinha e Aeronáutica, atuando em conjunto. Nesse contexto, o Manual de Doutrina de Operações Conjuntas do Ministério da Defesa afirma que:

> Os conflitos atuais tendem a ser limitados, não declarados, convencionais ou não, e de duração imprevisível. As ameaças são fluidas, difusas e também imprevisíveis. Tudo isso exige que o preparo das Forças Armadas seja baseado em capacidades, significando isto dispor de forças militares capazes de atuar de forma conjunta, dotadas de flexibilidade, versatilidade e mobilidade. As operações militares de grande envergadura exigem o emprego ponderável de elementos pertencentes a mais de uma Força Armada. Para tal, as Forças Singulares devem somar esforços, compatibilizar procedimentos e integrar as ações, de forma a se obter maior eficiência na execução das Operações Conjuntas (BRASIL, 2011a).

As Operações Conjuntas são coordenadas pelo Ministério da Defesa, através do Estado Maior Conjunto das Forças Armadas (EMCFA), que por sua vez, coordena as atividades dos Comandos Operacionais, sob os quais estão subordinadas as Forças Singulares. Compete ao EMCFA elaborar os Planos Estratégicos de Emprego Conjunto das Forças Armadas (PEECFA). O processo que engloba desde a elaboração até a execução do referido plano segue vários níveis (BRASIL, 2011a):

1. Nível político – São estabelecidos os objetivos políticos e as diretrizes para o planejamento, preparo e emprego Conjunto das Forças Armadas, que são consolidados na Diretriz Presidencial de Emprego e Defesa (DPED). Atividade desenvolvida pelo Presidente da Republica – Comandante Supremo das Forças Armadas.
2. Nível Estratégico – O planejamento estratégico é fundamentado por documentos como o Plano Nacional de Defesa, a Estratégia Nacional de Defesa e leis complementares que tratem da Organização, do preparo e do Emprego das Forças Armadas. Nesse nível, os objetivos e

as diretrizes políticas são transformadas em ações estratégicas, através do Planejamento Estratégico de Emprego Conjunto das Forças Armadas, pelo do Estado Maior Conjunto das Forças Armadas. Neste documento são adotados procedimentos de controle, que permitiram que os Comandos Operacionais ativados acompanhem e avaliem o desenvolvimento das operações e demais ações estratégicas, analisando se a evolução da situação está em conformidade com o Estado Final Desejado.

3. Nível Operacional – Com base no PEECFA e em outras diretrizes, o Comandante Operacional elaborará o Plano Militar de Campanha. Os objetivos operacionais e as atribuições das Forças Componentes serão estabelecidas, levando em conta os principais conceitos estratégicos, objetivos e estado final desejado.
4. Nível Tático – Neste nível, cada Força Componente elabora seu planejamento, tendo como ponto de partida o planejamento do Comando Operacional ativado. O Planejamento Tático pode ocorrer em paralelo ao Planejamento Operacional, visto que, antes destes planejamentos, é expedido o Conceito Preliminar da Operação (CPO), que disponibiliza a situação, a missão, o emprego das forças componentes, a Concepção da Manobra do Comandante, os riscos envolvidos, o estado final desejado e as diversas diretrizes relacionadas com as atividades operacionais.

Planejamento Estratégico Militar tem a finalidade de construir uma capacidade de defesa, com foco na orientação para o preparo e emprego conjunto das Forças Armadas, analisando prováveis interações com as demais expressões do Poder Nacional. Este planejamento é dividido em três etapas (BRASIL, 2011a):

1. Avaliação da Conjuntura e Elaboração de Cenários – precede o planejamento militar e ocorre de forma permanente, com o objetivo de identificar as Hipóteses de Emprego (HE), ou seja, detectar oportunidades, ameaças e vulnerabilidades que necessitem o emprego das Forças Armadas.

2. Exame de Situação e Planejamento – abrange o desenvolvimento do PEECFA através do EMCFA, envolvendo representantes das Forcas Armadas e quando necessário, outros órgãos governamentais. Para cada Hipótese de Emprego será confeccionado um PEECFA, de acordo com seu respectivo Exame de Situação.
3. Controle das Operações Militares – acompanha as operações militares e demais ações estratégicas, verificando a conformidade dos objetivos políticos e estratégicos.

No nível estratégico o planejamento deverá, entre outras características, identificar:

> a) os objetivos políticos e estratégicos; b) os centros de gravidade, do ponto de vista estratégico; c) as condicionantes políticas ao planejamento; d) o Estado Final Desejado; e) a Estrutura Militar a ser estabelecida; f) as áreas de responsabilidade dos Comandos Operacionais a serem ativados; g) os meios que poderão ser adjudicados aos Comandos Operacionais; e h) as principais ações estratégicas decorrentes, incluindo aquelas avaliadas como necessárias por segmentos das demais expressões do Poder Nacional (BRASIL, 2011a).

Os principais Planos que poderão constar no PEECFA são (BRASIL, 2011a):

a) Plano Estratégico de Comando e Controle;
b) Plano Estratégico de Inteligência;
c) Plano Estratégico de Operações de Informação;
d) Plano Estratégico de Assuntos Civis;
e) Plano Estratégico de Logística;
f) Plano Estratégico de Mobilização Militar;
g) Plano Estratégico de Administração Financeira;
h) Plano Estratégico de Deslocamento e Concentração de Forças; e
i) Lista de Necessidades.

Em condições de Normalidade do país, para cada Hipótese de Emprego, O PEECFA, será confeccionado e dinamicamente atualizado. Na situação de crise ou conflito armado, o planejamento estratégico será iniciado pelo Presidente da Republica, com a expedição do DPED, que ativa os Comandos Operacionais necessários e seus respectivos Comandantes, determina os objetivos, as condicionantes políti-

cas e o estado final desejado, dentre outros fatores. Em seguida o Ministério da Defesa elabora a Diretriz Ministerial de Emprego de Defesa (DMED), que contém o detalhamento das diretrizes políticas, orientações para mobilização e desmobilização, observações para a definição dos objetivos estratégicos, orientação para interação com outros órgãos e condicionantes e considerações para o planejamento militar. A partir deste documento cabe ao Estado Maior Conjunto das Forças Armadas atualizar o PEECFA, previamente elaborado em condições ou situação de normalidade. Caso surja uma nova Hipótese de Empego, um novo PEECFA será elaborado. O Estado Maior Conjunto das Forças Armadas emitirá a Diretriz de Planejamento Estratégico Militar (DPEM), que terá como finalidade orientar a elaboração ou a atualização do PEECFA. Este último documento orientará os planejamentos dos Comandos Operacionais e Táticos, respectivamente.

PLANEJAMENTO	
NÍVEIS	DOCUMENTOS
Político (CS)	Diretrizes Políticas (DPED).
Estratégico (MD)	Diretrizes Estratégicas: – Diretrizes Ministeriais (DMED). – Diretrizes do Chefe do Estado-Maior Conjunto das Forças Armadas (DPEM). Planos Estratégicos (PEECFA).
Operacional (Comandos Operacionais ativados)	Diretrizes de Planejamento Operacional. Planos Operacionais.
Tático (F Cte)	Diretrizes de Planejamentos Táticos. Ordens de Operações. Planos Táticos.

Fig. 7 Níveis de Planejamento. Fonte: Brasil (2011a)

Com o objetivo de cumprir as condicionantes políticas e as diretrizes estratégicas, o Comandante Operacional, definirá regras de engajamento, que serão devidamente observadas e detalhadas pelas Forças Singulares ou Componentes. Salientando que atualmente as Operações Militares ocorrem em ambientes de incerteza e caos, com permanente interação humana. Exigindo que as atividades que envolvem assuntos civis sejam cuidadosamente planejadas e executadas, a fim de reduzir atritos entre a população civil e a força militar. Nesse sentido, as Operações de Informação e Assuntos Civis tem sido privilegiadas nos conflitos atuais. Algumas ope-

rações podem ser executas, mesmo antes da elaboração do planejamento operacional e tático, desde que autorizado pelo comando superior, com o segue:

> Algumas ações poderão ser necessárias mesmo antes da ativação de um determinado Comando Operacional, desde que devidamente autorizadas e controladas pelo nível de decisão adequado. Exemplo: Operações Especiais, Operações Psicológicas e de Comunicação Social, Defesa Cibernética e, fundamentalmente, Inteligência. [...] A concentração estratégica das forças militares também pode contribuir para a dissimulação. Para isso, os locais de concentração devem ser estabelecidos de modo a não revelar a direção do esforço principal das operações militares. [...] A fim de iludir as forças oponentes em relação aos planejamentos, são adotadas medidas e ações de dissimulação nos níveis estratégico, operacional e tático. A dissimulação pode ser obtida pelo emprego da guerra eletrônica, camuflagem, desinformação, operações psicológicas, defesa cibernética e ações diversionárias (demonstrações e fintas), entre outras (BRASIL, 2011a).

O Comando Operacional Conjunto é constituído do seu Comandante, o Estado-Maior Conjunto e das Forças Componentes ou Singulares, que são a Força Naval Componente, a Força Terrestre Componente e a Força Aérea Componente. A critério do Comandante, Forças Conjuntas podem ser organizadas como: Comando Logístico, Força Conjunta de Operações Especiais, Força-Tarefa Conjunta, entre outras. As Forças Conjuntas concentram meios das Forças Componentes e de outros órgãos julgados necessários.

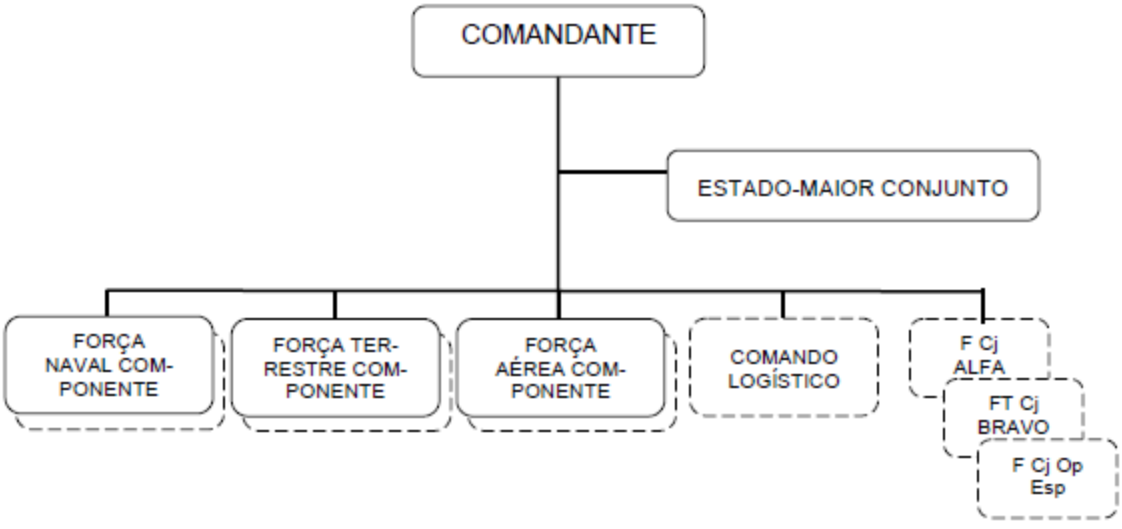

Fig. 8 Estrutura do Comando Operacional. Fonte: Brasil (2011)

O Estado-Maior Conjunto será organizado dependendo das características e demandas da Operação, que a princípio poderá ser constituído pelo Chefe do Estado-Maior e pelas seguintes seções com suas respectivas denominações, sendo que

outras seções podem ser criadas a depender da necessidade da operação (BRASIL, 2011a):

a) D1 – 1ª Seção – Pessoal;
b) D2 – 2ª Seção – Inteligência;
c) D3 – 3ª Seção – Operações;
d) D4 – 4ª Seção – Logística;
e) D5 – 5ª Seção – Planejamento;
f) D6 – 6ª Seção – Comando e Controle;
g) D7 – 7ª Seção – Comunicação Social;
h) D8 – 8ª Seção – Operações Psicológicas;
i) D9 – 9ª Seção – Assuntos Civis; e
j) D10 – 10ª Seção – Administração Financeira.

Entre as competências do chefe da seção de Comando e Controle podemos citar:

> [...] i) coordenar com as seções de Operações e Inteligência as atividades afetas à exploração do espectro eletromagnético e do ambiente cibernético, com vistas à obtenção de informações e à proteção de dados de interesse operacional, colaborando com a elaboração do Plano de Controle de Emissões Eletromagnéticas [...] com vistas à obtenção de informações e à proteção de dados de interesse operacional (BRASIL, 2011a).

A Operação ocorre sem interrupção durante até a sua finalização e em cada jornada de trabalho são realizadas diversas reuniões formais e informais e entre elas podemos citar: Reunião de Coordenação de Comando, Diária de Situação, Fogos, Operações, Operações de Informação, Inteligência, Espaço Aéreo, Aprovação da Ordem de Coordenação e Controle da Operação Planejada (BRASIL, 2011a).

Dos diversos Planos que poderão compor PEECFA, o Plano Estratégico de Operações de Informação consolida aspectos, do ponto de vista estratégico, da Defesa Cibernética, bem como de outras áreas, as quais, podemos citar: a Comunicação Social, a Guerra Eletrônica e as Operações Psicológicas. As Operações de Informação, que resultarão da execução deste plano, compreenderá as diretrizes e informações relacionadas com a sincronização e coordenação das atividades de comunicação destinadas aos sistemas das áreas já citadas, entre outros sistemas (BRASIL, 2011a).

A Análise de Inteligência necessária ao Plano de Inteligência para o Planejamento Operacional além de relatar as características da área em que ocorrerão as Operações, fornecerá todos os dados disponíveis sobre as Forças Inimigas, entre elas: *"Capacidade de utilização de guerra cibernética: 1) Analisar a estrutura de Defesa Cibernética do inimigo no TO; e 2) Descrever a doutrina, técnicas, métodos, organização e administração de Guerra Cibernética do inimigo".* (BRASIL, 2011a).

O Planejamento Operacional apresentará considerações sobre as atividades Cibernéticas, que tenha relação com as atividades de proteção, exploração e ataque cibernéticos. O Plano de Segurança da Área de Retaguarda e seu apêndice, Plano Controle de Danos, anexos ao Plano Operacional, apresentará todas as informações e diretrizes relacionadas às atividades de Comunicação Social, Operações Psicológicas, Guerra Cibernética e Guerra Eletrônica de interesse.

O Plano de Operação de Informação, anexo ao Plano Operacional, conterá o Plano de Defesa Cibernética e citando em seu corpo a Estrutura do Sistema de Defesa Cibernética e a distribuição de especialista e os meios de desdobramentos dos meios e/ou equipes na área de responsabilidade, tendo como missão:

> "Citar o envolvimento da Operação de Informação na missão do Comandante Operacional, descrevendo como devem ser desenvolvidas as ações de Comunicação Social, Operação Psicológica, Guerra Eletrônica e Defesa Cibernética em seu conjunto e sua integração na concepção geral da manobra" (BRASIL, 2011a).

Um representante da Guerra Cibernética deve assessorar o responsável pelo planejamento, acompanhamento e avaliação das Operações de Informações, no apoio referente à Guerra Cibernética e sobre os "feedback" de sua eficácia e é quem confeccionará o Plano de Guerra Cibernética, apêndice ao Plano de Operação de Informações (BRASIL, 2014b).

O Plano de Operações Psicológicas apêndice do Plano de Operações de Informação anexo ao Plano Operacional cita a interoperabilidade do sistema de Operações Psicológicas com os Sistemas de Comunicação Social, Guerra Eletrônica e Defesa Cibernética (BRASIL, 2011a).

2.5.2 – Sistema Miliar de Defesa Cibernética e as Operações Conjuntas

De acordo com a Doutrina Militar de Defesa Cibernética (BRASIL, 2014c), a Defesa Cibernética é um dos componentes da Defesa Nacional, por esse motivo, é

de responsabilidade das Forças Armadas. Entretanto, devido às peculiaridades do espaço cibernético, o cumprimento da missão de proteger as infraestruturas críticas do país, requer a cooperação da sociedade, que entre integrantes da sua constituição, podemos citar: os setores públicos e privados, e mais especificamente, a comunidade acadêmica e a área industrial de defesa. Sendo assim, torna-se de extrema importância a interação, o intercâmbio de informações e o estabelecimento e/ou fortalecimento de parcerias estratégicas entre o Ministério da defesa e os demais atores nacionais e internacionais que estão envolvidos com a Segurança e a Defesa Cibernética. Essa interação deve ser realizada de forma permanente, desde a situação de normalidade institucional, para que em situações de conflitos ou crises, as ações a serem tomadas sejam facilitadas.

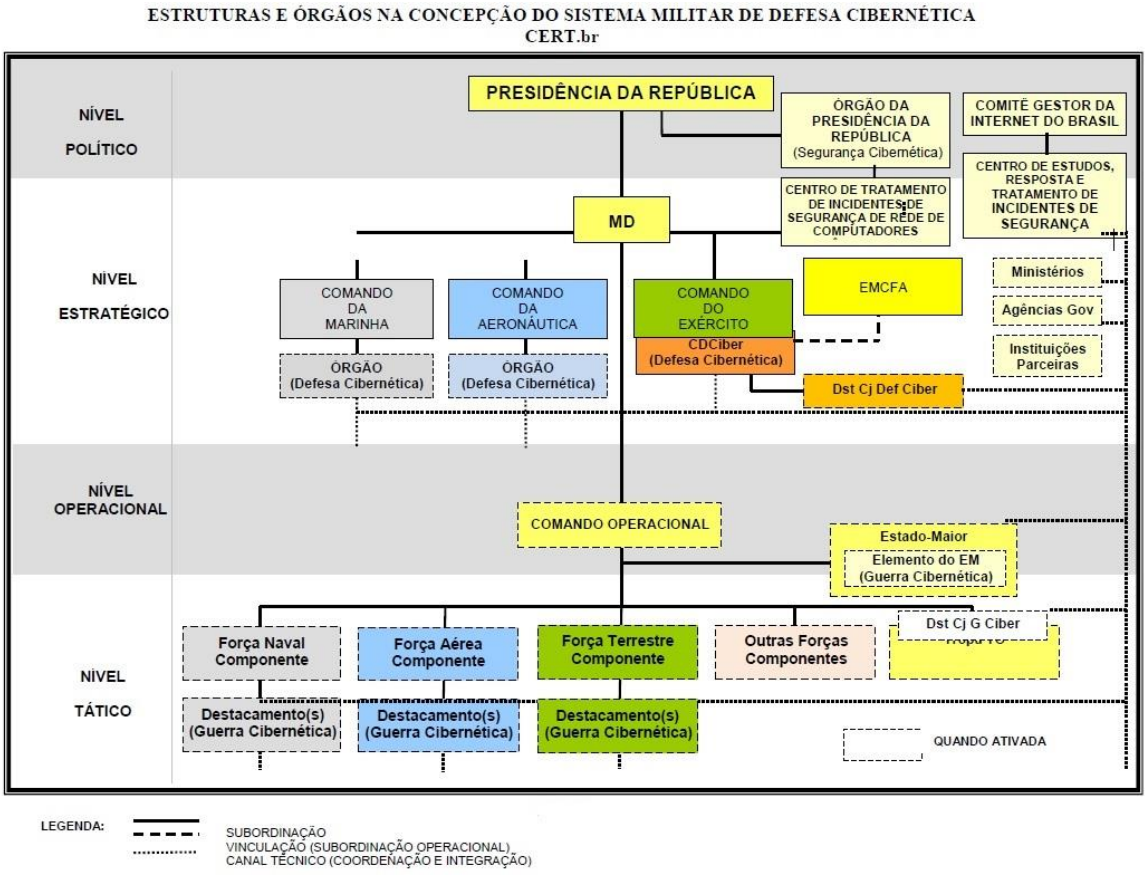

Fig. 9 Estrutura de atuação do Sistema Militar de Defesa Cibernética. Fonte: Brasil (2014c).

O Ministro de Estado de Defesa é o responsável pela implantação e gestão do Sistema Militar de Defesa Cibernética, no qual é assessorado pelo Estado-Maior Conjunto das Forças Armadas, com o objetivo de assegurar os níveis de segurança

desejado, a capacidade de operar em rede e a interoperabilidade dos sistemas, no âmbito da Defesa Nacional.

Nesse contexto, o Sistema Militar de Defesa Cibernética - SMDC pode ser definido como um conjunto de instalações, procedimentos, doutrinas, equipamentos, tecnologias, pessoas e serviços necessários à defesa do Espaço Cibernético. O sistema definido deve ser usado de maneira efetiva, dificultando ou impedindo que seja utilizado em desacordo com os interesses da Defesa Nacional (BRASIL, 2014c).

O Centro de Defesa Cibernética (CDCiber) é o órgão central do Sistema Militar de Defesa Cibernética, que nas Operações Conjuntas passa do controle operacional do Exército para o Ministério da Defesa. O Estado-Maior Conjunto é o responsável permanente por realizar e controlar as ações operacionais do CDCiber, com o objetivo de obter uma maior sinergia, o planejamento leva em consideração as particularidades de cada força singular. No nível estratégico, o CDCiber realiza ações de integração e coordenação dos setores cibernéticos das Forças Armadas, sob a supervisão e orientação do Ministério da Defesa, sempre buscando que as forcas singulares atuem em conjunto. Obtém e difunde informações colhidas das fontes Cibernéticas, para setores de inteligência das Forças Armadas. E por fim, mantem interação técnica para coordenação e integração com outros órgãos públicos e privados que atuam nas atividades de Segurança Cibernética. Nesse cenário a forma de atuação mais provável para o emprego nas Operações Conjuntas é o de Operações em Ambiente Interagências.

Nas Operações Conjuntas a coordenação entre as agencias é quem definirá a estrutura Cibernética a ser preparada para o cumprimento da missão. No nível estratégico será empregado um Destacamento Conjunto de Defesa Cibernética, no nível operacional e tático, um Destacamento de Guerra Cibernética, podendo ainda, haver elementos de Guerra Cibernética que integre as Forças Componentes. O planejamento e a execução da Guerra Cibernética são realizados de acordo com os efeitos desejados pelo Comandante Operacional, ou ainda, por delegação a outros grupos (BRASIL, 2014c).

O Comando Operacional Conjunto é o responsável por planejar e conduzir a Guerra Cibernética, que integra a célula de Operações de Informação, mas a sua célula de integração pode ser decidida pelo Comandante da Operação. A célula de Operações de Informação deve ser guarnecida com pelo menos um oficial especiali-

zado em Guerra Cibernética, preferencialmente, oficial superior com Curso de Estado-Maior ou outro curso equivalente. Entre as principais atribuições dos especialistas de Guerra Cibernética estão:

> 1) assessorar o Chefe da Seção dedicada às Op Info do Estado-Maior Conjunto (EMCj), no que se refere às possíveis ações cibernéticas e respectivos efeitos, em proveito das operações em curso, juntamente com as demais seções do EMCj; 2) sincronizar os efeitos desejados com as demais funções de combate e sistemas operacionais, de modo a maximizar o impacto das ações de Op Info, negando, dificultando ou influenciando o processo decisório do oponente, ou mesmo protegendo o nosso próprio processo decisório. O ponto focal normalmente será a obtenção da Superioridade da Informação (BRASIL, 2104c).

O CDCiber e seus Destacamentos de Defesa e Guerra Cibernética, juntamente com outros órgãos de Segurança e Defesa Cibernética, podem gerar conhecimentos de Fontes Cibernéticas que deverão ser usadas para produção de conhecimentos de Inteligência. Os conhecimentos das Fontes Cibernéticas podem ser utilizados de maneira eminentemente técnica, ou podem ser integrados com os conhecimentos produzidos pelas demais Fontes de Inteligência para confeccionar conhecimentos mais amplos. Essa integração normalmente é realizada por órgãos de Inteligência do Ministério da Defesa e das Forças Singulares. Nas Operações Conjuntas as Fontes Cibernéticas poderão ser integradas as demais fontes (humanas, sinais, imagens e etc) pela estrutura de inteligência, conforme Brasil (2014c).

O planejamento da Defesa e da Guerra Cibernética nas operações deve ter início:

> Por ocasião do Exame de Situação Estratégico e da elaboração do Plano Estratégico de Emprego Conjunto das Forças Armadas, com seu respectivo Plano Estratégico de Operações de Informação. Os militares especializados, designados para mobiliar a Seção dedicada às Operações de Informação, deverão participar do Processo de Planejamento para Operações Conjuntas, realizando a Análise de Guerra Cibernética. Além disso, devem elaborar o Apêndice de Guerra Cibernética ao Anexo de Operações de Informação ao Plano Operacional e cooperar com os assuntos de Guerra Cibernética que deverão constar do supracitado Anexo de Operações de Informação e de outros documentos integrantes do planejamento conjunto (BRASIL, 2014c).

2.5.3 Funções de Combate e a Guerra Cibernética

As Ações Cibernéticas são o emprego de recursos do espaço cibernético e tem como objetivo: proteger os próprios ativos de informação; explorar e atacar as redes do oponente e os ativos de informações do inimigo; como também interferir

nas condições de normalidade de uma região, buscando atingir o funcionamento dos serviços essenciais e estruturas estratégicas destinadas à população (BRASIL, 2014d). Englobam a Proteção Cibernética, o Ataque Cibernético e a Exploração Cibernética, para fins de produção de conhecimento de Inteligência, como descritas a seguir (BRASIL, 2011a):

a) **Exploração Cibernética** – são ações que buscam identificar vulnerabilidades nos Sistemas de Tecnologia de Informação do inimigo, bem como, obter dados, para a produção de conhecimento, de maneira não autorizada.
b) **Ataque Cibernético** – consiste em ações para negar, interromper, corromper, degradar ou destruir informações armazenadas em dispositivos, da mesma forma com as redes computacionais e de comunicações do inimigo.
c) **Proteção Cibernética** – compreende ações para neutralizar a exploração e ataques cibernéticos contra os próprios dispositivos computacionais, assim como, as nas redes de computadores e de comunicações.

A Guerra Cibernética exige uma estreita coordenação para evitar problemas indesejáveis nos sistemas das forças amigas e para negar, explorar, obter, corromper, dissimular ou degradar os sistemas de informação e/ou informações do inimigo, a fim de afetar o seu ciclo decisório, de acordo com Brasil (2014d). Em um nível Operacional, Tático ou de uma operação militar.

A Força Terrestre expressa à essência da sua capacidade de emprego em situações de Guerra e não Guerra através dos Elementos do Poder de Combate Terrestre que são: Liderança, Informações e as Funções de Combate - Movimento e Manobra, Fogos, Inteligência, Proteção, Comando e Controle e Logística. Na Força Terrestre a Guerra Cibernética é um dos Elementos de Apoio ao Combate, juntamente com a Artilharia de Campanha e Antiaérea, Comunicações, Engenharia, Guerra Eletrônica, Inteligência, DQBRN e Operações de Apoio a Informações. (BRASIL, 2014a).

Fig. 10 Poder de Combate. Fonte: Brasil (2014a)

O Comando e Controle reúne um conjunto de atividades, tarefas e sistemas inter-relacionados que garantem aos Comandantes o exercício do comando ou da autoridade, como também, a direção e o controle das ações. Combina a arte do comando com a ciência do controle. As atividades de Comando e Controle integram todas as demais Funções de Combate, conforme Brasil (2014a). A condução da gestão do Espaço Cibernético é uma das atividades da Função de Combate Comando e Controle, que tem como tarefa planejar, conduzir e coordenar ações, como a exploração, a defesa e o ataque no espaço cibernético (BRASIL, 2015a).

A Função de Combate Proteção (BRASIL, 2015f) agrega um conjunto de atividades para proteger e preservar a Força Terrestre, assim como, as populações e as infraestruturas civis. As suas tarefas permitem prevenir, identificar e mitigar ameaças à força, aos seus meios operacionais e aos civis. Requer uma sincronização com as atividades da Função de Combate Logística, para que seus meios possam estar sempre protegidos, dentre outras, das ameaças Cibernéticas. A Guerra Cibernética como sendo uma atividade da Função de Combate Proteção, atuará protegendo e garantindo o uso eficiente da rede de informação, suas tarefas devem ser coordenadas juntamente com a equipe de Comando e Controle. A ContraInteligência é uma atividade de proteção, que tem como objetivo obstruir e neutralizar a ação da Inteligência alheia e de qualquer outra ação que se constitua uma ameaça aos dados, informações, conhecimentos e seus suportes. As atividades de Guerra Ciber-

nética podem contribuir com informações, complementando os esforços da ContraInteligência.

A Função de Combate Fogos reúne um conjunto de atividades, tarefas e sistemas integrados que permitem o controle e aplicação de fogos. Além da utilização da artilharia tradicional e de outras armas capazes de lançar artefatos cinéticos, como foguetes, misseis e granadas, existe outras formas de ataques que não lançam artefatos cinéticos, os chamados, atuadores não cinéticos, mas que podem causar danos tanto na estrutura física, quanto na tropa oponente. Como exemplo desses atuadores não cinéticos, podemos citar: a Guerra Eletrônica, a Guerra Cibernética e as Operações de Apoio as Informações, de acordo com Brasil (2015b).

A Inteligência é uma Função de Combate (BRASIL, 2015c) que compreende um conjunto de atividades, tarefas e sistemas integrados que busca coletar informações que permitam compreender o ambiente operacional, os inimigos, o terreno, as ameaças e as considerações civis. Permitindo o Planejamento e a condução das operações. A Inteligência tem como uma das suas disciplinas, a Inteligência Cibernética, que por sua vez, elabora uma Inteligência a partir de dados obtidos no espaço cibernético, protegidos ou não.

2.6 DISCUSSÕES E RESULTADOS

A Defesa Cibernética integra o Setor Cibernético Nacional, sendo assim, mesmo nas Operações Conjuntas, a atuação Cibernética seguirá o modelo de emprego de operações em ambiente interagências (BRASIL, 2014c). Para as Operações Interagências que necessitem de coordenação no nível estratégico, o CDCiber poderá formar um Destacamento Conjunto de Defesa Cibernética, que possui estrutura análoga ao Destacamento Conjunto de Guerra Cibernética. Já para um Comando Operacional poderá ser alocado um Destacamento Conjunto de Guerra Cibernética, que passará a integrar as suas tropas. A estrutura e o efetivo que será necessário para compor o Destacamento Conjunto de Guerra Cibernética serão definidos por seu comandante, que fará um estudo detalhado da situação, buscando a separação entre planejamento e a execução das ações que visam à proteção dos ativos de informação, das de exploração e ataques cibernéticos. Levando em consideração as necessidades especificas de cada operação. Em Operações Singulares, os Des-

tacamentos de Guerra Cibernética podem ser análogos às das Operações Conjuntas, que poderá ficar subordinado a este, se na Operação, for um escalão superior. O Destacamento Conjunto de Guerra Cibernética quando ativado, poderá ser organizado genericamente da seguinte forma, de acordo com Brasil (2014c):

1. comandante e subcomandante;
2. elementos especializados em Guerra Cibernética das Forças Armadas;
3. elementos de ligação interagências; e
4. elementos civis especializados, para assessoria e operação assistida.

São possibilidades de atuação do Destacamento Conjunto de Guerra Cibernética (BRASIL, 2014c):

1. identificar e analisar vulnerabilidades nas redes de computadores da Operação Conjunta e nos Sistemas de Comando e Controle;
2. apoiar na mitigação das vulnerabilidades identificadas;
3. estudar as ameaças e analisar seus impactos nas infraestruturas da informação das forças amigas e nas redes de Comando e Controle;
4. verificar, no Sistema de Comando e Controle desdobrado para a operação, a conformidade de Segurança da Informação e Comunicações;
5. planejar e executar ações cibernéticas de proteção, exploração e ataque na Operação Conjunta;
6. assessorar os comandantes das Forças Componentes;
7. colaborar com a execução das Operações de Informação ; e
8. explorar o espaço cibernético para obtenção de dados para a produção de conhecimento de Inteligência.

A Guerra Cibernética exige uma estreita coordenação para evitar problemas indesejáveis nos sistemas das forças amigas e para negar, explorar, obter, corromper, dissimular ou degradar a infraestrutura de informação do inimigo, a fim de desestabilizar o seu ciclo decisório, conforme o manual de Operações de Informação Brasil (2014d). Na tabela abaixo, observa-se que a Guerra Cibernética está inserida diretamente na maioria das Funções de Combate e indiretamente em outras funções, como a Logística que não é listada no quadro, mas que deve ter seus meios

de Tecnologia da Informação e Comunicações protegidos contra a ação do inimigo, o mesmo ocorrendo com a Função de Combate Movimento e Manobra. Mostrando, assim, a importância dessa área, para os conflitos atuais e futuros.

Funções de Combate	Atribuições
Comando e Controle	Conduzir a gestão do Espaço Cibernético, que é uma atividade, que tem como tarefa planejar, conduzir e coordenar ações, como a exploração, a defesa e o ataque no espaço cibernético (BRASIL, 2015a).
Proteção	Atuar protegendo e garantindo o uso eficiente da rede de informação, suas tarefas devem ser coordenadas juntamente com a equipe de Comando e Controle (BRASIL, 2015f).
Fogos	Atacar o inimigo, essa ação Cibernética é classificada como sendo de atuadores não cinéticos, podendo causar sérios danos no inimigo, sem atuação de impactos físicos diretos (BRASIL, 2015b).
Inteligência	Elaborar uma Inteligência a partir de dados obtidos no espaço cibernético, protegidos ou não (BRASIL, 2015c).

Fig. 11 Atribuições das Funções de Combate. Fonte: o autor

As atividades Cibernéticas envolvem os principais elementos responsáveis pela condução das Operações Conjuntas, tais atividades necessitam da integração de quase todos os membros do Estado-Maior Conjunto, após a análise do Manual de Doutrina das Operações Conjuntas (BRASIL, 2012a), e o Manual de Doutrina Cibernética, (BRASIL, 2014c), entre outros documentos, pode-se inferir, as seguintes atribuições:

Militar Responsável	Atribuições
Comandante	Aprovar o Plano de Defesa ou Guerra Cibernética e decidir sobre os acontecimentos que ocorrerem fora do planejamento.
D2/E2 - Chefe da Seção de Inteligência.	Participar do planejamento e coordenação das atividades de inteligência, relativas à exploração do ciberespaço, com o objetivo de obter informações sobre o inimigo ou de alvos específicos.
D3/E3 – Chefe da Seção de Operações	Participar do planejamento e coordenação das atividades Cibernéticas de proteção e ataque, como o objetivo de proteger as instalações amigas e atacar as inimigas.
D5/E5 - Chefe da Seção de Planejamento	Participar do Planejamento e sincronização das atividades Cibernéticas com outras atividades operacionais.
D6/E6 - Chefe da Seção de Comando e Controle	Participar do planejamento e Coordenação das atividades afetas à exploração do ambiente cibernético, com vistas à obtenção de informações e à proteção de dados de interesse operacional e ataque ao inimigo.
D7/E7 Chefe da Seção Comunicação Social	Solicitar apoio Cibernético na busca de informações que ajude no desenvolvimento de suas atividades.

D9/E9 Chefe da Seção Assunto Civis	Solicitar apoio Cibernético na busca de informações que ajude no desenvolvimento de suas atividades.
Oficial de Guerra Cibernética	Assessorar o Chefe da Seção dedicada às Operações de Informação e sincronizar os efeitos desejados com as demais funções de combate e sistemas operacionais, de modo a maximizar o impacto das ações de Operações de Informação, negando, dificultando ou influenciando o processo decisório do oponente, ou mesmo protegendo o nosso próprio processo decisório.
Oficial de Segurança da Informação	Zelar pela Segurança da Informação na Operação Conjunta, garantindo que a infraestrutura de informação sobre sua responsabilidade esteja em conformidade com diretrizes de Segurança.
Demais Militares	Seguir as diretrizes de Segurança da Informação elaboradas pelo Oficial de Segurança da Informação.

Fig. 12 Atribuições dos Militares. Fonte: o autor.

As atividades Cibernéticas podem atuar cooperando com quase todas as seções do Estado-Maior Conjunto, apoiando na área de proteção, exploração e ataque, pode respectivamente, atuar:

1. protegendo os ativos de Comando e Controle da Operação e outros ativos críticos de Tecnologia da Informação e Comunicações, julgados necessários;
2. atuar na exploração da rede de Tecnologia da Informação e Comunicações dos oponentes fornecendo informações de inteligência, como também coletar informações relevantes para outras seções do Estado-Maior;
3. pode ainda, realizar atividade de ataque, buscando neutralizar, corromper ou destruir os meios de Comando e Controle do oponente, ou de outros ativos críticos de Tecnologia da Informação e Comunicações, julgados necessários.

A preocupação militar de proteger as infraestruturas críticas militares e civis de ataques alheios, mesmo em tempo de paz, demostra a existência de uma guerra virtual constante, não declarada e de inimigo, na maioria dos casos, desconhecido. Nesse contexto, estragos promovidos por ataques cibernéticos bem sucedidos, podem direcionar esforços das nações para a Guerra Cibernética, tornando-a a principal frente de batalha a ser vencida. Pois, uma guerra poderá ser vencida, sem mesmo ter sido declarada, o seu começo.

O Sistema Militar de Defesa Cibernética do Brasil pode ser definido como um conjunto de instalações, procedimentos, doutrinas, equipamentos, tecnologias, pessoas e serviços necessários à defesa do Espaço Cibernético (BRASIL, 2014c). Na questão da Doutrina nas Operações Conjuntas, o Plano da Defesa ou Guerra Cibernética é anexado ao Plano de Operações da Informação, nos níveis estratégicos, operacionais e táticos (BRASIL, 2012a). Diante do exposto, e da importância da Cibernética para os conflitos atuais e futuros, como citado no paragrafo anterior, verifica-se a necessidade do Plano de Cibernética deixar de ser um plano anexo aos Planos de Operações de Informação e torna-se um anexo direto do PEECFA, do Plano Operacional e do Tático, para que os principais integrantes das Operações compreendam a importância e as suas reponsabilidades com a Defesa ou Guerra Cibernética e que o Oficial de Cibernética faça parte do Estado-Maior Conjunto.

3 CONCLUSÃO

A atividade Cibernética atua em diversas áreas dentro de uma Operação Conjunta. Na proteção da infraestrutura de informações militares, defendendo as suas instituições e nos locais de conflito, principalmente, os grupamentos Logísticos e as estruturas de Comando e Controle. Assim como, tem a função de contribuir na proteção das organizações civis críticas para a manutenção da soberania do Estado e o bem-estar da sociedade, como as redes energia elétrica, comunicações, transportes, sistema financeiro, entre outros.

A Cibernética pode fornecer informações importantes para a Inteligência e ContraInteligência, através da identificação de vulnerabilidades do inimigo e das próprias instalações e organizações nacionais, respectivamente. A Cibernética também pode ser utilizada como força de ataque contra o inimigo, ao lado de outros meios de aplicação de fogos cinéticos e não cinéticos, entre os principais alvos, podemos citar: as infraestruturas de informação militares e civis, sistemas de Comando e Controle e Centros de Comunicação.

A Guerra Cibernética impõe regras para Segurança da Informação que envolve todos os indivíduos que de maneira direta ou indireta integram a Operação Conjunta. No contexto nacional, é função da Defesa Cibernética interagir com Órgãos da Segurança da Informação Pública e Privada, com o objetivo de conscientizar a soci-

edade, principalmente instituições críticas para a Segurança Nacional da Informação, as quais, há necessidade em proteger.

As ações Cibernéticas ganharam destaque nos últimos anos, devido a ataques bem sucedidos em alguns países, mostrando o potencial, de vencer sem utilizar o combate tradicional. A militarização da proteção e do ataque Cibernético pode elevar o desenvolvimento dessa área, estimulando a criação de armas tecnológicas de caráter nacional, tornando alguns países temidos por outros, em termos de Guerra Cibernética.

O General Americano Gordon Sullivan, afirmou: “a Guerra Cibernética será a forma básica de uma guerra futura”. Analisando essa afirmação publicada em 1999, observa-se, que já existe uma preocupação militar de proteger as infraestruturas críticas de informação, militares e civis de ataques alheios. Mesmo em tempo de paz, as nações podem está enfrentado uma guerra virtual não declarada e de inimigo desconhecido, podendo direcionar seus esforços para a Guerra Cibernética, tornando-a a principal frente de batalha a ser vencida. Pois, uma guerra poderá ser vencida, sem mesmo ser declarada o seu começo.

A criação do Centro de Defesa Cibernética, da Escola Nacional de Defesa Cibernética e do Comando de Defesa Cibernética são de suma importância para a defesa do país de ameaças externas e para preparar indivíduos capazes de atuar na proteção de ativos informacionais de interesse particular ou de organizações a que prestam serviço. Mesmo em Operações Conjuntas, a da Defesa Cibernética atua, também, em um ambiente de operações interagência. Todo esse esforço de integração mostra que os atuais e futuros inimigos podem atuar de forma invisível, isolada e imprevisível, mudando totalmente o paradigma da guerra atual em relação à guerra tradicional.

Nesse contexto, verifica-se a necessidade de ampliar a importância da Guerra Cibernética nas Operações Conjuntas, integrando o Oficial de Guerra Cibernética ao Estado-Maior Conjunto e transferindo o Plano de Defesa e Guerra Cibernética para ser um anexo do PEECFA, do Plano Operacional e do Plano Tático.

REFERÊNCIAS

BRASIL. Exército. **EB20-MC-10.205: Comando e Controle.** 1. ed. Brasília, DF, 2015a.

_____. _____. **EB20-MF-10.102: Doutrina Militar Terrestre.** 1. ed. Brasília, DF, 2014a.

_____. _____. **EB20-MC-10.206: Fogos**. 1. ed. Brasília, DF, 2015b.

_____. _____. **EB20-MC-10.207: Inteligência.** 1. ed. Brasília, DF, 2015c.

_____. _____. **EB20-MF-10.107: Inteligência Militar Terrestre.** 2. ed. Brasília, DF, 2015d.

_____. _____. **EB20-MC-10.206: Logística.** 3. ed. Brasília, DF, 2014b.

_____. _____. **EB20-MC-10.203: Movimento e Manobra**. 1. ed. Brasília, DF, 2015e.

_____. _____. **EB20-MC-10.208: Proteção.** 1. ed. Brasília, DF, 2015f.

_____. Gabinete de Segurança Institucional. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal**. 1. ed. Brasília, DF, 2015g.

_____. Ministério da Defesa. **MD30-M-01: Doutrina de Operações Conjuntas**. 1. ed. Brasília, DF, 2011a. 3 v.

_____. _____. **MD31-M-07: Doutrina Militar de Defesa Cibernética.** 1. ed. Brasília, DF, 2014c.

_____. _____. **Estratégia Nacional de Defesa**. Brasília, DF, 2012b.

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

_____. _____. **Livro Verde de Segurança Cibernética no Brasil**. Brasília, DF, 2010.

_____. _____. **MD31-P-02: Política Cibernética de Defesa**. 1. ed. Brasília, DF, 2012d.

_____. _____. **Política Nacional de Defesa**. Brasília, DF, 2012e.

_____._____. **Operações de Informação**. Brasília, DF, 2014c.

_____. Secretaria de Assuntos Estratégicos. **Desafios Estratégicos para a Segurança e Defesa Cibernética.** 1 ed. Brasília, DF, 2011b.

GIBSON, Willian. **Neuromancer.** 1984. Disponível em: http://www.libertarianismo.org/livros/wgneuromancer.pdf. Acessado em: 28/07/2016.

HUERTAS. José Antônio Espinosa. **Guerra Cibernética:** Um problema estratégico com envolvimento das forças Armadas. Rio de Janeiro, 2012. Disponível em: http://www.esg.br/images/Monografias/2012/ESPINOSAHUERTAS.pdf Acesso em: 03/07/2016.

JÚNIOR, Samuel César da Cruz. **Segurança e Defesa Cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Brasília: IPEA, 2013. Disponível em: <http://www.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1850.pdf>

LIANG, Qiao & XIANGSUI, Wang. **A Guerra além dos limites:** conjecturas sobre a guerra e a tática na era da globalização. Beijing: Pla Literarute and Arts Publisnhing House. 1999. Disponível em: https://www.egn.mar.mil.br/arquivos/cepe/GUERRAALEMLIMITES.pdf Acessado em: 08/08/2016.

MARTINS, Paula et al. **Da Cibersegurança à Ciberguerra:** O desenvolvimento de políticas de Vigilância no Brasil. São Paulo: artigo 19, 2016. Disponível em: http://artigo19.org/blog/2016/03/10/novo-estudo-da-artigo-19-analisa-o-aparato-de-vigilancia-do-estado-brasileiro/ Acesso em: 01/08/2016.

PINHEIRO, Fábio Ponte. **A Cibernética como arma de combate**. Rio de Janeiro, 2013. Disponível em: http://www.esg.br/images/Monografias/2013/PINHEIRO.pdf Acesso em: 03/07/2016.

RYAN, Jason. CIA Director Leon Panetta warns of possible cyber-Pearl Harbor. 2011. Disponível em: http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905. Acesso em: 08/08/2016.

RUIVO, Mariana Maia. **A Guerra Moderna e suas transformações:** da 1º geração à guerra cibernética e o impacto na segurança internacional. 2014. Disponível em: http://www.sistemas.fflch.usp.br/ocspkp/sdpscp/IVsem/paper/download/142/96 Acessado em: 08/08/2016.

RÚSSIA. Ministério da Defesa. **Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no espaço de informação**. Moscou, 2011. (Tradução do autor). Disponível em: <http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>. Acesso em: 05/08/2016.

SILVA. Júlio Barreto Leite da. **Guerra Cibernética**: A guerra no quinto domínio, conceituação e princípios. Disponível em: https://www.egn.mar.mil.br/ojs/index.php/revistadaegn/article/view/40 Acesso em: 03/07/2016.

WIENER, Nobert. **Cibernética e Sociedade:** O uso Humano de seres Humanos. 2 ed. São Paulo: Cultrix, 1954.

UNITED STATES. The White House. **International strategy for cyberspace**: prosperity, security, and openness in a networked world. Washington, 2011. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acessado em 05/08/2016.