Defesa Cibernética no Brasil

Distribuição de competências nas operações interagências

Luiz Eduardo Santos Cerávolo[1]

Walfredo Bento Ferreira Neto[2]

Introdução

Recentemente, Robert A. Johnson (2015), diretor do Programa de Pesquisa Changing Character of War ("Caráter Mutável da Guerra"), da Universidade de Oxford, demonstrou sua preocupação quanto à guerra do futuro. Mesmo ciente dos riscos que a tentativa de previsibilidade baseada em "bola de cristal" possa trazer — inclusive o de não vir a se realizar —, esse autor enfatizou alguns tópicos que, de fato, vêm, oportunamente, provocando intensas discussões: a aceleração das mudanças, sociais e dos (e nos) campos de batalha; a utilização, por diversos atores, dos recursos inerentes à guerra sistêmica, por meio das operações de informações, de crimes e bloqueios cibernéticos, de guerra eletrônica; a interrupção na geração e distribuição de energia e de outros setores estratégicos, e, talvez o de risco principal, a possibilidade de guerra em ambientes urbanos, no qual

> as Forças militares se veriam diante do colapso da autoridade civil; da presença de vários órgãos, com seus interesses específicos, atuando nos mesmos espaços; e de uma população civil vulnerável, à espera de assistência. (JOHNSON, 2015, p. 51)

O desenvolvimento das tecnologias da informação e das comunicações (TIC) e a sua difusão para diversos atores, não mais apenas estados ou grandes empresas, acarreta a necessidade de maior preocupação quanto à conectividade, à interoperabilidade e a descentralização de esforços, na busca de eficiência, eficácia e efetividade das operações militares, para garantia da defesa e manutenção da segurança. É justamente na necessidade de descentralização que surge uma das incógnitas desta pesquisa: como garantir a plena consciência situacional do tomador de decisões em um ambiente dessa natureza? Em outras palavras, como aumentar a probabilidade do êxito em operações de defesa e segurança com essa imperiosa necessidade de descentralização? Essa preocupação também pode ser inferida quando Joseph Nye (2011) ressaltou as possibilidades advindas do poder cibernético.

---

[1] Major do Exército Brasileiro, aluno da Escola de Comando e Estado-Maior do Exército. (*duduceravolo@uol.com.br*)

[2] Capitão do Exército Brasileiro, mestre em Estudos Estratégicos da Defesa e da Segurança (Instituto de Estudos Estratégicos da Universidade Federal Fluminense) e professor de Relações Internacionais da Academia Militar das Agulhas Negras. (*wbfneto@bol.com.br*)

Na verdade, podemos, ainda, remeter-nos a outra discussão, ligada à ampliação do conceito de Segurança (BUZAN, 1991). De fato, o setor político-militar e o Estado não mais possuem exclusividade na agenda internacional. O próprio sistema internacional, assim como os indivíduos, e outros setores, como o societal, o ambiental, o energético, o alimentar e o da informação **Figura 1**, vêm demandando atenção do ator que detém o monopólio legítimo da violência (o Estado) — cada vez mais exigido nesse ambiente complexo e difuso — e também de organismos, intergovernamentais ou não. É na busca de respostas a essas demandas que se insere a opção estatal e de organizações internacionais pelas operações interagências ou pelas multidimensionais, em situações de guerra e não guerra.

Tendo em vista tal apresentação, que traz, em grande parte, algumas de nossas inquietações pretéritas, procuramos, por meio de uma investigação em documentos oficiais nacionais e em uma bibliografia especializada no assunto, identificar e sistematizar as competências funcionais atribuídas aos diversos órgãos e agências da burocracia estatal brasileira ligados à defesa cibernética, tanto no tocante à situação de guerra como a de não guerra.

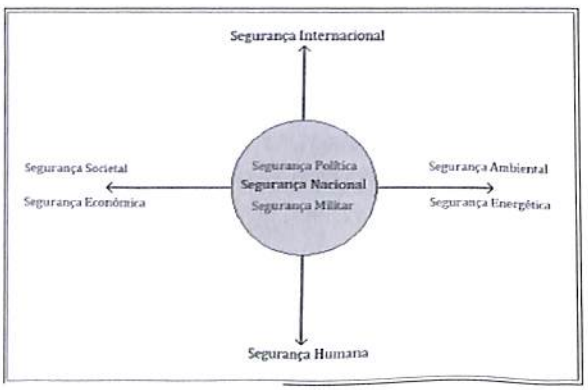

Figura 1 – Ampliação do conceito de *segurança*
Fonte: Marques; Medeiros Filho, 2011

Para isso, partimos do seguinte problema: existe uma distribuição de competências funcionais nas operações interagências no Brasil que envolvem a defesa cibernética? Caso positivo, de que forma e em que medida? Nossa hipótese é que, no Brasil, existe uma distribuição sistematizada, e que as atribuições e as competências dos órgãos que atuam nas operações interagências dessa natureza são distribuídas em atenção às próprias atribuições relacionadas aos níveis político, estratégico, operacional e tático, respectivamente. Essa distribuição funcional envolve tanto órgãos ligados diretamente à defesa, quanto outros voltados para a segurança, consequentemente envolvendo militares e civis, o Estado e a sociedade.

Para confirmarmos nossa hipótese, procuramos compreender os conceitos envolvidos na investigação, tais como *defesa cibernética* e *operações interagências*. O liame construído a partir desses entendimentos nos permitiu alcançar algumas considerações finais e, de certa maneira, alguns pontos que poderão servir para um necessário processo contínuo de aperfeiçoamento do tema.

O artigo ficou estruturado como descrito adiante.

Inicialmente, após esta introdução, abordamos a Defesa Cibernética, a partir da investigação sobre a implantação do setor cibernético no Brasil, elevado ao nível estratégico em 2008, por meio da Estratégia Nacional de Defesa (END). Nessa parte, expomos documentos oficiais acerca do tema, conceitos, princípios, ações, possibilidade e limites e projetos estruturantes relacionados à cibernética no país.

No segundo momento, entramos na seara das operações interagências, com a fi-

nalidade de compreender seu conceito e a sistemática de seu funcionamento, incluindo os princípios e o processamento da coordenação entre os órgãos participantes. Ainda nessa parte, encontramos organogramas que demonstram o funcionamento desse tipo de operação e construímos quadros, a fim de explicitar, de uma forma sintética, a participação e a responsabilidade dos diversos órgãos e agências da Administração Pública Brasileira envolvidos com o tema.

Como próximo passo, empreendemos esforços para correlacionar as duas seções anteriores — defesa cibernética e operações interagências —, focando a sistematização de operações dentro — e conforme — o ambiente cibernético. Nessa parte também elaboramos quadros que sintetizam as atribuições e as competências, no tocante ao setor cibernético, obedecendo aos níveis político, estratégico, operacional e tático. Talvez, por meio desses quadros, é que poderá ser constatada nossa maior contribuição, pois permitem às autoridades e os agentes envolvidos no tema e nessas ações, enxergarem, de forma sistematizada e simplificada, o mapeamento do processo relativo às competências e às respectivas atribuições.

Por fim, tecemos algumas considerações, que, pelo que pesquisamos e registramos, de fato, reforçam a importância desse tema para o Estado, mas não só para esse ator, uma vez que organismos, agências e a própria sociedade se encontram diretamente inseridos nesse contexto, tanto para usufruir seus infinitos benefícios, quanto para, infelizmente, sentir reflexos negativos. Sem intenção alguma de esgotar o objeto de nossa pesquisa, apontamos algumas direções, a título de eventual possibilidade de aperfeiçoamento.

Defesa cibernética

Implantação da cibernética como setor estratégico

O espaço cibernético é considerado o 5º domínio para fins militares, ao lado dos domínios: aéreo, marítimo, terrestre e espacial. Esse domínio assume especial importância no âmbito da segurança nacional (CRUZ, 2013, p.3).

Esse espaço é o ambiente da guerra cibernética, termo esse definido no glossário das Forças Armadas, MD35-G-01, como:

> Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil. (BRASIL, 2007, p.123).

O Exército Brasileiro realizou o primeiro estudo institucional para desenvolvimento da guerra cibernética em 2004, por meio da Secretaria de Tecnologia da Informação. Esse foi o primeiro documento a demonstrar a intenção da preparação de um ataque cibernético pelo Exército Brasileiro (EB) (CASEMIRO FILHO, 2010, p.34).

Em 2008, a Estratégia Nacional de Defesa (END) foi aprovada, por meio do decreto n° 6.703. Esse documento procurou orientar, de forma sistemática, a reorganização e a reorientação das Forças Armadas. Além disso, definiu três setores estratégicos para a defesa nacional: o cibernético, o espacial e o nuclear (POMPEU, 2012, p.2).

Desses setores, somente o cibernético não estava claramente definido para qual

Força seria designado. Por meio do ofício nº 035 de 03 de julho de 2009, o comandante do Exército solicitou ao Ministro da Defesa que o Exército fosse a principal força responsável pela condução do setor (CRUZ, 2013, p.1).

Com isso, a Diretriz Ministerial Nr 014/2009, atribuiu ao Exército Brasileiro a responsabilidade pela coordenação e integração do setor cibernético do Ministério da Defesa (CARVALHO, 2011, p.11).

Entre outras, essa diretriz previu:

> No desenvolvimento dos estudos e trabalhos determinados, atentar para as seguintes orientações: a) Gerais; [...] b) Específicas – Considerar: 1) **Setor Cibernético: - que ainda não existem quaisquer tipos de tratados e controles internacionais; – a possibilidade de criação de um centro para o desenvolvimento de quaisquer tipos de ações; e – a possibilidade de contratação de militares das três Forças em um mesmo ambiente de atuação.** (grifo do autor) (BRASIL, 2009, apud CARMO, 2011, p.22)

Além disso, fruto da supracitada diretriz, o Exército criou um grupo de trabalho (GT) que elaborou, inicialmente, oito projetos estratégicos que, visavam à implementação de ações nas seguintes áreas: expansão da estrutura de segurança cibernética; expansão e aprimoramento da estrutura de capacitação, adestramento e emprego operacional; estabelecimento de uma estrutura de apoio tecnológico e de pesquisa cibernética; estabelecimento de uma estrutura de gestão de pessoal e de arcabouço documental, doutrina em particular; formatação da estrutura e das missões do Centro de Defesa Cibernética do Exército. Em outubro de 2010, o Ministério da Defesa (MD) aprovou os projetos da **Figura 2** (FERREIRA NETO, 2013, p.150).

O Grupo Técnico de Segurança Cibernética (GT SEG CIBER) foi instituído em 2009, no âmbito da Câmara de Relações Exteriores e Defesa (CREDEN), alinhado à intenção estatal de fortalecer o setor cibernético. Esse grupo objetivou propor diretrizes

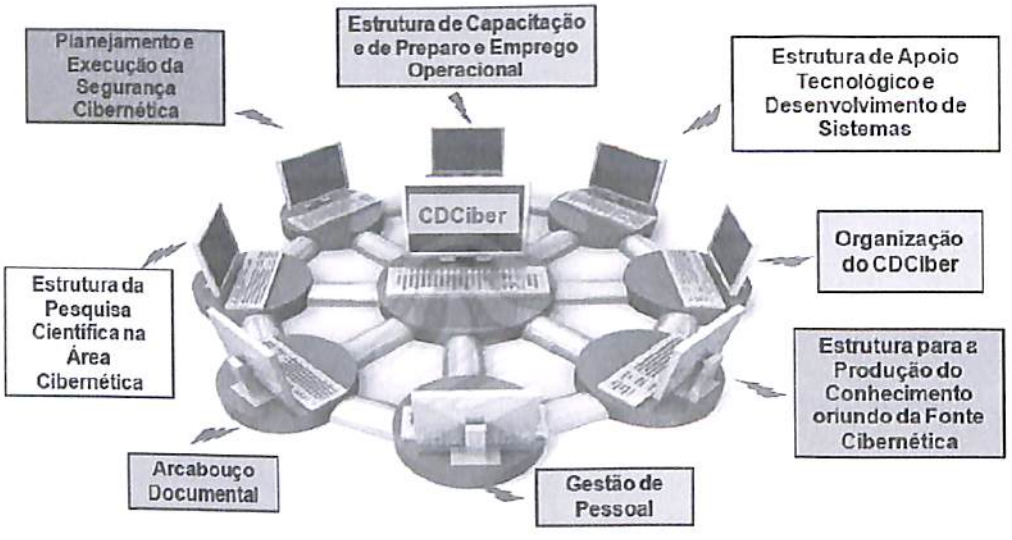

Figura 2 – Projetos Estruturantes do Setor Cibernético
Fonte: Núcleo do Centro de Defesa Cibernética (Ferreira Neto, 2013 apud Costa, 2012, p. 151)

e estratégias de Segurança Cibernética para a Administração Pública Federal e contou com representantes dos seguintes órgãos: Gabinete de Segurança Institucional da Presidência da República (GSIPR), Ministério da Defesa (MD), Ministério da Justiça (MJ), Ministério das Relações Exteriores (MRE), comandos da Marinha, do Exército e da Aeronáutica. A Coordenação do GT SEG CIBER é exercida pelo GSIPR, por intermédio de seu Departamento de Segurança da Informação e Comunicações (DSIC) (BRASIL, 2010, p. 11).

Em 2010, foi publicado o Livro Verde – Segurança Cibernética no Brasil, que apresentou propostas de diretrizes básicas, com objetivo de iniciar amplo debate social, econômico, político e técnico-científico sobre Segurança Cibernética no Brasil (BRASIL, 2010, p. 5).

Nesse mesmo ano, o comandante do Exército aprovou a Diretriz de Implantação do Setor Cibernético no EB. Foi ativado o Centro de Defesa Cibernética (CDCiber) do EB, tendo como principal atribuição a coordenação das atividades do setor cibernético da Força. Para implementar esse projeto, o CDCiber dividiu o estudo em cinco áreas de interesse: doutrina, inteligência, operações, recursos humanos e ciência e tecnologia (CRUZ, 2013, p.2).

Em 2012, o ministro da Defesa entregou a Política Nacional de Defesa (PND) ao Congresso Nacional. Esse documento condiciona o planejamento, no mais alto nível, de ações destinadas à defesa nacional coordenadas pelo Ministério da Defesa. Ainda nessa política, foi ratificado o setor cibernético como um dos estratégicos para o país (BRASIL, 2012, p.1).

Nesse mesmo ano, foi definida a Política Cibernética de Defesa, que definiu a atuação do Brasil em situações de ciberguerra. Essa política se aplica a todos os componentes da expressão militar do Poder Nacional, bem como às entidades que venham a participar de atividades de Defesa ou de Guerra Cibernética. Ela prevê a criação do Sistema Militar de Defesa Cibernética (SMDC), órgão que terá como prerrogativa, além de criar a infraestrutura de gestão das ações militares brasileiras no ciberespaço, fazer parcerias com setores acadêmicos e incentivar a pesquisa na área de segurança cibernética. O Estado-Maior Conjunto das Forças Armadas (EMCFA) é o órgão responsável por assessorar o ministro da Defesa na implementação e gestão do SMDC (BRASIL, 2013-b, p.1 e p.6).

Ainda em 2012, foi reeditada a Estratégia Nacional de Defesa, que focou na reorganização e reorientação das Forças Armadas, na organização da Base Industrial de Defesa e na política de composição dos efetivos da Marinha, do Exército e da Aeronáutica. Essa estratégia prevê os objetivos para o setor cibernético, apresentados no **Quadro 1**.

Dessa maneira, o estabelecimento desses objetivos favoreceu a projeção e o fomento do setor cibernético no âmbito nacional e proporcionou ampla visibilidade ao projeto cibernético brasileiro. Como repercussão desses objetivos e sua capilaridade, por exemplo, foi reformulado o currículo escolar da Academia Militar das Agulhas Negras, criando ou ampliando a carga horária de disciplinas ligadas à tecnologia da informação e comunicações (FERREIRA NETO, 2013, p. 155).

1. Fortalecimento do Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas
2. Aprimoramento da segurança da informação e comunicações
3. Fomento à pesquisa científica voltada para o setor cibernético, envolvendo a comunidade acadêmica nacional e internacional
4. Desenvolvimento de sistemas computacionais de defesa para emprego no setor cibernético e com possibilidade de uso dual
5. Desenvolvimento de tecnologias que permitam o planejamento e a execução da defesa cibernética no âmbito do MD e que contribuam com a segurança cibernética nacional
6. Desenvolvimento da capacitação, do preparo e do emprego dos poderes Cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas críticas nacionais
7. Incremento de medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas
8. Estruturação da produção de conhecimento oriundo da fonte cibernética

Quadro 1 – Objetivos para o setor cibernético (END/2012)
Fonte: BRASIL, 2012-a, p. 20, adaptado pelo autor

Defesa cibernética no Brasil

> Difícil — e necessário — é para um país que pouco trato teve com guerras convencer-se da necessidade de defender-se para poder construir-se. Não bastam, ainda que sejam proveitosos e até mesmo indispensáveis, os argumentos que invocam as utilidades das tecnologias e dos conhecimentos da defesa para o desenvolvimento do país. Os recursos demandados pela defesa exigem uma transformação de consciências para que se constitua uma estratégia de defesa para o Brasil. (BRASIL. 2012a., pp. 8-9)

Generalidades

O termo "defesa" possui diversos significados. Entretanto, visando reduzir o escopo para o tema do presente trabalho, deve ser entendido como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança" ou ainda a "reação contra qualquer ataque ou agressão real ou iminente" (FONTENELE, 2008, p. 15).

O supracitado termo segurança se caracteriza pela condição que permite ao país a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais (BRASIL, 2007, p. 235).

Para que se obtenha a Segurança Nacional, é necessária a eliminação das ameaças que são ou poderão ser lesivas aos Objetivos Fundamentais do país. Assim, a defesa nacional fica caracterizada quando o Poder Nacional é aplicado efetivamente, por intermédio de ações visando a superar antagonismos — internos ou externos — que possam afetar o alcance e/ou a manutenção dos Objetivos Fundamentais. A defesa nacional trata, portanto do conjunto de medidas e ações do Estado, com ênfase

na Expressão Militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais e manifestas (ESG, 2014, p. 82).

A defesa cibernética trata do conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (CARVALHO, 2011-a, p.8).

Esse tipo de defesa se constitui do conjunto de ações que visam a neutralizar a Guerra Cibernética, guerra essa que objetiva a quebra dos princípios da segurança da informação: disponibilidade, integridade, confidencialidade e autenticidade para se obterem vantagens que possam ser traduzidas nas mais variadas formas, como, por exemplo, causar danos ao inimigo com paradas de equipamentos e sistemas, alterar informações e parâmetros de sistemas, obter informações sigilosas e emitir ordens e comandos indesejados (BRAGA, 2011, p. 19).

A ameaça cibernética tornou-se uma preocupação por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional (BRASIL, 2012-b, p. 69).

A proteção do espaço cibernético abrange um grande número de áreas, como a capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacio-

Projetos	Início	Fim
6. Projeto sistema de proteção cibernética – defesa cibernética	2011	2023
Subprojetos		
Implantação da estrutura de planejamento e execução da Seg Cibernética	2012	2023
Implantação da estrutura de pesquisa científica na área cibernética	2012	2015
Implantação da estrutura de apoio tecnológico e desenvolvimento de sistemas voltada para as atividades do setor cibernético	2012	2015
Adequação da estrutura de capacitação, preparo e emprego operacional às necessidades do setor cibernético	2012	2015
Implantação do CDCiber, com capacidade para evoluir para Cmdo de Defesa Cibernética e criação da escola nacional de defesa cibernética	2012	2035
Desenvolvimento do rádio definido por *software* – RDS	2012	2035

Quadro 2 – Projetos e subprojetos na área de defesa e segurança cibernética
Fonte: elaborado e adaptado a partir de BRASIL, 2012-b, p. 251

nal e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede (BRASIL, 2012-b, p. 68).

Uma das novas capacidades prioritárias para a atuação do Exército é a liberdade de ação no espaço cibernético, tendo o Sistema de Proteção Cibernética – Defesa Cibernética como um dos projetos primordiais para contribuir para a transformação da Força Terrestre (**Quadro 2**).

O valor global estimado, até 2031, para investimento no projeto de Defesa Cibernética foi de R$ 839,90 milhões de reais. Curioso notar que o Livro Branco de Defesa Nacional (LBDN) fez referência à estimativa do aumento do efetivo atual do Exército (296.334 militares) em cerca de 20 mil militares, para atender, entre outras iniciativas, à implantação do setor Cibernético (BRASIL, 2012-b, p. 251).

Princípios de Emprego da Defesa Cibernética

Além dos tradicionais Princípios de Guerra, a Defesa Cibernética impõe que alguns outros princípios específicos sejam considerados (BRASIL, 2013-a, p. 18). São eles:

a) Princípio do Efeito;

b) Princípio da Dissimulação;

c) Princípio da Rastreabilidade;

d) Princípio da Adaptabilidade.

O princípio do efeito busca produzir efeitos que afetem o mundo real, mesmo que esses efeitos não sejam cinéticos.

O princípio da dissimulação visa dissimular no espaço cibernético, dificultando a rastreabilidade das ações cibernéticas ofensivas e exploratórias. Objetiva-se, assim, mascarar a autoria e o ponto de origem dessas ações.

O princípio da rastreabilidade são medidas efetivas que devem ser adotadas para se detectarem ações cibernéticas ofensivas e exploratórias contra os sistemas de tecnologia da informação e de comunicações amigos.

O princípio da adaptabilidade consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do espaço cibernético, mantendo a proatividade diante de mudanças súbitas e imprevisíveis.

Características da Defesa Cibernética e suas definições

As características da defesa cibernética e suas definições são apresentadas no **Quadro 3**.

Possibilidades e limitações da Defesa Cibernética

As possibilidades e limitações da Defesa Cibernética são apresentadas no **Quadro 4**.

Formas de atuação cibernética

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 veremos a seguir (BRASIL, 2013-a, p.21).

A atuação Cibernética Política/Estratégica ocorre desde o tempo de paz, para atingir um objetivo político ou estratégico definido no mais alto nível, normalmente

Característica	Definição
Insegurança Latente	Nenhum sistema computacional é totalmente seguro
Alcance Global	Possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes de combate
Vulnerabilidade das Fronteiras Geográficas	As ações de defesa cibernética não se limitam a fronteiras geograficamente definidas
Mutabilidade	Não existem leis de comportamento imutáveis no espaço cibernético porque as suas regras são arbitradas pelo homem e não pela natureza
Incerteza	As ações no espaço cibernético podem não gerar os efeitos desejados
Dualidade	As mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas
Paradoxo Tecnológico	Quanto maior é o estágio de desenvolvimento do oponente, maior é sua dependência da Tecnologia da Informação (TI) e, por conseguinte, mais propenso às ameaças cibernéticas. Contudo, ele possuirá maior possibilidade de se defender em virtude de seu alto grau de desenvolvimento tecnológico
Dilema do Atacante	Na descoberta da vulnerabilidade de um determinado sistema, o profissional depara com o dilema entre alertar ou manter em segredo para uso oportuno, explorando-a em um eventual ataque cibernético
Função Acessória	A defesa cibernética é empregada para apoiar a condução de outros tipos de operações
Assimetria	Baseada no desbalanceamento de forças causado pela introdução de um ou mais elementos de ruptura tecnológicos, metodológicos ou procedimentais

Quadro 3 – Características da Defesa Cibernética
Fonte: elaborado a partir de BRASIL, 2013-a, p. 19

dentro do contexto de uma operação de informação ou de inteligência.

Já a atuação Cibernética Operacional/Tática é tipicamente empregada no contexto de uma operação militar, contribuindo para a obtenção do efeito desejado.

As formas de atuação cibernética estão sintetizadas no **Quadro 5**.

Tipos de Ações Cibernéticas

Os tipos de ações cibernéticas são apresentados no **Quadro 6**.

Possibilidades	Limitações
Atuar no espaço cibernético, por meio de ações ofensivas, defensivas e exploratórias	Limitada capacidade de identificação da origem de ataques cibernéticos
Cooperar na produção do conhecimento de inteligência	Existência de vulnerabilidades nos sistemas computacionais
Atingir infraestruturas críticas de um oponente sem limitação de alcance	Dificuldade de identificação de talentos humanos
Cooperar com a Segurança Cibernética nacional	Dificuldade de acompanhar a evolução tecnológica
Cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da Defesa Cibernética	Grande vulnerabilidade a ações de oponentes com poder assimétrico
Obter a surpresa com mais facilidade, baseado na capacidade de inovação	Facilidade de ser surpreendido por inovação tecnológica
Atuar contra oponentes mais fortes, no conceito de guerra assimétrica	
Realizar ações com custos comparativamente menores que as demais operações militares	

Quadro 4 – Possibilidades e limitações da Defesa Cibernética
Fonte: elaborado a partir de BRASIL, 2013-a, p. 20

Operações interagências

Generalidades

Nas operações Interagências, ocorre a interação das Forças Armadas com outras agências, com a finalidade de conciliar interesses e coordenar esforços para a consecução de objetivos ou propósitos convergentes que atendam ao bem comum, evitando a duplicidade de ações, dispersão de recursos e a divergência de soluções com eficiência, eficácia, efetividade e menores custos (BRASIL, 2013, p.1-2).

A revolução tecnológica que o mundo experimenta também contribui para a alteração da natureza dos conflitos. Com essa evolução, muda a forma de fazer política e, consequentemente, a maneira como os estados enfrentam as novas ameaças. Essas mudanças tecnológicas influenciam diretamente a transformação dos conflitos da "Era Industrial" em conflitos da "Era do Conhecimento" (BRASIL, 2013, p.2-1).

Os Estados Nacionais têm enfrentado novas ameaças e riscos, com repercussão nos campos da Segurança e da Defesa, ao mesmo tempo em que seu leque de atribuições tem-se ampliado, na medida em que busca o objetivo de promover o bem comum de toda a sua população (COLÉGIO INTERAMERICANO DE DEFESA, 2008).

No entanto, as organizações que possuem as atribuições legais para enfrentar essas novas ameaças e riscos bem como fornecer o bem-estar a todos parecem não pos-

Forma de atuação cibernética	Política/Estratégica	Operacional/Tática
Nível dos objetivos	Políticos e Estratégicos	Operacionais e Táticos
Foco principal	Obtenção de inteligência	Preparação do campo de batalha
Nível de envolvimento nacional	Interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, ABIN, ANATEL etc.)	Normalmente dentro 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 inovadoras	Duração limitada, com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas

Quadro 5 – Formas de atuação cibernética
Fonte: elaborado a partir de BRASIL, 2013-a, p. 22

suir a capacidade de responder, satisfatoriamente e sozinhas, aos novos desafios que se apresentam (MIGUELETTO, 2001; ALVES, 2009; ZWICK, BORBA, TORRES, 2010; SILVEIRA, 2007).

Por outro lado, a forte tradição de independência das Organizações Públicas tem levado os governantes a mudar a maneira como conduzem a política pública, gerando novas formas de governança com a participação conjunta do setor público, privado e entidades da sociedade na Administração Pública (GONTIJO, 2007; SILVEIRA, 2007; BARBOSA, 2010; MIGUELETTO, 2001).

Diante desse quadro, surge a necessidade de conjugação das capacidades civis e militares com a finalidade de proporcionar ao Estado a necessária competência de solucionar os problemas decorrentes de ameaças e riscos à Segurança & Defesa Nacional e/ou cumprir com suas atribuições.

Tipo	Definição
Exploração Cibernética	Consiste em ações de busca ou coleta, nos sistemas TI de interesse, a fim de obter dados
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
Proteção Cibernética	Abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos e redes de computadores e de comunicações. É uma atividade de caráter permanente

Quadro 6 – Tipos de ações cibernéticas
Fonte: elaborado a partir de BRASIL, 2013-a, p. 23

Nesse contexto, as Forças Armadas têm participado de outras tarefas além das missões tradicionais de defesa da pátria e vêm, progressivamente, atuando em conjunto com várias organizações de níveis governamentais distintos (BRASIL, 2012-c, p.7).

Princípios de Emprego

Os Princípios de Emprego das Operações Interagências são como guia para o planejamento das operações. Em um ambiente onde se busca a sinergia de esforços de várias agências, existe uma série de dificuldades de coordenação.

A fim de se alcançar um resultado de colaboração de todos, as características positivas de cada agência devem ser exploradas, e, para facilitar esse ensejo, são considerados os Princípios de Emprego das Operações Interagências apresentados no **Quadro 7**.

Coordenação entre as agências

Para lidar com a complexidade dos desafios impostos pelas operações desencadeadas no atual ambiente operacional, além de se estabelecerem princípios, é necessário um esforço concertado de todos os instrumentos do Poder Nacional, o que inclui forças militares, organizações governamentais (nacionais e estrangeiras) e agências civis (de governo ou não). Essa integração entre o vetor militar e as estruturas civis é essencial para o êxito das operações (BRASIL, 2013, p.2-4). Assim, as operações interagências demandam ações para a conciliação de interesses e conjugação de esforços civis e militares para a consecução de um objetivo, tarefa, propósito ou missão comum, proporcionando ao Estado a necessária habilidade de solucionar os problemas (CROPPER E COL., 2008a).

Princípio de emprego	Característica
Cooperação	União de esforços na consecução de objetivos comuns
Integração	Sinergia dos esforços por meio do apoio mútuo entre as diversas agências participantes
Complementariedade	Busca pelo que há de melhor em cada agência que integra as operações
Legalidade	As ações devem submeter-se à força imperativa da lei vigente
Adaptabilidade	Capacidade de adaptação às mudanças impostas
Flexibilidade	Busca pelo mínimo de rigidez organizacional das diversas agências que integram um esforço interagências
Elasticidade	Capacidade de inserir novas agências nas operações
Modularidade	Capacidade de pequenos efetivos das agências de atuarem de forma independente, utilizando "módulos"
Simplicidade	Planos claros e de fácil compreensão por todos
Sustentabilidade	Capacidade de se sustentar ativo durante as operações, sempre com o foco no cumprimento da missão imposta
Unidade de esforços	Esforços coordenados em torno da cooperação mútua

Quadro 7 – Princípios de emprego das operações interagências
Fonte: elaborado a partir de BRASIL, 2013, p. 3-4 e 3-5

O emprego das Forças Armadas progressivamente tem ocorrido com maior frequência em um ambiente interorganizacional composto por atores estatais e não estatais, presentes na área de operações, acarretando maior atuação das Forças Armadas em conjunto com outras organizações, seja em conflitos armados ou outro tipo de missão (ARAUJO, 2012, p. 42).

O **Quadro 8** exemplifica, de forma pontual, a estrutura normalmente empregada, nos diversos níveis, quando se estabelece uma operação interagências.

Nesse ambiente interagências, a atuação do Exército pode ocorrer sob a coordenação do Ministério da Defesa (MD), por intermédio do Estado-Maior Conjunto das Forças Armadas (EMCFA), ou de forma singular (BRASIL, 2013 p.2-5).

A coordenação interagências na situação de guerra e não guerra

A coordenação interagências nas situações de guerra e de não guerra é estabelecida em diversos níveis, seja político, estratégico, operacional e tático. Além disso, essa

coordenação se diferencia substancialmente nas situações de guerra e não guerra, em função do ambiente operacional e dos atores envolvidos.

De forma geral, o primeiro nível, o *político*, é coordenado por meio da diretriz presidencial que define a atuação de cada vetor (civil ou militar) participante. Para isso, o diploma legal especifica o ministério ao qual caberá o encargo de coordenar as ações. No caso do emprego das Forças Armadas, caberá ao presidente da República (PR) emitir a diretriz, determinando ao ministro da Defesa (MD) a ativação de comandos (operacionais ou táticos) pertinentes e a designação de um comandante militar (BRASIL, 2013 p.5-2).

O segundo nível, o *estratégico*, é ativado quando houver autorização ou determinação presidencial para emprego de tropa das Forças Armadas, e a coordenação será exercida pelo Ministério da Defesa. O MD, assessorado pelo Estado-Maior Conjunto das Forças Armadas (EMCFA), emitirá a diretriz ministerial (DM) que orientará os trabalhos de planejamento no nível operacional e manterá a comunicação com os atores do nível es-

Forças Armadas, órgãos e agências (órgãos locais federais, estaduais e municipais)			
Estratégico	Ministério da Defesa	Ministérios, secretarias, conselhos, agências reguladoras, autarquias, fundações, diretorias da ABIN, DPF, IBAMA, DPRF, FUNAI, SENASP, FNSP, INFRAERO, RF, CONESP, entre outros	Governadores dos estados, prefeitos dos municípios e CONDEC, dentro outras
	EMCFA		
	Comandos da Marinha, do Exército e da Aeronáutica		
	COMDABRA		
	DECEA		
Operacional	Cmt TO / A Op	Superintendências da ABIN, DPF, IBAMA, PRF, FUNAI, INFRAERO, DRF, das agencias reguladoras	Secretarias de estados e municípios, SEDEC, CORDEC e outros
	Cmdo Cj		
	EM Cmdo Cj		
Tático	FNC, FTC e FAC	Órgãos, agências, instituições executoras integrantes do SISBIN, frações da FNSP, entre outros	OSP
	F Cj		Defesas civis estaduais e municipais (CEDEC e COMDEC)
	FT Cj		Guardas municipais
	DN, C Mil A, COMAR, DE, CINDACTA, CP, OM		Outros

Quadro 8 – Níveis de Planejamento das Estruturas Organizacionais e Agências
Fonte: elaborado a partir de BRASIL, 2013, p. 5-2

tratégico que tratam dos assuntos correlatos na operação (BRASIL, 2013. p.5-2).

O terceiro nível, o *operacional*, é composto pelo Cmt TO/A Op e pelo Estado-Maior Conjunto das Forças Armadas (EMCFA), que elabora o Plano Estratégico de Emprego Conjunto das Forças Armadas (PEECFA). Por meio desse planejamento, a concepção estratégica da operação é transformada em ordens de emprego de meios militares (pessoal e material) de modo a permitir a execução efetiva no próximo nível de coordenação (BRASIL, 2013. p.5-3).

O quarto e último nível, o *tático*, é coordenado pelo comandante da Força Terrestre Componente (FTC), a quem compete estabelecer, explorar e manter a coordenação com os participantes (civis e militares) da operação e com o sistema Exército (BRASIL, 2013 p.5-4).

Uma das principais diferenças entre a **Figura 3** e a **Figura 4** é o processo de solicitação de emprego, que, na situação de não guerra, pode ser iniciado por outras esferas que não o Executivo Federal, possibilidade não prevista na situação de guerra.

Características e Atribuições dos Órgãos: uma sistematização

Com o intuito de sistematizarmos as características e informações sobre órgãos relacionados, direta ou indiretamente, à Defesa no Brasil, elaboramos o **Quadro 9**, apresentando os principais órgãos envolvidos nas operações interagências e suas atribuições. Esse quadro, quando visto em superposição aos organogramas das figuras **3** e **4**, permitirá uma visão panorâmica dessas operações.

Nesse contexto, a arte da guerra depara com novos desafios e complexidades, potencializados pela facilidade de acesso às novas tecnologias, pela socialização da Internet, pelo surgimento das redes sociais e pela atuação da mídia (BRASIL, 2013, p. 2-1). Se, por um lado, há inúmeros benefícios, por outro, também surgem infinitas oportunidades para ameaças. Em algum momento, a liberdade e a segurança ficam em lados conflitantes. Contudo, sob a luz do contrato social, o equilíbrio salutar deverá ser buscado, constantemente — o que não é fácil.

Coordenação e controle das operações interagências: restringindo o sistema

Nas operações militares, a *unidade de esforços* é assegurada por meio da *unidade de comando*, que é baseada na designação de um único comandante com a autoridade para dirigir e coordenar os esforços de todas as forças subordinadas em busca de um objetivo comum.

A aplicação decisiva do poder de combate exige unidade de comando e possibilita a unidade de esforços, pela coordenação de todas as forças e cooperação das agências, de forma integrada, no amplo espectro dos conflitos sobre um objetivo comum (BRASIL, 2014, p. 5-5).

Assim sendo, a combinação dos meios, a convergência de esforços e a interoperabilidade são essenciais para obtenção do máximo rendimento das forças disponíveis. Para cada operação, a obtenção da unidade de comando e unidade de esforços é condição essencial para o êxito (BRASIL, 2014, p. 5-5).

Nas operações desencadeadas no ambiente interagências, que envolvem parcei-

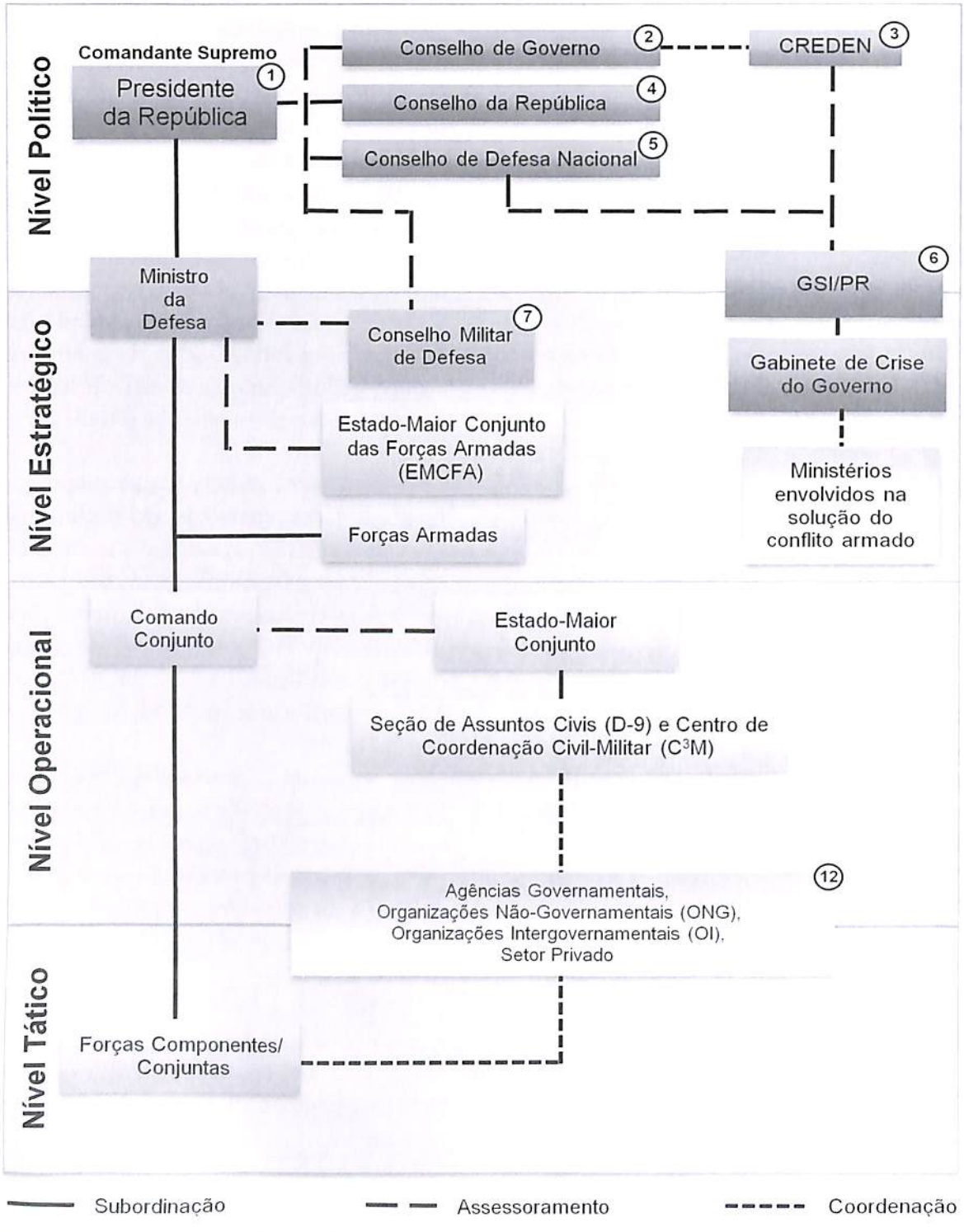

Figura 3 – Organograma da coordenação interagências na situação de guerra
Fonte: BRASIL, 2013, p. A1

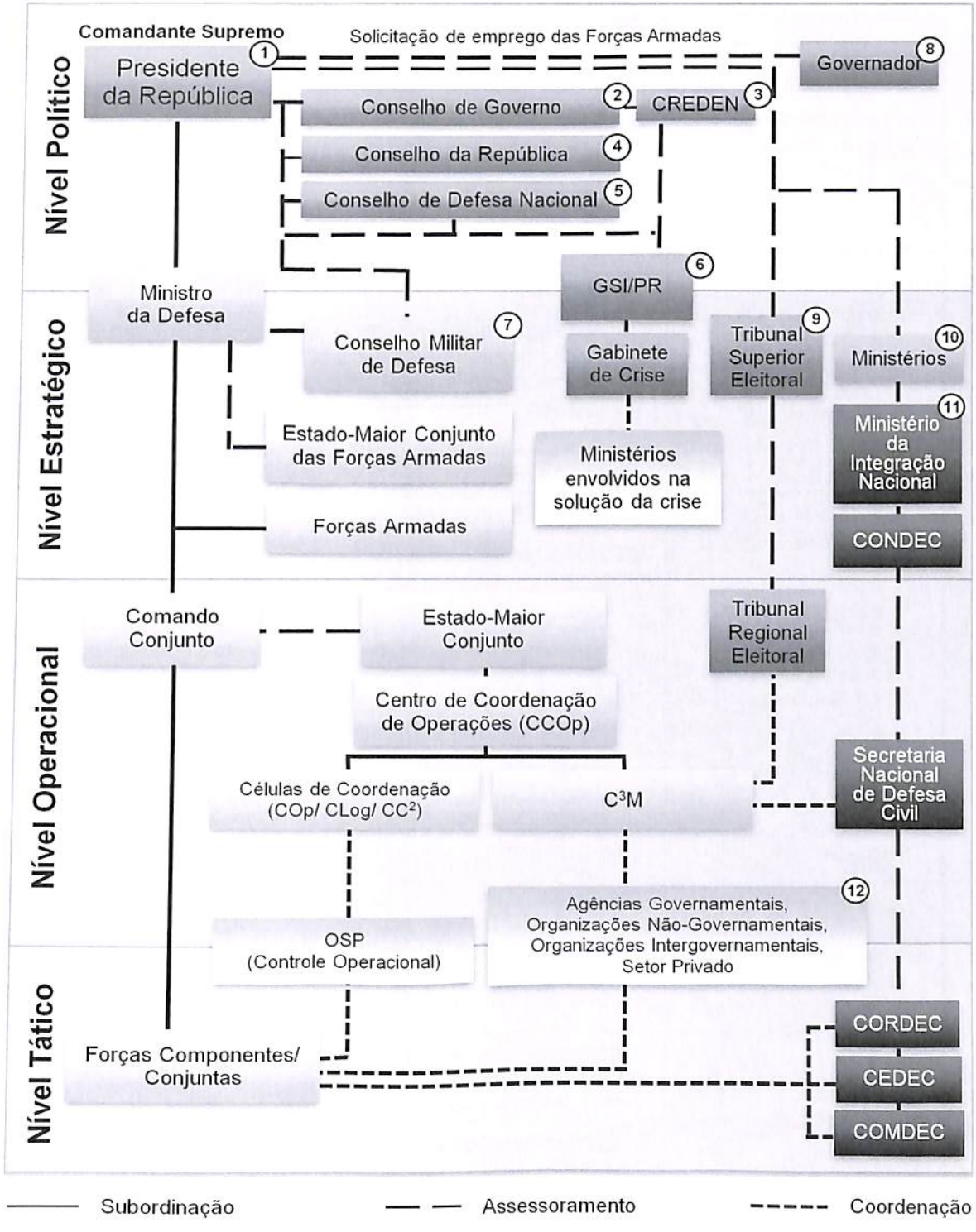

Figura 4 – Organograma da Coordenação interagências na situação de não guerra
Fonte: BRASIL, 2013, p. A2

Órgão	Característica
Câmara de Relações Exteriores e Defesa Nacional (CREDEN)	1. Finalidade: formular políticas públicas e diretrizes relacionadas às Relações Exteriores e Defesa Nacional 2. Integrada pelos Chefes do GSIPR, que a presidirá, da Casa Civil da Presidência da República e pelos Ministros do MJ, MD, MRE, MCTI, MPOG e MMA 3. São convidados, em caráter permanente, os comandantes da Marinha, do Exército e da Aeronáutica
Conselho da República	1. Presidido pelo presidente da República 2. Participantes: vice-presidente da República, presidente da Câmara dos Deputados, presidente do Senado Federal, líderes da maioria e da minoria na Câmara dos Deputados, líderes da maioria e da minoria no Senado Federal, ministro da Justiça e seis cidadãos brasileiros natos 3. Compete se pronunciar sobre intervenção federal, estado de defesa e estado de sítio e as questões relevantes
Conselho de Defesa Nacional	1. Presidido pelo presidente da República 2. É o órgão superior de consulta do presidente nos assuntos relacionados à soberania e à defesa do Estado democrático 3. Participantes: o Vice-presidente, o presidente da Câmara dos Deputados e do Senado Federal, os ministros da Justiça, da Defesa, das Relações Exteriores, do Planejamento, Orçamento e Gestão e os comandantes das três Forças 4. Compete ao Conselho opinar nas hipóteses de declaração de guerra e de celebração da paz, sobre a decretação do estado de defesa, do estado de sítio e da intervenção federal
Gabinete de Segurança Institucional da Presidência da República (GSI-PR)	1. Compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições 2. Prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional
Conselho Militar de Defesa	1. Assessorar o presidente no que concerne ao emprego de meios militares e o ministro da Defesa no que concerne aos demais assuntos pertinentes à área militar 2. É composto pelos comandantes da Marinha, do Exército e da Aeronáutica e pelo chefe do Estado-Maior Conjunto das Forças Armadas

Quadro 9 – Características e atribuições dos órgãos
Fonte: elaborado a partir de BRASIL, 2013, p. A-3

ros e outros vetores, o comandante militar não comanda todos os atores em presença. Dessa forma, ele busca a cooperação e constrói o consenso para alcançar a almejada *unidade de esforços*, por meio da coordenação Interagências (BRASIL, 2013, p. 6-3).

Competências na Defesa Cibernética brasileira

Nesta seção, buscamos apresentar um acoplamento entre o que foi visto sobre defesa e operações interagências, tendo como base sua aplicação no (e a partir do) ambiente cibernético.

No contexto do Ministério da Defesa, as ações no espaço cibernético deverão ter as denominações apresentadas na **Figura 5** e no **Quadro 10**, de acordo com o nível de decisão.

Os órgãos de estado e de governo que apresentam atividades relacionadas ao Setor Cibernético são: o Conselho de Defesa Nacional (CDN), Câmara de Relações Exteriores e Defesa Nacional (CREDEN), Casa Civil da Presidência da República, Gabinete de Segurança Institucional da Presidência da República (GSI-PR), Departamento de Segurança da Informação e Comunicações (DSIC), Agência Brasileira de Inteligência (ABIN) (CARVALHO, 2011, p.10).

A estruturação do Setor Cibernético se insere em um contexto de atuação de diversos órgãos brasileiros. Em 27 de outubro de 2014, por meio da Portaria Normativa Nº 2.777-MD, foram estabelecidas as diretrizes de implanta-

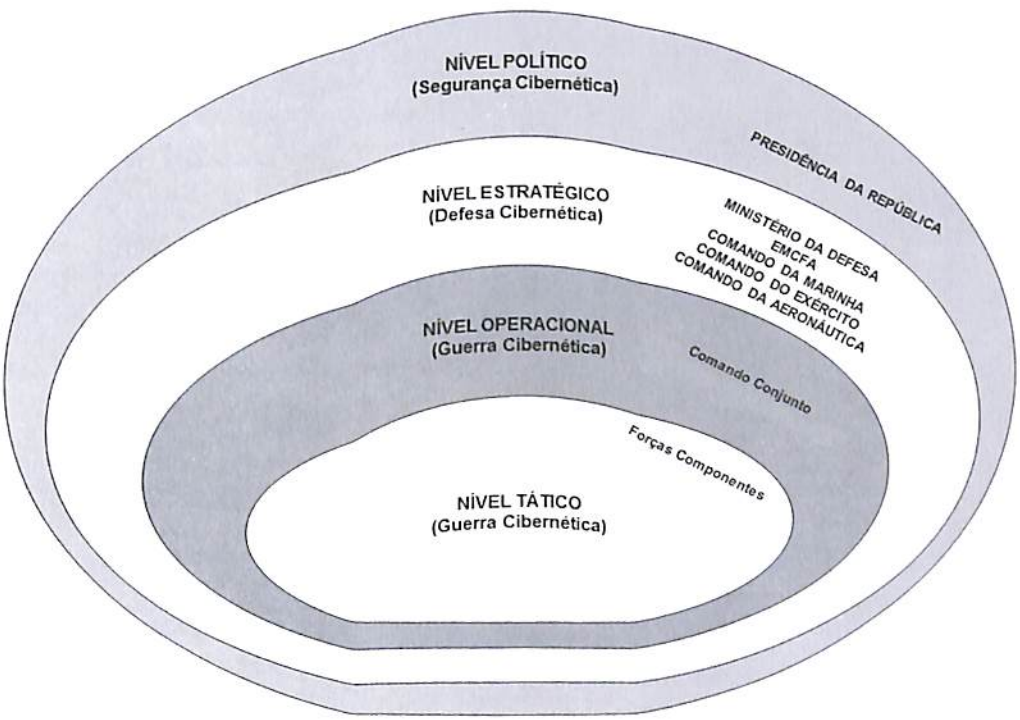

Figura 5 – Níveis de decisão
Fonte: elaborado a partir de BRASIL, 2013a, p. 32

Nível	Atribuições
Nível político	Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, coordenadas pela Presidência da República (PR) e abrangendo a Administração Pública Federal (APF) direta e indireta, bem como as infraestruturas críticas da informação dos setores público e privado
Nível estratégico	Defesa Cibernética, a cargo do Ministério da Defesa, interagindo com a PR e APF
Níveis operacional e tático	Guerra Cibernética, denominação restrita ao âmbito interno das Forças Armadas

Quadro 10 – Atribuições segundo os níveis de decisão
Fonte: elaborado a partir de BRASIL, 2013a, p. 32

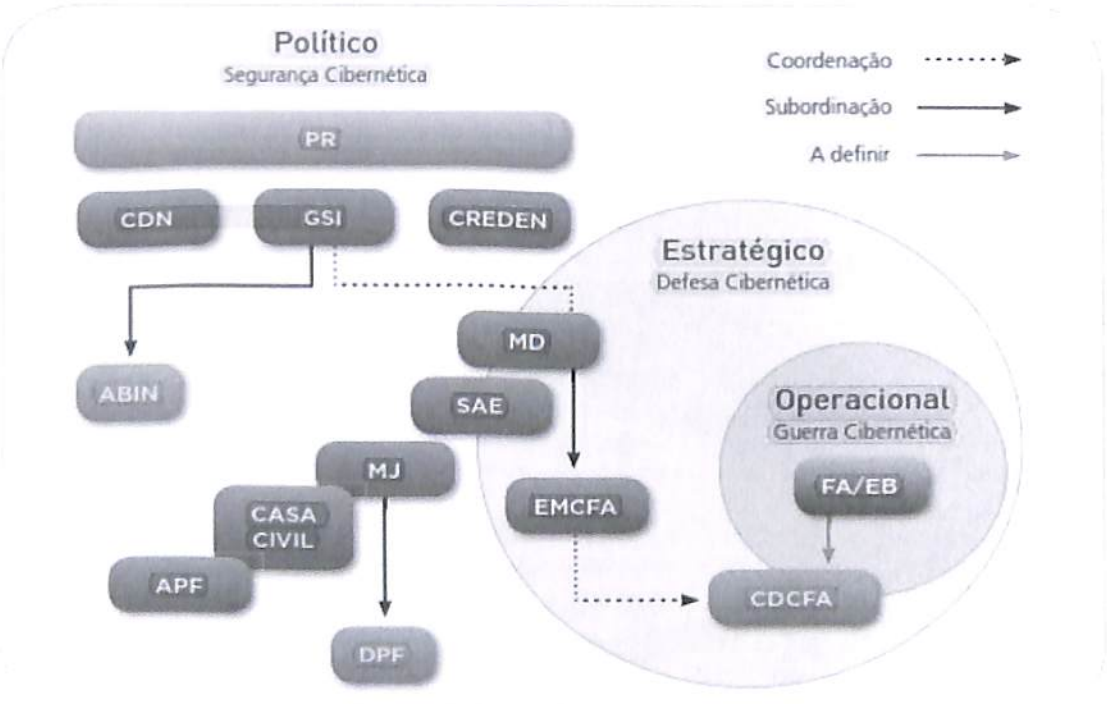

Figura 6 – Sistema de Segurança e Defesa Cibernética Brasileiro
Fonte: FERREIRA NETO, 2013 apud BARROS; GOMES, 2011 p. 138

ção de medidas visando à potencialização da Defesa Cibernética Nacional. Nesse sentido, foram estabelecidas, dentre outras, as seguintes iniciativas: criação do Comando de Defesa Cibernética (ComDCiber) na Estrutura Regimental do Comando do Exército, que contará, na forma da legislação, com o exercício de militares das três Forças Armadas, cabendo ao EMCFA as atividades de coordenação nos casos de operações conjuntas, especificando-se, em atos próprios, os aspectos inerentes ao controle operacional; e a criação da Escola Nacional de Defesa Cibernética na Estrutura Regimental do Comando do Exército, que contará, na forma da legislação, com o exercício de militares das três Forças Armadas.

Das atribuições gerais e específicas apresentadas, somada a criação do ComDCiber, chegamos à conclusão de que, no caso da Defesa Cibernética, o Comando Operacional da Defesa Cibernética será coordenado pelo ComDCiber, apoiado pelos órgãos apresentados na **Figura 7**.

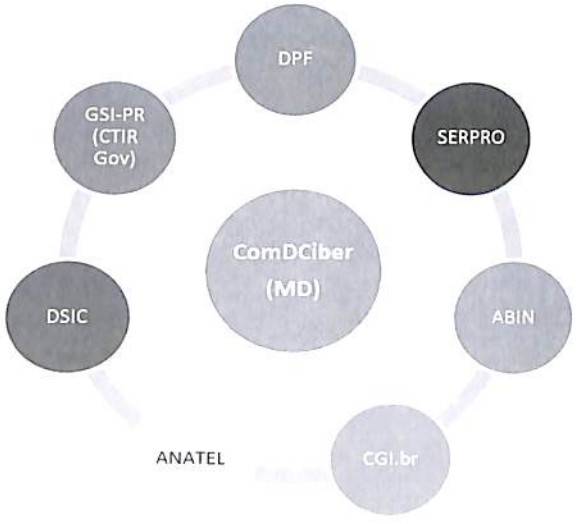

Figura 7 – Coordenação operacional da Defesa Cibernética

Fonte: elaborado a partir de BRASIL, 2013a, p. 32

Conclusão e recomendações

Este trabalho teve como objetivo principal destacar a importância da definição sobre a distribuição de competências da Defesa Cibernética, no âmbito das operações interagências.

Setor estratégico para a soberania de um Estado da estatura geopolítica do Brasil, a Defesa Cibernética encontra-se, atualmente, em pleno processo de consolidação, de modo que possa assegurar ao país que seus objetivos como nação soberana, em um panorama internacional cada vez mais complexo e difuso, possam ser conquistados.

Para atingir este objetivo, dividimos o trabalho em seções, que, após a análise durante sua construção, confirmaram a hipótese inicial formulada:

> No Brasil, as atribuições e as competências dos órgãos que atuam nas operações interagências são distribuídas e obedecem à divisão entre os setores político, estratégico, operacional e tático.

Ainda, pelo estudo das experiências recentes, podemos afirmar que é possível haver essa distribuição e que esta vem funcionando com êxito, apesar de diagnosticadas oportunidades de melhoria.

O item *Operações inter*agências apresentou um histórico e conceitos diversos sobre defesa cibernética. Nele, foi verificado que o tema é relevante, contemporâneo e necessário, e que vem sendo conduzido por meio das Forças Armadas, especificamente pelo Exército Brasileiro.

Além disso, identificamos, por meio do Projeto Nr 6 do Livro Branco de Defesa Nacional (Projeto sistema de proteção ciber-

nética – defesa cibernética), a importância que o Estado Brasileiro vem dando ao tema, incluindo o necessário aporte financeiro e, por conseguinte, orçamentário.

Ainda nessa fase, podemos perceber a importância da defesa cibernética no cenário atual, sobretudo em função da dependência das informações organizadas no ciberespaço para o desenvolvimento nacional. Verificamos também a marcante integração existente entre o EB e outras agências, sobretudo governamentais, visando ao desenvolvimento e ao fortalecimento do setor cibernético.

No tópico seguinte, o trabalho discorreu sobre as operações interagências, que visam conciliar interesses e coordenar esforços para a consecução de objetivos ou propósitos convergentes, que atendam ao bem comum, evitando a duplicidade de ações, dispersão de recursos e a divergência de soluções. Assim, verificou-se a necessidade da conjugação de capacidades civis e militares com a finalidade de favorecer a solução de problemas. Abordamos tópicos descritos no Manual de Operações em Ambientes Interagências, editado em 2013, sobretudo os que tratam da coordenação em situações diversas.

Por último, identificamos as competências das diversas agências ligadas especificamente à defesa cibernética. Esse tipo de atividade, embora em ambiente diverso, somente é assegurado por meio da *unidade de comando*, o que favorece a unificação de esforços. Nessa parte, foram identificadas as atribuições gerais e as missões específicas dos diversos órgãos e agências que participam direta ou indiretamente na Defesa Cibernética. Para a elaboração desse quadro, foram utilizadas como base as missões precípuas das entidades e artigos de renomados autores da área.

No contexto da Defesa Cibernética, ficou evidenciado que o comando da operação será do MD, por meio do Comando de Defesa Cibernética. O ComDCiber coordenará todas as atividades de Defesa Cibernética e será apoiado por diversos órgãos governamentais, como o GSI-PR (CTIR Gov), DSIC, DPF, ANATEL, SERPRO, ABIN e CGI.br.

Dessa forma, a recente criação do ComDCiber, órgão central do Sistema Cibernético Brasileiro, está alinhado com o objetivo desse trabalho, que é a identificação da importância da distribuição de competências e atribuições no contexto da Defesa Cibernética. Esse órgão favorecerá sobremaneira a ordenação das operações interagências, por ser o grande administrador das agências em atividades de Defesa Cibernética.

Além disso, a criação do ComDCiber se alinha com os princípios de emprego da defesa cibernética, que são, em suma, para assegurar a unidade de esforços. Esses princípios são fundamentais nas operações interagências, em virtude da necessidade de coordenação e integração de órgãos que não operam em conjunto constantemente.

Ainda, em razão de as diversas agências e órgãos possuírem estrutura de segurança cibernética preestabelecidas para uma situação de normalidade, o ComDCiber vem buscando estabelecer a coordenação em situações especiais, em particular no caso de defesa cibernética, que é o foco deste trabalho, a fim de se evitarem a sobreposição de atribuições e o desperdício de tempo e de recursos orçamentários.

Ações estratégicas de médio e longo prazo, capitaneadas pelo Governo brasileiro, por meio do Exército, estão sendo colocadas em prática, sobretudo em função da crescente projeção brasileira no cenário internacional.

Um grande marco foi a elaboração da Estratégia Nacional de Defesa, a qual define três setores estratégicos para a Defesa Nacional, sendo o cibernético um desses setores. Em função disso, o controle do espaço cibernético se tornou um objetivo estratégico do Estado brasileiro. Além disso, o momento é propício, pois a sociedade, academia e o meio político têm-se conscientizado, gradativamente, da importância dos assuntos relacionados à defesa para um país do porte do Brasil.

Por fim, concluímos que o controle do espaço cibernético é uma condição indispensável para o fortalecimento da soberania e para a concretização dos interesses do país no cenário político internacional, pois é a partir do ciberespaço que se aumenta a probabilidade de êxito nas operações realizadas nos espaços tradicionais. Da mesma forma, o controle dessa ferramenta proporciona, certamente, uma grande chance de sucesso nas evidenciadas hipóteses e visões — confirmadas ou não — sobre a guerra do futuro.

Referências

ALVES, André Hiroshi Hayashi. **Características das Redes e Vínculos de Cooperação entre o Tribunal de Contas da União e Outras Organizações na área de Treinamento, Desenvolvimento e Educação.** 2009. Monografia (Especialização em Gestão da Educação Corporativa) – Universidade Gama Filho, Tribunal de Contas da União, Instituto Serzedello Corrêa, Brasília, DF, 2009.

ALVES-MAZZOTTI, Alda Judith; GEWANDSZNAJDER, Fernando. **O método nas ciências naturais e sociais: pesquisa quantitativa e qualitativa.** São Paulo: Pioneira Thomsom Learning, 2001.

ARAUJO, A. P. **O emprego das Forças Armadas em desastres naturais, com ênfase na coordenação interorganizacional.** 2012. Tese (Doutorado em Ciências Militares) – Escola de Comando e Estado-Maior, Rio de Janeiro 2012.

BARBOSA, Sheila Cristina Tolentino. **Implementação de Programas Públicos Federais: Caráter da Coordenação Interorganizacional**. 2010. 190 f. Tese (Doutorado em Administração) – Universidade de Brasília, Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Brasília, DF, 2010.

BRASIL. Exército. Escola de Comando e Estado-Maior do Exército. **Manual Escolar de trabalhos acadêmicos na ECEME.** Rio de Janeiro, RJ, 2004.

BRASIL, Ministério da Defesa. **Glossário das Forças Armadas** (MD35-G-01); Brasília, DF, 2007.

BRASIL, GSIPR. DSIC. **Livro verde de segurança cibernética**. Brasília, DF, 2010.

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

BRASIL, Ministério da Defesa. MD. **Estratégia Nacional de Defesa**, Brasília, DF, 2012 a.

BRASIL, Presidência da República. **Livro Branco de Defesa Nacional**, Brasília, 2012 b.

BRASIL. Exército. Escola de Comando e Estado-Maior do Exército. **Análise de Operação Militar Executada em um Ambiente Interagências – OPERAÇÃO ITAJAÍ-AÇU**. Rio de Janeiro, RJ, 2012 c.

BRASIL. Ministério da Defesa. **Operações em ambientes interagências**. 1. ed. Brasília, DF, 2013.

BRASIL, Ministério da Defesa. **Minuta da publicação "Doutrina Cibernética de Defesa"** Brasília, DF, 2013 a.

BRASIL, Ministério da Defesa. **Política Nacional de Defesa Cibernética**, Brasília, DF, 2013 b.

BRASIL, Ministério da Defesa. **Doutrina Militar Terrestre**, 1. ed. Brasília, DF, 2014.

BUZAN Barry. **People, States and Fear: an Agenda for Security Studies in the Post-Cold War Era**. Londres: Wheatsheaf, 1991.

CARMO, Euzimar K. do. **O Sistema de Defesa Cibernético Brasileiro** – uma proposta. 2011. 135 f. Trabalho de Conclusão (Curso de Especialização em Gestão de Segurança da Informação e Comunicação) – Instituto de Ciências Exatas, Universidade de Brasília. 2011.

CARNEIRO, J. M. E **A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro**. 2012. Tese (Doutorado em Ciências Militares) – Escola de Comando e Estado-Maior, Rio de Janeiro 2012.

CARVALHO, Paulo S M. **O setor cibernético nas Forças Armadas Brasileiras**. Artigo publicado em Desafios estratégicos para a segurança e defesa cibernética, 1. Ed. Brasília 2011.

CARVALHO, Paulo S M. **A defesa cibernética e as infraestruturas críticas nacionais**. Artigo publicado no X Ciclo de Estudos Estratégicos, Rio de Janeiro, 2011 a.

CARRION, Alexandre L M. Exército. Escola de Comando e Estado-Maior do Exército. **Segurança e defesa cibernética no Brasil**. Rio de janeiro, RJ, 2013.

CASEMIRO FILHO, M. **A Guerra cibernética: uma proposta de elementos para formulação doutrinaria do Exército Brasileiro**. Tese de doutorado, Brasília, 2010.

CLARKE, R. A.; KNAKE, R. **Cyber War – The Next Threat to National Security and What to do About it**. HarperCollins: New York, 2010.

COLÉGIO INTERAMERICANO DE DEFESA. **As relações civis-militares no contexto interagências**. Washington, 2008.

CORBARI; **Operações Interagências e a Coordenação Interorganizacional na Guerra do Afeganistão**. Rio de Janeiro, RJ, 2012.

CROPPER, S.; EBERS, M.; HUXHAM, C.; RING, P.S. **Introducing Inter-organizational Relations.** In: _____.(Eds.), The oxford handbook of inter-organizational relations. New York: Oxford University Press Inc. (p. 3-21), 2008a.

CRUZ, Ricardo H. P. da. Escola de Comando e Estado-Maior do Exército. **A defesa e segurança cibernética – Concepção de Emprego**. Rio de Janeiro, RJ, 2013.

EPSTEIN, Isaac. **Cibernética**. São Paulo: Ática. 1986.

ESG, Escola Superior de Guerra. **Manual Básico - Volume I Elementos Fundamentais**. Rio de Janeiro, 2014.

FERREIRA NETO, Walfredo Bento. **Por uma Geopolítica Cibernética: apontamentos da Grande Estratégia brasileira para uma nova dimensão da guerra**. Niterói, RJ, 211f. Dissertação (Mestrado em Estudos Estratégicos). Universidade Federal Fluminense, 2013.

GONTIJO, José Geraldo Leandro. **Políticas Públicas para a Juventude: a atuação da Secretaria Nacional de Juventude durante o primeiro mandato do Governo Lula**. 2007. Dissertação (Mestrado em Políticas Públicas) Universidade Federal de Minas Gerais, Departamento de Ciência Política, Belo Horizonte, 2007.

KIM, Joon Ho. **Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural**. Dissertação (Mestrado em Antropologia Social) Universidade de São Paulo, 2004.

JOHNSON, Robert A. "Como Prever a Guerra do Futuro". In: **Military Review**, t. 70, n. 4, jul.-ago., 2015.

MANDARINO, Jr Rafael. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**, Brasília, 2009.

MARQUES, Adriana; MEDEIROS FILHO, Oscar. **Entre a "defesa integral" e a "segurança democrática"**: uma análise de duas doutrinas militares no canto noroeste do subcontinente sul-americano. In: ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 5., Anais... Fortaleza: ABED, 2011.

MIGUELETTO, Danielle Costa Reis. **Organizações em Rede**. 2001. Dissertação (Mestrado em Administração Pública) – Fundação Getúlio Vargas, Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro 2001.

NYE, Joseph S. **O Futuro do Poder**. São Paulo: Benvirá, 2012.

POMPEU, Alessandro. **A estratégia nacional de defesa e o setor cibernético**, Brasília 2012.

ROCHA, A. R.; **Análise de operação militar executada em um ambiente interagência – Operação Itajaí-Açu**, Rio de Janeiro, RJ, 2012.

SILVA, O. C. C. Universidade Católica de Brasília, **A segurança e as ameaças cibernéticas**, Brasília 2011.

SILVEIRA, Henrique Flávio Rodrigues da. **Planejamento governamental e coordenação interorganizacional – um espaço para aplicação de organizações virtuais no setor público?** Caderno de Finanças Públicas, Brasília, n.8, p. 123-179, dez. 2007.

ZWICK, Elisa; BORBA, Érika Loureiro; TORRES, Kelly Aparecida. **Redes interorganizacionais na administração pública brasileira – formação e aspectos culturais**. In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 7., 2010, Local. Anais... Resende, RJ: Associação Educacional. Dom Bosco, 2010, v. VII, p. 276-289.

NR: A adequação das referências às prescrições da Associação Brasileira de Normas Técnicas (ABNT) é de exclusiva responsabilidade dos articulistas.