Política de Defesa Cibernética Brasileira: Um Mapeamento dos Atores e Processos

Camila Bezerra (Graduanda no Curso de Ciência Política com Ênfase em Relações Internacionais da Universidade Federal de Pernambuco)
Caroline Lucena Cruz (Graduanda no Curso de Ciência Política com Ênfase em Relações Internacionais da Universidade Federal de Pernambuco)
David Victor de Melo Chaves (Graduando no Curso de Ciência Política com Ênfase em Relações Internacionais da Universidade Federal de Pernambuco)
Fernando Henrique Casalunga (Graduando no Curso de Ciência Política com Ênfase em Relações Internacionais da Universidade Federal de Pernambuco e Mestrando no Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco)
Ana Carolina de Oliveira Assis (Mestranda no Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco)

RESUMO

Quais são as principais normas e os agentes responsáveis pela defesa cibernética no Brasil? Mediante o quadro de crescente relevância da discussão sobre a questão da defesa cibernética no Brasil e no cenário internacional, o presente artigo tem como objetivo descrever a evolução normativa da Política de Defesa Cibernética no Brasil e apresentar os principais atores que participam da consolidação dessa Política. A análise é feita a partir de três das sete etapas do ciclo das Políticas Públicas: a construção da agenda, a formulação e a implementação da política. Trata-se de um estudo qualitativo, que emprega o método descritivo e exploratório com base em documentos oficiais do Brasil. Faz uso da literatura sobre Política de Defesa como Política Pública e apresenta conceitos chave sobre Defesa Cibernética. Conclui apontando os avanços feitos na área cibernética no Brasil, os quais se pautaram, principalmente, na cooperação interagências e na cooperação internacional.
Palavras-Chave: Defesa, Políticas Públicas, Cibernética.

1. INTRODUÇÃO

O presente artigo se insere em um contexto de proeminência das questões relacionadas à Defesa Cibernética, em especial no Brasil. Com a realização de grandes eventos, como a Conferência Rio+20 (2012), a Copa do Mundo (2014) e as Olímpiadas (2016), em nosso território, observou-se a crescente necessidade de proteção da informação que se encontra disponível no espaço cibernético.

Diante desse cenário, o tema da Defesa Cibernética passou a ocupar espaço preponderante na agenda do Executivo brasileiro, repercutindo no fortalecimento do Centro de Defesa Cibernética (CDCiber), ativado em 2010, ao qual compete a detecção das ameaças virtuais, bem como o aperfeiçoamento dos recursos humanos empregados na defesa do ciberespaço.

Em 2013, a divulgação de informações sigilosas por Edward Snowden, expôs a vulnerabilidade de personalidades, públicas e privadas, ao sequestro de informações. O conjunto de acontecimentos que se seguiu à ação de Snowden contribuiu para consolidar a relevância da Defesa Cibernética para os Estados no que tange o âmbito social, o político e o econômico, concomitantemente reforçou a urgência de se estabelecer uma cooperação técnica e de defesa com os demais países.

De forma a nortear a pesquisa, a seguinte pergunta é proposta: Quais são as principais normas e os agentes responsáveis pela Defesa Cibernética no Brasil? Frente ao questionamento, o presente artigo objetiva descrever a evolução normativa da Política de Defesa Cibernética no Brasil e apresentar seus principais atores. Por meio de um estudo descritivo e exploratório, confere-se um panorama geral sobre um objeto ainda pouco estudado.

A primeira sessão dedica-se a definição dos conceitos contíguos à ciberdefesa, utilizados ao longo do artigo. Em sequência, traremos o marco das políticas públicas a fim de compreendermos a Política de Defesa como uma delas, sujeita aos *inputs* externos[1]. Nesse momento, o desafio é associar essas duas arenas conceituais, apesar da escassez de estudos e dos propósitos de cada corrente serem, a priori, distintos[2].

Superada essa etapa, passa-se, na segunda sessão, à descrição das principais normas que regem a política de Defesa Cibernética brasileira e dos atores envolvidos, ou seja, delinearemos o processo de formulação e implementação da política. Por fim, à guisa de conclusão, são indicados possíveis caminhos para análises futuras, atentas ao processo de avaliação da política em voga.

2. . DEFINIÇÃO DE CONCEITOS

2.1 Ciberdefesa

O estudo aqui apresentado será norteado por conceitos-chaves. O primeiro deles diz respeito ao espaço cibernético, compreendido como um "espaço virtual, composto por dispositivos computacionais conectados (...), onde as informações digitais transitam e são processadas e/ou armazenadas" (BRASIL, 2011, p. 17). Ambiente que guarda uma peculiaridade fundamental, pois, diferentemente do meio aéreo, marítimo e espacial, é o único construído, exclusivamente, pela ação humana. E, embora não seja tangível, ele existe em decorrência de estruturas tecnológicas que estão em um processo constante de mutação.

Já a ciberguerra, é compreendida como "uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar, ou destruir capacidades do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar" (BRASIL, 2015a, p. 134). Destarte, entende-se por proteção cibernética as ações permanentes para neutralizar ataques e exploração cibernética contra dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito (BRASIL, 2015a, p. 227).

Ambos os conceitos, são amplamente debatidos pela literatura, não havendo consenso (ARAGÃO, 2014). Para Singer e Friedman (2014), guerra é um termo utilizado para descrever os conflitos armados e contestações simbólicas entre as nações. Já a Guerra cibernética tratar-se-ia do uso de tecnologia cibernética para intervir em estruturas físicas e obter vantagens militares estratégicas. Ataques contra essas estruturas poderiam gerar ou

[1] De acordo com Easton (1957) o sistema político processa demandas e apoios denominados como *inputs* (do ambiente externo) e *withinputs* (provenientes do próprio sistema político).

[2] Os estudos sobre política de defesa conferem maior atenção aos condicionantes externos, já aqueles que tratam sobre as políticas públicas concentram-se, especialmente, nos aspectos internos, com ênfase para as relações entre Executivo e Legislativo.

potencializar uma guerra (ACÁCIO, 2016). Clarke e Knake (2010) adicionam ao conceito a dimensão civil - diretamente afetada. Em comum, as definições apontam para a importância do avanço da capacidade de uso militar do ciberespaço (BOHN; NOTHEN, 2016).

No que tange ao objetivo delineado, tem-se a divisão entre Defesa Cibernética e cibersegurança. Conforme indicado pela doutrina Militar de Defesa Cibernetica o primeiro conceito relaciona-se com:

> "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, 2014, p.18).

Em contrapartida, a cibersegurança se "refere à proteção e garantia de utilização de ativos de informação estratégicos (...) que controlam as infraestruturas críticas nacionais", envolvendo a interação entre órgãos públicos e privados (BRASIL, 2011).

Depreende-se, pois, que o planejamento estratégico e as ações ofensivas se inserem no escopo da ciberdefesa, já a cibersegurança possui um aspecto defensivo (ACÁCIO, 2016).

2.2 Política de Defesa

De acordo com Muller e Gobert (1987, apud HOFLING, 2001) as Políticas Públicas são "o Estado em ação ", ou seja, são as ações do Estado que não pertencem à esfera privada. As análises de Políticas Públicas têm como objeto a atuação governamental como provedora de serviços públicos (SOUZA, 2006, p. 26 apud ALMEIDA, 2010, p. 222), frutos materiais e concretos de discussões políticas sobre quais serviços o governo deve fornecer à sociedade (RUA, 1998, p.1 apud ALMEIDA, 2010, p. 222).

Com intuito de compreendermos a Política de Defesa (PD) como uma Política Pública, precisamos, primeiramente, conceituá-la. A PD trata da independência do Estado no âmbito nacional, e concretiza-se na prática, através do emprego da geopolítica e da inteligência (NASCIMENTO, 2015, p. 9).

Uma vez que a PD aborda questões de competência estatal muito específicas, dificilmente delegadas ao âmbito privado, e que, paralelamente, trata-se de um serviço público não-rival, haja visto que não é possível excluir nenhum cidadão do benefício produzido por ela, temos, então, subsídios para abordá-la como uma Política Pública. Outrossim, toda Política Pública tem um objetivo, no caso da defesa, a sua finalidade consiste na manutenção da soberania estatal (ALMEIDA, 2010, p. 222).

Ao aclarar como a PD pode ser entendida uma Política Pública, um segundo debate gira em torno de classificá-la como uma Política de Estado ou de Governo. Nesse sentido, por um lado aqueles que defendem ser esta uma Política de Estado o fazem tendo em vista que a mesma integra a estrutura estatal, e, portanto, não deve estar submetida às mudanças de governo e intrigas presentes na discussão política (ALMEIDA, 2010, p. 223). Por outro lado, os que a entendem como uma Política de Governo sustentam que desse modo há maior incentivo ao controle civil dos militares, sendo assim, as forças armadas estariam submetidas à vontade da liderança política eleita, suscetível a mudanças, adaptações e correções de rumo (RUDZIT, CASARÕES, 2015).

Neste estudo, compreendemos a PD como uma Política de Estado, com efeitos de curto, médio e longo prazo, e que, por essa razão, reverberam durante anos. Ao ser planejada

a partir de um orçamento limitado, a mesma segue o ciclo de produção de Políticas Públicas por meio do qual são estabelecidas as prioridades. De acordo com Enrique Saravia(2013), esse ciclo é composto por sete etapas: construção da agenda, elaboração, formulação, implementação, execução, acompanhamento e avaliação. Trataremos, brevemente, de três delas na seção seguinte.

3. A POLÍTICA DE DEFESA NACIONAL: AGENDA, FORMULAÇÃO E IMPLEMENTAÇÃO

No Brasil, a Política de Defesa Nacional (PDN, de 1996) e a criação do Ministério da Defesa (MD, em 1999), nos governos Fernando Henrique Cardoso (1995-2002), a atualização da PDN (2005) e a Estratégia de Defesa Nacional (EDN, 2008) nos governos Luiz Inácio Lula da Silva (2003-2010) e a proposição de revisão dos documentos de defesa, durante o governo Dilma Rousseff (2011-2016), são os marcos normativos da fase de construção da agenda.

Do ponto de vista da formulação, com o fim da Guerra Fria, as estratégias de defesa nacional, que antes eram elaboradas autonomamente pelos Estados Maiores de cada força, depararam-se com a necessidade de estabelecimento de maior diálogo com o poder público. Nesse momento, a PDN rompe com o padrão de influência dos militares na política e insere a esfera civil na sua formulação (NASCIMENTO, 2015). Todavia, observamos que a PD brasileira, em seu sentido mais amplo, não possui normas de responsabilização dos entes federados na formulação e execução da política, desse modo, a alta especialização militar faz com que eles sejam, a priori, os responsáveis diretos pela formulação, implementação e avaliação da política (NASCIMENTO, 2015).

No que tange a implementação, em virtude do distanciamento da sociedade, nota-se uma relação inversamente proporcional entre o poderio militar de uma nação e o conhecimento por parte dos cidadãos sobre a PD, ou seja, quanto maior a importância, o tamanho e a influência do país, menor o conhecimento da população sobre os impactos externos das políticas (WIRLS, 2010, p. 11, *apud* NASCIMENTO, 2015, p. 12). No caso brasileiro, observamos que a defesa está centrada nas mãos do Executivo e há baixa participação do Legislativo, Senado Federal e a Câmara dos Deputados, no processo, principalmente, no que tange a elaboração do orçamento (GIRALDO, 2001; BRIGAGÃO, 2007, *apud* ALMEIDA, 2010).

Destarte, embora sejam notáveis os avanços na defesa nacional iniciados no governo FHC e ampliados no governo Lula, fica evidente que a área ainda carece de maior aproximação com o poder público e a sociedade civil. Neste estudo, não é nosso objetivo aprofundarmos nessas questões, contudo, o debate é profícuo e deverá receber maior atenção em futuros trabalhos sobre a temática.

Os subtópicos a seguir indicam como a Política de Defesa voltada para a área da cibernética tornou-se chave para o Brasil. Neles relacionamos, em dois níveis de análise - externo e interno-, os novos desafios enfrentados pelo Estado brasileiro frente ao desenvolvimento tecnológico, e, a urgência de proteção dos dados presentes em sistemas informacionais integrados contra novas ameaças presentes no ciberespaço.

3.1 Política de Defesa Cibernética brasileira

3.1.1 Âmbito Externo: Parcerias Internacionais

A tecnologia transformou irreversivelmente a sociedade em que vivemos. Atualmente, ela exerce papel fundamental nas transações financeiras e comerciais e possibilita que territórios distantes se conectem. Ao mesmo tempo em que, tornou o mundo mais sensível a ataques maliciosos, conhecidos como ciberataques e cibercrimes (HUERTAS, 2012).

Segundo Huertas (2012) o principal desafio para lidar com essa externalidade negativa da tecnologia está relacionado com a natureza efêmera da mesma. As soluções carecem de atualização contínua e os desafios são cada vez maiores. Além disso, os países precisam adaptar sua infraestrutura, normas e os mecanismos de defesa e investigação, bem como treinar seu pessoal. Adiciona-se a isso o aumento progressivo do número de computadores em uso na sociedade, em decorrência do aprimoramento tecnológico e da redução de custos (HUERTAS, 2012).

Portanto, a evolução da tecnologia apresenta-se como uma via de mão dupla, embora auxilie os Estados na realização de seus objetivos, em contrapartida, aumenta sua exposição às ameaças que circulam no ciberespaço. Os Estados Unidos, por exemplo, apesar de serem um dos países mais avançados tecnologicamente no globo, e ocuparem espaço central no sistema internacional, são também um dos mais sensíveis aos ciberataques[3]. O Brasil, comparativamente, é menos suscetível aos ataques cibernéticos, haja vista o *gap* tecnológico[4] desse país, e o papel secundário que desempenha no cenário internacional.

No entanto, é prioritário que o país esteja preparado para futuras ameaças[5] (HUERTAS, 2012). A preocupação internacional do Brasil em Defesa Cibernética, até o início do século XXI, era limitada aos acordos de troca e proteção mútua de informações sigilosas. Essa postura se alterou quando, em 2013, o ex-técnico da Central Intelligence Agency (CIA), Edward Snowden revelou que empresas e cidadãos brasileiros estavam sendo vigiados. Após o evento de repercussão mundial, o Brasil passou a buscar novos tratados bi e multilaterais, bem como modernizar sua estrutura interna de Defesa Cibernética. Naquele ano, o então ministro das Relações Exteriores, Antônio Patriota, afirmou que os países do Mercosul deveriam procurar reduzir a dependência tecnológica estrangeira para evitar novas espionagens em telecomunicações (Computer World, 2013 *apud* ARTIGO 19, 2017).

O Brasil passou, então, a buscar um maior protagonismo através da pesquisa, tecnologia e inovação. Nesse sentido, o primeiro parceiro foi a Argentina. Através da Declaração de Buenos Aires, de setembro 2013, os ministros da Defesa dos dois países, Celso Amorim e Agustín Rossi, firmaram a criação de um grupo de estudos bilateral e marcaram uma visita às instalações militares brasileiras (ARTIGO 19, 2017, p.18-19; RFI, 2013).

---

[3] Os Estados Unidos sofreram quatro dos dezesseis ataques cibernéticos, o que representa 25% dos casos. Para Huertas (2012) tal fato explica-se em virtude da grande quantidade de computadores naquele país.

[4] Por *gap* tecnológico compreendemos o baixo desempenho da indústria nacional em referência aos mercados internacionais em termos de atividade inovadora e dinâmica produtiva do trabalho (CASTELLACCI, 2008, p. 990 - 991; apud MELO, T., CORREA, A., CARVALHO, E., POSSAS, M., 2017, p. 132).

[5] De acordo com Huertas (2012, p. 31-32), a defesa brasileira não foi atingida por nenhum ataque cibernético, porém as contas .br sofreram cerca de 400.000 investidas. Em 2009, um *hacker* modificou a senha de acesso do governo e solicitou resgate milionário para sua devolução. Em 2011, o grupo "LulzSec", que já perpetrou ataques aos governos do Reino Unido e dos EUA, derrubou os sites da presidência e governo brasileiro.

Ainda em 2013, ocorreu a I Reunião do Subgrupo de Trabalho Bilateral em Cooperação de Defesa Cibernética. No mesmo período, a ministra da Defesa da Venezuela, Carmen Meléndez, em viagem ao Brasil, discutiu possíveis parcerias e requisitou o assessoramento do país para evitar quebras de sistemas operacionais. No ano seguinte, Brasil e Chile, em reunião para impulsionar iniciativas já estabelecidas em acordos entre os dois países, debateram sobre Defesa Cibernética (BRASIL, 2014). Em 2015, o Brasil e a Argentina realizaram uma série de reuniões de cooperação em defesa e nelas expressaram interesse mútuo em estabelecer estágios de Defesa Cibernética (BRASIL, 2015b).

No âmbito regional, o Brasil já participou de discussões acerca de Defesa Cibernética no Mercado Comum do Sul (Mercosul), na União de Nações Sul-americanas (UNASUL) e na Organização dos Estados Americanos (OEA). Em 2013, os cinco países membros do Mercosul, Argentina, Bolívia, Brasil, Uruguai e Venezuela, assinaram a Decisão sobre o Repúdio à Espionagem por parte dos Estados Unidos da América nos Países da Região, na qual se comprometiam em "trabalhar em conjunto para garantir a segurança cibernética dos Estados Partes do MERCOSUL" (MERCOSUL, 2013, p.1).

A UNASUL possui um grupo de trabalho (GT), criado em 2012, para desenvolver e implementar mecanismos regionais de assistência mútua e coordenação no enfrentamento de ameaças cibernéticas. O GT também realiza atividades de cunho didático, de capacitação e de intercâmbio de políticas públicas no ramo. Já no âmbito da OEA, o Brasil possui grande colaboração com o bloco desde 2007, ano em que foi sede para um curso de treinamento de equipes de resposta para incidentes de redes de computadores governamentais organizado pelo bloco. Desde então, o Brasil tem sido sede de diversos seminários fomentados pela Organização, bem como enviou representantes para esses eventos em outros países (ARTIGO 19, 2017).

Além da cooperação regional com os países da América do Sul, pode-se observar que o Brasil já promoveu e assinou Acordos de Troca e Proteção Mútua de Informações Classificadas com diversos países. São esses: Portugal (2005), Espanha (2007, atualizado em 2015), Rússia (2008), Itália (2010), Israel (2010) e Suécia (2014)[6] (BRASIL, 2015 *apud* GUEDES et al., 2017; RECH, 2017; LIMA, 2017). Em 2015, o Brasil e a Índia assinaram um acordo de cooperação aeroespacial, o qual prevê aproximações na área militar, em especial, intercâmbios nas áreas de Defesa Cibernética, abertura de centros de estudos estratégicos em Segurança e Defesa Cibernética e criação de um curso doutrinário sobre Segurança e Defesa Cibernética (MOTA, 2015).

As iniciativas acima estão em consonância com a Estratégia de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética da Administração Pública Federal (APF) aprovada pela a Portaria CDN nº 14, de 11 de maio de 2015, a qual reconhece, na cooperação, um meio de promover a soberania nacional e a defesa dos interesses do Estado. O Brasil visa através da participação em eventos e fóruns internacionais, ampliar seus conhecimentos em SIC e Segurança Cibernética para gerar um "ciclo virtuoso de colaboração" entre atores nacionais e internacionais (BRASIL, 2015d, p. 50). Percebe-se, portanto, que o Brasil tem-se mostrado mais atuante, desde 2013, na aquisição de técnicas e informações e no câmbio de conhecimento e *know-how* em Defesa Cibernética.

[6] Desde o início das discussões de cooperação entre o Brasil e a Suécia, em 2014, até 2016, quando aconteceu o 3º Encontro Bilateral do Grupo de Defesa Brasil-Suécia, os países realizaram diversas trocas de experiências e conhecimento na área de Defesa Cibernética. Um exemplo disso foi a visita às instalações do CDCiber por uma delegação sueca. Naquela ocasião, o Brasil também foi convidado para conhecer equipamentos militares na Suécia.

3.1.2 Âmbito Interno: Processo Normativo

Nacionalmente, os primeiros debates a respeito da Ciberdefesa possuíam a tônica da Segurança da Informação, fator preponderante para que, em 31 de agosto de 2001, por meio de medida provisória, fosse instituído o Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Anos depois, em dezembro de 2008, a Estratégia Nacional de Defesa (END), elencou os setores: Nuclear, Espacial e Cibernética como estratégicos para a Política Nacional de Defesa (PND) (BRASIL, 2008).

Em sequência a Diretriz Ministerial nº 0014, de 9 de novembro de 2009, ativou o Núcleo do Centro de Defesa Cibernética, vinculado ao Exército Brasileiro. Em tal Diretriz, encarrega-se ao Exército a coordenação e integração da área de Cibernética. Em 20 de setembro de 2012 o decreto Presidencial nº7. 809 modifica a estrutura regimental do Comando do Exército, e inclui sob sua coordenação o Centro de Defesa Cibernética (CDCiber) (BRASIL, 2009).

A Portaria Normativa nº 3.389 aprovou em 21 de dezembro de 2012 a Política Cibernética de Defesa, a qual entrou em vigor no dia 27 do mesmo mês, após publicação no Diário Oficial da União (DOU). Elaborada pelo Ministério da Defesa (MD), com a assessoria do Estado-Maior Conjunto das Forças Armadas (EMCFA), visava orientar as atividades de Defesa Cibernética, nos níveis estratégico, operacional e tático, para uma atuação em rede, e em prol do alcance dos níveis de segurança desejados (BRASIL, 2012).

Entre seus pressupostos básicos destacam-se: a importância da atuação e conscientização da sociedade para consecução dos seus objetivos; a ação coordenada e planejada de acordo com as necessidades e interesses do país; o estabelecimento de *hipóteses de emprego* para ações de cunho ofensivo; a harmonização com a Política de Ciência, Tecnologia e Inovação para a Defesa Nacional (C,T&I); e, a relevância das ações de Segurança da Informação e Comunicações (SIC) concomitantes à Defesa Cibernética (BRASIl, 2012).

Pretende-se com o estabelecimento da Política assegurar o uso efetivo do espaço cibernético pelas Forças Armadas, impedindo ações contrárias ao interesse nacional; capacitar recursos humanos para atuação no Setor Cibernético (St Ciber) e produzir conhecimento relevante ao Sistema de Inteligência de Defesa (SINDE) e ao Gabinete de Segurança Institucional da Presidência da República (GSI-PR); desenvolver e atualizar a doutrina de emprego do St Ciber, com normas específicas que fortaleçam sua capacidade dissuasória; gerir a SIC no âmbito do MD e fora dele; além de, adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa (BRASIL, 2012, p. 13).

Para tanto, são estabelecidas diretrizes específicas que auxiliam no alcance dos objetivos. De forma resumida são elas: a concepção do Sistema Militar de Defesa Cibernética (SMDC) composto por civis e militares; a delimitação das infraestruturas críticas associadas ao St Ciber; a padronização de procedimentos e o estabelecimento de programas e políticas. A concepção de um perfil adequado do pessoal empregado, e de cargos e funções que condizem com as necessidades, bem como a constante atualização dos funcionários por meio de congressos e cursos, no Brasil e exterior (BRASIL, 2012, p. 15).

Ademais, compõem as iniciativas: parcerias estratégicas entre Forças Armadas e instituições de interesse; a inclusão da Defesa Cibernética nos currículos dos cursos ofertados pelo MD; a criação de estruturas capazes de fornecer dados para produção de conhecimento. A proposição de uma doutrina de Defesa Cibernética pelo SMDC; o apoio às pesquisas acadêmicas e a promoção do intercâmbio doutrinário, técnico e normativo com civis e demais países (BRASIL, 2012, p. 16). Do mesmo modo que, a característica dual das tecnologias da

informação e comunicação (TIC) devem nortear os programas, e a PCD deve estar em sincronia com a Política Nacional de Segurança Cibernética (BRASIL, 2012, p. 17).

Igualmente importante ao processo foi a aprovação pelo decreto nº 373, em 12 de setembro de 2013, do Livro Branco de Defesa Nacional (LBDN). Tal aprovação possibilitou uma mudança na percepção e organização do setor cibernético no país, a partir do entendimento de que temas relacionados à Defesa e à Cibernética carecem de diálogo com setores distintos da vida nacional, tais como: investimento em pesquisa científica; capacitação de profissionais; gestão de recursos e pessoas e ensinamento da Doutrina Militar (BRASIL, 2013).

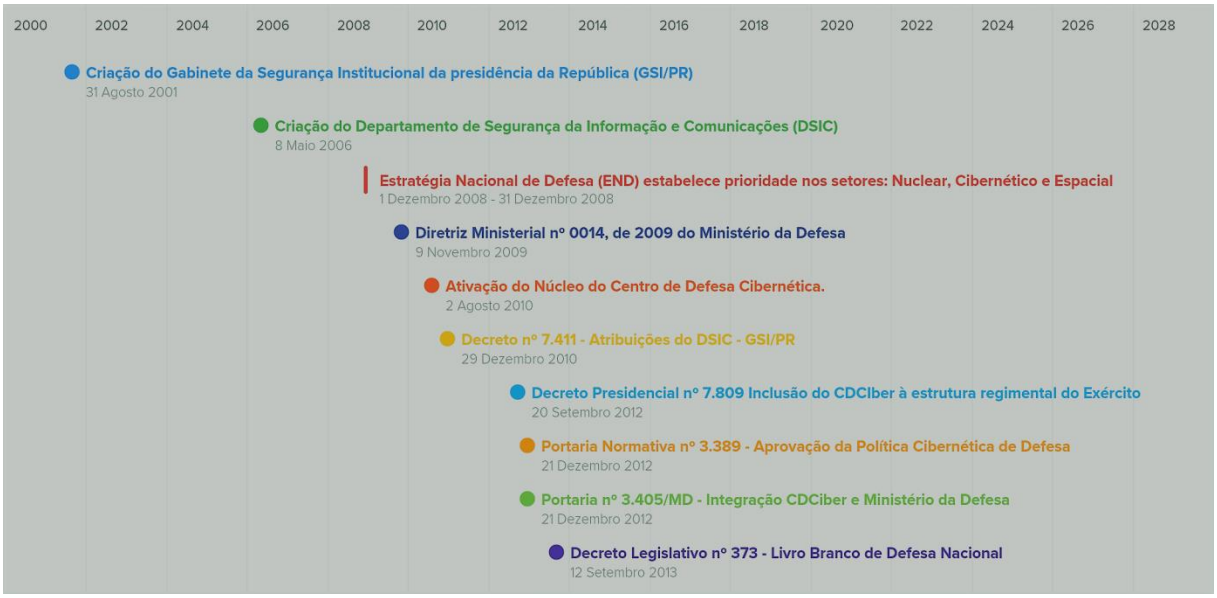
Dessa forma, em 18 de novembro 2014 é estabelecida pela Portaria Normativa nº 3.010/MD a Doutrina Militar de Defesa Cibernética, do Ministério da Defesa. Nela estão contidos os "aspectos mais técnicos e operacionais sobre as ações militares em Defesa Cibernética. Em virtude disso, aborda os fundamentos de Defesa Cibernética, o Sistema Militar de Defesa Cibernética e a Defesa Cibernética dentro das operações" (OLIVEIRA, et. al., 2017, p. 72).

O corpo do texto está dividido em 5 capítulos ordenados entre: 1- Introdução, 2- Fundamentos, 3- Sistema Militar de Defesa Cibernética, 4- Defesa e Guerra Cibernética nas operações e 5- disposições finais. Na seção de anexos a Doutrina de Defesa Cibernética traz um organograma detalhado das estruturas e órgãos na concepção do sistema militar de Defesa Cibernética, diferenciando as prerrogativas da defesa e cibernética em níveis gerenciais, e elenca as instituições e os atores com poder decisório em cada nível (BRASIL, 2014).

A Doutrina propicia "unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético" (BRASIL 2014, p. 13), em um contexto marcado "por incerteza, mutabilidade e volatilidade das ameaças potenciais" (BRASIL, 2014, p. 13).

Com a pretensão de elucidar os principais acontecimentos do processo de concepção e implementação da política de Defesa Cibernética brasileira detalhados acima, foram dispostos, a seguir, em uma linha cronológica os marcos presentes na legislação nacional:

Figura 1: Evolução da Política de Defesa e Cibernética.



Fonte: Elaboração própria, segundo dados da Doutrina Militar de Defesa Cibernética, MINISTÉRIO DA DEFESA DO BRASIL, 2014.

Frente ao exposto, a seção seguinte procura aprofundar a exploração da etapa de implementação da Política de Defesa Cibernética no Brasil com ênfase na descrição de seus órgãos competentes de acordo com os documentos oficiais analisados.

4. IMPLEMENTAÇÃO DA POLÍTICA DE DEFESA CIBERNÉTICA NO BRASIL

O principal órgão responsável pela implementação da Política de Defesa Cibernética no Brasil é o Centro de Defesa Cibernética (CDCiber), criado em 2008, o qual desde 2010 está sob tutela do Exército Brasileiro. Apesar de estar encarregado da defesa do ciberespaço brasileiro, não atua sozinho, pois desenvolve parcerias com a Força Aérea Brasileira e com a Marinha do Brasil. Essas duas últimas são incumbidas do programa espacial e do programa nuclear respectivamente.

A Doutrina Militar (2017) classifica as atribuições ao Espaço Cibernético com base em três níveis fundamentais, quais sejam o (1) Nível Político, (2) Nível Estratégico e o (3) Nível Operacional e Tático. De responsabilidade da Presidência da República e compreendendo a esfera da Administração Federal, o *Nível Político* compreende a "Segurança da Informação e Comunicações e Segurança Cibernética". É o Ministério da Defesa, o Estado-Maior Conjunto das Forças Armadas (EMCFA) e Comandos das Forças Armadas os responsáveis pelo *Nível Estratégico*, que compreende a Defesa Cibernética propriamente dita, comunicando-se também com a Presidência da República e a Administração Pública Federal. E o *Nível Operacional e Tático*, cuja responsabilidade é própria das Forças Armadas, é acionado em casos de Guerra Cibernética.

Sendo assim, o nível político de atuação pode, usualmente, carecer de ações integradas com outros ministérios como o das Relações Exteriores, agências como a ABIN (Agência Brasileira de Inteligência), bem como ações diplomáticas com outros Estados-nação. Já o EMCFA atua quando a Doutrina Militar não prevê casos específicos que necessitem de

tomada de decisão, bem como "auxilia o Ministério da Defesa na gestão do Sistema Militar de Defesa Cibernética e garante a capacidade de atuação em rede das forças armadas" OLIVEIRA, *et.al*, 2017, p. 74). Em complementaridade, as ações de ciberguerra ficam a cargo dos Comandos Operacionais e de seus Estados-Maiores no nível operacional, e, no nível tático, são responsabilidade das Forças Componentes e dos elementos de Guerra Cibernética e dos Destacamentos Conjuntos[7] (BRASIL, 2015a, p. 229).

O Manual de Campanha de Guerra Cibernética do Exército Brasileiro estabelece no capítulo terceiro as estruturas e atribuições da força armada terrestre. O Sistema de Guerra Cibernética do Exército (SGCEx) figura como órgão central de um "conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal para realizar atividades de guerra cibernética" (BRASIL, 2017, p. 3-1).

No nível tático, o Manual prevê a ativação da Estrutura Militar de Defesa (Etta Mi D) que terá apoio da Estrutura de Guerra Cibernética (Etta G. Ciber) responsável por coordenar o: 1º Batalhão de Guerra Eletrônica (BGE), o Batalhão de Comunicação (BCom), o Batalhão de Comunicações e Guerra Eletrônica (B com GE), o Batalhão de Inteligência Militar (BIM), as Companhias de Comando e Controle (Cia C2) e Comunicações (Cia Com). As competências de tais órgãos são descritas a seguir:

> Ao BGE cabe a proteção cibernética dos sistemas de informação da unidade e a exploração de ataques cibernéticos. Já ao BCom a proteção cibernética dos sistemas de informação do grande comando e ao BcomGE a proteção cibernética dos sistemas de informação da Força Terrestre Componente (FTC) e a exploração cibernética limitada em proveito do escalão. Ao BIM a proteção cibernética dos sistemas da própria unidade e assessoramento às ações de exploração cibernética para operações de inteligência conduzidas para manobra da FTC e para produção do conhecimento e inteligência. A Cia C2 realiza a proteção cibernética dos postos de comando da FTC e a Cia Com a proteção dos sistemas de informação de uma grande unidade. Por fim, os elementos das Organizações Militares (OM) que integram a estrutura do estado-maior da FTC realizam a proteção cibernética preventiva dos sistemas de informação da OM, podendo variar a Etta G. C de acordo com a missão da FTC (BRASIL, 2017, p. 32-33).

No nível operacional, as atividades do SGCEx englobam a proteção, o ataque e a exploração cibernética. Seu objetivo é assegurar o Sistema de Comando e Controle do Exército (C2) e proteger as infraestruturas críticas da informação sob jurisdição do Exército (BRASIL, 2017, p. 23). Com vistas à proteção, conduz ações para neutralizar ataques contra dispositivos computacionais, redes de computadores e comunicações. Em ataque, desenvolve ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicação do oponente. Ao explorar, faz a coleta de dados, de modo sigiloso, nos Sistemas de Tecnologia da Informação de interesse, evitando o rastreio das ações e a produção de conhecimento e identificação de vulnerabilidade do sistema (BRASIL, 2017).

No que concerne à Força Naval, o Plano Estratégico de Tecnologia da Informação da Marinha indica a necessidade de fortalecer a capacidade da Marinha para atuar na defesa do ambiente cibernético, realizando "o monitoramento dos riscos e das ameaças ao espaço cibernético da MB, incrementando ações para ampliar a capacidade de Defesa Cibernética e minimizar as vulnerabilidades identificadas". A criação do Centro de Ações de Guerra Cibernética (ComOpNav) para coordenação dos recursos e ações preventivas contra a Guerra Cibernética da MB contempla tal propósito (BRASIL, 2016b, p.12).

[7] Os destacamentos estão localizados em Brasília, Rio de Janeiro, São Paulo, Belo Horizonte, Salvador e Manaus.

No nível tático, os principais órgãos responsáveis são: o Centro de Inteligência da Marinha (CIM); o Centro de Apoio a Sistemas Operativos (CASOP); e, o Centro de Análises de Sistemas Navais (CASNAV). O CIM colabora com a investigação de casos relacionados à ataques cibernéticos, enquanto que o CASOP realiza o planejamento, execução e análise de exercícios no espaço de informação, já o CASNAV contribui para o desenvolvimento tecnológico da Marinha (BRASIL, 2016b).

Na Força Aérea os órgãos centrais responsáveis pelo controle de ameaças cibernéticas são: o Centro de Inteligência Aeronáutica (CIAER); o Centro de Estudo e Avaliação da Guerra (CEAGAR); o Centro de Computação da Aeronáutica (CCA); e, a Diretoria de Tecnologia da Informação da Aeronáutica (DTI). Essas entidades devem promover a integração dos Sistemas de Informação, planejar, implantar, coordenar e fiscalizar atividades relativas à Tecnologia da Informação do Comando da Aeronáutica (COMAER). Conta, ainda, com o Centro de Tratamento de Incidentes de Rede (CTIR), com o objetivo de interceptar "todo evento que afeta a segurança da informação que trafega em meios digitais" afirma o Chefe da Divisão Técnica de Brasília, Major Gustavo Vieira (*apud* BERNARDO, 2014). São considerados incidentes, por exemplo, a divulgação de informação sensível, a interrupção de serviços de TI e o acesso à informação sigilosa.

A descrição da etapa de implementação nos ajuda a clarificar a estrutura organizacional disposta pelas Forças Armadas brasileiras para atuar na defesa e combate aos desafios contemporâneos impostos ao Estado pelo avanço tecnológico. Frente às ameaças à segurança de infraestruturas críticas e a vulnerabilidade dos dados informacionais presentes no ciberespaço é fundamental para o país que a Política de Defesa Cibernética funcione a contento, uma avaliação profunda de seu funcionamento e consistência será objeto de nossas análises futuras.

5. CONCLUSÕES

Neste estudo, primeiramente procuramos delinear o marco teórico das Políticas Públicas a fim de abordarmos a Política de Defesa como uma delas. Desse modo, nos foi possível adentrar as etapas que compõem o processo de construção de uma Política Pública pelo Estado. Diante de nosso espaço limitado, focamos em três das sete etapas do processo, discutindo, de modo geral, a construção da agenda, a formulação e a implementação da Política de Defesa (PD).

Especificamente, adentramos à exploração da etapa de implementação da Política de Defesa Cibernética do Brasil, objeto de análise deste estudo. Para tanto descrevemos as principais normas e os agentes responsáveis pela política. Discutimos, também, como a Defesa Cibernética passou a ocupar espaço preponderante na agenda do Executivo frente aos novos desafios impostos pelo avanço tecnológico aos Estados contemporâneos.

Destarte, em concordância com o Chefe do CDCiber em Brasília, General José Carlos dos Santos, reconhece-se que muitos avanços na área cibernética foram feitos no Brasil, sobretudo em virtude da cooperação interagências e da cooperação com os demais países.

A guisa de conclusão, indicamos possíveis caminhos para análises futuras, atentas ao processo de avaliação da política em voga. Defendemos, ainda, a necessidade de que se mantenham atualizados os estudos sobre Defesa Cibernética no Brasil, haja visto a rápida evolução das ameaças presentes no ciberespaço e sua relevância para a segurança nacional. Cientes de que estamos apenas iniciando o processo de construção do conhecimento

acadêmico sobre o tema fazemos votos de que essa seara não cesse, e que o interesse por essa área de estudos venha a crescer exponencialmente.

REFERÊNCIAS BIBLIOGRÁFICAS

ACÁCIO, Igor Daniel Palhares. Segurança Internacional no século XXI: o que as teorias de Relações Internacionais têm a dizer sobre o ciberespaço? In: OLIVEIRA, Marcos Aurélio Guedes de; GAMA NETO, Ricardo Borges; LOPES, Gills Vilar (Org.). Relações Internacionais Cibernéticas (CiberRI): Oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. 23. ed. Recife: Ufpe, 2016. p. 35-58.

ALMEIDA, Carlos Wellington de. Política de defesa no Brasil: considerações do ponto de vista das políticas públicas. Opin. Pública, Campinas, v. 16, n. 1, p. 220-250, Junho 2010. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-62762010000100009&lng=en&nrm=iso>. Acesso em: 10 abril 2018.

ARAGÃO, Alexandre. Ciber guerra: Foco brasileiro é ciberdefesa consistente. 2014. Disponível em: <http://www.defesaaereanaval.com.br/ciber-guerra-foco-brasileiro-e-ciberdefesa-consistente/>. Acesso em: 10 abril 2018.

ARTIGO 19. *Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul- Estudo de caso sobre a atuação governamental brasileira*. Brasil. 2017.

BERNARDO, Kaluan. Por dentro do CDCiber, o Centro de Defesa Cibernética do Exército Brasileiro. *Medium Brasil*, 2014. Disponível em: https://medium.com/brasil/por-dentro-do-cdciber-o-centro-de-defesa-cibernetica-do-exercito-brasileiro-40ce637d119. Acesso em 15.03.2018.

BOHN, Eduardo Cesar; NOTHEN, Maurício Reis. Considerações sobre o ciberespaço e sua inserção nos Estudos Estratégicos. In: OLIVEIRA, Marcos Aurélio Guedes de; GAMA NETO, Ricardo Borges; LOPES, Gills Vilar (Org.). Relações Internacionais Cibernéticas (CiberRI): Oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. 23. ed. Recife: Ufpe, 2016. p. 83-105.

BRASIL**.**Decreto nº7.809 de 2013. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem nº 83, de 2012. Diário Oficial da União, Brasília, 26/09/2013.

BRASIL. Política de Defesa Nacional. Brasília, Ministério da Defesa, 1996.

BRASIL. Política de Defesa Nacional. Brasília, Ministério da Defesa, 2005.

BRASIL. Estratégia Nacional de Defesa. Brasília, Ministério da Defesa, 2008.

BRASIL, MINISTÉRIO DA DEFESA. *Diretriz Ministerial nº 14/2009*, Brasília: Ministério da Defesa, 2009.

BRASIL, Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Brasília, 2010, 9p.

BRASIL, Presidência da República. Secretaria de Assuntos Estratégicos da Presidência da República. *Desafios estratégicos para segurança e Defesa Cibernética*. Brasília, 2011, 20p.

BRASIL, Ministério da Defesa. Política Cibernética de Defesa, MD31-P-02, 1ªed., Brasília, 2012, 24p.

BRASIL. *Brasil e Venezuela estudam parceria na área de Defesa Cibernética*. Ministério da Defesa. 2013. Disponível em: http://www.defesa.gov.br/noticias/4377-08-08-2013-defesa-brasil-e-venezuela-estudam-parceria-na-area-de-defesa-cibernetica. Acesso em: 27 mar. 2018.

BRASIL, MINISTÉRIO DA DEFESA. *Doutrina Militar de Defesa Cibernética*. MD31-M-07. Brasília: EMCFA, 2014.
BRASIL. *Parceria vai alavancar indústria de defesa no Brasil e no Chile.* Ministério da Defesa. 2014. Disponível em: http://www.brasil.gov.br/defesa-e-seguranca/2014/09/parceria-vai-alavancar-industria-de-defesa-no-brasil-e-no-chile. Acesso em: 27 mar. 2018.
BRASIL, Ministério da Defesa. Glossário das Forças Armadas. MD35-G-01, 5ªed., Brasília, 2015a, 294p.
BRASIL. *Brasil e Argentina realizam reuniões de cooperação na área de defesa*. Ministério da Defesa. 2015b. Disponível em: http://www.defesa.gov.br/noticias/16301-brasil-e-argentina-realizam-reunioes-de-cooperacao-na-area-de-defesa. Acesso em: 27 mar. 2018.
BRASIL. *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018*. Gabinete de Segurança Institucional. Brasília: Presidência da República, 2015c.
BRASIL. Portaria nº 14 CDN. Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR nº 01/2008, 2015d.
BRASIL. *Brasil e Suécia realizam encontro bilateral na área de Defesa*. Ministério da Defesa. 2016. Disponível em: http://www.defesa.gov.br/noticias/18286-brasil-e-suecia-realizam-encontro-bilateral-na-area-de-defesa. Acesso em: 27 mar. 2018.
BRASIL, Marinha do. Plano Estratégico de Tecnologia da Informação. Conselho de Informação da Marinha, 2016b.
BRASIL, Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. Manual de Campanha Guerra Cibernética. Brasília, EB70-MC-10.232, 1ªed., Brasília, 2017, 45p.
CLARKE, Richard A., KNAKE, Robert K. *Cyber war: the next threat to national security and what to do about it.* Nova Iorque: HarperCollins, 2010.
EASTON, David. *An Approach to the Analysis of Political Systems*. World Politics, EUA, v. 9, n. 3, p.383-400, abr. 1957.

HÖFLING, E. M. Estado e políticas (públicas) sociais. Cadernos Cedes [online], v. 21, nº 55, Nov. 2001, p. 30-41. Disponível em: <http://www.scielo.br/pdf/ccedes/v21n55/5539.pdf>. Acesso em 11 de mar. 2018.
HUERTAS, José Antônio Espinosa. *Guerra Cibernética: Um problema estratégico com envolvimento das Forças Armadas* / CEL José Antonio Espinosa Huertas – Rio de Janeiro: ESG, 2012.
LIMA, Paola. *Senado aprova texto de acordo entre Brasil e Espanha*. Senado Federal. 2017. Disponível em: https://www12.senado.leg.br/noticias/materias/2017/05/24/senado-aprova-texto-de-acordo-entre-brasil-e-espanha. Acesso em: 27 mar. 2018.
MELO, T., CORREA, A., CARVALHO, E., POSSAS, M., Competitividade e gap tecnológico: uma análise comparativa entre Brasil e países europeus selecionados. Revista Brasileira de Inovação, v. 16, n. 1, 2017.
MERCOSUL. *Decisão sobre o Repúdio à Espionagem por parte dos Estados Unidos da América nos Países da Região*. Montevidéu, 12 de julho de 2013.
MOTA, Renato. *Brasil e Índia fecharam acordo de cooperação aeroespacial*. Mundo Bit. 2015. Disponível em: http://blogs.ne10.uol.com.br/mundobit/2015/06/24/brasil-e-india-fecharam-acordo-de-cooperacao-aeroespacial/. Acesso em: 27 mar. 2018.
NASCIMENTO, André Jansen. A política de defesa como política pública no Brasil. Fórum Administrativo Direito Público, ano 15, n. 177, 2015. p. 9-26.

OLIVEIRA, Marcos A. Guedes, et all. *Guia de Defesa Cibernética na América do Sul*. Recife: Ed. UFPE, 2017. 162 p. : il.
RECH, Marcelo. *CREDN aprova acordo sobre Informações Classificadas com a Suécia*. Câmara dos Deputados. 2017. Disponível em: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/credn-aprova-acordo-sobre-informacoes-classificadas-com-a-suecia. Acesso em: 27 mar. 2018.
RFI. *Brasil e Argentina reforçam cooperação em Defesa Cibernética*. 2013. Disponível em: http://pt.rfi.fr/brasil/20130914-brasil-e-argentina-reforcam-cooperacao-em-defesa-cibernetica. Acesso em: 27 mar. 2018.
RUDZIT, Gunther, CASARÕES, Guilherme. Política de Defesa é uma Política de Governo. Revista Brasileira de Estudos de Defesa, v. 2, 2015. p. 33-52.
SARAVIA, Enrique. Ciclo de vida da política pública. In: Di GIOVANNI, Geraldo; NOGUEIRA, Marco Aurélio (orgs.) Dicionário de Políticas Públicas. v. 1. 1. ed. São Paulo: FUNDAP, 2013.
SINGER, Peter W.; FRIEDMAN, Allan. Cybersecurity and Cyberwar: What everyone needs to know. New York: Oxford University Press, 2014. 305 p.