MINISTÉRIO DA DEFESA

MD31-M-07

DOUTRINA MILITAR
DE
DEFESA CIBERNÉTICA

2014

MINISTÉRIO DA DEFESA
ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS

DOUTRINA MILITAR
DE
DEFESA CIBERNÉTICA

1ª Edição
2014

MINISTÉRIO DA DEFESA
GABINETE DO MINISTRO

PORTARIA NORMATIVA Nº 3.010/MD, DE 18 DE NOVEMBRO DE 2014.

Aprova a Doutrina Militar de Defesa Cibernética.

O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe confere o inciso II do parágrafo único do art. 87 da Constituição Federal, combinado com a alínea "c", do inciso VII, do art. 27, da Lei nº 10.683, de 28 de maio de 2003, e em conformidade ao disposto no art. 1º, inciso III, do Anexo I ao Decreto nº 7.974, de 1º de abril de 2013, resolve:

Art. 1º Aprovar a publicação "Doutrina Militar de Defesa Cibernética - MD31-M-07 (1ª Edição/2014)", na forma do Anexo a esta Portaria Normativa.

Parágrafo único. O Anexo de que trata o **caput** deste artigo estará disponível na Assessoria de Doutrina e Legislação do Estado-Maior Conjunto das Forças Armadas.

Art. 2º Esta Portaria Normativa entra em vigor na data de sua publicação.

CELSO AMORIM

(Publicado no D.O.U. nº 224 de 19 de novembro de 2014.)

INTENCIONALMENTE EM BRANCO

REGISTRO DE MODIFICAÇÕES

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA	RUBRICA DO RESPONSÁVEL

INTENCIONALMENTE EM BRANCO

SUMÁRIO

INTENCIONALMENTE EM BRANCO

LISTA DE DISTRIBUIÇÃO

INTERNA	
ÓRGÃOS	**EXEMPLARES**
GABINETE DO MINISTRO DE ESTADO DA DEFESA	1
GABINETE ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS	1
CHEFIA DE OPERAÇÕES CONJUNTAS	1
CHEFIA DE ASSUNTOS ESTRATÉGICOS	1
CHEFIA DE LOGÍSTICA	1
ASSESSORIA DE DOUTRINA E LEGISLAÇÃO - **Exemplar Mestre**	1
SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL	1
SECRETARIA DE PESSOAL, ENSINO, SAÚDE E DESPORTO	1
SECRETARIA DE PRODUTOS DE DEFESA	1
CENTRO GESTOR E OPERACIONAL DOS SISTEMAS DE PROTEÇÃO DA AMAZÔNIA	1
PROTOCOLO GERAL	1
ESCOLA SUPERIOR DE GUERRA	1
HOSPITAL DAS FORÇAS ARMADAS	1
SUBTOTAL	**13**

EXTERNA	
ÓRGÃOS	**EXEMPLARES**
COMANDO DA MARINHA	1
COMANDO DO EXÉRCITO	1
COMANDO DA AERONÁUTICA	1
ESTADO-MAIOR DA ARMADA	1
ESTADO-MAIOR DO EXÉRCITO	1
ESTADO-MAIOR DA AERONÁUTICA	1
COMANDO DE OPERAÇÕES NAVAIS	1
COMANDO DE OPERAÇÕES TERRESTRES	1
COMANDO-GERAL DE OPERAÇÕES AÉREAS	1
SUBTOTAL	**9**
TOTAL	**22**

INTENCIONALMENTE EM BRANCO

CAPÍTULO I

INTRODUÇÃO

1.1 Finalidade

Estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionando unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético.

1.2 Considerações Preliminares

1.2.1 O Brasil, como nação soberana, necessita possuir capacidade para se contrapor às ameaças externas, de modo compatível com sua própria dimensão e suas aspirações político-estratégicas no cenário internacional. Isso possibilita ao país a consecução de objetivos estratégicos e a preservação dos interesses nacionais, além do exercício do direito de defesa assegurado pela Constituição Federal e pelo ordenamento jurídico internacional.

1.2.2 Na atual conjuntura mundial, caracterizada por incerteza, mutabilidade e volatilidade das ameaças potenciais, bem como pela presença de novos atores não estatais nos possíveis cenários de conflito, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de forma a capacitá-la a responder oportuna e adequadamente, antecipando os possíveis cenários adversos à Defesa Nacional.

1.2.3 Agravando ainda esse quadro, observa-se o aumento do risco de perpetração de ataques por Estados, organizações e até mesmo pequenos grupos, com as mais diversas motivações.

1.2.4 Dentro desse cenário, a Defesa Cibernética vem se estabelecendo como atividade fundamental ao êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do Comando e Controle (C^2), por meio da proteção dos ativos de informação, ao mesmo tempo permitindo que esse exercício seja negado ao oponente. Na condição de atividade especializada, sua execução se baseia em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares.

1.3 Histórico

1.3.1 No contexto nacional, particularmente na área governamental, o tema foi tratado, inicialmente, com o desenvolvimento da Segurança da Informação, o que se caracterizou com a criação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001, que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998. Ao novo órgão, dentre outras competências, coube à coordenação das atividades de Segurança da Informação.

1.3.2 Pelo Decreto nº 5.772, de 8 de maio de 2006, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no GSI/PR, com a missão de planejar e coordenar a execução das atividades de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal (APF).

1.3.3 Em dezembro de 2008, a Estratégia Nacional de Defesa (END) estabeleceu prioridade em três setores estratégicos para a Defesa Nacional: Nuclear, Cibernético e Espacial.

1.3.4 A Diretriz Ministerial nº 0014, de 2009 do Ministério da Defesa, de 9 de novembro de 2009, definiu providências para o cumprimento da END nos setores estratégicos da defesa, estabelecendo as responsabilidades para cada Força Armada. Ao Exército, coube a responsabilidade pela coordenação e pela integração do Setor Cibernético.

1.3.5 Na mesma diretriz, foi estabelecido que, para cada setor, numa primeira fase, seriam definidos a abrangência do tema e os objetivos setoriais. Numa segunda fase, os objetivos setoriais seriam detalhados em ações estratégicas e a adequabilidade das estruturas existentes seria estudada, propondo-se alternativas e soluções.

1.3.6 Em cumprimento à diretriz citada no item 1.3.4., foi ativado, em 2 de agosto de 2010, o Núcleo do Centro de Defesa Cibernética.

1.3.7 O Decreto nº 7.411, de 29 de dezembro de 2010, explicitou nas atribuições do DSIC - GSI/PR a sua competência de planejar e coordenar a execução das atividades de Segurança Cibernética e de Segurança da Informação e Comunicações na Administração Pública Federal.

1.3.8 Em 20 de setembro de 2012, o Decreto Presidencial nº 7.809, entre outras medidas, incluiu, na Estrutura Regimental do Comando do Exército, o Centro de Defesa Cibernética.

1.3.9 Posteriormente, o Ministério da Defesa, por intermédio da Portaria nº 3.405/MD, de 21 de dezembro de 2012, atribuiu ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e pela integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, consoante o disposto no Decreto nº 6.703, de 2008 (END).

1.3.10 Concomitantemente, a Portaria Normativa nº 3.389, do Ministério da Defesa, de 21 de dezembro de 2012, aprovou a Política Cibernética de Defesa. Entre seus objetivos estão os de desenvolver e de manter atualizada a doutrina de emprego do Setor Cibernético, cujos fundamentos estão consubstanciados nesta publicação.

1.3.11 Finalmente o Decreto Legislativo nº 373, de 12 de setembro de 2013, atualizou a Estratégia Nacional de Defesa e aprovou o Livro Branco de Defesa Nacional. Dentre as premissas sobre o setor cibernético, cita que a proteção do espaço cibernético abrange um grande número de áreas, como: capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional; e gestão de pessoal.

1.4 Referências

Os documentos consultados e que fundamentaram a elaboração desta publicação foram:

a) Constituição da República Federativa do Brasil, de 1988;

b) Lei Complementar (LC) nº 97, de 9 de junho de 1999, alterada pelas LC nº 117, de 2 de setembro de 2004, e nº 136, de 25 de agosto de 2010 (dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas);

c) Lei nº 12.965, de 23 de abril de 2014 (estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil);

d) Decreto Legislativo nº 373, 25 de setembro de 2013 (aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa);

e) Decreto nº 7.276, de 25 de agosto de 2010 (aprova a Estrutura Militar de Defesa e dá outras providências);

f) Decreto nº 7.411, de 29 de dezembro de 2010 (define as competências do DSIC – GSI/PR, dentre outras);

g) Decreto nº 7.809, de 20 de setembro de 2012 (altera a estrutura regimental da Marinha, do Exército e da Aeronáutica);

h) Portaria nº 400/SPEAI/MD, de 21 de setembro de 2005 (aprova a Política Militar de Defesa - MD51-P-02);

i) Portaria Normativa nº 578/SPEAI/MD, de 27 de dezembro de 2006 (aprova a Estratégia Militar de Defesa - MD51-M-03);

j) Portaria Normativa nº 113/DPE/SPEAI/MD, de 1º de fevereiro de 2007 (aprova a Doutrina Militar de Defesa - MD51-M-04);

k) Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007 (aprova o Glossário das Forças Armadas - MD35-G-01, 4ª Edição);

l) Portaria Normativa nº 513/EMD/MD, de 26 de março de 2008 (aprova o Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas - MD33-M-02, 3ª Edição/2008);

m) Portaria Normativa nº 3810/MD, de 8 de dezembro de 2011(aprova a Doutrina de Operações Conjuntas - MD30-M-01, Volumes 1, 2, e 3 - 1ª Edição/2011);

n) Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012 (aprova a Política Cibernética de Defesa - MD31-P-02 - 1ª Edição/2012);

o) Portaria nº 3.405/MD, de 21 de dezembro de 2012, (atribui ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, consoante o disposto no Decreto nº 6.703/08);

p) Portaria Normativa nº 229/MD, de 28 de janeiro de 2013 (aprova a publicação Operações Interagências - MD33-M-12, 1ª Edição/2012);

q) Diretriz Ministerial nº 14/2009 do Ministério da Defesa, de 9 de novembro de 2009 (dispõe sobre integração e coordenação dos setores estratégicos da Defesa);

r) Instrução Normativa nº 1/GSI/PR, de 13 de junho de 2008 (disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências) e suas Normas Complementares; e

s) Instrução Normativa nº 001/EMCFA/MD, de 25 de julho de 2011 (aprova as Instruções para Confecção de Publicações Padronizadas do Estado-Maior Conjunto das Forças Armadas – EMCFA - MD20-I-01, 1ª Edição/2011).

INTENCIONALMENTE EM BRANCO

CAPÍTULO II

FUNDAMENTOS

2.1 Generalidades

2.1.1 A partir do estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa, em 2008, dois campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR), e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas.

2.1.2 No contexto do Ministério da Defesa, as ações no Espaço Cibernético deverão ter as seguintes denominações, de acordo com o nível de decisão (conforme apresentado na figura 1):

nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;

nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e

níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas.

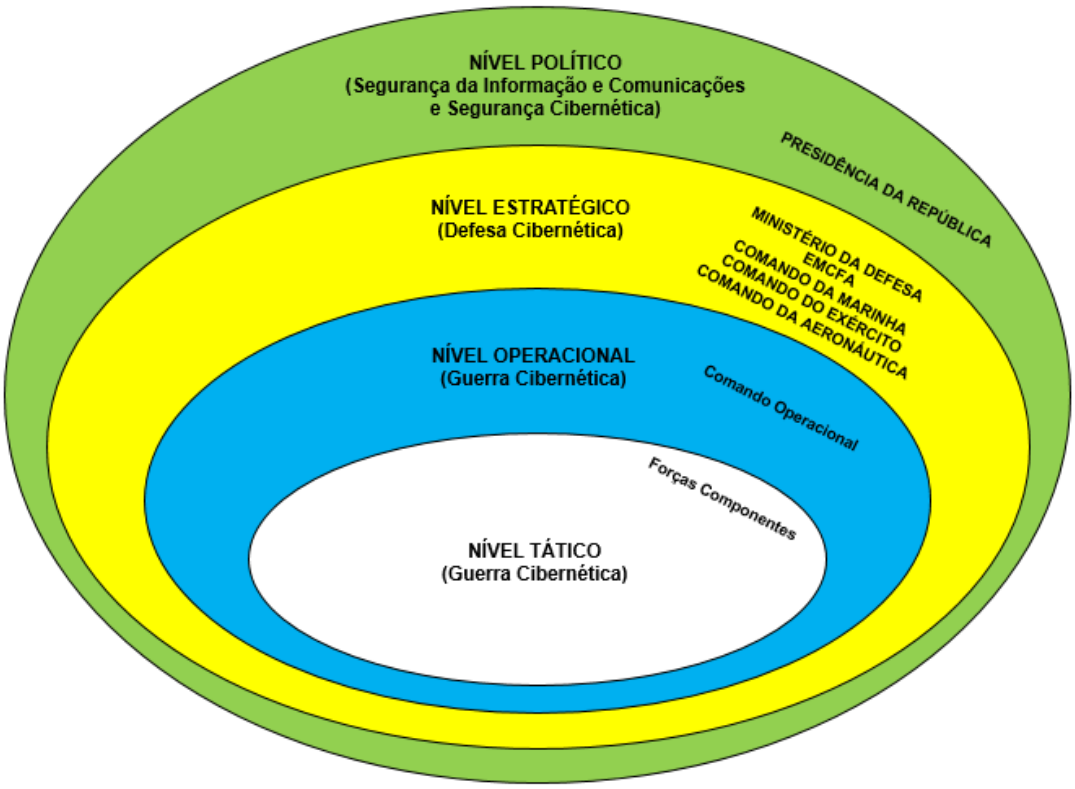


Figura 1: Níveis de decisão

2.1.3 Em conformidade com o exposto no item 2.1.2, será utilizada a denominação Defesa Cibernética quando do planejamento e da execução de ações cibernéticas afetas ao nível estratégico de decisão. Da mesma forma, será utilizada a denominação Guerra Cibernética quando o nível de decisão considerado for o operacional ou o tático.

2.1.4 De modo análogo, os conceitos formulados para a Defesa Cibernética são aplicados no contexto da Guerra Cibernética, uma vez que essa última está contida na primeira.

2.2 Conceitos

2.2.1 **Ameaça Cibernética** - causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse.

2.2.2 **Artefato Cibernético** - equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos.

2.2.3 **Ativos de informação** - meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

2.2.4 **Cibernética** - termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC^2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais.

2.2.5 **Defesa Cibernética** - conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente.

2.2.6 **"Dia-Zero"** - designação atribuída à situação na qual há uma ameaça capaz de explorar uma vulnerabilidade de segurança descoberta em sistemas computacionais e que não teve, ainda, correção disponibilizada pelo desenvolvedor ou fabricante.

2.2.7 **Domínios Operacionais** - o Espaço Cibernético é um dos cinco domínios operacionais e permeia todos os demais. São eles: o terrestre, o marítimo, o aéreo e o espacial, que são interdependentes. As atividades no Espaço Cibernético podem criar liberdade de ação para atividades em outros domínios, assim como atividades em outros domínios também criam efeitos dentro e através do Espaço Cibernético. O objetivo central da integração dos domínios é a habilidade de se alavancar capacidades de vários domínios para que sejam criados efeitos únicos e, frequentemente, decisivos.

2.2.8 **Espaço Cibernético** - espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.

2.2.9 **Fonte Cibernética** - recurso por intermédio do qual se pode obter dados no Espaço Cibernético utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A Fonte Cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de Inteligência.

2.2.10 **Guerra Cibernética** - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C^2 do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle ($STIC^2$) do oponente e defender os próprios $STIC^2$. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC.

2.2.11 **Infraestrutura Crítica da Informação** - subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

2.2.12 **Infraestruturas Críticas** - instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

2.2.13 **Operação de Informação** - ações coordenadas sobre o ambiente de informação e executadas, com o apoio da inteligência, para influenciar um oponente real ou potencial, diminuindo sua combatividade, coesão interna e externa e capacidade de tomada de decisão, bem como para a proteção do próprio processo decisório, concorrendo, assim, para a consecução dos objetivos políticos e militares.

2.2.14 **Poder Cibernético** - capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder.

2.2.15 **Resiliência Cibernética** - capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa.

2.2.16 **Risco Cibernético** - probabilidade de ocorrência de um incidente cibernético associado à magnitude do dano por ele provocado.

2.2.17 **Segurança Cibernética** - arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas.

2.2.18 **Segurança da Informação e Comunicações (SIC)** - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações.

2.3 Princípios de Emprego da Defesa Cibernética

2.3.1 As operações militares, incluindo as realizadas no Espaço Cibernético, guiam-se pelos princípios surgidos do estudo de campanhas militares e que estão elencados na Doutrina Militar de Defesa. As peculiaridades da Defesa Cibernética impõem, ainda que outros princípios relevantes sejam considerados.

2.3.2 São princípios relevantes de emprego da Defesa Cibernética:

a) Princípio do Efeito;
b) Princípio da Dissimulação;
c) Princípio da Rastreabilidade; e
d) Princípio da Adaptabilidade.

2.3.3. **Princípio do Efeito** - as ações no Espaço Cibernético devem produzir efeitos que se traduzam em vantagem estratégica, operacional ou tática que afetem o mundo real, mesmo que esses efeitos não sejam cinéticos.

2.3.4. **Princípio da Dissimulação** - medidas ativas devem ser adotadas para se dissimular no Espaço Cibernético, dificultando a rastreabilidade das ações cibernéticas ofensivas e exploratórias levadas a efeito contra os sistemas de tecnologia da informação e de comunicações do oponente. Objetiva-se, assim, mascarar a autoria e o ponto de origem dessas ações.

2.3.5. **Princípio da Rastreabilidade** - medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra os sistemas de tecnologia da informação e de comunicações amigos. Quase sempre, as ações adotadas no Espaço Cibernético envolvem a movimentação ou a manipulação de dados, as quais podem ser registradas nos sistemas de TIC.

2.3.6. **Princípio da Adaptabilidade** - consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do Espaço Cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis.

2.4 Características da Defesa Cibernética

2.4.1 Além de atender aos seus princípios relevantes e de guerra, a Defesa Cibernética dispõe de características apresentadas a seguir:

a) Insegurança Latente;
b) Alcance Global;
c) Vulnerabilidade das Fronteiras Geográficas;
d) Mutabilidade;
e) Incerteza;
f) Dualidade;
g) Paradoxo Tecnológico;
h) Dilema do Atacante;
i) Função Assessoria; e
j) Assimetria.

2.4.2 **Insegurança Latente** - nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos de informação serão sempre objeto de exploração por ameaças cibernéticas.
2.4.3 **Alcance Global** - a Defesa Cibernética possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes. Limitações físicas de distância e espaço não se aplicam ao Espaço Cibernético.

2.4.4 **Vulnerabilidade das Fronteiras Geográficas** - as ações de Defesa Cibernética não se limitam a fronteiras geograficamente definidas, pois os agentes podem atuar a partir de qualquer local e provocar efeito em qualquer lugar.

2.4.5 **Mutabilidade** - não existem leis de comportamento imutáveis no Espaço Cibernético, pois podem adaptar-se as condições ambientais e da criatividade do ser humano.

2.4.6 **Incerteza** - as ações no Espaço Cibernético podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados.

2.4.7 **Dualidade** - na Defesa Cibernética, as mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas alvos e, por administradores, para descobrir as fraquezas de equipamentos e redes.

2.4.8 **Paradoxo Tecnológico** - quanto mais tecnologicamente desenvolvido estiver um sistema, mais dependente da TI estará e consequentemente mais vulnerável às ações cibernéticas. Contudo, paradoxalmente, este mesmo oponente possuirá mais condições de se defender dos ataques cibernéticos, em virtude de seu alto grau de desenvolvimento tecnológico.

2.4.9 **Dilema do Atacante** - dúvida que o atacante enfrenta na busca ou não da correção de uma vulnerabilidade identificada, sabendo que a correção tornará mais eficiente a sua defesa, enquanto que a não correção aumenta sua capacidade de ataque.

2.4.10 **Função Assessoria** - as ações de Defesa Cibernética não são um fim em si mesmas, sendo, geralmente, empregadas para apoiar a condução de outros tipos de operação.

2.4.11 **Assimetria** - baseada no desbalanceamento de forças, causado pela introdução de um ou mais elementos de ruptura tecnológicos, metodológicos ou procedimentais que podem vir a causar danos tão prejudiciais quanto aqueles perpetrados por Estados ou organizações com maiores condições econômicas, por exemplo.

2.5 Possibilidades da Defesa Cibernética

2.5.1 São possibilidades da Defesa Cibernética:

a) atuar no Espaço Cibernético, por meio de ações ofensivas, defensivas e exploratórias;

b) cooperar na produção do conhecimento de Inteligência por meio da Fonte Cibernética;

c) atingir infraestruturas críticas de um oponente sem limitação de alcance físico e exposição de tropa;

d) cooperar com a Segurança Cibernética, inclusive, de órgãos externos ao MD, mediante solicitação ou no contexto de uma operação;

e) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da Defesa Cibernética;

f) obter a surpresa com mais facilidade, baseado na capacidade de explorar as vulnerabilidades dos sistemas de informação do oponente;

g) realizar ações contra oponentes mais fortes, dentro do conceito de Guerra Assimétrica; e

h) realizar ações com custos significativamente menores que as operações militares nos demais domínios.

2.6 Limitações da Defesa Cibernética

2.6.1. São limitações da Defesa Cibernética:

a) limitada capacidade de identificação da origem de ataques cibernéticos;
b) existência de vulnerabilidades nos sistemas computacionais;
c) dificuldade de identificação de talentos humanos;
d) grande vulnerabilidade a ações de oponentes com poder assimétrico;
e) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e
f) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação.

2.7 Formas de atuação cibernética

2.7.1. As formas de atuação cibernética podem variar de acordo com o nível dos objetivos (político, estratégico, operacional ou tático), nível de envolvimento nacional, contexto de emprego, nível tecnológico empregado, sincronização e tempo de preparação, como será apresentado a seguir.

2.7.2. Atuação Cibernética Política/Estratégica - a atuação cibernética política/estratégica ocorre desde o tempo de paz, para atingir um objetivo político ou estratégico definido no mais alto nível, normalmente no contexto de uma Operação de Informação ou de Inteligência.

2.7.3. Atuação Cibernética Operacional/Tática - a atuação cibernética operacional/tática é tipicamente empregada no contexto de uma Operação Militar, contribuindo para a obtenção de um efeito desejado.

2.7.4. As formas de atuação cibernética estão exemplificadas no quadro a seguir, o qual exibe as possibilidades de atuação cibernética e os critérios que podem ser utilizados para diferenciar as formas de atuação:

FORMA DE ATUAÇÃO CIBERNÉTICA / **CRITÉRIOS**	**POLÍTICA / ESTRATÉGICA**	**OPERACIONAL / TÁTICA**
Nível dos Objetivos	Políticos e/ou Estratégicos	Operacionais e/ou Táticos
Foco	Obtenção de Inteligência	Preparação do campo de batalha
Nível de envolvimento nacional	Normalmente interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, Agência Brasileira de Inteligência - ABIN, Agência Nacional de Telecomunicações - ANATEL etc.)	Normalmente no âmbito do Ministério da Defesa, podendo contar com apoio do Ministério das Relações Exteriores
Contexto	Desde o tempo de paz, podendo fazer parte de uma Operação de Informação ou de Inteligência	Em um ambiente de crise ou conflito, apoiando uma ação militar
Nível tecnológico empregado	Normalmente alto ou muito alto	Normalmente médio ou baixo
Sincronização	Dentro do contexto de uma sofisticada Operação de Inteligência, podendo requerer ações diplomáticas anteriores ou posteriores	Dentro do contexto dos sistemas operacionais de uma Operação Militar, sincronizado com a manobra
Tempo de Preparação e Duração	Duração prolongada, com tempo de preparação normalmente mais longo, com desenvolvimento e emprego de técnicas de difícil detecção	Duração limitada, normalmente com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas

2.8 Tipos de Ações Cibernéticas

2.8.1. Os tipos de ações cibernéticas são os seguintes:

a) ataque cibernético;
b) proteção cibernética; e
c) exploração cibernética.

2.8.2. **Ataque Cibernético** - compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.

2.8.3. **Proteção Cibernética** - abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.

2.8.4. **Exploração Cibernética** - consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e

servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas.

2.8.5. Limites às Ações Cibernéticas:

2.8.5.1. **Operações de Não Guerra**. Por ocasião da execução de Operações de Não-Guerra, o emprego de ações de ataque cibernético necessita de autorização expressa de autoridade competente, normalmente em nível político. Para as ações de exploração cibernética, deverão ser observados atos normativos do ordenamento jurídico em vigor. Em caso de dúvidas, caberá ao EMCFA consultar o nível político acerca do emprego das ações anteriormente mencionadas.

2.8.5.2. **Operações de Guerra**. Somente serão executadas as ações efetivamente necessárias para o cumprimento do item 2.7.4. Em caso de dúvidas, caberá ao EMCFA consultar o nível político acerca do emprego dessas ações.

CAPÍTULO III

SISTEMA MILITAR DE DEFESA CIBERNÉTICA

3.1 Generalidades

3.1.1 A Defesa Cibernética, por ser um dos componentes da Defesa Nacional, é missão das Forças Armadas (FA), conforme a legislação referenciada no capítulo I. Entretanto, as peculiaridades do Espaço Cibernético tornam impraticável o cumprimento dessa missão se não houver o comprometimento da sociedade como um todo, imbuída do sentimento de responsabilidade individual e coletiva pela proteção das infraestruturas críticas nacionais no Espaço Cibernético.

3.1.2 A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, avulta de importância a necessidade de interação permanente entre o MD e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a END.

3.1.3 As atividades de Defesa Cibernética no MD são orientadas para atender às necessidades da Defesa Nacional. A integração com órgãos de interesse deve ser buscada desde a situação de normalidade institucional, com a finalidade de facilitar as ações decorrentes de uma evolução para situações de crise ou conflitos, levando em consideração o amplo espectro dessas situações.

3.1.4 O Sistema Militar de Defesa Cibernética (SMDC) é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional.

3.1.5 Cabe também ao SMDC assegurar a proteção cibernética do SISMC^2, assegurando a capacidade de atuar em rede com segurança, bem como coordenar e integrar a proteção das infraestruturas críticas da Informação de interesse da Defesa Nacional, definidas pelo MD.

3.2 Níveis de Decisão

3.2.1 No contexto do SMDC, os níveis de decisão são os seguintes:

a) **Nível político** - abrange as ações de SIC e Segurança Cibernética, cujos principais atores são a Presidência da República e o Comitê Gestor da Internet no Brasil;

b) **Nível estratégico** - abrange as ações de Defesa Cibernética, a cargo do EMCFA, por intermédio do Centro de Defesa Cibernética, bem como dos Comandos das FA, por intermédio de seus respectivos órgãos de Defesa Cibernética, além de Centros de Tratamento de Incidentes de Redes (CTIR), da APF, de outras instituições parceiras e do Destacamento Conjunto de Defesa Cibernética, quando constituído;

c) **Nível Operacional** - abrange as ações de Guerra Cibernética, a cargo dos Comandos Operacionais e de seus Estados-Maiores, quando ativados; e

d) **Nível Tático** - abrange as ações de Guerra Cibernética, a cargo das Forças Componentes com seus elementos de Guerra Cibernética e o Destacamento Conjunto de Guerra Cibernética, quando ativados.

3.3 A concepção do Sistema Militar de Defesa Cibernética

3.3.1 O EMCFA é o órgão responsável por assessorar o Ministro de Estado da Defesa na implantação e na gestão do SMDC, com a finalidade de garantir, no âmbito da Defesa Nacional, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança necessários.

3.3.2 A concepção geral do SMDC pode ser vista no Anexo e conta com a participação de militares das FA e civis.

3.3.3 O órgão central do SMDC é o Centro de Defesa Cibernética (CDCiber), que passa ao controle operacional do MD nas Operações Conjuntas e conta, permanentemente, com um Estado-Maior Conjunto para realizar o planejamento e o controle das ações planejadas, levando em conta as particularidades de cada Força Armada, de modo a obter uma atuação sinérgica.

3.3.4 O CDCiber atua sob orientação e supervisão do MD, no nível estratégico, realizando as ações de coordenação e integração do Setor Cibernético nas Forças Armadas e privilegiando, sempre que possível, uma forma de atuação conjunta.

3.3.5 O CDCiber mantém canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de Defesa Cibernética (CERT.br, CTIR Gov, órgãos de Defesa/Guerra Cibernética das FA, Ministérios, Agências Governamentais, APF e outros).

3.3.6 O CDCiber mantém canal sistêmico/técnico com os órgãos centrais de inteligência das FA, no âmbito do Sistema de Inteligência de Defesa (SINDE), no tocante ao Setor Cibernético, para a difusão e obtenção dos dados obtidos por intermédio da Fonte Cibernética.

3.4 Níveis de Alerta Cibernético

3.4.1 Entende-se por Nível de Alerta Cibernético, para emprego no âmbito do MD e das FA, seja em operações conjuntas, seja nas atividades diárias, a classificação dada ao estado em que se encontra o Espaço Cibernético de interesse do MD e das FA, no tocante à possibilidade de concretização de ameaças cibernéticas.

3.4.2 Para o estabelecimento dos níveis de alerta cibernético a seguir definidos, foram considerados os seguintes critérios básicos:

a) os níveis de alerta cibernético são utilizados em situações nas quais haja probabilidade de concretização de ameaças cibernéticas no Espaço Cibernético de interesse do MD e das FA;

b) a interpretação de cada nível de alerta está associada a um ou mais cenários de riscos, os quais podem ser hipotéticos ou advindos de lições aprendidas obtidas em exercícios simulados ou missões reais;

c) a mudança de um nível para outro pode ser ou não sequencial, ou seja, existe a possibilidade de mudanças entre níveis não sucessivos, saltando-se níveis intermediários;

d) a variação de um nível para outro está associada a um ou mais dos seguintes fatores:

- mudança da probabilidade de ocorrência das ameaças existentes, segundo os critérios de análise de riscos adotados;
- concretização de ameaças existentes;
- abrangência do impacto da concretização de ameaças, segundo os critérios de análise de risco adotados.

e) os níveis de alerta são compatíveis e relacionáveis com as metodologias de gestão de riscos adotadas pelas FA;

f) cada nível de alerta demanda um conjunto de procedimentos correspondentes, os quais devem atender as especificidades de cada FA ou serem próprios para o emprego pelo MD e pelas FA, nas atividades diárias ou em Operações Conjuntas. Estes procedimentos devem ser explicitados no planejamento da operação ou em publicações pertinentes; e

g) cada nível é designado por uma cor e por um nome que evocam o grau de risco correspondente à possibilidade de concretização de ameaças cibernéticas no Espaço Cibernético de interesse do MD e das FA.

3.4.3 Os níveis de alerta cibernético, para emprego no âmbito do MD, com seus respectivos significados e/ou interpretações, são os seguintes:

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

Nível de Alerta		Significado / Interpretação (*)
Cor	**Nome**	
Vermelho	Muito Alto	– Aplicável quando ações cibernéticas hostis exploram ou negam a disponibilidade das infraestruturas críticas da informação. – Probabilidade de concretização de ameaças cibernéticas muito alta, considerando o histórico. – Infraestrutura Crítica da Informação atingida com impacto alto ou superior, considerando o histórico. – Infraestrutura Crítica da Informação atingida, com possibilidade de restabelecimento da condição de segurança ou dos serviços em tempos além dos aceitáveis para o cumprimento da missão.

(*) **Observações:**

- os enunciados da coluna “Significado/Interpretação” representam possíveis cenários**,** propositadamente simplificados para fins de clareza e síntese;
- para classificar o nível, pode-se tomar uma ou mais das possibilidades discriminadas em cada uma das linhas da coluna “Significado/Interpretação”;
- os cenários possíveis são inúmeros e as possibilidades registradas neste documento constituem um núcleo básico, que pode ser desdobrado e enriquecido conforme a aplicação dos níveis em planejamentos de situações específicas reais ou simuladas;
- quando se enuncia que uma ameaça “afeta” o Espaço Cibernético, subentende-se que uma ou mais das ameaças percebidas se concretizam e causam um impacto correspondente.

3.4.4 É prerrogativa do Chefe do EMCFA ratificar o nível de alerta cibernético acima de amarelo, sugerido pelos órgãos de Defesa Cibernética das FA. Durante operações, os níveis até amarelo, inclusive, serão estabelecidos pelo Chefe do CDCiber.

3.4.5 O nível de alerta cibernético de cada FA não deverá ser inferior ao nível de alerta cibernético adotado pelo Ministério da Defesa.

3.4.6 É responsabilidade de cada FA a adoção de medidas de proteção e Defesa Cibernética dos seus Ativos de Informação.

CAPÍTULO IV

DEFESA E GUERRA CIBERNÉTICA NAS OPERAÇÕES

4.1 Generalidades

4.1.1 O Setor Cibernético nacional envolve a atuação integrada de vários órgãos, sejam civis ou militares, cada um com atribuições específicas. Desta forma, o modelo de atuação cibernética mais provável para emprego em operações normalmente será o de operações em ambiente interagências.

4.1.2 Os processos de C^2 para as ações de Guerra Cibernética (G Ciber) devem estar integrados aos processos de C^2 já definidos na Doutrina de Operações Conjuntas.

4.1.3 A necessidade de coordenação entre as agências define a estrutura a ser organizada para o cumprimento da missão, seja no nível estratégico, seja nos níveis operacional e tático. Desta forma, ficará configurado o emprego de um Destacamento Conjunto de Defesa Cibernética e/ou um Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber), além de elementos de Guerra Cibernética integrantes das Forças Componentes.

4.1.4 Em qualquer operação militar que envolva o componente cibernético, a cooperação e o intercâmbio de informações são fatores essenciais para uma atuação efetiva. Esses aspectos tornam essencial o estabelecimento e/ou o fortalecimento de parcerias estratégicas com órgãos de Segurança e/ou Defesa Cibernética nacionais e internacionais.

4.1.5 A Guerra Cibernética poderá ser planejada e executada mediante solicitações de efeitos desejados pelo Comando Operacional, por grupos específicos designados para tal, empregando o canal técnico com os órgãos responsáveis pela Defesa Cibernética de cada FA e do Ministério da Defesa.

4.2 Operações de Informação no Estado-Maior Conjunto do Comando Operacional

4.2.1. A G Ciber em Operações Conjuntas deverá, em princípio, ser planejada e conduzida, no nível do Comando Operacional Conjunto, integrando a célula de Operações de Informação (Op Info) ou a critério do Comandante Operacional.

4.2.2. A Seção dedicada às Op Info deve ser mobiliada com, pelo menos, 1 (um) oficial especializado em G Ciber, preferencialmente, oficial superior com o Curso de Estado-Maior ou equivalente.

4.2.3. As principais atribuições dos especialistas em G Ciber durante as operações incluem:

a) 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; e

b) 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.[1]

4.3 Destacamento Conjunto de Defesa Cibernética e Destacamentos de Guerra Cibernética

4.3.1. Poderá ser constituído, pelo CDCiber, um Destacamento Conjunto de Defesa Cibernética, para atuação em operações em ambiente interagências que requeiram uma coordenação em nível estratégico. As possibilidades e estrutura do referido destacamento são análogas às que orientam o Destacamento Conjunto de Guerra Cibernética, as quais são apresentados nos itens 4.3.3 a 4.3.6.

4.3.2. Poderá ser adjudicado ao Comando Operacional ativado 01 (um) Dst Cj G Ciber, diretamente subordinado ao referido Comando Operacional, integrando suas tropas.

4.3.3. O Dst Cj G Ciber, quando ativado, poderá ser estruturado da seguinte maneira:

a) comandante e subcomandante (ou imediato);
b) elementos especializados em G Ciber das FA;
c) elementos de ligação interagências; e
d) elementos civis especialistas, para operação assistida e assessoria.

4.3.4. O detalhamento da estrutura e o efetivo do Dst Cj G Ciber deverá ser definido e proposto após estudo específico elaborado por seu comandante, levando em conta as necessidades específicas de cada operação, segundo os fatores da decisão.

4.3.4.1. É desejável que, na concepção da estrutura do destacamento, haja separação quanto ao planejamento e a execução das ações de proteção das de exploração e ataque cibernético.

4.3.5. São possibilidades do Dst Cj G Ciber:

a) identificar e analisar vulnerabilidades (conhecidas) nas redes de computadores e aplicações empregadas no Sistema de C^2 desdobrado para a operação;
b) recomendar ações para mitigar as vulnerabilidades identificadas;
c) estudar as ameaças e entender seu impacto nas redes de C^2 ou quaisquer outras estruturas/recursos computacionais das forças amigas;
d) verificar a conformidade de Segurança da Informação e Comunicações no Sistema de C^2 desdobrado para a operação;
e) planejar e executar ações cibernéticas (proteção, exploração e ataque), no contexto da operação conjunta, com apoio dos órgãos de Defesa Cibernética das Forças Armadas em cumprimento às orientações e diretrizes emanadas do Comando Operacional;
f) assessorar o(s) comandante(s) da(s) Força(s) Componente(s) nos pedidos de efeito desejado dirigidos ao escalão competente para obtê-los;
g) colaborar com a execução das Op Info planejadas; e

[1] Vantagem operacional resultante da habilidade de coletar, processar e disseminar um fluxo ininterrupto de informação, enquanto explora ou nega ao oponente a capacidade de fazer o mesmo.

h) colaborar com o esforço de obtenção de dados para a produção de conhecimento de Inteligência, por intermédio da Fonte Cibernética, no contexto da operação conjunta, em cumprimento às orientações e diretrizes emanadas pelo EMCj.

4.3.6. Nas operações singulares, as possibilidades e estruturas dos destacamentos de G Ciber são análogas às das operações conjuntas. Nesse caso, os elementos especializados em G Ciber integram a estrutura similar do Estado-Maior do mais alto escalão da Operação e o Destacamento de Guerra Cibernética será diretamente subordinado a esse escalão.

4.4 Inteligência de Fonte Cibernética

4.4.1. A Fonte Cibernética pode tanto ser utilizada para produção de conhecimento de caráter eminentemente técnico, quanto pode ser integrada às demais fontes (humanas, imagens, sinais e outras) para a produção de conhecimento de caráter mais amplo.

4.4.2. A integração das diferentes fontes de Inteligência para a produção de conhecimento é, normalmente, realizada nos órgãos de Inteligência do Ministério da Defesa, Marinha do Brasil, Exército Brasileiro e Força Aérea Brasileira.

4.4.3. O CDCiber e os órgãos de Defesa Cibernética das Forças Armadas, agindo como Agências Especiais de Inteligência, poderão produzir conhecimento oriundo exclusivamente da Fonte Cibernética, como também pode empregar conhecimento de outras fontes para melhor desempenhar suas funções.

4.4.4. Nas operações, a Fonte Cibernética poderá ser integrada às demais fontes pela estrutura de Inteligência do escalão considerado.

4.5 Planejamento da Defesa e da Guerra Cibernética nas Operações

4.5.1 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.

4.5.2 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 G Ciber que deverão constar do supracitado Anexo de Op Info e de outros documentos integrantes do planejamento conjunto. Esses documentos estão descritos na publicação Doutrina de Operações Conjuntas (MD30-M-01).

INTENCIONALMENTE EM BRANCO

CAPÍTULO V
DISPOSIÇÕES FINAIS

5.1 Aplicação

Esta doutrina aplica-se ao Ministério da Defesa e aos Comandos da Marinha, do Exército e da Aeronáutica, devendo ser observada por ocasião da elaboração ou da reedição de outras publicações relacionados ao tratado nestas páginas.

5.2 Sugestões

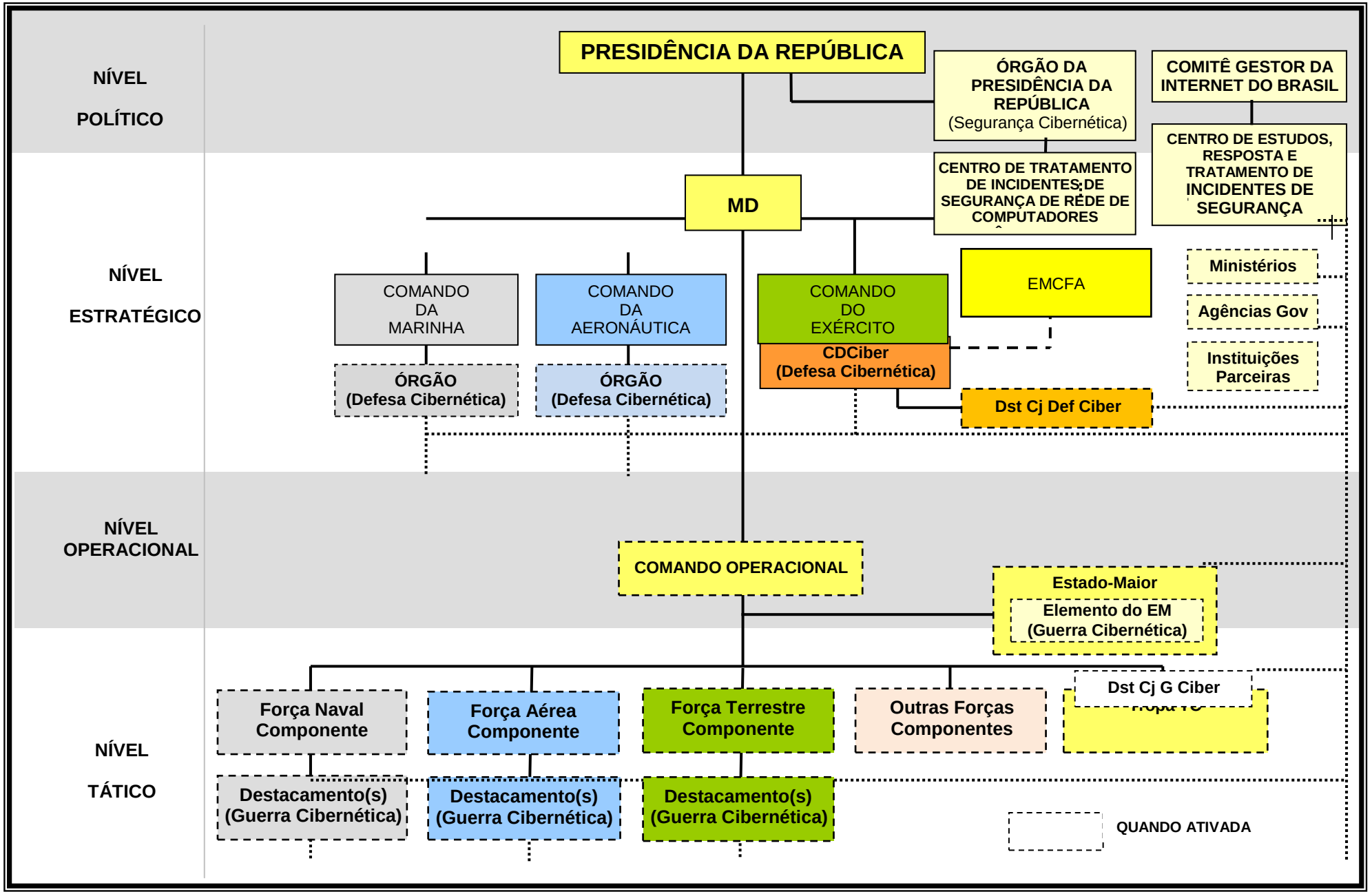
As sugestões para aperfeiçoamento deste documento são estimuladas e devem ser encaminhadas ao Estado-Maior Conjunto das Forças Armadas, em qualquer oportunidade, por meio do e-mail: adl1.emcfa@defesa.gov.br.

5.3 Atualização

O Ministério da Defesa, sempre que necessário, promoverá a atualização desta doutrina. O primeiro ciclo de atualização está previsto para 2017, quando poderão ser aproveitadas as lições aprendidas ao longo das operações de apoio aos grandes eventos.

INTENCIONALMENTE EM BRANCO

APÊNDICE
ESTRUTURAS E ÓRGÃOS NA CONCEPÇÃO DO SISTEMA MILITAR DE DEFESA CIBERNÉTICA
CERT.br



LEGENDA:

SUBORDINAÇÃO
VINCULAÇÃO (SUBORDINAÇÃO OPERACIONAL)
CANAL TÉCNICO (COORDENAÇÃO E INTEGRAÇÃO)

INTENCIONALMENTE EM BRANCO

Ministério da Defesa
Estado-Maior Conjunto das Forças Armadas
Brasília, 18 de novembro de 2014

MINISTÉRIO DA DEFESA
Esplanada dos Ministérios – Bloco Q – 7º Andar
Brasília – DF – 70049-900
www.defesa.gov.br