ESCOLA DE GUERRA NAVAL

CC (FN) CARLOS ROCHA DE LIMA

A CONSTRUÇÃO DO SISTEMA INSTITUCIONAL DE DEFESA E SEGURANÇA CIBERNÉTICA:

fundamentos, desenvolvimento e consolidação para enfrentar os desafios do século XXI

Rio de Janeiro

2019

CC (FN) CARLOS ROCHA DE LIMA

A CONSTRUÇÃO DO SISTEMA INSTITUCIONAL DE DEFESA E SEGURANÇA CIBERNÉTICA:

fundamentos, desenvolvimento e consolidação para enfrentar os desafios do século XXI

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF (RM1) Ohara Barbosa Nagashima

Rio de Janeiro

Escola de Guerra Naval

2019

AGRADECIMENTOS

Primeiramente, rendo minha gratidão a Deus por proporcionar-me saúde e inspiração para superar esta longa e desafiadora jornada de pesquisa e estudo. Sem a ajuda Dele eu não sou nada. À minha amada esposa, Ingrid, pessoa mais importantes da minha vida, que me proporcionou todos os recursos necessários para um ambiente propício à realização desta pesquisa. Não há palavras que expressem o nível de gratidão e amor que tenho por você. Muito obrigado!

Ao meu orientador, CF (RM1) Ohara Barbosa Nagashima, pelo seu apoio e inspiração no amadurecimento dos meus conhecimentos e conceitos que me levaram à conclusão desta monografia. Aos amigos Zarath e Nachard pela oportunidade de convívio e, em especial, ao amigo Renato que, com muita paciência e atenção, dedicou um pedaço do seu tempo para me apoiar e incentivar durante todo o curso, tanto nesta pesquisa quanto no nosso cotidiano de aulas presenciais.

Aos meus companheiros do C-EMOS 2019 que contribuíram para que eu pudesse subir mais este degrau. Vocês são os profissionais que me inspiram diariamente.

RESUMO

Este trabalho teve por finalidade descrever e analisar a construção e a evolução das Políticas Públicas de Defesa e Segurança, bem como a criação e a consolidação dos programas e das organizações físicas do setor cibernético que nortearam a edificação do atual Sistema Institucional Defesa e Segurança Cibernética, para responder ao seguinte questionamento: em face das políticas e estruturas cibernéticas em funcionamento, o Estado Brasileiro está capacitado para enfrentar as ameaças cibernéticas que comprometam a soberania e defesa nacional? De modo a responder à pergunta proposta, este trabalho se baseou na pesquisa bibliográfica, utilizando a abordagem descritiva, por meio da coleta e análise de dados. Neste sentido, foram examinados os aspectos mais relevantes da edificação e do desenvolvimento de três documentos Estratégicos de Defesa e Segurança Nacional de mais alto nível político, quais sejam: a Política de Defesa Nacional, a Estratégia Nacional de Defesa e o Livro Branco de Defesa, que constituem um eixo estruturante e normativo para fundamentar todas as questões contendo o tema defesa nacional. Salienta-se que as Políticas Públicas de Defesa pós-regime militar se desenvolveram com uma nova visão geopolítica do Estado Brasileiro. Assim, a temática cibernética foi efetivamente incorporada a partir da publicação da Política de Defesa Nacional de 2005. Posteriormente, a Estratégia Nacional de Defesa de 2008 consolidou o setor cibernético como estratégico e precípuo para a defesa e segurança nacional. Dentro dessa conjuntura, o Ministério da Defesa, no que tange à sistematização e à articulação das esferas da defesa, divulgou a Diretriz Ministerial n° 14/2009, estabelecendo a responsabilidade pela coordenação e pela integração do setor cibernético ao Exército. A Implantação do desse setor no Exército foi materializada com a inclusão do Centro de Defesa Cibernética na Estrutura Regimental do Comando do Exército, visando a preencher a carência de um órgão com a competência de desempenhar a governança de maneira colaborativa, entre os vetores componentes da defesa no campo cibernético. O centro recebeu a missão de coordenar e integrar as atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, relacionadas à detecção das ameaças virtuais e ao aprimoramento dos recursos humanos usados na defesa do espaço cibernético. No Brasil, as ações nesse espaço são divididas em três níveis de decisão. No nível político a Segurança da Informação e Comunicações, a Segurança Cibernética e a Segurança das Infraestruturas Nacionais são coordenadas pelo Gabinete de Segurança Institucional da Presidência da República, abrangendo a Administração Pública Federal direta e indireta. Já no nível estratégico, a Defesa Cibernética está a cargo do Ministério da Defesa, do Estado-Maior Conjunto das Forças Armadas e dos Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal. Nos níveis operacional e tático, a Guerra Cibernética é restrita ao âmbito interno dos Comandos das três Forças. As diretrizes técnico-estratégicas do Livro Verde de Segurança Cibernética e da Política Cibernética de Defesa, programas de desenvolvimento do setor cibernético, enfatizam a importância de proteger dentro do espaço cibernético as ações de segurança da informação e comunicação. Assim sendo, pode-se concluir que as estruturas e organizações, bem como as Políticas Públicas de Defesa adotadas pelo Brasil são muito apropriadas e adequadas não apenas no contexto da afirmação da capacidade brasileira perante o mundo, mas também para preparar o Estado para defender seus interesses no espaço cibernético e proteger suas infraestruturas críticas nacionais contra ataques cibernéticos.

Palavras-chave: Sistema Institucional de Defesa e Segurança Cibernética. Políticas Públicas de Defesa. Defesa Cibernética. Segurança Cibernética. Espaço Cibernético.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

APF – Administração Pública Federal

CDCiber – Centro de Defesa Cibernética

CDN – Conselho de Defesa Nacional

CIA – Agência Central de Inteligência dos EUA

ComDCiber – Comando de Defesa Cibernética

CPI – Comissão Parlamentar de Inquérito

CREDEN – Câmara de Relações Exteriores e Defesa Nacional

DSIC – Departamento de Segurança da Informação e Comunicações

EB – Exército Brasileiro

EMCFA – Estado-Maior Conjunto das Forças Armadas

ENaDCiber – Escola Nacional de Defesa Cibernética

END – Estratégia Nacional de Defesa

ESG – Escola Superior de Guerra

EUA – Estados Unidos da América

FA – Forças Armadas

FAB – Força Aérea Brasileira

GSI-PR – Gabinete de Segurança Institucional do Presidente da República

INMETRO – Instituto Nacional de Metrologia, Qualidade e Tecnologia

LBDN – Livro Branco de Defesa Nacional

LC – Lei Complementar

MB – Marinha do Brasil

MD – Ministério da Defesa

MP – Medida Provisória

MRE – Ministério das Relações Exteriores

NSA – *National Security Agency*

NuCDCiber – Núcleo do Centro de Defesa Cibernética

OND – Objetivo Nacional de Defesa

OEA – Organização dos Estados Americanos

PNSC – Política Nacional de Segurança Cibernética

PDC – Política de Defesa Cibernética

PDN – Política de Defesa Nacional

PND – Política Nacional de Defesa

PNSI – Política Nacional de Segurança da Informação

St Ciber – Setor Cibernético

SMDC – Sistema Militar de Defesa Cibernética

Sisbin – Sistema Brasileiro de Inteligência

SIC – Sistema de Informação e Comunicação

TI – Tecnologia da Informação

TIC – Tecnologias de Informações e Comunicação

SUMÁRIO

1 INTRODUÇÃO

O término da Guerra Fria (1947-1989), simbolizado pela queda do muro de Berlim, intensificou o andamento de intensas e complexas mudanças nas relações econômicas, culturais, políticas, militares e sociais no seio do Sistema Internacional. Essas alterações estabeleceram a hegemonia do Capitalismo financeiro globalizado como um dos fatores preponderantes na edificação da nova Ordem Global.

Nesse sentido, a recente ordem caracteriza uma nova composição geopolítica no plano mundial, sobreposta a um mundo instável, competitivo e repleto de incertezas. As transformações ocorridas promoveram um incremento na liberdade para os fluxos de bens, serviços, capital, pessoas, informação, dados e tecnologia entre os Estados. Além disso, impulsionaram o aparecimento de diferentes atores, tais como as empresas multinacionais, os mercados regionais, a mídia global e as organizações não governamentais, dentre outros.

O processo de globalização[1], aliado à nova era da Tecnologia da Informação[2] (TI), aumentou a interdependência econômica dos países e possibilitou o surgimento de novos meios para realizar a troca de informações, dotados de tecnologia com ciclo de vida muito rápido, sem controle do Estado e sem vínculo nacionais. Assim, a imensa popularização do computador pessoal e da internet permitiram a comunicação e a distribuição de informação entre diferentes pessoas, Estados, organizações e instituições dos mais variados rincões do planeta.

O aparecimento das Tecnologias de Informações e Comunicação (TIC) abrangeu a sociedade em praticamente todos as suas esferas e possibilitou a emergência do que se pode denominar de sociedade informacional ou sociedade da informação. Para autores como Jorge Werthein (2000), o conceito de sociedade informacional surgiu para substituir o conceito de

---

[1] É um processo histórico que envolve ampliação, aprofundamento, aceleração e impacto crescente de interconexão em nível mundial (PECEQUILO, 2004, p. 48).

[2] TI (Tecnologia da Informação) – É o conjunto de todas as atividades e soluções providas por recursos de computação que visam permitir a produção, armazenamento, transmissão, acesso e o uso das informações. (ALECRIM, 2011).

sociedade pós-industrial e como forma de assimilar a aparecimento de um novo paradigma técnico-econômico. Portanto, potencializado pelo uso intenso das tecnologias da informação e comunicação nas atividades diárias, sua ideia central engloba mudanças sociais nos mais diversos campos da atividade humana.

Percebe-se que a sociedade contemporânea está se transformando de uma maneira mais acelerada do que a capacidade de adaptação do Estado. Isso porque os governos têm criado um conjunto regulatório, traduzidos em políticas públicas, leis, diretrizes e órgãos estatais, visando a disciplinar o novo espaço virtual chamado de espaço cibernético[3], bem como a impedir ou minimizar a exploração das vulnerabilidades da TI sobre as infraestruturas críticas[4] do Estado.

Depreende-se, desse cenário, que a criação do espaço cibernético alterou profundamente as relações internacionais em face das delimitações de fronteiras não serem mais aplicadas nesse espaço. Assim, as novas ameaças cibernéticas[5], fruto da exploração de vulnerabilidades podem ser realizadas por Estados, organizações não estatais e até mesmo pequenos grupos, com as mais diversas motivações. Como consequência, imensos riscos e perigos ligados ao funcionamento legal e harmônico do Estado podem ser gerados.

O Brasil tem buscado inserir o aspecto cibernético[6] na agenda nacional, especialmente nas questões de defesa e segurança, e elaborar um planejamento de longo prazo para o Estado. Com o fim do Regime Militar (1964-1986) e a publicação da Constituição de

---

[3] Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e ou armazenadas (BRASIL, 2014a, p. 18).

[4] Instalações, serviços, bens e sistemas cuja interrupção ou destruição total ou parcial, provoque sério impacto social, ambiental, político, internacional ou à segurança do Estado e da Sociedade (BRASIL, 2014a, p.19).

[5] Causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse. (BRASIL, 2014a, p. 18).

[6] 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 (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais (Brasil, 2014a, p. 18).

1988, os rumos da política brasileira sofreram alterações nas relações civis-militares, inclusive ensejando uma nova visão geopolítica do Governo.

Essas mudanças refletiram na área da defesa e segurança nacional tanto institucionalmente, com a formação do Ministério da Defesa (MD), do Estado-Maior Conjunto das Forças Armadas (EMCFA) e da Câmara de Relações Exteriores e Defesa Nacional[7] (CREDEN), quanto nas atividades estatais, com construção da Política de Defesa Nacional (PDN), da Estratégia Nacional de Defesa (END) e do Livro Branco de Defesa Nacional (LBDN), instrumentos orientadores das Políticas Públicas de Defesa.

Com o intuito de aprofundar o entendimento do Sistema de Defesa Cibernético Nacional, este estudo se propõe a descrever e analisar a construção e a evolução das Políticas Públicas de Defesa e Segurança, bem como os consolidação dos programas e das organizações físicas essenciais do setor cibernético que nortearam a edificação do atual Sistema Institucional Defesa e Segurança Cibernética, para responder ao seguinte questionamento: em face das políticas e estruturas cibernéticas em funcionamento, o Estado Brasileiro está capacitado para enfrentar as ameaças cibernéticas que comprometam a soberania e defesa nacional?

De modo a responder à pergunta proposta, este trabalho se baseou na pesquisa bibliográfica. Portanto, recorreu a livros, artigos científicos e documentos oficiais, bem como utilizou a abordagem descritiva, por meio da coleta e análise de dados.

Ademais, cabe ressaltar que a justificativa do trabalho pretende incentivar o debate acerca do processo de modernização das capacidades estratégicas de defesa e segurança cibernéticas do Brasil, tendo em vista que o estudo na área cibernética tem se desenvolvido exponencialmente a uma velocidade assustadora e sem referências na memória dos Homens.

---

[7] Órgão de assessoramento do Presidente da República nos assuntos pertinentes às relações exteriores e à Defesa Nacional, tratando-se de um órgão de governo, cabendo a Presidência ao Ministro-Chefe do Gabinete de Segurança Institucional do Presidente da República (Brasil, 2019, p. 01).

Para alcançar o propósito estabelecido, o estudo foi estruturado em cinco capítulos. Na sequência desta introdução, o segundo capítulo descreve e analisa, de forma bem sucinta, a construção e a evolução de três documentos estratégicos de defesa e segurança nacional de mais alto nível político: a PDN, a END e o LBDN. Salienta-se que sua apresentação se faz necessária, pois serve para entender a esquematização e a definição das habilidades necessárias das instituições responsáveis pelo desenvolvimento, funcionamento e consolidação do setor cibernético (St Ciber).

Já o Capítulo 3 retrata e examina, primeiramente, os fundamentos da Doutrina Militar de Defesa Cibernética que favorecem a unicidade de pensamento sobre o St Ciber. Posteriormente, são exploradas duas propostas técnico-estratégicas do Livro Verde de Segurança Cibernética e da Política Cibernética de Defesa (PCD), que enfatizam a importância de proteger dentro do espaço cibernético as ações de segurança da informação e comunicação.

Por sua vez, dedica-se o quarto capítulo para explorar o desenvolvimento da atual estrutura de defesa e segurança cibernética, ressaltando as organizações existentes para se opor às crescentes e complexas ameaças cibernéticas que surgem todos os dias.

Por fim, no quinto capítulo, expõe-se, à luz do atual estágio das políticas e estruturas cibernéticas em funcionamento, as principais conclusões quanto à capacidade do Estado Brasileiro para enfrentar as ameaças cibernéticas que comprometam a soberania e a defesa nacional, apontando possíveis linhas de pesquisa futuras atinentes ao tema e que não puderam ser aprofundadas no presente trabalho. De fato, a temática em tela caracteriza-se de valorosa relevância tendo em vista que se verifica uma ampla ocorrência de ataques cibernéticos na atualidade, que desafiam o progresso prosperidade, o desenvolvimento sustentável e a proteção da soberania nacional em variadas circunstâncias ao redor do mundo.

2 FUNDAMENTOS DA ESTRATÉGIA CIBERNÉTICA BRASILEIRA

O início da moldura temporal do estudo deste capítulo é caracterizado pela passagem do Regime Militar para o Regime Democrático de Direito. Aponta-se, assim, que se trata de período que retrata um processo evolutivo de lentas e graduais transformações, por meio das quais os civis mais uma vez voltaram a ocupar a Presidência da República**.**

Por conseguinte, a edificação das Políticas Públicas[8] de Defesa, alicerçadas nos princípios[9] e fundamentos[10] constitucionais da Carta Magna de 1988, representam uma nova visão no tocante a transparência e a disseminação de informações de defesa e segurança do Estado Brasileiro para a sua sociedade e para a comunidade mundial.

De modo a melhor compreender este cenário, este capítulo encontra-se dividido em seis seções. Para tanto, a primeira e segunda apresentam a PDN editada em 1996 e 2005, respectivamente. Já a terceira seção versa sobre a END, publicada em 2008. Por fim, a quarta, quinta e sexta seções abordam as versões dos mencionados dispositivos legais, além da primeira edição do LBDN, atualmente em vigor, em que pese existir o Decreto Legislativo nº 179/2018, que aprovou as revisões da PND, da END e da LBDN, mas que ainda permanece dependente de sanção presidencial para sua validação no ordenamento jurídico do Brasil.

Inicialmente, são discutidos alguns pontos relevantes da composição da organização da PDN de 1996. Para tanto, as características da nova relação entre os militares e civis, após os governos militares e a reestruturação do sistema institucional de defesa com a criação do MD, são descritas.

---

[8] São conjuntos de programas, ações e decisões tomadas pelo Governo com a participação direta ou indireta, com participação de entes públicos ou privados que visam assegurar determinado direito de cidadania, de forma difusa ou para determinado seguimento social, étnico, cultural ou econômico. Disponível em: <www.politize.com.br>. Acesso em: 30 mai. 2019.

[9] Verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízo, ordenados, em um sistema de conceitos relativos a dada porção da realidade (REALE, 1999, p. 60).

[10] Estão relacionados no art. 1° da Constituição Federal de 1988: a soberania, a cidadania; a dignidade da pessoa humana; os valores sociais do trabalho e da livre iniciativa e o pluralismo político.

2.1 Política de Defesa Nacional de 1996

A edição inicial da PDN foi aprovada em 1996, no primeiro governo do Presidente Fernando Henrique Cardoso (1995-1998). Sua estrutura textual era composta de cinco capítulos. Assim, nesta ordem, primeiramente constava o capítulo I – Introdução. Em seguida, o capítulo II – Quadro Internacional, que retratava o fim do confronto Leste-Oeste e o nascimento de cenário internacional multipolar indefinido e instável. Por sua vez, o terceiro capítulo, III – Objetivos, elenca sete objetivos da defesa nacional, decorrentes do interesse nacional, na quarta parte. Já o capítulo IV – Orientação Estratégica, fundamentava a atuação do Estado Brasileiro em uma diplomacia ativa orientada para a paz e uma conduta estratégica dissuasória de natureza defensiva. Finalizando o documento, o quinto capítulo, V – Diretrizes, enumerava as atribuições a serem observados para consecução dos objetivos já definidos anteriormente.

Apesar de não apresentar grande inovação conceitual, essa política foi um elemento impulsionador do processo de mudança nas relações entre civis e militares, que até então caminhava lentamente. Percebe-se, assim, o início da escrituração de orientações e conceitos basilares para o comportamento do Estado, diante das transformações ocorridas em âmbito interno, regional e global.

A nova relação foi fundamentada em um modelo de atuação do Estado, no qual a cultura de defesa deixou de ser um monopólio das Forças Armadas (FA). Cabe sublinhar que, nesse processo, os programas prioritários de defesa devem estar em harmonia com os representantes legítimos do povo Brasileiro, que detêm o poder de aprovação, respeitando as peculiaridades técnicas da área militar.

No capítulo I – Introdução, a PDN descreveu que:

> A Política de Defesa Nacional, voltada para ameaças externas, tem por finalidade fixar os objetivos para Defesa da Nação, bem como orientar o preparo e o emprego

> da capacitação nacional, em todos os níveis e esferas de poder, e com envolvimento dos setores civil e militar (BRASIL, 1996, p. 3).

Dessa forma, observa-se o começo de uma restruturação do sistema institucional Brasileiro atinente ao domínio militar, no qual as missões prioritárias dos militares passam a ser de defesa externa, conectando de maneira nítida os militares e os diplomatas, particularmente nos assuntos relacionados a política externa Brasileira. Dentro desse escopo, percebe-se a intenção do legislador de realçar a abrangência do campo de atuação dos militares, estabelecendo uma preferência para âmbito externo.

O avanço do processo reformista deixou aberta a porta para legitimação técnica e política da criação do MD, em 1999, o qual agrupou os antigos Ministérios da Marinha do Brasil (MB), do Exército Brasileiro (EB) e da Força Aérea Brasileira (FAB) em um único órgão executivo. Consequentemente, o MD passou a exercer a direção superior das FA, colaborando para remodelar o setor de defesa nacional no processo de democratização do Estado Brasileiro.

Nota-se uma construção de um posicionamento explícito do Poder Executivo de que os assuntos de defesa deixam de ser de interesse apenas dos militares. Verifica-se uma dissipação de uma visão militar, amparada na Doutrina de Segurança Nacional e Desenvolvimento, que foi elaborada pela Escola Superior de Guerra (ESG), à luz da ideologia da bipolaridade do Sistema Internacional, em Socialismo[11] e Capitalismo[12], durante o período da Guerra Fria.

Diante dessa nova conjuntura política interna, a administração dos assuntos de defesa e segurança, que antes eram puramente tratados pelos altos Comandos das FA,

---

[11] Doutrina política e econômica que prega a coletivização dos meios de produção e de distribuição, mediante a supressão da propriedade privada e das classes sociais. Disponível em: <www.politize.com.br>. Acesso em: 05 jun. 2019.

[12] É um sistema econômico baseado na propriedade privada dos meios de produção e sua operação com fins lucrativos. Disponível em: <www.politize.com.br>. Acesso em: 05 jun. 2019.

passaram a admitir uma maior participação civil na discussão sobre esses conteúdos, precipuamente os relacionados à defesa nacional.

Feita esta breve explicação, apresenta-se, a seguir, a uma breve exposição conceitual de defesa e segurança nacional, assim como o vínculo das FA com a sociedade civil nas questões cibernéticas incorporadas pela primeira vez na PDN de 2005.

2.2 Política de Defesa Nacional de 2005

A segunda PDN, atualizada pelo Decreto n° 5.484/2005, expressou uma atuação mais intensa de alguns segmentos da sociedade civil, representados por acadêmicos, empresários, jornalistas e intelectuais, além das organizações do MD e do Ministério das Relações Exteriores (MRE), que buscavam uma maior conscientização da sociedade Brasileira quanto ao dever de seus cidadãos à causa da defesa do Estado.

Esse novo arcabouço jurídico conceituou a defesa e a segurança nacional, dois termos empregados normalmente em conjunto, porém com significados distintos na Ciência Política, (BRASIL, 2005, p. 2 grifo nosso):

> **I - Segurança** é a 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;
> **II - Defesa** Nacional é o 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 ou manifestas.

Das definições citadas acima, verifica-se que a defesa nacional possui caráter preponderante na capacidade militar, em consequência de seu poder de coação e efeito dissuasório. Suas ações são conduzidas pelo emprego das FA corroboradas na sua missão constitucional, aludida no artigo[13] 142 da Constituição da República Federativa do Brasil de

---

[13] As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob autoridade suprema do

1988. As FA são uma ferramenta militar responsável pela defesa da Pátria e pela garantia dos Poderes Constitucionais estabelecidos e, por iniciativa de qualquer destes, atuar na garantia da lei e da ordem para, preservar a soberania do Estado e a indissolubilidade da Federação.

Em contrapartida, a segurança nacional está concatenada em um estado intimamente de proteção, devendo fomentar cada vez mais a integração dos campos não-militares do Poder Nacional[14] com os componentes da expressão militar, constituído pelo Poder Naval, pelo Poder Militar Terrestre e pelo Poder Militar Aeroespacial. Percebe-se, assim, que as expressões do Poder Nacional são ferramentas nas ações de defesa, a fim de fornecer o sentimento de segurança, ou seja, sem uma defesa adequada, a segurança está comprometida.

No tema VII – Diretrizes, menciona-se que os meios e procedimentos de Segurança que restringem as fragilidades dos sistemas alusivos à defesa nacional em oposição aos ataques cibernéticos[15] devem ser aprimorados e, se for o caso, prontamente restabelecidos (BRASIL, 2005).

Constata-se que a II PDN é o primeiro documento de alto nível político que faz uma referência direta ao St Ciber. Observa-se, também, a demonstração de uma grande aflição do Estado, tendo em vista as mudanças causadas pelos notáveis avanços tecnológicos nos sistemas de informação e comunicação que passaram a estar interconectados e interdependentes com os primordiais mecanismos vitais de funcionamento do Estado Brasileiro.

Presidente da República, e destinam-se à defesa da Pátria, à garantia dos Poderes Constitucionais e, por iniciativa de qualquer destes, da lei e da ordem (CONSTITUIÇÃO FEDERAL, 1998, art.142).

[14] Manifesta-se de forma sistêmica por meio de cinco expressões: a política, a econômica, a científico-tecnológica, a militar e a psicossocial (BRASIL, 2017, p. 5).

[15] Compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente (BRASIL, 2014a, p. 23).

Nesse quadro, avulta de importância a conexão entre as FA e a sociedade civil, principalmente nos âmbitos acadêmico, científico-tecnológico e industrial, de modo que o integrante militar do Poder Nacional esteja dotado das capacidades de resposta imprescindíveis para liderar a defrontação contra as possíveis ameaças externas, capazes de desestruturar a economia do país e os sistemas centrais de defesa.

Ressalta-se, assim, que, na próxima seção, são abordados os aspectos da base estrutural da END, da fixação dos setores estratégicos de defesa, tal como da criação das organizações necessários para a contextualização dos fatos que são descritos nas seções seguintes.

2.3 Estratégia Nacional de Defesa de 2008

A END apontou um progresso inédito em planejamento Estratégico, ao apresentar uma norma rara no tocante à defesa e à segurança nacional. Formulada no âmbito do MD, a END tem seu marco legal no Decreto n°6.703/2008, que estabelece como aplicar o Poder Nacional para alcançar os Objetivos Nacionais de Defesa (OND) decorrentes da PDN.

Encontra-se organizada em torno de três eixos estruturantes, quais sejam, a reorganização e a reorientação das FA, a reestruturação da indústria de material de defesa com o domínio de tecnologia e a definição da política de composição dos efetivos das FA, sobretudo a reconsideração do serviço militar obrigatório. Além disso, institui ações estratégicas e as estratégias necessárias de médio e longo prazo visando ao desenvolvimento das capacidades essenciais para enfrentar os desafios do presente e as incertezas do amanhã (BRASIL, 2008).

Baseado nos elementos de sustentação citados anteriormente, a END enumera, no total, vinte e três diretrizes dentre as quais merece significativo destaque a que determina os

setores espacial, cibernético e nuclear como estratégicos e precípuos para a defesa e segurança nacional.

Dentro desse contexto, o MD, no que tange à sistematização e à articulação das esferas da defesa, divulgou a Diretriz Ministerial n° 14/2009, que evidencia a imperativa necessidade de que exista absoluta coordenação e integração na exposição e no desenvolvimento dos programas e das ações que digam respeito, particularmente, ao St Ciber, definido como estratégico pela END de 2008, que ficaria sob a responsabilidade do EB (BRASIL, 2009).

A mesma Diretriz estabeleceu duas fases. Assim, em uma primeira fase, seriam definidos a abrangência do tema e os objetivos setoriais e, em uma segunda fase, os objetivos setoriais seriam detalhados em ações estratégicas e a adequabilidade das estruturas existentes nas três forças seria estudada, propondo-se alternativas e soluções para implementação dos preceitos cibernéticas (BRASIL, 2009).

Como resultado dessa delegação e consoante ao disposto no Decreto que aprovou a END de 2008, foi ativado, em 2010, o Núcleo do Centro de Defesa Cibernética (NuCDCiber), o qual foi transformado, em 2012, em uma Organização Militar (OM) de estrutura conjunta. Organizou-se, dessa maneira, o CDCiber.

Incluído na Estrutura Regimental do Comando do Exército pelo Decreto Presidencial nº 7.809/2012, o CDCiber recebeu a missão de coordenar e integrar as atividades de defesa cibernética[16], no âmbito do MD, relacionadas à detecção das ameaças virtuais e ao aprimoramento dos recursos humanos utilizados na defesa do espaço cibernético.

---

[16] 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 (BRASIL, 2014a, p. 18).

Cabe ressaltar que a criação dessa OM buscou preencher a carência de um órgão com a competência de desempenhar a governança de maneira colaborativa, entre os vetores componentes da defesa no campo cibernético.

Além disso, é importante ter em mente que o conceito de espaço cibernético é entendido como um terreno de interação humana, de gênero intangível e abstrata, que utiliza o espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informação por meio de redes interconectadas. Trata-se, assim, de um terreno capaz de impactar a vida cotidiana de autoridades governamentais, de empreendimentos privados e dos próprios cidadãos.

O espaço cibernético apresenta como características peculiares: o alcance global, a inexistência de fronteiras físicas, a incerteza da segurança, a simplicidade de acesso e as velocidades instantâneas. Dentre os domínios operacionais[17], aéreo, marítimo e espacial, o espaço cibernético é o único campo produzido, exclusivamente pela da ação humana.

Observa-se que espaço cibernético, aproveitando-se de TIC, pode ser compreendido como uma área não física criada por meios computacionais, no qual a necessidade de segurança é indispensável para certificar a confiabilidade e a preservação dos sistemas empregados.

Diante da adequação e da modernização do cabedal jurídico frente aos desafios que se apresentam para a defesa, a Lei Complementar (LC) nº 136/2010 criou o EMCFA e disciplina as atribuições do MD. Como consequência, modificou a LC nº 97/1999 que trata sobre a organização, o preparo e o emprego das FA.

---

[17] 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 (BRASIL, 2014a, p. 18).

Essa transformação unificou as três Forças por meio da criação do EMCFA. Isso porque estabeleceu mais um patamar na cadeia de comando, reduzindo o prestígio dos Comandantes das três forças e consolidando a autoridade civil perante os militares.

Em face das complexas e constantes evoluções tecnológicas ocorrida nos últimos anos, o legislador no artigo 9º da LC nº 136/2010 determinou a compulsoriedade legal da publicação do LBDN em companhia com as políticas e estratégias do Brasil para a área de defesa, a cada quatro anos, a partir de 2012. Para tanto, exigia as devidas atualizações, e sua submissão, ao Congresso Nacional, na primeira metade da sessão legislativa ordinária.

Nota-se que a obrigatoriedade de revisão dos documentos de estratégicos de defesa e segurança deve ser compreendida como um indício de que essa legislação não é um produto finalizado. Assim, tal obrigatoriedade carece de ser reformulada, constantemente, em face da realidade disruptiva em termos econômicos, sociais, políticos, tecnológicos, militares dentre outros.

Além do mais, ao definir a revisão, o governo almeja aperfeiçoar e, até mesmo, retificar as diretrizes estabelecidas referentes à defesa nacional de forma que esteja alinhado com as políticas globais. Ademais, pretende que as deficiências indispensáveis para o progresso do Estado sejam atendidas.

Assim, após esta apresentação, destaca-se, na próxima seção, as bases de sustentação da III PND e a relevância da proteção das infraestruturas críticas do Estado no St Ciber.

2.4 Política Nacional de Defesa de 2012

A 3º edição da PDN foi lançada em 2012 como "Política Nacional de Defesa (PND)". Sua concepção política está firmada em 03 pilares: desenvolvimento, diplomacia e

defesa. Trata-se de pilares que fomentam atividades integradas e coordenadas, visando a garantir a segurança e a defesa nacional.

A concretização da pertinência das questões cibernéticas é ratificada novamente no capítulo VII – Orientações, em que o St Ciber é ressaltado mais uma vez como estratégico para a defesa do Estado. O fortalecimento deste setor transcorre do aperfeiçoamento dos dispositivos de segurança, tendo como propósito a adoção de ações que minimizem a vulnerabilidade dos sistemas detentores de tecnologia da informação e comunicação. Havendo a ruptura do serviço, o seu pronto restabelecimento será a cargo da Casa Civil da Presidência da República, dos ministérios da Defesa, das Comunicações e da Ciência, Tecnologia e Inovação, e do GSI-PR (BRASIL, 2012a).

Observa-se que as medidas para a segurança das áreas de infraestruturas estratégicas, incluindo serviços, em especial no que se refere à energia, transporte, água, finanças, telecomunicações, atinentes ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, abrangem as ações efetivas de integração e otimização de múltiplos atores governamentais e privados que atuam diretamente ou indiretamente no tema cibernético.

Esses esforços estão materializados pela promoção de diálogos e de intercâmbios de ideias, de iniciativas, de dados e informações e de melhores condutas, visando garantir o funcionamento das infraestruturas críticas, essenciais à operação e ao controle de sistemas relacionados à segurança e à defesa nacional.

Dessa maneira, observa-se que a institucionalização progressiva da dimensão cibernética na agenda nacional faz parte de um processo político-estratégico de reestruturação e de desenvolvimento tecnológico do Brasil, atinente não somente ao domínio militar. Assim, vê-se, a seguir, que o fortalecimento do St Ciber é imprescindível para o desenvolvimento do Estado.

2.5 Estratégia Nacional de Defesa de 2012

Emitida em 2012 no governo da Presidente Dilma Vana Rousseff, concomitantemente com a PND e com o LBDN, a nova END apontou, sob o espectro cibernético, em uma seção exclusiva, as ações estratégicas e as estratégias prioritárias a serem adotadas para alcançarmos o fortalecimento desse setor. Sob a coordenação do EB, foi previsto a expansão do CDCiber para uma atuação integrada das Forças Armadas, materializadas pela ativação dos núcleos do Comando de Defesa Cibernético das FA (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber).

A ativação do núcleo dessas OM possibilitou o avanço das questões de defesa cibernética nacional, singularmente nos campos da capacitação e gestão de pessoal especializado, no fomento à pesquisa científica, na atualização doutrinária e no preparo e emprego do poder cibernético operacional e estratégico, dentre outros. Essas ações são fundamentais para que o sistema de informação e comunicação digital do Brasil seja um dos instrumentos de desenvolvimento do Estado (BRASIL, 2012a).

Por fim, ressalta-se que a confiabilidade, a disponibilidade, a integridade e a autenticidade desse sistema digital de interesse do Estado, por meio das quais transitam dispositivos computacionais conectados em redes ou não, são vitais para a manutenção do funcionamento das infraestruturas críticas do Estado.

Assim, trata-se, na próxima seção, dos objetivos do LBDN e da preocupação das ameaças cibernéticas para defesa e segurança nacional.

2.6 Livro Branco de Defesa Nacional de 2012

A primeira edição do LBDN simboliza um marco no processo de solidificação da liderança civil. Veiculado em 2012, o documento teve como objetivo divulgar e elucidar de

forma transparente para sociedade Brasileira e para a comunidade Internacional a respeito das políticas e das ações relacionadas à defesa nacional.

Essas ações evidenciam um grande empenho político democrático na construção de uma defesa moderna que o Brasil tanto almeja, e constituem uma ferramenta importantíssima para o aprofundamento do cabedal de conhecimentos da sociedade sobre a temática militar em três níveis: sensibilização/conscientização, treinamento e educação.

O LBDN, no capítulo III – A Defesa e o Instrumento Militar, disserta, no item alusivo ao setor estratégico, que "A ameaça cibernética[18] 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, 2012b, p. 68).

Dessa forma, identifica-se a apreensão do Estado Brasileiro com o St Ciber. Para isso, basta ver que boa parte da infraestrutura crítica[19] do Estado Brasileiro é administrada, manuseada e mantida por companhias privadas, como os setores de telecomunicação, transporte, finanças, água e energia.

Sendo assim, torna-se oportuno conscientizar e incentivar, em amplitude nacional, a formação de comportamento colaborativo das empresas privadas com os órgãos governamentais envolvidos no tema, de modo que todos os ramos da sociedade compreendam os benefícios e os imensos riscos circundados para a segurança e defesa nacional.

---

[18] Causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse (BRASIL, 2014a, p. 18).

[19] Instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2014a, p. 19).

3 CONCEITOS, DEFINIÇÕES E PROGRAMAS

Com o objetivo de padronizar o conhecimento e compreender com maior precisão e clareza os conceitos-chave utilizadas no presente estudo, faz-se mister estudar os fundamentos listados na Doutrina Militar de Defesa Cibernética (DMDC), de forma a proporcionar unidade de pensamento sobre o assunto cibernético, em que pese suas definições e entendimentos serem abrangentes e encontrarem-se em constante evolução. Posteriormente, são apresentadas e examinadas duas diretrizes básicas do Livro Verde de Segurança Cibernética a serem observadas na confecção de uma Política Nacional de Segurança Cibernética (PNSC) e da PCD, que foram necessários para a consolidação e desenvolvimento do St Ciber.

Portanto, a abordagem deste capítulo foi estruturada em três seções, as quais apreciam as noções básicas da DMDC e as potenciais ações estratégicas para o estabelecimento da PNSC e, por fim, as atividades a serem implementadas pelo MD para alcançar os objetivos constantes da PCD.

3. 1 Doutrina Militar de Defesa Cibernética

No que diz respeito à DMDC, a escrituração do seu conteúdo está ordenado em 05 capítulos, quais sejam: I – Introdução, II – Fundamentos, III – Sistema Militar de Defesa Cibernética, IV – Defesa e Guerra Cibernética nas Operações, e V – Disposições Finais. Na seção "Anexo", o documento demostra um organograma detalhado das estruturas e órgãos na concepção do Sistema Militar de Defesa Cibernética[20] (SMDC), sinalizando a subordinação, a vinculação e o canal técnico dos atores estatais nos níveis político, estratégico, operacional e

[20] 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. (Brasil, 2014a, p. 25).

tático, como se pode ver na FIG.1 (BRASIL, 2014a). Cabe mencionar que esse organograma está em fase de atualização devido às alterações realizadas na estrutura do SMDC.

Cabe, então, destacar que a introdução do conteúdo aborda a indispensabilidade do Estado Brasil de dispor de capacidade de reposta oportuna e adequada para se opor às ameaças externas à defesa nacional, de modo coadunável com sua própria extensão e suas pretensões político-estratégicas no cenário global. Essas ameaças são agravadas pelo atual quadro internacional, qualificado como mutável e volátil.

Aplicando os conceitos de segurança e defesa mencionados inicialmente na PDN de 2005, e ratificados na PND de 2012, surgiram os conceitos de segurança e defesa cibernética. Nesse sentido, o primeiro conceito engloba atividades de prevenção e repressão, atentando para restringir ou suprimir as vulnerabilidades da sociedade de informação do Estado e suas infraestruturas críticas de informação, enquanto o segundo preocupa-se com as ações defensivas e se, for o caso, ofensivas.

Na conjuntura de atividade especializada, a SMDC é um instrumento catalizador da unificação do estabelecimento de um padrão de conhecimento sobre o conteúdo cibernético, no campo do MD, a fim de contribuir para as operações conjuntas das FA na defesa do Brasil no espaço cibernético. Assim, as ações nesse espaço são divididas de acordo com três níveis de decisão. No nível político, a segurança da informação e comunicações e segurança cibernética[21] são coordenadas pela Presidência da República, abrangendo a APF direta e indireta, bem como as infraestruturas críticas da informação nacionais.

Já no nível estratégico, a defesa cibernética está a cargo do MD, EMCFA e Comandos das FA, interagindo com a Presidência da República e a APF. Nos níveis

---

[21] 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 (BRASIL, 2014a, p. 19).

operacional e tático, a guerra cibernética[22] é restrita ao âmbito interno das FA, conforme apresentado na FIG. 2 (BRASIL, 2014a).

Verifica-se que a guerra cibernética está incorporada na defesa cibernética sob o prisma do MD, de modo que a edificação dos conceitos formulados é aplicada tanto em um como no outro. Além do mais, nota-se que ademais dos princípios clássicos oriundos da experiência adquirida das campanhas militares elencados na Doutrina Militar de Defesa[23] do Brasil, as operações do St Ciber, em face de suas peculiaridades, baseiam-se em quatro princípios de emprego (BRASIL, 2014a, p. 20):

> I - 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.
> II - 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.
> III - 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.
> IV - 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.

As formas de atuação cibernética podem se diferenciar conforme os níveis dos objetivos político, estratégico, operacional ou tático; nível de envolvimento nacional; contexto de emprego; nível tecnológico empregado; sincronização; e tempo de preparação. No nível político/estratégico a atuação ocorre desde o tempo de paz, para atingir um objetivo político

---

[22] Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² 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 (STIC2) do oponente e defender os próprios STIC2. 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 (BRASIL, 2014a, p. 19).

[23] Tem como finalidade estabelecer os fundamentos para o emprego das Forças Armada em atendimento às demandas da Defesa Nacional (BRASIL, 2007, p. 13).

ou estratégico definido no mais alto nível, normalmente no contexto de uma operação de informação ou de inteligência. Já o nível operacional/tático é tipicamente empregado no contexto de uma operação militar, contribuindo para a obtenção de um efeito desejado. (BRASIL, 2014a).

Dessa forma, no que tange às formas de atuação, o contexto pode estar atrelado a uma situação de paz, a um ambiente de crise ou conflito ou em apoio a uma operação militar. Assim, para realizar um ataque contra um sistema de computadores, normalmente a força adversa obedecerá a uma cadeia lógica de atividades, que se inicia com o levantamento de dados necessários, passando pelas ações propriamente ditas até a limpeza de vestígios que, por acaso, tenha deixado.

Para escolher a melhor medida a ser empregada, visando a proteção dessas ações, torna-se imperativo conhecer profundamente os três os tipos de possibilidade de emprego em ações cibernéticas, os quais são apresentados a seguir:

O Ataque Cibernético é uma ação agressiva, praticada pelo oponente, que compreende ações para interromper, negar, degradar, corromper ou destruir informações, equipamentos ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações (BRASIL, 2014a).

Já a Exploração Cibernética consiste em ações de busca ou de coleta nas redes de dados ou nos sistemas de tecnologia da informação do inimigo, a fim de obter a consciência situacional do ambiente cibernético e informações importantes que podem ser usadas em planejamento de ataque cibernético, desde que não causem danos ou prejuízos às redes de dados e Sistemas do forças oponente, de forma evitar o rastreamento das ações (BRASIL, 2014a).

Por seu turno, a Proteção Cibernética está ligada a ações preventivas para neutralizar ataques e exploração cibernética contra os dispositivos computacionais e redes de

computadores e de comunicações nacionais. Por isso, incrementa as ações de segurança, defesa e guerra cibernética em face de uma situação de crise ou conflito (BRASIL, 2014a).

Observar-se que o planejamento relacionado a essas ações possui uma característica básica da insegurança latente[24], na qual nenhum sistema computacional é 100% seguro, tendo em vista que será sempre objeto de exploração por ameaças cibernética, ou seja, essas atividades devem ter um caráter permanente.

As ações cibernéticas contêm limitações na execução de Operações de Não Guerra e Operações de Guerra. Na situação de paz, as ações de ataque cibernético carecem de aprovação expressa de autoridade política. Na exploração cibernética, as regras do ordenamento jurídico em vigor deverão ser observadas. E caso haja alguma dúvida, competirá ao EMCFA consultar o nível político (BRASIL, 2014a).

Já no caso de Operações de Guerra, serão efetuadas as atividades essenciais ao cumprimento da missão. Portanto, cabe ao EMCFA consultar o nível político, em caso de dúvidas.

3.2 Livro Verde de Segurança Cibernética

A criação deste arcabouço teórico foi influenciada por alguns incidentes no espaço cibernético, intensamente divulgados pela imprensa internacional e amplamente discutidos pelas autoridades de defesa dos Estados desenvolvidos[25].

Dentre os casos disseminados nas mídias internacionais[26], é possível destacar a suspeita de ataques cibernéticos russos nos sites do Governo da Estônia, que inviabilizaram

---

[24] Nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos de informação serão sempre objeto de exploração por ameaças cibernéticas (BRASIL, 2014a, p. 21).

[25] São nações que apresentam elevado desenvolvimento socioeconômico, tomando como base o PIB, renda per capita, IDH e grau de industrialização. Disponível em: <www.mundoeducacao.bol.uol.com.br>. Acesso em: 25 mai. 2019.

sua operação por três semanas. Além disso, há a desconfiança de ataques cibernéticos chineses nas redes de informação de órgãos políticos e de defesa dos Estados Unidos da América (EUA) e da Alemanha, durante o ano de 2007.

O Grupo Técnico de Segurança Cibernética, constituído no contexto da CREDEN, elaborou, em 2010, a partir de uma visão multidisciplinar e interinstitucional, sob a coordenação do GSI-PR, com a participação dos Ministérios da Justiça, das Relações Exteriores e de Defesa, e dos Comandos da Marinha, do Exército e da Aeronáutica, o Livro Verde de Segurança Cibernética. O documento expressa a preocupação do governo em fomentar a coordenação e a integração interna entre os diversos órgãos da administração pública, das corporações da iniciativa privada e das instituições de ensino e pesquisa, bem como a cooperação técnica internacional, de maneira que possa convergir esforços para formação de uma PNSC.

O documento está organizado em quatro capítulos. Ressalta-se, aqui, que o terceiro capítulo apresenta as diretrizes cruciais a serem contempladas, sobretudo, no que corresponde à proteção da sociedade e do Estado. Dos oito vetores contidos nessas diretrizes, dois se apresentam interessantes para a presente análise, quais sejam: o vetor político-estratégico e o vetor de segurança das infraestruturas críticas do Estado. Primeiramente, descrevem-se as instruções do vetor político-estratégico (BRASIL, 2010, p. 43):

> CARACTERIZAR a segurança cibernética como alta prioridade e de extrema urgência para o país, no curto prazo, implementando uma robusta estratégia nacional de segurança cibernética;
> VALORIZAR E AMPLIAR as competências nos diversos temas que perpassam a temática da segurança cibernética, e temas correlatos, como o de segurança das infraestruturas críticas da informação, no curto e médio prazo;
> LANÇAR, no curto prazo, a Política Nacional de Segurança Cibernética;
> CRIAR órgão central para macro-coordenação da Política Nacional de Segurança Cibernética, no curto prazo;

---

[26] A Ciberguerra é moderna! Uma investigação sobre a relação entre Tecnologia e Modernização na Guerra. Disponível em: <www.scielo.br>. Acesso em: 27 mai. 2019.

> ESTABELECER programas de cooperação específicos entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional, no curto, médio e longo prazo;
> DESENVOLVER arcabouço conceitual da segurança cibernética para o Estado brasileiro, no curto prazo;
> ESTENDER a capacidade da Defesa do País para proteção da nação no espaço cibernético; e
> INCREMENTAR a capacidade dissuasória da Defesa do País para fazer frente a ameaça cibernética.

Observa-se que o desenho das propostas tem como finalidade a produção de um marco teórico e legal sobre a segurança cibernética. Isso ocorre a fim de que sejam adotadas as medidas cabíveis para a redução de vulnerabilidades dos sistemas de comunicação e informação que comprometam o funcionamento harmônico, regular e contínuo da operação das estruturas consideradas cruciais do Estado.

Analisando sob o espectro do conflito do espaço cibernético, os crimes são caracterizados pelo desenvolvimento de atividades ilícitas com o emprego de computadores e da internet. Já na perspectiva do terrorismo cibernético, os ataques ilícitos contra computadores e redes de computadores possuem a finalidade de aterrorizar ou pressionar governos e/ou suas populações para a conquista de objetivos políticos e/ou ideológicos. Decorrente da utilização da violência contra os bens e pessoas, tanto quanto for necessário para provocar um sentimento de medo social, o terrorismo cibernético é uma ameaça à paz e à segurança dos Estados.

Nesta direção, destaca-se a proteção do espaço cibernético e das infraestruturas críticas de informação. Estes aspectos desempenham papel estratégico para a segurança e soberania nacional, assim como para o desenvolvimento econômico, tecnológico, social e político, dentre outros.

O segundo vetor é o de segurança das infraestruturas críticas do Estado que tem como desafios: o fortalecimento da resiliência cibernética[27], a carência de uma Política Nacional de Segurança das Infraestruturas Críticas no curto prazo, e a falta de coordenação para o desenvolvimento de sistema de monitoramento de ameaças cibernéticas e para divulgação de alertas de suporte às infraestruturas críticas.

Nesse sentido, um passo importante para alcançar o sucesso das atividades propostas passa pelo fortalecimento das relações da Tríplice Hélice[28]. Esse conceito foi desenvolvido por Henry Etzkowitz e Loet Leydesdoeff, com base na perspectiva da universidade como promotora das relações com as empresas do setor produtivo de bens e serviços e com o governo sendo o setor regulador e estimulador da atividade econômica, visando à produção de novos conhecimentos, atinente à inovação tecnológica e ao desenvolvimento econômico em matéria de segurança cibernética, que será abordado com mais detalhes no próximo capítulo.

Ressalta-se, portanto, que cabe passar para a próxima seção, a qual analisa, no âmbito do MD, as atividades de defesa cibernética, no nível estratégico, e de guerra cibernética, nos níveis operacional e tático,

3.3 Política Cibernética de Defesa

Em continuidade ao progresso das normas legais no campo cibernético, por meio da Portaria Normativa nº 3389/2012 do MD, o Ministro de Estado de Defesa, no uso das atribuições que lhe conferem o inciso[29] II do parágrafo único do art. 87 da Constituição

---

[27] 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 (Brasil, 2010, p.19).

[29] Expedir instruções para a execução de leis, direitos regulamentos (Brasil, 1988, pág. 61).

Federal, aprovou a PCD, manual MD31-P-02. Como resultado, conferiu ao CDCiber a responsabilidade pela implementação dessa política no Brasil.

Importante mencionar que a realização de marcantes eventos internacionais no Estado Brasileiro, tais como a Conferência das Nações Unidas sobre o Desenvolvimento Natural, chamada também Rio+20 (2012), a Jornada Mundial da Juventude (2013), a Copa das Confederações (2013), a Copa do Mundo (2014) e as Olimpíadas e Paraolimpíadas (2016), favoreceram o aperfeiçoamento dos procedimentos operativos e da doutrina.

Assim, o estabelecimento de ações colaborativas de defesa entre os órgãos públicos, o setor privado, a academia e sociedade em geral, além da integração com agências governamentais estrangeiras, como FBI, dos EUA, e o comitê organizador dos jogos Olímpicos no Japão para 2020, motivaram o amadurecimento da área de defesa e segurança cibernética, alcançando um bom nível de preparo. Além do mais, a alocação de pessoal capacitado tecnicamente, de infraestruturas e de recursos financeiros adequados permitiram criar uma arquitetura de conhecimentos necessários para se contrapor aos ataques cibernéticos oriundos tanto de atores estatais como não estatais, como as organizações e até mesmo os pequenos grupos, com as mais diversas motivações.

No que tange à PCD, sua aplicação se dá a todos os integrantes da expressão militar, bem como às entidades que tenham ou venham a ter participação no St Ciber, devendo orientar as atividades de defesa cibernética, no nível estratégico, e de guerra cibernética, nos níveis operacional e tático, tendo em vista o êxito dos seguintes objetivos (BRASIL, 2012c, p.13):

> a) assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional;
> b) capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD;
> c) colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os

> órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
> d) desenvolver e manter atualizada a doutrina de emprego do St Ciber;
> e) implementar medidas que contribuam para a Gestão da SIC no âmbito do MD;
> f) adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber;
> g) definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber;
> h) cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber; e
> i) contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no que se refere à Segurança Cibernética, situados fora do âmbito do MD.

Visando a atingir os objetivos mencionados acima, a PCD estabeleceu procedimentos específicas para cada objetivo, detalhando as atividades a serem efetivadas pelo MD. De forma sucinta, aborda-se, aqui, algumas: a demarcação das infraestruturas críticas associadas ao St Ciber a fim de cooperar para construção da consciência situacional de defesa cibernética; a padronização de procedimentos de segurança cibernética no âmbito das infraestruturas críticas de informação de interesse da defesa nacional; e instauração do SMDC, composto por civis e militares (BRASIL, 2012c).

Órgão central do SMDC, o EMCFA, é o responsável por assessorar a implementação e a gestão, por propor inovações e atualizações, bem como pela criação da doutrina cibernética, tendo como base o planejamento estratégico e emprego conjunto das FA.

Além disso, a indicação das diretrizes e a descrição dos objetivos da PCD submetem-se aos seguintes pressupostos básicos: atuação cooperativa da sociedade brasileira, FA, comunidade acadêmica, corporações públicas e privadas e da Base Industrial de Defesa e a ação organizada e elaborada conforme as necessidades e preferências nacionais (BRASIL, 2012c).

Assim, a formação de hipóteses de emprego para ações de caráter ofensivo, a harmonização com a Política de Ciência, Tecnologia e Inovação para a Defesa Nacional, a conscientização pela sociedade brasileira acerca da cultura cibernética, a relevância das ações

de Segurança da Informação e Comunicações[30] (SIC), concomitantes à defesa cibernética e utilização do espaço cibernético de acordo com a conveniência do Estado Brasileiro, também são pressupostos básicos (BRASIL, 2012c).

Por fim, ressalta-se que, em cumprimento às diretrizes da PCD atinente ao objetivo n° IV- desenvolver e manter atualizada a doutrina de emprego do St Ciber, o Ministro de Estado de Defesa por meio da Portaria Normativa n° 3.010/2014 do MD, aprovou a publicação da DMDC, MD31-M-07, especificando conceitos mais técnicos e operacionais sobre as condutas militares em defesa cibernética.

Portanto, a PCD tem como propósito conduzir e consolidar a atuação da defesa e da guerra cibernética, no campo do MD, no nível estratégico e nos níveis operacional e tático, respectivamente, pretendendo nortear as ações a serem implementadas pelas instituições e organizações que realizam o planejamento, o preparo e a aplicação das ações cibernéticas para se opor as ameaças cibernéticas, com ênfase na proteção das estruturas críticas do Estado Brasileiro.

.

[30] Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações (Brasil, 2014a, p. 19).

4 SISTEMA INSTITUCIONAL DEFESA E SEGURANÇA CIBERNÉTICA

Nos capítulos anteriores, descreveu-se, a partir do enfoque na perspectiva do St Ciber, os documentos de defesa e segurança, de mais alto nível, que foram regulados por meio de Políticas Públicas de Defesa como resposta a problemas cibernéticos. Dessa mesma forma, estudou-se como se evoluiu os fundamentos e as diretrizes do St Ciber, no âmbito do MD e do GSI-PR.

Doravante, é feita uma análise do atual estágio de desenvolvimento do tema cibernético no Brasil, e do nível de preparo e de capacidade de defesa e segurança para se contrapor as ações cibernéticas que representem potenciais ameaças à defesa nacional, particularmente às estruturas críticas do Estado Brasileiro.

4.1 Estruturas de Segurança Cibernética

Esta seção pretende trazer uma visão geral das ações realizadas atinentes ao desenvolvimento e consolidação das organizações existente, na área de segurança cibernética e analisar o estágio atual do St Ciber para enfrentar as ameaças que atentam contra a soberania e a integridade territorial do Brasil.

De uma forma geral, a Segurança do espaço cibernético foi debatida, inicialmente, com o desenvolvimento da segurança da informação, haja vista que, a criação do Gabinete de Segurança Institucional do Presidente da República (GSI-PR), firmada pela Medida Provisória (MP) nº 2.216-37/ 2001, recebeu, dentre outras competências, a coordenação das atividades de segurança da informação e das infraestruturas críticas nacionais.

No que se refere às infraestruturas críticas nacionais, foram designadas seis áreas preferenciais, a saber: energia, telecomunicações, transportes, água, finanças e informação, sendo que a última penetra todas as antecedentes. Observa-se que a gerência e o controle das informações e das comunicações estão cada vez mais dependentes de redes de informação.

A partir disso, foi criado, de acordo com o Decreto nº 5.772/2006 do MD, o Departamento de Segurança da Informação e Comunicações (DSIC) subordinado ao GSI-PR com a missão de planejar e coordenar a execução das atividades de Segurança da Informação e Comunicações[31] (SIC) na Administração Pública Federal (APF), como, representar o Brasil junto à Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético.

Pode-se considerar que essa medida foi um passo inicial para oficializar a preocupação do Estado com segurança cibernética. Em seguida, a atribuição do DSIC do GSI-PR foi ampliada com a inclusão da tarefa de planejar e coordenar a execução das atividades de segurança cibernética, estabelecida por meio do Decreto nº 7.411/2010 do MD.

Em sua estrutura organizacional, o GSI-PR conta, ainda, com a Agência Brasileira de Inteligência (ABIN), Órgão Central do Sistema Brasileiro de Inteligência (Sisbin). Dentre suas atribuições, vincula-se ao St Ciber, avaliar as ameaças cibernéticas internas e externas à ordem constitucional, bem como promover a pesquisa científica e tecnológica adotada a programas de segurança das comunicações.

No âmbito das decisões estratégicas voltadas ao St Ciber, o Conselho de Defesa Nacional (CDN), órgão de consulta do Presidente da República nas matérias associadas à soberania nacional e à defesa do Estado democrático de direito, cuja presidência cabe ao ministro-chefe do GSI, tem a reponsabilidade de elaborar as políticas públicas e diretrizes, bem como a conexão de atividades que permeiam mais de um Ministério. Cabendo mencionar que o MD e as FA colaboram com as ações realizadas pelo GSI-PR, particularmente a SIC e a segurança cibernética.

---

[31] Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (Brasil, 2014a, p. 19).

Dada a natureza compartilhada das informações a serem protegidas, o sucesso da segurança desses ações depende da parceria sistêmica de diversas instituições estatais e entidades não governamentais representando o setor privado.

As transformações do arranjo organizacional promovidas pelo Governo Brasileiro, no que se refere ao assunto cibernético, sofreram consideráveis reflexos dos ataques cibernéticos da Federação Russa à Estônia, em 2007, e à Geórgia, em 2008. Na Estônia o ataque virtual foi direcionado a sites do governo, buscando sobrecarregar as páginas da internet, por meio da inserção de um volume de dados maior que o sistema poderia suportar. Esse ataque provocou um colapso nos recursos de comando e controle do Estado, tornando o servidor indisponível.

Em 2010 talvez tenha acontecido o exemplo mais importante dos últimos tempos. Isso porque, no que tange às ações de emprego cibernético, o projeto nuclear do Irã, foi impactado pelo Stuxnet[32], programa auto-replicante, semelhante a um vírus.

Esse programa foi projetado para atacar o sistema de controle das centrífugas de enriquecimento de urânio, fazendo-as girar mais rapidamente do que o normal e causando rachaduras em seu interior, sem que os operadores percebessem o ocorrido. Como o estabelecimento industrial não tinha acesso à Internet, estima-se que o vírus tenha sido infiltrado por algum dispositivo com saída USB, como pen drive.

No Brasil, não há relatos oficiais de ataques cibernéticos produzidos com o propósito de corromper os sistemas estratégicos. Os meios de comunicação, inclusive internacional, conjecturaram que o chamado “apagão elétrico”, verificado no fim de 2009, tivesse alguma relação ligada a ataques cibernéticos, o que, verdadeiramente, não foi

---

[32] É um ataque cibernético que visa à destruição de um processo industrial no mundo físico. Acredita-se que o vírus foi desenvolvido por algum governo, pois era muito complexo para ser desenvolvido em um grande apoio financeiro e tecnológico. Disponível em <http://www.aereo.jor.br/sobre2/>. Acesso em 14 abr. 2019.

confirmado. Sendo assim, percebe-se que as consequências dos ataques cibernéticos não permanecem apenas no âmbito virtual, mas podem alcançar o plano real, podendo causar danos prejudicais ao desenvolvimento do Estado e a sociedade em geral.

Visando a aprimorar os dispositivos legais para uma maior integração e coordenação das ações de segurança da informação do Estado Brasileiro, tendo como finalidade garantir a disponibilidade, a integralidade, a confiabilidade e a autenticidade da informação a nível nacional, foi instituída a Política Nacional de Segurança da Informação (PNSI) pelo Decreto nº 9.637/18. A PNSI englobou a segurança e defesa cibernética, cabendo ao MD servir de base ao GSI-PR nas tarefas tocantes à segurança cibernética, assim como formular as diretrizes, os dispositivos e os procedimentos de defesa que atuem nos sistemas pertencentes à defesa nacional contra ataques cibernéticos (BRASIL, 2018).

A segurança da informação das infraestruturas críticas é um dos objetivos estratégicos e permanentes da PNSI, de maneira a garantir o prosseguimento das operações dos serviços considerados essenciais. Esses serviços exercem papel vital, tanto para a segurança e soberania nacional, como para o progresso econômico. É notório, portanto, observar que as ações visam a criar condições preeminentes para segurança das infraestruturas críticas de informação, principalmente, no que diz respeito ao entendimento das diretrizes para a proteção da sociedade e do Estado.

Em face do incremento de sua notoriedade como função estratégica de Estado, a segurança e a defesa cibernética são fundamentais para a estabilidade e para o desempenho das instalações, serviços, bens e sistemas que se forem corrompidos ou inutilizados, acarretará inúmeros danos para Segurança do Estado e da sociedade.

4.2 Estruturas da Defesa Cibernética

Esta seção analisa as ações realizadas atinentes ao desenvolvimento, ao funcionamento e à consolidação das organizações existente, na área de defesa cibernética, para enfrentar as ameaças que atentam contra a soberania e a integridade territorial do Brasil.

Decorrente da designação do St Ciber como Estratégico pela END de 2008, a Diretriz Ministerial nº14/2009 atribuiu ao EB a responsabilidade sobre a coordenação e a liderança das atividades desse setor no âmbito da defesa nacional. Visando dar provimento as competências recebidas, a força terrestre estabeleceu duas ações estratégicas: a criação de uma estrutura de defesa cibernética subordinada ao EMCFA, para incluir o assunto nos planejamentos militares conjuntos, e a criação do CDCiber para dar efetividade aos objetivos estratégicos selecionados para o setor.

A medida foi aprovada visando à segurança dos grandes eventos — Copa das Confederações, em 2013, Copa do Mundo neste ano e Jogos Olímpicos de 2016. Havia a previsão de criar o SMDC, que contaria com a participação de civis e militares.

O St Ciber teve um enorme desenvolvimento após a divulgação do "caso Snowden" em 2013, quando, denúncias baseadas em documentos vazados com informações sigilosos do Governo dos EUA revelaram em detalhes alguns dos programas de vigilância perante os Estados da Europa e América Latina. Esse caso foi batizado com essa nomenclatura por causa do delator do esquema de monitoramento: Edward Snowden, americano e ex-consultor técnico da Agência Central de Inteligência (CIA) dos EUA.

No caso do Brasil tornou-se público a espionagem, repetidamente das atividades estratégicas da Petrobrás e das comunicações da então Presidente Dilma Rousseff. Essa espionagem desencadeou, no Poder Legislativo, a abertura de uma Comissão Parlamentar de Inquérito (CPI) da Espionagem destinada a investigar a denúncia de existência de um Sistema

de Espionagem, organizado pelo Governo dos EUA, com o propósito de monitorar *e-mails*, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal (RELATÓRIO DA CPI DA ESPIONAGEM, 2014,b).

Segundo o Relatório da CPI da Espionagem, os documentos divulgados por Edward Snowden denotam o uso da internet como principal meio de espionagem da NSA. Há indícios de que ela opera programas para coletar e analisar o tráfego da rede, dispondo de acordos secretos com companhias de telecomunicação estadunidense e de outros Estados. No andamento dos trabalhos da Comissão, evidenciou-se uma grande vulnerabilidade das redes de comunicação e uma oportunidade para construção e modernização tecnológica e legislativa para enfrentar os crescentes desafios do St Ciber.

O St Ciber cresceu também a partir da implantação do CDCiber, que evoluiu com as necessidades levadas pelos grandes eventos sediados no Brasil, desde a Conferência das Nações Unidas sobre o Desenvolvimento Sustentável em 2012, até os jogos Olímpicos de 2016.

Progredindo com a evolução das normas de estruturação do setor foi criado, conforme a Portaria nº 2.777/2014 do MD, o Programa de Defesa Cibernética Nacional, que definiu as competências para implantação de deliberações, visando a aumentar as ações de capacitação, doutrina, ciência, tecnologia e inovação, inteligência por meio de coordenação e integração sistêmica, de modo a potencializar a defesa cibernética nacional.

O EMCFA foi responsável pela inserção de atividades necessárias para criação do Observatório de Defesa Cibernética, do ComDCiber e da ENaDCiber que hoje contam com militares das três FA, bem como pela organização e execução dos programas de defesa cibernética com enfoque para a implantação e a consolidação do desenvolvimento conjunto de defesa cibernética, do Sistema de Homologação e Certificação de produtos de defesa

cibernética, além do apoio à pesquisa e ao desenvolvimento de produtos de defesa cibernética (BRASIL, 2014b).

O Observatório de Defesa Cibernética é uma ferramenta para construção de um espaço cibernético de cooperação que impulsionará o diálogo entre as esferas acadêmicas, empresariais e militares em várias cidades do Brasil, a fim de contribuir para disseminação de conhecimentos cibernéticos e para colaboração de pesquisa científica. Tal contribuição se dará de maneira que St Ciber possa se desenvolver continuamente, gerando benefícios para a população brasileira. Para tanto, será materializado por um Banco de Dados de Conhecimento especializado e compartilhado.

Subordinada ao ComDCiber, a ENaDCiber foi concebida com a missão de preparar e qualificar os recursos humanos civis e militares, no âmbito da defesa nacional, para que a mão-de-obra nacional possa ter as capacitações necessárias para se confrontar com as ameaças cibernéticas. Eixo acadêmico do ComDCiber, seu arranjo estrutural de ensino tem como característica o emprego dual, retratado pela disponibilização de cursos e estágios para militares das três FA e para meio acadêmico.

Observa-se, assim, que o ComDCiber foi organizado de forma conjunta para planejar, coordenar, integrar, conduzir e supervisionar as ações cibernéticas diante das ameaças cibernéticas, no campo do SMDC, que surgem a cada dia, visando a proteger e defender os ativos informação do MD e das FA. Cabe mencionar que a integração entre as três FA é traduzida pelo seguinte organograma: comandado por um General-de-Divisão, o ComDCiber tem subordinado um Estado-Maior Conjunto e um Departamento de Gestão e Ensino, chefiados por um Contra-Almirante e um Brigadeiro ou vice-versa, além de um CDCiber chefiado por um General-de-Brigada.

Essa estruturação retrata um momento histórico para as FA, pois é a primeira vez que Oficiais Generais da MB e do FAB integram a ordenação hierárquica do EB. Isso porque

a esquematização conjunta do organograma proporciona o aperfeiçoamento das FA por meio da economia de recursos humanos e financeiros, da uniformização de procedimentos, da troca de experiências e do compartilhamento de informações sensíveis de defesa cibernética, cujo organograma pode ser visualizado na FIG. 3.

Por fim, ressalta-se que, alçado a órgão central do SMDC, o ComDCiber busca propiciar o uso efetivo do espaço cibernético pelas Forças Armadas, impossibilitando ou dificultando sua utilização contra os interesses da defesa nacional. Dentre as várias ações desenvolvidas para proteção desse espaço, destaca-se a parceria com o Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) para certificar a qualidade *hardware* usados nos Sistema de Tecnologia da Informação pertencentes as estruturas de defesa cibernética.

Assim, ao explorar a evolução da atual estrutura de defesa e segurança cibernética para se contrapor às progressivas e obscuras ameaças cibernéticas, identificou-se os processos que resultaram na diversificação e no amadurecimento da presente arquitetura, com a criação de novas instituições de natureza técnica, estratégica e operacional, bem como a inclusão de novas orientações atinente a defesa e segurança cibernéticas as instituições já existentes.

5 CONCLUSÃO

Esta pesquisa foi desenvolvida a partir do desafio de trazer a reflexão sobre as principais capacidades do Estado Brasileiro, à luz do atual estágio de funcionamento das políticas e estruturas cibernéticas, para enfrentar as ameaças cibernéticas que comprometam a soberania e defesa nacional. Portanto, este trabalho se propôs a descrever e analisar a construção, o desenvolvimento e a consolidação das políticas públicas e dos relevantes programas de Defesa e Segurança que nortearam a edificação do Sistema Institucional Defesa e Segurança Cibernética

Para atingir seu objetivo, a pesquisa foi estruturada em três capítulos de desenvolvimento. Um capítulo destinou-se a descrever e analisar, de forma bem sucinta, a construção e a evolução de três documentos estratégicos de defesa e segurança nacional de mais alto nível político, a PDN, a END e o LBDN, de forma a entender a esquematização e as competências atribuídas as organizações essenciais ao funcionamento do St Ciber.

Importante sublinhar que, ao abordar o desenvolvimento das políticas públicas na área de defesa no Brasil, a partir do término do regime militar, não é desejável omitir a contextualização relacionada à estabilização das relações civil-militar após os governos militares, assim como, externamente, o contexto internacional pós-Guerra Fria. Ressalta-se, assim, que, internamente, essa estabilização visa a proporcionar a edificação de instituições e organizações que ofereçam soluções oriundas da ação colaborativa entre os detentores da rígida formação militar e os representantes do povo que exercem o controle acerca do utilização do poder militar, sob o prenúncio da nova ordem constitucional.

Entretanto, o início do arranjo político implícito na estrutura de defesa nacional evidencia que, supostamente, as políticas de defesa estavam contaminadas de ressentimento e desconfiança mútuas. Assim, a reconstrução da relação entre os agentes políticos e as

instituições militares, após um período de isolamento, é materializada pela limitada participação ativa da classe política no desenvolvimento das políticas públicas de defesa, assim como na dificuldade de definir prioridades e de alocar recursos necessários para o adequado reaparelhamento do setor de defesa, em especial no período dos governos do Presidente Fernando Henrique Cardoso.

Paralelamente ao início dos governos civis, a globalização impulsiona os avanços na área de TIC desencadeando transformações nunca antes vistas. O surgimento da internet impôs a necessidade de formular políticas públicas de defesa para o uso confiável do novo domínio operacional, chamado de espaço cibernético, um ambiente ainda obscuro, mal delineado, sem fronteiras nem leis, com enorme capacidade para se tornar palco de mais uma disputa de poder no cenário internacional.

No Brasil, apesar de ser relativamente recente a preocupação com o tema cibernético, as ações têm-se intensificado nos últimos anos. No plano da segurança cibernética, as atividades auferiram maior estímulo a partir da criação do DSIC do GSI-PR, em 2006, tendo no GSI-PR a base para consolidar as diretrizes e estruturar as organizações de apoio. **N**o âmbito da defesa cibernética, o destaque passou a ser observado a partir da publicação da END, em 2008, bem como a criação do CDCiber.

Sublinha-se que a edição das políticas públicas na área de defesa de 2012 é essencial para o fortalecimento do St Ciber, se expressa pela expansão do CDCiber na busca de uma atuação integrada das FA, e se materializa pela ativação do ComDCiber e da ENaDCiber.

Assim sendo, pode-se afirmar que, sem dúvidas, as medidas recentemente adotadas pelo Brasil, seja em nível de governo com as Políticas Públicas de Defesa, ou no âmbito do MD com a consolidação do St Ciber, são muito apropriadas e propícias não apenas na conjuntura da afirmação da capacidade Brasileira perante o mundo, mas também para

planejar e aprestar o Estado para defender e salvaguardar seus interesses no espaço cibernético e proteger ou minimizar a probabilidade de ocorrência de um ataque cibernético contra as infraestruturas críticas nacionais.

Em resumo, pode-se afirmar que o Brasil se encontra no rumo certo e que, em termos de conhecimento, habilidade, competência e talentos não ficam a dever em relação a nenhum dos Estados mais bem posicionado econômica e tecnologicamente. Por isso, caso o Brasil seja competente na adoção das medidas que se fazem necessárias para acompanhar a evolução no espaço cibernético e se o Brasil conseguir motivar, conscientizar e mobilizar a população brasileira sobre a importância do tema e para a relação custo-benefício altamente positiva da cooperação nos esforços de Segurança e Defesa Cibernética, não correrá o risco de ficar alijado do seleto clube de países detentores de capacidade de atuar, com desenvoltura e liberdade, nesse novo ambiente de atividade humana.

REFERÊNCIAS

ALECRIM, E. **O que é firewall? - Conceito, tipos e arquiteturas.** 2013. Disponível em: <http://www. infowester.com/firewall.php>. Acesso em: 27 mar. 2019.

_____. **O que é tecnologia da informação?** 2011. Disponível em: <http://www.infowester.com/ ti.php>. Acesso em: fev. 27 mar 2019.

AURÉLIO, Marcos. G. O; DE CONTI, GRACIELA. P; APARECIDA, ADRIANA. M; SOARES Lucas. S. P; BENTO WALFREDO. F. N. **Guia de Defesa Cibernética na América do Sul.** Pernanbuco: UFPE, 2017, 162p.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasilia, DF: Senado Federal: Centro Gráfico, 1988.

_____. **Política de Defesa Nacional.** Presidência da República: Secretaria de Comunicação Social. Imprensa Nacional: Brasília, 1996.

_____. **Política de Nacional de Defesa - Estratégia Nacional de Defesa.** Presidência da República: Secretaria de Comunicação Social. Imprensa Nacional: Brasília, 2012a.

_____. **Livro Branco de Defesa Nacional.** Presidência da República: Secretaria de Comunicação Social. Imprensa Nacional: Brasília, 2012b.

_____. **Decreto nº 5.484, de 30 de junho de 2005.** Política de Defesa Nacional. 2ª Ed. Brasília, 2005;

_____. **Decreto nº 6.703, de 18 dezembro de 2008.** Estratégia Nacional de Defesa Nacional. 1ª Ed. Brasília, 2008.

_____. **Decreto nº 7.809, de 20 de setembro de 2012.** (altera a Estrutura Regimenta da Marinha, do Exército e da Aeronáutica). Brasília, 2012.

_____. **Decreto nº 9.637, de 26 de dezembro de 2018.** Política Nacional de Segurança da Informação. Brasília, 1ª Ed. 2012.

_____. **Decreto nº 9.819, de 03 de junho de 2019.** (dispõe sobre a câmara de Relações Exteriores e Defesa Nacional).

_____. **Decreto nº 5.772, de 8 de maio de 2006.** (cria 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). Brasília, 2006.

_____. **Decreto nº 7.411, de 29 de dezembro de 2010.** (explica as 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). Brasília, 2010.

._____**. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018.** Brasília: GSI, 2015.

_____**.** Ministério da Defesa. **MD35-G-01 – Glossário das Forças Armadas.** 5ªEd. Brasília, 2015.

_____**.**_____**. MD51-M-04 – Doutrina Militar de Defesa.** 2ªEd. Brasília, 2007.

_____**.**_____**. MD31-P-02 – Política Cibernética De Defesa.** 1ª Ed. Brasília, 2012c.

_____**.**_____**. MD31-M-07 – Doutrina Militar de Defesa Cibernética.** 1ª Ed. Brasília, 2014a.

_____**.**_____**. Diretriz Ministerial nº 14 de 09 de novembro de 2009** (dispõe sobre integração e coordenação dos setores estratégicos da Defesa).

_____.Comando da Marinha. **EMA-305 – Doutrina Militar Naval.** 1ª Ed. Brasília 2017.

_____.Comando do Exército. **EB70-MC-10.232 – Guerra Cibernética.** 1ª Ed. Brasília 2017.

_____**. Decreto Legislativo nº 179, de 14 novembro de 2018.** Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional.

_____. Lei Complementar (LC) nº 97, de 09 de junho de 1999, alterada pelas LC nº117, 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", para criar o Estado-Maior Conjunto das Forças Armadas e disciplinar as atribuições do Ministro de Estado da Defesa.

_____. 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 pela integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, consoante o disposto no Decreto nº 6.703, de 2008).

_____. Portaria nº 2.777/MD, 27 de outubro de 2014c. (dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências).

_____. Senado Federal. Senador Ricardo Ferraço, **Relatório Final da Comissão Parlamentar de Inquérito da Espionagem.** Brasília, 2014b. <http://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>. Acesso em: 28 maio. 2019.

DUARTE, L. O. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio**. 2003. Monografia (Bacharelado em Ciência da Computação) NESP/ IBILCE - São José do Rio Preto, SP. 55p. Disponível em: <http://www.academia.edu/483738/ Analise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio >. Acesso em: 21 abril. 2019.

Escola Superior de Guerra. **Manual Básico**. Vol I. Elementos Fundamentais. Rio de Janeiro, RJ: ESG, 2009

GALANTE, Alexandre. **'Malware' Stuxnet foi desenvolvido para destruir usina nuclear iraniana. Poder Áereo, 2010.** Disponível em < http://www.aereo.jor.br/sobre2/>. Acesso em 14 abr. 2019.

MANDARINO JR., Raphael; CANONGIA, Claudia. **Livro Verde:** Segurança Cibernética no Brasil. Departamento de Segurança da Informação e Comunicações. Brasília: GSI, 2010.

MINGST, Karen A. **Princípios de relações internacionais**. Tradução de Cristina de Assis Serra. Rio de Janeiro: Elsevier, 2014, 590p.

PECEQUILO, Cristina Soreanu. **Introdução às relações internacionais**: temas, atores e visões. Petrópolis, RJ: Vozes, 2004, 246p. (Coleções Relações Internacionais).

REALE, Miguel. **Filosofia do direito.** 24. Ed. São Paulo: Saraiva, 1999.

WERTHEIR, Jorge. **A sociedade da Informação e seus desafios. Ciência da Informação.** Brasília, v.29, n.2, p. 71-77, mai/ago2000. <http://revista.ibict.br/ciinf/article/view/889>. Acesso em: 22 abril. 2019.

ANEXOS

ANEXO A

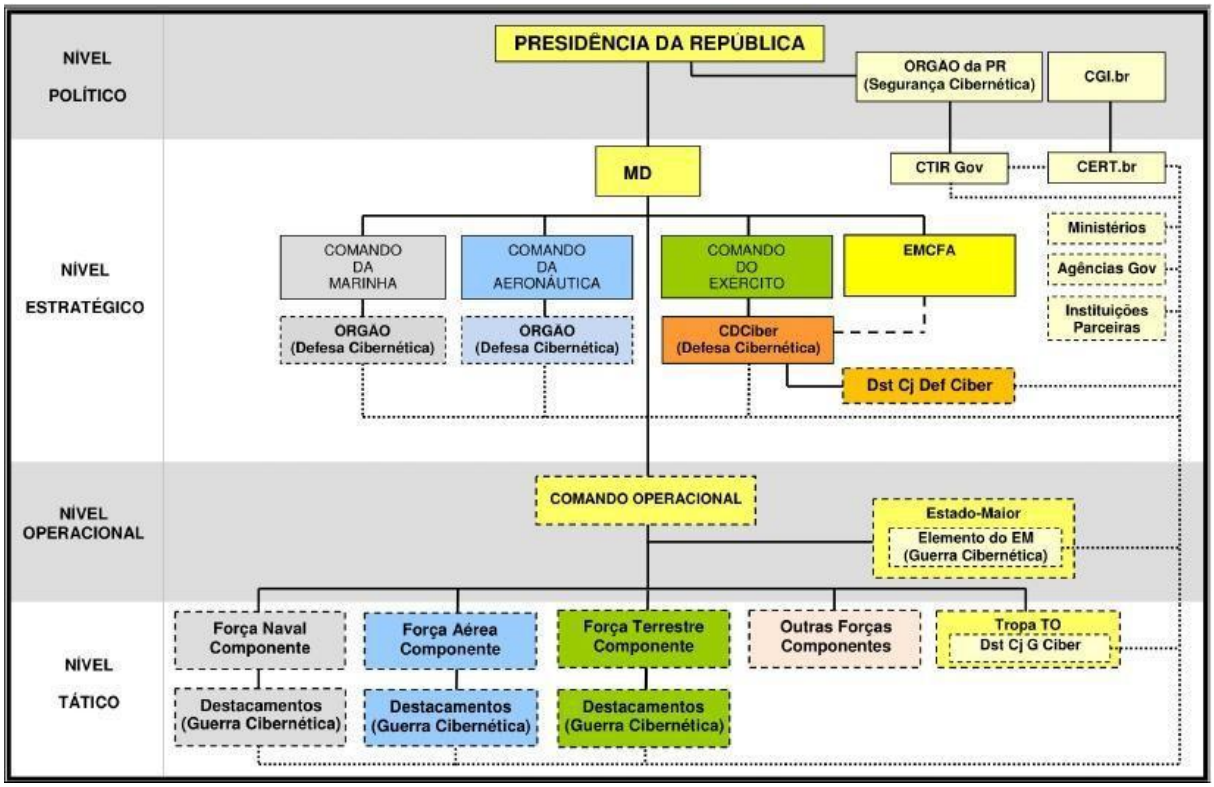

FIGURA 1 – Organograma detalhado das estruturas e órgãos na concepção do SMDC.
Fonte: MD31-M-07 – Doutrina Militar de Defesa Cibernética, 2014.

ANEXO B

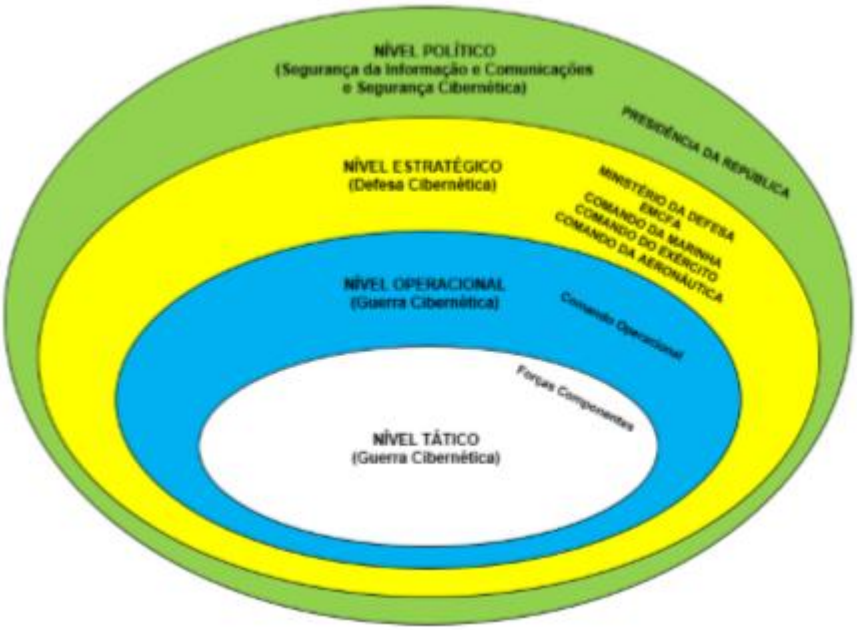

FIGURA 2: Níveis de decisão
Fonte: MD31-M-07 – Doutrina Militar de Defesa Cibernética, 2014.

ANEXO C

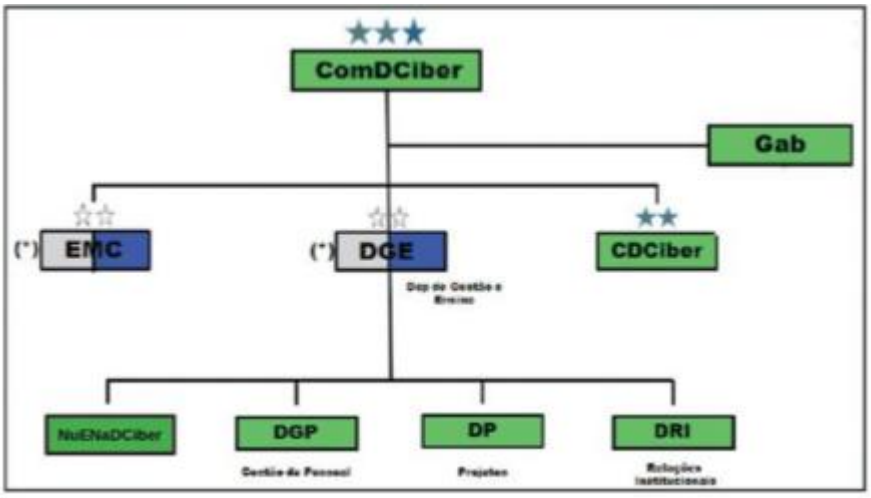

FIGURA 3 – Organograma do ComDCiber

Fonte: Exército Brasileiro, 2019