As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil

The layers of cyber space under the perspective of Brazil's defense documents

Rev. Bras. Est. Def. v. 4, nº 2, jul./dez. 2017, p. 77-99
DOI: 10.26792/RBED.v4n2.2017.75014
ISSN 2358-3932

MARCOS AURELIO GUEDES DE OLIVEIRA
LUCAS SOARES PORTELA

INTRODUÇÃO

Para lidar com a segurança e a defesa do espaço cibernético, os documentos brasileiros de defesa – Política Nacional de Defesa (PND), Estratégia Nacional de Defesa (END) e Livro Branco de Defesa Nacional (LBDN) – orientam as forças armadas a investirem nas três camadas que compõe esse ambiente: *hardware*, *software* e *peopleware*. A primeira camada é aquela em que estão todas as estruturas físicas, como computadores, placas, roteadores, cabos e outros. A camada *software* engloba todos os sistemas e aplicativos que permitem as operações, ações no espaço cibernético e o gerenciamento dos *hardwares*. Por último e não menos importante, encontra-se a camada de *peopleware* que são os recursos humanos empregados nesse espaço, desde *hackers* até simples usuários da Internet.

O Brasil apresenta deficiência principalmente na camada de *hardware*, devido ao histórico de baixos investimentos em Ciência e Tecnologia. No que diz respeito ao setor de *software*, o país desempenha importante papel e vem se posicionando como um dos maiores produtores de programas do mundo (Lins 2007). Até a virada do século, a produção de *software* era voltada para o mercado interno, mas atualmente o Brasil figura como um exportador (Lins 2007). No que tange à camada *peopleware*, o país é conhe-

Marcos Aurelio Guedes de Oliveira – Professor Titular de Ciência Política da UFPE, PhD em Ciência Política pela University of Essex e Pós-doutoramento em Relações Internacionais no Institut des Hautes Études de l'Amerique Latine, Sorbonne, Paris III.
Lucas Soares Portela – Mestre em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME) e bacharel em Relações Internacionais (UDF).

cido pelos seus *hackers*, que usualmente conseguem boas colocações nas principais competições ciberespaciais do mundo.

O objetivo do presente artigo foi analisar a abordagem das três camadas do espaço cibernética – *hardware*, *software* e *peopleware* – pelos documentos nacionais de defesa do Brasil, publicados entre 2005 e 2016. O método de procedimento empregado por esse artigo foi o monográfico, que analisa um caso ou tema específico visando sua generalização (Marconi; Lakatos, 2003). Nesse sentido, buscou-se, através da análise de fontes primárias – Livro Branco de Defesa, Política Nacional de Defesa e Estratégia Nacional de Defesa – generalizar que todos os investimentos realizados em defesa cibernética devem abarcar as três camadas do espaço cibernético: *hardware*, *software* e *peopleware*.

O recorte temporal utilizado no artigo foi o longitudinal, em que se avalia um período específico (Richardson 1999), neste caso o período entre a primeira abordagem de defesa cibernética em um documento nacional de defesa e o último documento proposto, ou seja, entre 2005 e 2016. As fontes observadas nesse processo foram primárias e secundárias. As primárias englobaram os próprios documentos de defesa e as secundárias foram compostas por teóricos, como Clarke e Knake (2012) e Daniel Ventre (2012).

Cabe ressaltar que não foi abordada a literatura internacional sobre documentos de defesa. Embora interessante e pertinente, a utilização dessa literatura poderia desviar o foco do artigo, que foi a abordagem da defesa cibernética pelos documentos de defesa do Brasil e as camadas do espaço cibernético. Além disso, tal abordagem seria tão longa, que deveria ser tratado em um instrumento de pesquisa mais extenso do que este artigo.

Da mesma forma, o esforço despendido no presente artigo é inicial e de caráter motivacional. A abordagem da defesa cibernética no Brasil ainda pode ser considerada em estágio inicial, igualmente são caracterizadas assim as pesquisas sobre o espaço cibernético. Dessa forma, não se teve aqui a ambição de se observar o processo de formulação e contexto dos documentos, missão para futuras publicações, mas apenas verificar como a defesa cibernética vem sendo tratada nos ditos documentos de defesa do Brasil. Entretanto, os limites apresentados aqui não inviabilizaram a pesquisa, tão pouco limitam sua contribuição para o mundo acadêmico.

Dito isso, a estrutura do artigo foi dividida em três partes. A primeira, de caráter teórico-conceitual, trabalha as três camadas do espaço cibernético. A segunda apresenta como cada um dos documentos aborda os *hardwares*, *softwares* e *peoplewares*. Por último, realizou-se uma análise comparativa sobre as abordagens demonstradas.

CAMADAS DO ESPAÇO CIBERNÉTICO

O espaço cibernético, por vezes, parece algo bastante abstrato e intangível. Mesmo quando familiarizado com esse ambiente, não deixamos de lado aquela visão de uma tela preta com códigos binários verdes brilhantes, subindo e descendo aleatoriamente, empregada por filmes de Hollywood, conforme explicado por Richard Clarke e Robert Knake (2012). Diferente dos espaços geográficos tradicionais – terrestre, marítimo e aéreo –, que preexistiam antes da ação humana, o espaço cibernético foi construído pelo imaginário humano ainda no século passado, talvez por isso dessa visão fantasiosa.

O espaço terrestre, por exemplo, existia antes mesmo do surgimento do homem e da sua transformação pelo homem, chamada na geografia de processo de territorialização (Raffestin 1993), que somente começou a ocorrer com o estabelecimento das primeiras tribos, culminando atualmente em regiões trabalhadas, como a região urbana e a rural. Ainda assim, encontramos locais não territorializados no mundo, como a região do Vale da Morte na Rússia, considerada inabitável mesmo atualmente. O processo de territorialização pode ser considerado comum nos demais espaços geográficos clássicos, mas diferente no espaço cibernético, que tem sua totalidade territorializada.

O espaço cibernético não existia anteriormente ao homem, mas foi produto da ação humana. Como dito, esse espaço cibergeográfico resultou do imaginário humano e não pode ser confundido como a criação do computador, pois é posterior a essa invenção. Datado na década de 60, o espaço cibernético surge com a criação da própria Internet, quando um grupo de pesquisadores do Instituto de Tecnologia de Massachusetts (MIT) tentavam interconectar computadores e equipamentos para operação em rede (Knight 2014).

Embora construído pelo homem, o espaço cibernético ainda não apresenta um significado universalmente aceito, o que impossibilita uma definição mais rigorosa sobre o conceito. O principal obstáculo para uma universalização desse conceito são o ineditismo desse espaço, principalmente quando comparado com os demais espaços geográficos. Destacam-se também a continua evolução e mudanças de estruturas e dinâmicas do próprio espaço cibernético, assim como a intangibilidade de algumas das suas fronteiras, que dificulta o apontamento da dimensão do espaço cibernético, ou seja, sua transversalidade dentro de todos os demais espaços, também chamada de fronteira-ponto por Walfredo Ferreira Neto (2014), também é um obstáculo de definição.

Ainda assim, vale abordar os autores que se esforçam na conceituação do espaço cibernético. Daqueles pesquisadores que conceituam esse espaço

tendo como referência os equipamentos físicos, abordamos aqui Richard Clarke e Robert Knake (2012). De acordo com eles, o espaço cibernético consiste em todas as redes de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles. De acordo com seu conceito, uma rede privada composta por três computadores que se comunicam somente entre eles constituí um espaço cibernético, assim como uma ilha no meio do oceano é considerada como um espaço geográfico terrestre.

Assim, o raciocínio de Clarke e Knake (2012) evidencia que a internet e o espaço cibernético não são sinônimos. Para esses autores, a internet está dentro do espaço cibernético, mas esse não pode ser resumido somente a ela. O espaço cibernético é mais abrangente, pois também se refere às estruturas que não estão conectadas à internet e todos os aparelhos submetidos a ela, como no já citado exemplo dos três computadores.

Embora baseada nas estruturas físicas, a amplitude do conceito de Clarke e Knake (2012) sobre espaço cibernético é concebível devido à propriedade informacional. Ainda acordo com eles, informações que são encontradas nas redes isoladas da Internet também moldam o mundo, portanto, não podem ser desconsideradas dentro do conceito. Na verdade, os principais fatores que moldam o mundo globalizado estão nessas redes, como flutuações de dinheiro, transações de créditos, comércio e até sistemas de controle, como aqueles de geradores e de usinas nucleares.

Também dentro de uma perspectiva de estruturas físicas, o brasileiro Rafael Mandarino Jr. (2010) conceitua o espaço cibernético como o conjunto de infraestruturas críticas, os locais de armazenamento e processamento de dados e o conjunto de pessoas que interage com esses sistemas. A visão conceitual de Mandarino Jr. não discorda daquela apresentada por Clarke e Knake, mas a complementa. O conceito desse autor não resume o espaço cibernético as suas estruturas físicas, mas também considera as informações e os usuários.

Dessa forma, a conceituação de Mandarino Jr. (2010) em relação a de Clarke e Knake (2012) se distingue um pouco quanto à referência. Estes últimos reconhecem os meios em que a informação trafega como parte do espaço cibernético, por exemplo, os cabos de fibra óticas, transmissores de ondas eletromagnéticas e equipamentos. Já Mandarino Jr. (2010) considera o próprio dado, que forma as informações, como fragmentos desse espaço cibernético.

Outra distinção entre as duas visões refere-se ao papel que os usuários desempenham em cada um dos conceitos. Clarke e Knake (2012) imaginam os usuários do espaço cibernético como seus operadores, não fazendo parte do conceito territorial, assim como os navios que navegam nos mares. Para

Mandarino Jr. (2010), os recursos humanos são incluídos dentro do espaço cibernético, por interagirem com os sistemas cibernéticos.

Diferente dos demais territórios, em que os espaços não dependem da territorialização humana para existirem, o espaço cibernético tem um vínculo estrito com as ações do homem. Assim, embora ousada a visão de observar os usuários como componentes estruturais, o apontamento de Mandarino Jr. (2010) é relevante na medida em que a ausência de ação humana ameaça a existência do espaço cibernético. Uma visão mais harmônica sobre o papel do homem na definição do espaço cibernético é oferecida por Daniel Ventre (2012), que observa o espaço cibernético como formado por três camadas: *hardware*, *software* e *peopleware*.

Embora não tenha claramente conceituado o espaço cibernético como os autores anteriores, Daniel Ventre (2012) deixa transparecer sua percepção sobre o conceito de espaço cibernético. Para Ventre (2012), as três camadas são complementares, uma vez que os equipamentos necessitam de programação, a qual é operada pelos usuários. Assim, vale notar que enquanto Mandarino Jr. (2012) considera o usuário como parte do espaço cibernético, Ventre (2012) o aponta apenas como operador e agente de territorialização.

Diante disso, as ações no espaço cibernético dependem da integralidade das três camadas, especialmente as duas primeiras. Sem equipamentos adequados, um programa sofisticado não conseguiria processar as informações demandadas pelos usuários. Por outro lado, ao dispor de equipamentos avançados sem programas igualmente desenvolvidos, um usuário não utilizaria todo o potencial disponível. Além disso, caso o operador não tenha formação e capacitação adequada, os usos das estruturas e dos programas seriam limitados.

Dessa forma, podemos afirmar que a primeira camada (*hardware*) é estrutural e a terceira (*peopleware*) é operacional, enquanto a segunda (*software*) exerce as duas funções. Em virtude disso, os documentos que abordam e orientam a defesa cibernética devem considerar ações para o fortalecimento das três camadas.

POLÍTICA NACIONAL DE DEFESA

Dois anos depois da publicação da primeira END de 2008, o Congresso Nacional decretou a Lei Complementar nº 136/2010, que alterou a Lei Complementar nº 97/1999. A lei de 2010 dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Essa legislação também criou o Estado-Maior Conjunto das Forças Armadas, que posteriormente incorporou o organograma da defesa cibernética brasileira.

A Lei Complementar nº 136 impactou, ainda, nas publicações dos documentos de Defesa do Brasil. Em seu artigo 9º, § 3º, o documento afirma que a cada quatro anos, a partir de 2012, o Poder Executivo deve encaminhar para o Congresso Nacional atualizações de três documentos de defesa, a saber, a Política de Defesa Nacional, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. A partir da sanção presidencial dessa Lei, podemos separar os documentos de defesa em gerações. Vale ressaltar que essa separação, antes de uma ambição teórico-conceitual, é apenas uma ferramenta didática que facilita a comparação e compreensão da evolução do trato do espaço cibernético pelos documentos de defesa do Brasil.

Dito isso, a primeira geração é composta pela Política de Defesa Nacional e a Estratégia Nacional de Defesa, sendo estas do ano de 2005 e 2008, respectivamente. A segunda geração data de 2012, constituída pela revisão da estratégia e da política da primeira geração, acrescida do Livro Branco de Defesa Nacional e do Plano de Articulação e Equipamentos de Defesa. A terceira geração é vivenciada no tempo presente, em que novas versões dos documentos de defesa estão em vias novas publicações.

A preocupação com as mudanças que o espaço cibernético provoca nas dinâmicas da sociedade surge juntamente com a construção desse mesmo espaço. No entanto, a incorporação oficial dessa temática nos principais documentos brasileiros de defesa ocorreu apenas em 2005, com a publicação da Política de Defesa Nacional e, posteriormente, com a Estratégia Nacional de Defesa de 2008. Primeiramente, esses documentos eram mais discretos, enfatizavam a importância de se proteger o espaço cibernético e atribuíam a responsabilidade de sua defesa para o Exército.

A Política de Defesa Nacional de 2005 foi promulgada pelo Decreto Presidencial 5484/2005 e era composta por uma parte política e outra estratégica. A parte política foi dividida em conceitos de Estado, Segurança e de Defesa, ambientes nacional e internacional e trazia uma breve conjuntura do Brasil. Na segunda parte, o documento apresentou os objetivos da Defesa Nacional, orientações estratégicas e diretrizes finais.

Cabe destacar que, embora considerado como próprio da defesa, este documento também foi pensado para envolver o setor civil. De acordo com ele, para preparar o emprego de uma capacidade nominal que garantisse o Poder Nacional, o envolvimento das duas esferas seria necessário. Apesar disso, a política mantém o Ministério da Defesa (MD) como coordenador da defesa nacional.

A defesa cibernética foi abordada apenas duas vezes nesse documento. A primeira vez surgiu nas orientações estratégicas, quando afirma que "para minimizar os danos de possível ataque cibernético, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção

de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento" (Brasil 2005, 6). A Política de Defesa Nacional buscou reaquecer o pensamento em prol de uma reestruturação e fortalecimento da defesa, por isso ao abordar a defesa cibernética enfatizou a necessidade de tê-la para permitir a resiliência do país e salvaguardar os sistemas de defesa do país.

A segunda abordagem apareceu apenas nas diretrizes finais do documento, quando explica que as políticas e ações que eram definidas pelos setores do país deveriam contribuir para o alcance dos objetivos da defesa nacional. Dentre as observações que deveriam ser realizadas, o documento indicou "aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, permitam seu pronto restabelecimento" (Brasil 2005, 6).

Em 2012, essa política foi renomeada de Política de Defesa Nacional para Política Nacional de Defesa. A alteração do nome demonstrou que não se estava tratando somente de um documento setorial do Ministério da Defesa para as forças singulares, mas de um documento que orientaria todos os setores envolvidos na segurança e defesa nacional. Por isso, esses dois conceitos foram distinguidos logo no início do documento de 2012.

Nessa versão, foi acrescentada apenas uma abordagem sobre o espaço cibernético nas tratativas do ambiente internacional, quando o documento afirmou "para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, cibernético e nuclear" (Brasil 2012a, 19). Assim, a política retomou a necessidade de se manter tecnologias autônomas para garantir um desenvolvimento nacional sem interferência estrangeira, ou seja, a capacidade de se dizer "não" para outros países, que foi abordada nos documentos da primeira geração.

Diferente da anterior, a minuta da próxima política, que está em apreciação no Congresso Nacional, trata o espaço cibernético já dentro do ambiente nacional:

> Adicionalmente, o amplo espectro de possibilidades no ambiente cibernético requer especial atenção à segurança e à defesa desse espaço virtual, composto por dispositivos computacionais conectados em redes ou não, no qual transitam, processam-se e armazenam-se informações digitais, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações, dos quais depende parcela significativa das atividades humanas (Brasil 2016a, 8).

Tanto esse trecho, quanto os demais apresentam um teor mais crítico e real sobre a condição da defesa no Brasil, menos ideológico e mais direto. Por exemplo, enquanto na versão vigente, a PND almeja e incentiva a busca por uma independência tecnológica, na minuta apresentada há o reconhecimento da impossibilidade dessa liberdade, face aos recursos orçamentários escassos e à falta de regularidade para aquisição de produtos de defesa.

ESTRATÉGIA NACIONAL DE DEFESA

A Estratégia Nacional de Defesa de 2008 foi promulgada pelo Decreto Presidencial 6.703/2008 e está basicamente dividida em três partes. Após a introdução, o documento realiza uma apresentação do tema de defesa, enfatizando sua importância e apresentando os eixos que nortearam a estratégia brasileira após a entrada do Decreto em vigor. Na segunda parte, o documento traz diretrizes para a própria estratégia, orientações para cada uma das forças e para os setores estratégicos. Por fim, o texto também aborda alguns assuntos complementares da defesa nacional.

A importância desse documento está em si mesmo, pois foi a primeira estratégia de defesa brasileira. De acordo com o próprio documento, a vocação pacifista do Brasil havia impedido a promulgação de uma estratégia de defesa:

> País em desenvolvimento, o Brasil ascenderá ao primeiro plano no mundo sem exercer hegemonia ou dominação. O povo brasileiro não deseja exercer mando sobre outros povos. Quer que o Brasil se engrandeça sem imperar. Talvez por isso nunca tenha sido realizado no Brasil, em toda a sua história, amplo debate sobre os assuntos de defesa. Periodicamente, os governos autorizavam a compra ou a produção de novos materiais de defesa e introduziam reformas pontuais nas Forças Armadas. No entanto, **nunca propuseram uma estratégia nacional de defesa para orientar de forma sistemática a reorganização e reorientação das Forças Armadas; a organização da indústria de material de defesa, com a finalidade de assegurar a autonomia operacional para as três Forças: a Marinha, o Exército e a Aeronáutica**; e a política de composição dos seus efetivos, sobretudo a reconsideração do Serviço Militar Obrigatório. Porém, se o Brasil quiser ocupar o lugar que lhe cabe no mundo, **precisará estar preparado para defender-se não somente das agressões, mas também das ameaças**. Vive-se em um mundo em que a intimidação tripudia sobre a boa fé. Nada substitui o envolvimento do povo brasileiro no debate e na construção da sua própria defesa (Brasil 2008, 1, grifo próprio).

Conforme o trecho, as estratégias até então publicadas somente apresentavam diretrizes orientandas para a guerra. Entretanto, como também exposto, a defesa é necessária tanto em tempos de agressões como para prevenir ameaças, carecendo também de uma estratégia. Mais adiante, o documento afirmou que o desenvolvimento e concretização das capacidades defensivas são necessárias para que o país tenha condição de dizer "não" quando necessário. Assim, na perspectiva do documento, a estratégia deixa de ser um instrumento de preparação para a guerra e passa a ser uma ferramenta para orientar, organizar e assegurar a autonomia operacional para as forças singulares também em períodos de paz.

A defesa cibernética se relaciona com o restante do documento em três pontos, a saber, operação em rede, independência tecnológica e uso industrial para esse setor. A principal função da defesa cibernética é garantir a operação em rede das três forças, assegurando o princípio da flexibilidade, que para isso necessita de uma autonomia tecnológica. A capacidade de desenvolver tecnologias com autonomia permite que o país explore o uso dual dos equipamentos, permitindo a fabricação industrial e comercialização.

O documento traz um posicionamento distinto ao afirmar como conseguir desenvolvimento tecnológico e autonomia:

> O futuro das capacitações tecnológicas nacionais de defesa depende mais da formação de recursos humanos do que do desenvolvimento de aparato industrial. Daí a primazia da política de formação de cientistas, em ciência aplicada e básica, já abordada no tratamento dos setores espacial, cibernético e nuclear (Brasil 2008, 13).

De acordo com a citação, a maturidade tecnológica depende mais da formação de recursos humanos do que da aquisição ou importação de tecnologias. Isso fica evidente no texto de 2012, ao tratar da impossibilidade de independência tecnológica do país enquanto faltarem condições para que os indivíduos possam aprender, trabalhar e produzir.

No tocante à defesa cibernética, o documento de 2008 enfatizou a necessidade das capacitações cibernéticas para usos industriais, educativos e militares de forma a garantir a atuação em rede, principalmente entre os contingentes militares, que foi mantida na edição de 2012. A novidade da nova edição foi o estabelecimento de prioridades para se alcançar o objetivo acima exposto. Ao todo, a END de 2012 elencou oito prioridades a serem observadas:

Quadro 1
Prioridades da END 2012 para a Defesa Cibernética do Brasil

Prioridades	Descrições
a	Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;
b	Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à certificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;
c	Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;
d	Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;
e	Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como
f	Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;
g	Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas;
h	Estruturar a produção de conhecimento oriundo da fonte cibernética

Fonte: Elaboração própria baseada em Brasil (2012a, 93-95).

A END de 2012 prevê, ainda, o uso dual de equipamentos de defesa cibernética, instigando uma rentabilidade para a indústria de defesa cibernética e criando uma independência tecnológica. Para isso, o documento prevê a criação de 15 sistemas de defesa cibernética, dentre eles o simulador de defesa cibernética que já está em operação no CDCiber. Além de pesquisas científicas sobre a temática, tanto no âmbito da ENaDCiber, como também em instituições de nível superior, nacionais e internacionais.

Na minuta de 2016, que está sendo apreciada no Congresso, a END apresenta alteração em relação ao conteúdo, afetando também a defesa cibernética. Ela não observa o uso dual e industrial no setor cibernético, assim como os documentos anteriores. A principal ênfase dada está na relação necessária entre ambientes militar e civil.

O último incremento da minuta da END são os Objetivos Nacionais de Defesa (ONDs), que são compostos por Estratégias de Defesas pontuais e Ações Estratégicas de Defesa para cada estratégia menor. Na primeira e na segunda geração, as ENDs apresentaram apenas orientações gerais que nortearam a defesa brasileira. A versão que está em apreciação no Congresso apresenta orientações mais específicas por meio dos ONDs.

No primeiro objetivo, por exemplo, sobre a garantia da soberania, patrimônio nacional e integridade territorial, encontramos a ação de número 2 da primeira estratégia pontual de defesa, a saber, o fortalecimento do poder nacional, o qual requer que a defesa brasileira contribua para o incremento do nível de segurança das Estruturas Estratégicas. A END entende que essas estruturas são sistemas essenciais para o Estado e são compostas, por exemplo, pelo sistema de distribuição de água e energia elétrica. Também são compreendidos como uma estrutura estratégica, o sistema de comunicação e cibernética.

Ainda dentro desse objetivo, a segunda estratégia pontual, qual seja, fortalecimento da capacidade de dissuasão, prevê o desenvolvimento das capacidades de controle do espaço aéreo, cibernético, territorial, águas jurisdicionais e demais áreas de interesse. Prevê, também, o incremento da capacidade de defender e de explorar o espaço cibernético. A promoção do desenvolvimento da tecnologia cibernética, a fim de fortalecer a área de Ciência e Tecnologia de Defesa também é listada no referido documento.

LIVRO BRANCO DE DEFESA

Como previsto pela Lei Complementar nº 136/2010, o Congresso Nacional também deveria apresentar também um Livro Branco de Defesa Nacional (LBDN) em 2012, como de fato veio a fazer. O livro seguiu praticamente a mesma estrutura da END de 2012, porém com maior profundidade e detalhes. Nas palavras do então ministro de defesa, Celso Amorim, o objetivo do LBDN era, conjuntamente com a END e a PND, ser "um documento esclarecedor sobre as atividades de defesa do Brasil" (Brasil 2012b).

Nesse livro, a defesa cibernética começa a ser tratada no tópico que aborda o ambiente estratégico do século XXI. Nessa parte, esse ambiente é abordado como um novo tema ou novas abordagens, que influenciam no sistema internacional do século e, por isso, têm implicações para a soberania dos países. Dentre os problemas apresentados como as drogas e delitos conexos, o documento aponta para a necessidade da defesa cibernética.

O LBDN também incentiva o fomento da base industrial de defesa e a inovação. Além disso, evidencia que o país precisa produzir componentes críticos nacionais, de forma a garantir a independência tecnológica do país.

Por isso, a defesa cibernética consiste em um projeto prioritário de equipamentos. Os projetos elencados pelo documento para este fim são seis, com data de execução entre 2011 e 2035:

Quadro 2
Subprojetos do Sistema de Proteção Cibernética — Defesa Cibernética

Descrições	Início	Fim
Subprojeto Implantação da estrutura de planejamento e execução da Segurança Cibernética	2012	2023
Subprojeto Implantação da estrutura de pesquisa científica na área cibernética	2012	2015
Subprojeto Implantação da estrutura de apoio tecnológico e desenvolvimento de sistemas voltada para as atividades do Setor Cibernético	2012	2015
Subprojeto Adequação da estrutura de Capacitação, Preparo e Emprego Operacional às necessidades do Setor Cibernético	2012	2015
Subprojeto Implantação do Centro de Defesa Cibernética (	2012	2023
Subprojeto Desenvolvimento do Rádio Definido por *Software*	2012	2035

Fonte: Elaboração própria baseada em Brasil (2012b, 251).

Além disso, o Livro Branco afirma que para rever suas capacidades, o Exército necessita da implementação de alguns sistemas, como por exemplo, Recuperação da Capacidade Operacional da Força Terrestre (Recop), Sistema de Proteção Cibernética – Defesa Cibernética, Sistema Integrado de Monitoramento das Fronteiras Terrestres (Sisfron), Sistema Integrado de Proteção de Estruturas Estratégicas Terrestres Críticas (Proteger), Nova Família de Veículos Blindados de Rodas de Fabricação Nacional.

Ainda, dentro do projeto do Exército de defesa cibernética, são previstas quatro ações: construção da sede definitiva do Centro de Defesa Cibernética e aquisição da infraestrutura de apoio, aquisição de equipamentos e capacitação de recursos humanos, aquisições de soluções de *hardware* e *software* de defesa cibernética e implantação dos projetos estruturantes do Setor Cibernético, a fim de ampliar a capacidade de resposta às ameaças. Esses projetos tiveram previsão de curto prazo pelo LBD e abarcam todas as três camadas do espaço cibernético: *hardware*, *software* e *peopleware*. Para o projeto de defesa cibernético, o LBD prevê gastos de R$ 839,9 milhões até 2031, com período de execução até 2035.

Embora tenha foco no setor nuclear, a Marinha considera que sua re-aparelhagem e modernização observe também o setor cibernético. Ele é abordado dentro do projeto de construção do Núcleo do Poder Naval, com previsão de finalização até 2047 e valor global estimado em R$ 7,3 bilhões.

Dentro do projeto, a Marinha pretende criar uma estrutura organizacional para a defesa e ataque de redes de computadores. Cabe ressaltar que não se trata de um projeto de equipamentos e sim de um projeto de articulação.

A capacidade também é observada na minuta do Livro Branco, quando prevê o macroprojeto "Força Terrestre 2035", que ficou sob coordenação do Escritório de Projetos do Exército (EPEx). Este projeto tem entre suas prioridades a construção da Defesa Cibernética do país. Dessa forma, nesse documento, a defesa cibernética continua sendo desenhada como na versão da segunda geração, contendo inclusive o Sistema de Proteção Cibernética – Defesa Cibernética como uma das prioridades.

A maior inovação que o documento traz, conceitualmente falando, é a definição dos chamados "conflitos do futuro", em que a guerra cibernética é apresentada como um componente:

> Outros desafios que se apresentam ao País dizem respeito à sua capacidade de fazer face aos chamados "conflitos do futuro", ou de natureza "híbrida", em que ações de combate convencional são aglutinadas, no tempo e no espaço com operações de natureza irregular, de guerra cibernética e de operações de informação, dentre outras, com atores estatais e não estatais, no ambiente real e informacional, incluindo as redes sociais (Brasil 2016b, 28).

O reconhecimento da Guerra Híbrida, como um desafio a ser enfrentado pelo país foi abordado pela primeira vez nos documentos dessa geração. Seguindo a tendência de novos temas e desafios, o documento também aponta para as novas tecnologias da informação e da comunicação, que de acordo com o texto, trazem implicações para a proteção da soberania brasileira, principalmente por causa das "guerras cibernéticas". O texto aponta, dessa forma, para o uso indevido, como ferramentas militares, do espaço cibernético e das tecnologias que o tangenciam.

ANÁLISE COMPARADA

Podemos inferir que a Política de Defesa Nacional (2005) apresentou um amadurecimento quanto à necessidade de uma defesa bem estruturada, mesmo em um país em que não se envolve em conflito há muito tempo. Essa ausência de conflito provocou uma insensibilidade da população brasileira para com a salvaguarda nacional diante de possíveis ameaças externas.

Diante disso, a política compreende que seu papel também "é conscientizar todos os segmentos da sociedade brasileira de que a defesa da Nação é um dever de todos os brasileiros" (Brasil 2005, 1), principalmente porque espera-se uma disputa e antagonismo na medida em que o Brasil busca

alcançar seus interesses, que, de acordo com o próprio documento, é o protagonismo internacional equivalente à sua posição titânica.

As menções de defesa cibernética feitas no documento se resumem na redução de vulnerabilidades e garantia da resiliência dos demais sistemas de defesa. Ainda que discreta, a abordagem realizada é ampliada nos documentos de defesa seguintes. Entretanto, a essência dos próximos documentos continua sendo esses dois pilares citados na política de 2005.

Comparada com o documento de 2005, a PND de 2012 e a minuta de 2016 pouco acrescentaram nas tratativas referentes à defesa cibernética do país. A nova versão continuou esboçando a preocupação em fortalecer a defesa cibernética, mas a tratou conjuntamente com os demais setores estratégicos: nuclear e aeroespacial. Também manteve a orientação de aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem as vulnerabilidades, permitindo uma ação em rede entre as Forças e a resiliência do sistema.

Já a diferença entre a minuta de 2016 e a PND de 2012 está no realismo adquirido. De acordo com o documento de 2016, não se pode almejar tal independência pelos próximos 20 anos. Isso também impacta negativamente na defesa cibernética, pois significa continuar dependendo de *hardware* estrangeiro e de pontos de transmissão de Internet por satélites, que também são estrangeiros. Entretanto, se faz justo aqui citar que, apesar da insuficiência tecnológica, o país lançou recentemente seu satélite geoestacionário para transmissão de Internet, que está em operação desde junho de 2017, o qual é resultado de um projeto conjunto entre Ministério de Ciência e Tecnologia e Ministério da Defesa (EBC, 2017). Cabe ressaltar que essa conquista ainda não elimina totalmente o risco de ausência de serviço, pois é apenas um satélite, que se neutralizado prejudica ou até mesmo elimina nosso acesso ao espaço cibernético.

No que diz respeito à Estratégia Nacional de Defesa, o documento de 2008 explica que a solução para o desenvolvimento da camada de *hardware* é a camada de *peopleware*. Devemos pensar aqui em operadores capazes de atuarem no espaço cibernético e também de desenvolver tecnologias que possam aumentar nossas capacidades, sem depender do auxílio estrangeiro. Isso garantiria a redução de vulnerabilidades e as resiliências dos sistemas de defesa cibernética, assim como previsto na política de 2005.

A preparação dos recursos humanos não se limita apenas às formações, mas também carece da organização da defesa cibernética e de seus organismos. Neste caso, o documento de 2008 não cita a criação de um Centro de Defesa Cibernética. Apesar disso, este foi ativado em agosto de 2010 e, como previsto na versão de 2012, o centro passaria a ser Comando de Defesa Cibernética (CDCiber), que somente veio a acontecer em 2016.

Cabe ressaltar, entretanto, que embora se diga em evolução organizacional, o CDCiber não deixou de existir com a criação do comando, mas foi subordinado a ele. Com essa previsão, o comando ganharia mais autonomia para operar no espaço cibernético, mas como o intuito desse artigo foi vislumbrar os documentos pertinentes à defesa do Brasil, não adentraremos nessa questão.

A certificação digital também já foi ativada. De acordo com o Instituto Nacional de Tecnologia da Informação (ITI), a defesa brasileira credenciou-se como autoridade certificadora, chamada de AC Defesa, em outubro de 2017 (ITI 2017), com vigência de novembro de 2017 até março de 2019. Cabe ressaltar que as operações de certificação são geradas por tecnologia soberana, fornecida pela empresa totalmente nacional e independente KRYPRUS (Defesanet 2015), observando, assim, os critérios estabelecidos pelos documentos observados de independência tecnológica.

Da mesma forma, foi implementada a Escola Nacional de Defesa Cibernética no ano de 2014, pela Portaria Normativa 2777/2017 do Ministério da Defesa. Ainda nessa portaria, o MD atribuiu ao Estado-Maior Conjunto das Forças Armadas a função de formatar tanto a ENaDCiber quanto a CDCiber. Vale enfatizar aqui a conexão dessas duas instituições com as demais prioridades, especialmente no desenvolvimento de conhecimento e capacitação de *peopleware*.

No decorrer das publicações dos novos documentos, o espaço cibernético foi percebido como um ambiente estratégico para a defesa nacional como um todo, requisitando a atuação em rede. Devido a essa especificidade, o Livro Branco de 2012 afirma que todo o sistema de defesa pode ser comprometido por meio do espaço cibernético. A proteção desses espaços é composta pelas áreas de capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e de pessoal, ou seja, desenvolvimento de *peopleware*. Também necessita de proteção de seus próprios ativos (*hardware* e *software*) e a capacidade de atuação em rede. Todos os investimentos nesse setor consistem em garantir o seguinte objetivo:

> A implantação do Setor Cibernético tem como propósito conferir: confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em suas redes, os quais são processados e armazenados. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas de ciência e tecnologia e operacional (Brasil 2012b, 69).

Esse trecho evidencia que o Exército deverá seguir as premissas da multidisciplinaridade e dualidade. Além disso, essa força também deverá observar a sua atuação no espaço cibernético como uma garantia de liber-

dade das forças armadas como um todo. Conforme o texto, para desenvolver as capacidades, o Brasil deve desenvolver suas capacidades para se defender nesse ambiente informacional.

Em uma atuação mais ampla, o documento afirma que a comunidade internacional deve buscar construir um ambiente cibernético aberto, estável, transparente e seguro. Nesse ponto, o documento entra em desacordo com a política de alguns países, como Estados Unidos e China, que pensam o espaço cibernético como próprio do monopólio dos mais fortes.

Essa preocupação é uma ampliação do debate que já era feito no documento de 2012, inclusive, reafirmando a imagem das ameaças cibernéticas abordadas nos documentos de segunda geração, com seus elementos intra e interorganizacionais. Nessa oportunidade, o documento inclusive cita algumas estruturas que foram previstas na versão anterior e suas funções, as quais ser vislumbradas abaixo:

Quadro 3
Organismos de defesa cibernética citados na minuta do LBDN de 2016

Organização	Descrição
Comando de Defesa Cibernética	Organização militar conjunta, na estrutura organizacional do Comando do Exército, ativada em 15 de abril de 2016 e soma esforços com as organizações governamentais já existentes. Tem como principais atribuições, dentre outras, planejar, orientar, supervisionar e controlar as atividades operacional, de inteligência, doutrinária, de ciência e tecnologia, bem como de capacitação no Setor Cibernético de Defesa.
Centro de Defesa Cibernética	Órgão subordinado ao ComDCiber, que tem por finalidade a execução das atividades operacional e de inteligência no âmbito do Sistema Militar de Defesa Cibernética
Escola Nacional de Defesa Cibernética	Órgão subordinado ao ComDCiber e tem por missão fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, nos níveis de sensibilização, conscientização, formação e aperfeiçoamento.

Fonte: elaboração própria com base em Brasil (2016b).

Esses três órgãos já estão ativos e operam conjuntamente e com composição das três Forças Singulares. Dessa forma, apesar de não tratar de defesa cibernética na sua parte do LBDN, a aeronáutica também participa da defesa cibernética, respeitando, logicamente, a posição do Exército como Força Singular responsável. Para finalizar esse tópico, o documento expõe a mentalidade do Ministério da Defesa que trata a segurança e a defesa cibernética como capacidades de atuação em rede que podem minimizar despesas, aumentar produtividade, conferir efetividade e otimizar

as estruturas tecnológica, informação e comunicação, contribuindo para o desenvolvimento da defesa do Brasil.

Os projetos expostos no livro seguem o princípio do uso dual e industrial exposto na primeira geração de documentos. O Livro Branco exemplifica, ainda, que a "implantação de um Centro de Defesa Cibernético contribuirá para elevar e segurança e a capacidade de atuar em rede tanto na área militar quanto em diferentes setores do governo e da sociedade" (Brasil 2012b, 209). Cabe lembrar que esse exemplo específico somente abarca a classificação dual, não engloba o uso industrial, já que trata de uma estrutura específica da defesa cibernética do Brasil.

Em novembro de 2017 o envio para análise completou um ano e caso seja aprovado em 2018, a Defesa Brasileira somente terá mais dois anos para aplicá-lo. Essa ausência de celeridade no processo legislativo e as mudanças constantes na conjuntura da defesa, que requer constante atualização, demonstra que os processos estipulados para a atualização dos documentos podem afetar a defesa do país. Tal debate deveria ser explorado, tanto na questão do conhecimento como também na forma de pressão acadêmica, mas não vem ao caso nesse artigo, visto que vislumbra somente a evolução da defesa cibernética nesses documentos.

CONSIDERAÇÕES FINAIS

A primeira menção de defesa cibernética nos grandes documentos de defesa do Brasil ocorreu em 2005, com a publicação da Política de Defesa Nacional, que se repetiu na Estratégia Nacional de Defesa de 2008. Em 2010, com o decreto da Lei Complementar nº 136/2010, as atualizações dos documentos de defesa deveriam ser encaminhadas para apreciação do Congresso Nacional de quatro em quatro anos. Desde então podemos considerar os documentos de defesa em gerações, a saber, 1ª Geração (2005 e 2008), 2ª Geração (2012) e 3ª Geração (em apreciação do Congresso Nacional).

Na primeira vez que foi citada, a responsabilidade pela defesa cibernética do Brasil foi atribuída ao Exército e permaneceu assim até os dias atuais. Também ainda são observados atualmente o princípio da mitigação de vulnerabilidades e garantia de resiliência do sistema de defesa brasileiro, apontados na política da primeira geração. Principalmente porque poucas foram as alterações das tratativas de defesa cibernética nas versões seguintes da Política Nacional de Defesa.

A principal alteração que a próxima política terá em relação às versões anteriores é o tom crítico e real de suas colocações. Desde a primeira geração, sendo reforçada na segunda, a PND afirma que o Brasil deve buscar

uma independência tecnológica para garantir sua soberania. Na minuta que está sendo observada pelo Congresso Nacional, o documento deixa claro que nos próximos 20 anos essa conquista não será alcançada, em virtude da atual condição econômica e orçamentária do país.

A Estratégia Nacional de Defesa, nas três gerações, se harmoniza com os demais documentos de defesa no que tange à operação em rede, independência tecnológica e uso industrial do espaço cibernético. Apesar da END de primeira geração não ter trabalhado especificadamente a estrutura do futuro Sistema Brasileiro de Defesa Cibernética, o Centro de Defesa Cibernética foi ativado em 2010 e inaugurado em 2012. Na segunda geração foram colocadas oito prioridades para o Sistema Brasileiro de Defesa Cibernético.

Dentre os pontos que foram abordados nesse documento, vale citar a criação do Centro de Defesa Cibernética, a Escola Nacional de Defesa Cibernética e o credenciamento de uma autoridade para certificação digital específica da Defesa. Além disso, igualmente como podemos observar na PND, a versão da END que está em apreciação se apresenta mais tangível, listando Objetivos Nacionais de Defesa. Por fim, a END da terceira geração observará a defesa cibernética em todas as três forças, singularmente falando, enquanto nas gerações anteriores somente era abordada no âmbito do Exército e da Marinha.

Por sua vez, o Livro Branco de Defesa Nacional que trata da defesa cibernética somente foi publicado na segunda geração. A função desse documento era esclarecer as atividades de defesa realizadas pelo país. Na segunda geração, o documento engloba as questões tratadas nos demais documentos, inclusive os de primeira geração, mas também trata da questão estrutural da defesa cibernética e também do projeto do Sistema Brasileira de Defesa Cibernética. Em seu texto, aponta, principalmente, a necessidade de desenvolvimento da camada *peopleware*, sem esquecer da proteção do *hardware* e *software*.

Na próxima versão do Livro Branco, documento da terceira geração, ainda são reafirmadas as exposições realizadas na versão anterior sobre o espaço cibernético. Também será evidenciada a mentalidade do Ministério da Defesa que trata a segurança e a defesa cibernética como capacidades de atuação em rede que podem minimizar despesas, aumentar produtividade, conferir efetividade e otimizar as estruturas de tecnológica, informação e comunicação, contribuindo para o desenvolvimento da defesa do Brasil. Cabe explicar que a nova versão não aborda tão profundamente todos os aspectos da defesa cibernética, como projetos e estruturas, que havia sido realizada na versão anterior.

Essa ausência de aprofundamento também é percebida nas minutas da Política Nacional de Defesa e Estratégia Nacional de Defesa. Por ser uma versão de apreciação, espera-se que na versão final essas questões sejam abordadas, bem como sejam mais abrangentes, principalmente com a anexação do Plano de Articulação e de Equipamento de Defesa do Ministério da Defesa.

Mesmo que ainda de forma limitada, já podemos dizer que uma das maiores contribuições que os documentos da terceira geração apresenta é o tratamento conflito chamado de "Guerra Híbrida". Nesse conflito, a questão do espaço cibernético se faz evidente, por meio da guerra cibernética. Os documentos inovaram ao demonstrar que o Brasil está preocupado com os desdobramentos desse tipo de guerra, especialmente porque alguns países estão utilizando o espaço cibernético e suas ferramentas como armamentos de guerra.

Por fim, os documentos brasileiros de defesa têm observado com mais veemência a camada *peopleware* do espaço cibernético. Ressaltamos que a abordagem das outras camadas também é considerada, mas com menor ênfase. Isso resulta da necessidade inicial de se organizar o setor, que passa primeiramente pelos recursos humanos, e da dependência brasileira de tecnologia estrangeiras, especialmente devido às restrições econômica e orçamentária enfrentadas pelo país, especialmente no âmbito da defesa nacional.

REFERÊNCIAS

Brasil. 2005. *Decreto 5484/2005:* Política de Defesa Nacional. Brasília: Ministério da Defesa.

_____. 2008. *Decreto 6703/2008:* Estratégia Nacional de Defesa. Brasília: Ministério da Defesa.

_____. 2012a. *Política Nacional de Defesa – Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa.

_____. 2012b. *Livro Branco de Defesa Nacional*. Brasília: Ministério da Defesa.

_____. 2016a. *Minuta da Política Nacional de Defesa e Estratégia Nacional de Defesa*: versão sob apreciação do Congresso Nacional. Brasília: Ministério da Defesa.

_____. 2016b. *Minuta do Livro Branco de Defesa Nacional*: versão sob apreciação do Congresso Nacional. Brasília: Ministério da Defesa.

Brasscom. 2017. *Brasil TI-BPO Book*. Brasil IT+. Brasília: ApexBrasil.

Clarke, Richard A; Knake, Robert A. 2012. *Cyber War*: The Next Threat to National Security and What to do About It. New York: HarperCollins Publishers.

Defesanet. 2017. Kryptus: Fornecerá para a Autoridade Certificadora da Defesa (AC-DEFESA). Defesanet, Porto Alegre, mar. 2015. Tecnologia. Disponível em <http://www. defesanet. com. br/cyberwar/noticia/18349/KRYPTUS---Fornecera-para-a-Autoridade-Certificadora-da-Defesa-%28AC-DEFESA%29/>. Acesso em 04 dez. 2017.

EBC. 2017. Primeiro Satélite Brasileiro inicia operações e fica sob responsabilidade da FAB. *Agência Brasil*. Geral. 05 de julho de 2017. Disponível em: <http://agenciabrasil. ebc. com. br/geral/noticia/2017-07/primeiro-satelite-brasileiro-inicia-operacoes-e-fica-sob-responsabilidade-da>. Acesso em 28 nov. 2017.

Ferreira Neto, Walfredo B. 2014. Territorializando o "Novo" e (Re)Territorializando os Tradicionais: a Cibernética como Espaço e Recurso do Poder. In: Medeiros Filho, Oscar; Ferreira Neto, Walfredo B. ; Gonzales, Selma Lúcia de Moura (Org.). *Segurança e Defesa Cibernética*: da Fronteira Física aos Muros Virtuais. Pernambuco: Editora UFPE. (Coleção I - Defesa e Fronteiras Cibernética).

ITI. 2017. *AC Defesa é credenciada à ICP-Brasil. Brasília*: Casa Civil da Presidência da República. Disponível em <http://www. iti. gov. br/noticias/indice-de-noticias/711-ac-defesa-e-credenciada-a-icp-brasil>. Acesso em 04 dez. 2017.

Knight, Peter T. A. 2014. *Internet no Brasil*: Origens, Estratégia, Desenvolvimento e Governança. Bloomington: AuthorHouse.

Mandarino Jr. , Raphael. 2010. *Segurança e Defesa do Espaço Cibernético Brasileiro*. Recife: Cubzac.

Marconi, Marina de A. ; Lakatos, Eva M. 2003. *Fundamentos de Metodologia Científica*. São Paulo: Atlas.

Ministério da Defesa. 2014. *Doutrina Militar de Defesa Cibernética*. Brasília: Estado-Maior Conjunto das Forças Armadas.

Lins, Bernardo. 2007. Perfil Industrial do Setor de Software. In. : Conselho de Altos Estudos e Avaliação Tecnológica. *O Mercado de Software no Brasil: Problemas Institucionais e Fiscais*. Brasília: Câmara de Deputados.

Raffestin, Claude. 1993. *Por uma Geografia do Poder*. Paris: Ed. Ática.

Richardson, Roberto J. 1999. *Pesquisa Social:* Métodos e Técnicas. São Paulo: Atlas.

Unctad. 2017. *Information Economy Report 2017*. Switzerland: United Nations Publications.

Unoosa. 2016. *Lauched into Outer Space:* Database of Unoosa. Vienna: United Nation.

Ventre, Daniel. 2012. Ciberguerra. In: Academia General Militar. *Seguridad Global y Potencias Emergentes en un Mundo Multipolar*. XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza.

AS CAMADAS DO ESPAÇO CIBERNÉTICO
SOB A PERSPECTIVA DOS DOCUMENTOS DE DEFESA DO BRASIL

RESUMO

O espaço cibernético se concretizou no decorrer da história como um espaço geográfico contemporâneo, onde as relações político-sociais encontram continuidade. No âmbito da defesa, esse espaço se tornou mais uma arena de jogo de poder das relações internacionais. Apesar do espaço cibernético já ter sido considerado importante desde sua criação, a percepção estratégica dele para defesa é relativamente recente.
No Brasil, o espaço cibernético se tornou focal apenas na Política de Defesa Nacional de 2005, ocasião em que foi equiparada a mais duas áreas: aeroespacial e nuclear. No documento daquele ano, a defesa cibernética do país foi atribuída ao Exército, que deveria coordenar as operações, inclusive nos âmbitos das demais forças. No Livro Branco de 2012, a preocupação pela defesa desse espaço gerou objetivos concretos, como a criação do Centro de Defesa Cibernética (CDCiber) e o Sistema Brasileiro de Defesa Cibernética.
Atualmente, os documentos que abordaram essa temática estão sendo debatidos e rediscutidos. As novas edições estão próximas de serem finalizadas e nos causa uma indagação: como esses documentos abordam as três camadas que compões o espaço cibernético (*hardware*, *software*, *peopleware*), especialmente as próximas versões. Por fim, esse artigo é dividido em três partes: considerações iniciais; documentos de primeira geração; documentos de segunda geração e as minutas dos novos documentos, que estão em apreciação no Congresso Nacional.

Palavras-chaves: Espaço Cibernético; Livro Branco de Defesa Nacional; Estratégia Nacional de Defesa; Política Nacional de Defesa; Brasil.

ABSTRACT

Cyberspace has become, in the course of history, a contemporary geographic space, where political-social relations find continuity. In the area of defense, this space has become another playing field of international relations. Although cyberspace has already been considered important since its inception, its strategic perception for defense is relatively recent.
In Brazil, this space became focal only in the National Defense Policy of 2005, when it was equated with two other areas: aerospace and nuclear. In the document, the Brazil's cyber defense was assigned to the Army, which

was to coordinate operations, including in the ambits of other forces. In the White Paper of 2012, the concern for the defense of this space generated concrete objectives, such as the creation of the Center for Cyber Defense and the Brazilian System of Cyber Defense.
Currently, the White Paper, the National Defense Strategy and the National Defense Policy are being debated and revised. The new issues are close to being finalized and cause us a question: how do these documents approaches the three layers that make up the cyberspace (*hardware*, *software*, *peopleware*), especially the news versions. This article is divided into three parts: initial considerations; first-generation documents; second generation documents and the drafts of the new documents, which are under consideration in the National Congress.

Keywords: Cyberspace; White Paper on National Defense; National Defense Strategy; National Defense Policy; Brazil.

Recebido em 19/12/2017. Aceito para publicação em 24/04/2018.