ISSN: 2525-457X
Análise Estratégica
Vol 17 (3) Jun/ Ago 2020

Cibernética como Setor Estratégico no Brasil e seus Reflexos para a Estrutura da Defesa (2008-2018)

Cybernetics as a Strategic Sector in Brazil and its Effects on the Defense Structure (2008-2018)

Walfredo Bento Ferreira Neto*

RESUMO

O presente artigo trata da cibernética como setor estratégico no Brasil e seus reflexos para a estrutura de Defesa, no recorte de 2008 a 2018. Apresenta-se a constituição do setor cibernético no País, sua posição dentro da estrutura da Defesa e a que procurou responder. Após análise dos principais documentos de Defesa, destaca-se as diretrizes relacionadas com a cibernética e as ações implementadas pelo Exército Brasileiro, Força responsável pela coordenação desse setor, em face de questões teóricas e reais, de ordem geopolítica e econômica, que envolvem as relações internacionais. Como conclusão, pode-se observar que a condução desse setor procurou responder não só a questões ligadas à especialização da segurança do ciberespaço em si e de sua estrutura, mas também ao aumento da capacidade de monitoramento e controle do território e, ainda, ao desenvolvimento, visando a fornecer um bem público puro para a sociedade, porém com externalidades positivas e transbordamentos de natureza econômico-tecnológica (*spin-off*). Buscou-se, portanto, conciliar o clássico dilema acerca do investimento público em "espadas ou arados".

Palavras-chave: Cibernética; Setor Estratégico; Defesa; Brasil.

ABSTRACT

This article deals with cybernetics as a strategic sector in Brazil and its reflexes for the Defense structure, from 2008 to 2018. It presents the constitution of the cyber sector in the Country, its position within the Defense structure and which it sought to answer. After analyzing the main Defense documents, the guidelines related to cybernetics and the actions implemented by the Brazilian Army stand out, Force responsible for the coordination of this sector, in the face of theoretical and real issues, of a geopolitical and economic order that involve international relations . As a conclusion, the conduct of this sector sought to answer not only questions related to the specialization of cyberspace security itself and its structure, but also to the increase in the monitoring and control capacity of the territory and, also, to development, aiming to provide a good pure public for society, but with positive externalities and spillovers of an economic-technological nature (spin-off). It sought, therefore, to reconcile the classic dilemma about public investment in "swords or plowshares".

Keywords: Cybernetics; Strategic Sector; Defense; Brazil.

* Major do Exército Brasileiro do QCO Mag/Geografia. Mestre em Estudos Estratégicos pelo Inest/UFF e Doutor em Economia Política Internacional, pelo Pepi/UFRJ. É Professor de Geopolítica da AMAN.

1. Introdução

O presente texto teve como base pesquisa de tese de doutorado realizada no Programa de Economia Política Internacional (Pepi) da Universidade Federal do Rio de Janeiro (UFRJ), intitulada "*Uma Estratégia Nacional de Defesa para Além da Guerra: geopolítica cibernética no Brasil e seu transbordamento econômico-tecnológico (2008-2018)*", mais precisamente em seu capítulo 3, que tratou da cibernética vista como um setor estratégico para o Brasil, a partir da Estratégia Nacional de Defesa (2008), e suas consequências para a estrutura de Defesa[1] do País.

Nessa referida pesquisa foi constatado que o tratamento dado à cibernética vai além de recurso com emprego na indústria e no comércio (*e-commerce*). Na verdade, a cibernética – que foi idealizada, em meados do século XX, como o ramo científico que pudesse, dentre outros, prever a trajetória balística de um projetil de artilharia em direção ao seu alvo, logo idealizada na seara militar – ganhou alcance global pela sua capilaridade geográfica e pela velocidade temporal, por meio de infovias, a partir da criação de redes de computadores e de pontos por onde circula e é difundida a informação digitalizada.

Da mesma forma que na sua origem, nos Estados Unidos, fruto de esforços voltados para a corrida armamentista durante a Guerra Fria, esse recurso continuou – e continua – a ser tratado como crucial para questões envolvendo segurança e abrigo, poder e riqueza. A conjugação das ações estadunidenses para o ramo de tecnologia na área de Defesa ensina o quanto pode ser produtivo o capital empregado nesse setor, tanto pela capacidade de dissuasão do Estado, quanto pela possibilidade de transbordamento para a área privada, o que fomenta a economia e, por conseguinte, o Desenvolvimento. Isso é alcançado por meio do efeito multiplicador[2] econômico que proporciona o setor cibernético, pelo uso, em sua essência, de equipamentos de TIC (Tecnologias da informação e comunicação), que pode ser associado ao *core* de mais um dos ciclos econômicos virtuosos de inspiração *schumpteriana*.

Outra lição apreendida trata da sinergia obtida entre Estado, indústria e academia, também nos Estados Unidos, denominado complexo militar, industrial-acadêmico. Inúmeros são os exemplos de artefatos com fins militares, planejados no âmbito da Defesa, pensados na academia e produzidos pela indústria: microondas, *internet*, computadores, GPS etc. (MEDEIROS, 2004; MORAES, 2004; RUTTAN, 2006; WU, 2006; MAZZUCATO, 2014).

De tudo isso restou, em síntese, que movimentos políticos, visando à preparação para a guerra, podem estar imbricados a ganhos econômicos, desde que coerentemente planejados, atendendo às particularidades geográficas e históricas de cada território e sociedade. Assim, é possível tornar virtuosa a preparação para o "jogo das guerras" (FIORI, 2004) e para o "das trocas" (BRAUDEL, 1987), ainda mais no ciberespaço, meio no qual trafega uma das principais fontes de segurança e de riqueza. Assim, o Estado, e sua sociedade, podem conseguir conciliar o longínquo dilema entre "espadas e arados", ou entre "canhões e manteiga".

Pode-se constatar que esforços realizados nesse sentido consideram indubitavelmente a geopolítica tradicional (clássica) e a contemporânea, mas não ignoram de forma alguma a geoeconomia (BLACKWILL; HARRIS, 2016), na busca de interação exitosa, com *spin-off* [3], algo do tipo:

[1] Como padronização, optou-se pela grafia de Defesa com inicial em maiúscula, quando referente à instituição e não a ações de defesa propriamente dito. Da mesma forma Desenvolvimento, quando se referir ao esforço nacional como um todo.

[2] Efeito multiplicador: "[...] é a razão entre a mudança no PIB real causada por uma mudança autônoma no gasto agregado e o tamanho da mudança autônoma." (KRUGMAN, 2007, p. 610). Deriva do efeito indireto obtido com um aumento do gasto agregado. No caso de investimento público em fornecimento de *internet*, por exemplo, pode ser gerado o denominado *benefício marginal social*, quando uma unidade adicional de um bem público é maior que o *benefício marginal individual*. É uma externalidade positiva.

[3] Segundo Rossetti, podem ser vistos pelos "'transbordamentos' de tecnologias militares para fins

"uma ação, dois ou mais movimentos". Tudo isso tratado no nível mais profundo da economia nacional, conforme trouxe Friedrich List e sua formulação do sistema nacional de inovação (PADULA, 2007), no qual os pressupostos da corrente liberal ou neoliberal das relações internacionais não conseguem responder à toda realidade, pelo menos não àquela dos que não possuem o controle das infovias.

O recorte textual se restringe às iniciativas brasileiras para o setor estratégico da cibernética, com ações ora visando ao ciberespaço, ora visto como recurso de poder, relacionado a esforços que vão para além do setor Defesa *stricto sensu*, mas que também influenciam este diretamente e, mais que isso, fomentam o desenvolvimento tecnológico e, por consequência, o econômico-social.

O objeto de estudo, estritamente tratando, passa a ser o desenvolvimento do setor estratégico da cibernética a partir da publicação da Estratégia Nacional de Defesa (END) de 2008, e de suas versões posteriormente publicadas (2012 e 2016), e de documentos afins, publicados em consequência ou posteriormente, como a Política Nacional de Defesa (PND) (2012 e 2016) e o Livro Branco de Defesa Nacional (LBDN) (2012 e 2016).

Inicialmente, a título de contextualização, são apresentadas as principais partes da END, as intenções nela contidas, a formulação de seus eixos estruturantes, diretrizes e setores estratégicos.

A seguir, verifica-se outro ponto que despertou muita atenção, no tocante à intenção de conjugar Defesa e Desenvolvimento, isto é, o que foi pensado oficialmente abarcava tanto a necessidade de melhoria dos materiais e equipamentos das Forças Armadas (coerção), quanto o fomento do desenvolvimento (riqueza), por meio de estreitamento institucional entre Estado, indústria e academia. Ainda sobre esse ponto, assim mencionou a END no primeiro parágrafo de sua Introdução:

> Estratégia nacional de defesa é inseparável de estratégia nacional de desenvolvimento. Esta motiva aquela. Aquela fornece escudo para esta. Cada uma reforça as razões da outra. Em ambas, se desperta para a nacionalidade e constrói-se a Nação. Defendido, o Brasil terá como dizer não, quando tiver que dizer não. Terá capacidade para construir seu próprio modelo de desenvolvimento. (BRASIL, 2008, p. 8)

Na sequência do texto aborda-se o setor estratégico da cibernética e respectivos programas e projetos. Quando verificado a pertinência, foram inseridos elementos e ideias constantes de outros documentos de Defesa, na expectativa de mostrar de forma mais completa possível o arcabouço montado para o setor cibernético. Ainda, na medida em que seu conteúdo permitiu comentário e emissão de juízo de valor, com ligação a outros aspectos, teóricos ou reais, foram feitos alguns acréscimos, a fim tornar mais fluidos o texto e a compreensão por parte do leitor, também buscando a ideia de "uma ação, dois movimentos".

2. A END e os setores estratégicos dentro da concepção do binômio *Defesa-Desenvolvimento*

2.1 Da necessidade do binômio *Defesa-Desenvolvimento*; *coerção-capital*; *poder-riqueza*

Talvez esse seja o ponto que mais despertou interesse para a pesquisa realizada. Desde que se iniciou percurso pela seara da Defesa, tinha-se algumas inquietações que perpassavam pela busca da conciliação entre necessidades da Defesa com suas possibilidades de Desenvolvimento. Essa questão é crucial, pois da forma como é respondida, a princípio, pode servir de aspecto positivo, para além da própria Defesa, ou de negativo, constituindo-se tanto em mais um não cumpridor do mínimo necessário com relação à área de Defesa, como em mais um

civis ou [...] de transferência de P&D originários de investimentos em C&T dos institutos militares de pesquisa e convertidos em produtos de interesse da indústria privada de bens finais de consumo ou de acumulação de capital produtivo." (ROSSETTI, 2016, p 222).

dreno de recursos públicos de um País em desenvolvimento com todas as características que lhes são peculiares. Aqui se procurou responder à seguinte questão: como conciliar Defesa-Desenvolvimento em um País que não se envolve em guerras? Como garantir investimentos em Defesa e, ao mesmo tempo, conseguir se desenvolver ou, pelo menos, ocasionar benefícios econômico-sociais?

Faz-se necessário lembrar que Defesa é tida, economicamente tratando, como um bem público, "pelo fato de seu consumo não ser excludente e não rival, isto é, o consumo de uma pessoa não reduz a disponibilidade do bem, e não impede (não exclui) o consumo de outra. [...] Exemplos disso são os casos de segurança nacional, da justiça, [...]." (VASCONCELOS, 2015, p. 105). Mais que bem público, Defesa (segurança nacional) é bem público *puro*, eis que o Estado mantém a exclusividade de deu fornecimento, oriundo do monopólio da coerção *weberiano*, o que exclui, legalmente, qualquer outra possibilidade de oferta. Dessa forma, a abordagem sobre a tarefa de proporcionar esse bem à sociedade deve buscar consequências, preferencialmente, para além da área de Defesa, pois assim se minimiza os reflexos no orçamento. As intenções do Estado brasileiro, de maneira geral, apontam nessa direção, apesar de em alguns momentos estar disposto a priorizar a segurança em relação à economia:

> O componente estatal da Base Industrial de Defesa deverá, em princípio, projetar e produzir o que o setor privado não pode fazê-lo de forma rentável no curto e no médio prazos. Dessa forma, o Estado buscará atuar no teto tecnológico, em estreito vínculo com os centros avançados de pesquisa das Forças Armadas e das instituições acadêmicas brasileiras. (BRASIL, 2017, p. 38) [4]

De 2008 até 2012, houve avanço no tocante a esse intento, isto é, em conjugar o dilema entre "espadas e arados" (ROSSETTI, 2016), entre capital não reprodutivo e reprodutivo. O marco legal anunciado como necessário na primeira edição da END foi consolidado por meio de uma medida provisória (MP nº 544/2011), transformada em lei (Lei nº 12.598, de 22 de março de 2012), e que teve por finalidade "determinar normas especiais para as compras, contratações e desenvolvimento de produtos e sistemas de defesa" (BRASIL, 2012, p. 100), visando incentivar a área de Defesa. Ficou conhecido como Retid (Regime Especial Tributário para Indústria de Defesa).

O teor dessa lei e o espírito contido nela, o que os juristas denominam *mens legis*, trouxe indubitavelmente lições apreendidas a partir de Friedrich List (PADULA, 2007) e de Ha-Joom Chang (2004), e por quem se debruçou sobre a história das grandes potências, uma vez que alerta que o incremento do setor de Defesa deve ser visto para além de fórmulas e métodos quantitativos ligados à economia ou à famosa lei do mercado. Em várias passagens textuais a END chama atenção para isso:

> A defesa do Brasil requer a reorganização da Base Industrial de Defesa [...] – o que deve ser feito de acordo com as seguintes diretrizes: (b) Subordinar as considerações comerciais aos imperativos estratégicos. (BRASIL, 2012, p. 99).

> Tal regime (o da Lei nº 12.598) resguardará as empresas que fornecem produtos de defesa às Forças Armadas, das pressões do imediatismo mercantil [...]. (BRASIL, 2012, p. 100).

Do geral para o particular, e não de forma taxativa, buscou-se esforços do Exército – Força responsável pelo setor cibernético – para atender à END. No todo, esses são os benefícios divulgados pelo Escritório de Projetos do Exército (EPEx), conforme Quadro 1, no que diz respeito aos programas e projetos desenvolvidos por esta Força:

[4] Projeto de Decreto Legislativo nº 847, de 2017, do Senado Federal. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=CE373BF6ED4A5CF5DFEF7ED0D9191025.proposicoesWebExterno2?codteor=1675427&filename=Avulso+-PDC+847/2017. Acesso em: 18 nov. 2019.

Quadro 1: Benefícios à Sociedade do Portfólio Estratégico do Exército

- **Estimular o Desenvolvimento Nacional** pela geração de empregos e aumento da renda, pelo fortalecimento da Base Industrial de Defesa (BID) e pela capacitação da mão-de-obra brasileira.
- **Proporcionar o apoio à Segurança Pública** pelo incremento da interoperabilidade dos Órgãos e Agências Governamentais, pelo fortalecimento da presença do Estado nas fronteiras e pelo combate a ilícitos transfronteiriços e aumento da segurança nos centros urbanos.
- **Promover a Paz Social** por meio da presença do Estado Brasileiro nos rincões mais desabitados do Brasil, da garantia do patrimônio público, da prevenção e redução da ocorrência de crises, da proteção de infraestruturas estratégicas e pela ampliação da integração nacional.
- **Incrementar a Pesquisa, o Desenvolvimento e a Inovação** pelo fomento dos institutos tecnológicos e entidades acadêmicas, pelo fortalecimento do modelo sustentável, pelo uso dual de tecnologia, pela promoção da independência tecnológica e pelo domínio de tecnologias sensíveis.
- **Aumentar a capacidade de Dissuasão contra Ameaças** por intermédio do incremento da capacidade operacional da Força Terrestre, da rearticulação de tropas no território nacional, e da criação de novas capacidades militares terrestres.
- **Promover a Projeção Internacional,** que se dará pelo respaldo à Política Externa brasileira, pelo aumento de exportação de bens e serviços com alto valor agregado, pela diversificação da pauta de exportações e pelo aumento do prestígio internacional, gerando confiança e atraindo investimentos.

Fonte: o autor, a partir do *site* do EPEx (2019).

Como dito, esses benefícios constam como componentes do planejamento de todos os programas conduzidos pelo Exército, o que inclui os ligados à defesa cibernética. Em todos esses também foi perceptível o alinhamento com a END, sobretudo quanto à relação Defesa-Desenvolvimento, coerção e riqueza.

O EB sistematizou essas ações em portfólio com três dimensões. Foram essas: 1) Defesa da Sociedade; 2) Geração de Força; 3) Dimensão Humana. Desses elencados, merece destaque o subportfólio *Defesa da Sociedade* e, especificamente, inserido nesse, os programas *Defesa Cibernética na Defesa Nacional* e o *Estratégico da Defesa Cibernética*. Contudo, identificou-se que há áreas de interseção entre este e os outros subportfólios. Antes de conhecer esses programas, porém, é preciso identificar a sua origem, concretizada via um documento oficial intitulado *Estratégia Nacional de Defesa*, publicado em 2008, e em suas atualizações.

2.2 Estratégia Nacional de Defesa (2008, 2012 e 2016) [5]

A publicação da primeira Estratégia Nacional de Defesa do Brasil ocorreu em 2008, constituindo assim um marco no que diz respeito à Defesa. Com isso, não se está afirmando que anteriormente não existiam documentos de Defesa no Brasil, mas sim é registrada a novidade que trouxe este especificamente, tanto por detalhar a política de Defesa existente até então, pois à época a política em vigor era a de 2005, quanto servir de base para implementação de ações concretas no tocante à Defesa. Além disso, disse a literatura especializada no assunto (OLIVEIRA, 2009; LIMA, 2010) que esse documento teve também a intenção de convidar a sociedade para os debates acerca da definição dos objetivos da Defesa brasileira[6].

[5] As duas primeiras edições da END são bem parecidas, textualmente tratando. Deu-se mais ênfase quando se detectou mudança de rumo em alguma diretriz ou objetivo, ocasião em que se informou o ano-referência do documento-fonte. A END encaminhada ao Congresso Nacional em 22 Jul 2020 não foi objeto desta pesquisa.

[6] A END (2008) foi tão marcante em termos de proposta de aproximação Estado-Sociedade, no que diz respeito à Defesa, que a própria nomenclatura dos documentos foi alterada: a política de defesa, apresentada em 2012 e aprovada em 2013, era antes denominada Política de Defesa Nacional (1996 e 2005) e veio, nessa então nova versão, sob o título de Política Nacional de Defesa. A alteração da posição do termo Nacional não foi por descuido ou por erro técnico gramatical. Em discussões sobre este assunto específico, a ideia extraída foi a de realmente se materializar a proposta de que Defesa deveria ser um

2.2.1 Eixos Estruturantes e Diretrizes Estratégicas

A END (2008) foi sistematizada em 3 eixos estruturantes: a) reorganização das Forças Armadas; b) reestruturação da indústria brasileira de material de defesa e c) política de composição dos efetivos das Forças Armadas. De maneira geral, esses eixos trazem implicações para a implantação e condução do setor cibernético, como a criação de instalações físicas para as operações cibernéticas, a capacitação e retenção de recursos humanos nessa seara e a sinergia entre necessidades das Forças, capacidade industrial e possibilidades acadêmicas. Continuando, buscou-se analisar esse documento e suas intenções mais detalhadamente com base nas 25 diretrizes gerais de Defesa e nos objetivos estratégicos específicos de cada Força[7].

Das diretrizes gerais, as que possuem relação direta, quando citam o setor cibernético explicitamente, ou indireta, na medida em que influem ou podem ser influenciadas por este, são apresentadas abaixo, consoante o número atribuído a elas na END (2008). Assim:

– **Diretriz Estratégica nº 2**: declarou que as Forças Armadas devem se organizar sob o trinômio *monitoramento/controle*, *mobilidade* e *presença*. Desses, destaca-se o primeiro conceito, tendo em vista a possibilidade que traz para os outros dois, que são, portanto, seus derivados.

A *mobilidade* pode ser relativa ao nível estratégico, entendida neste caso como "a aptidão para se chegar rapidamente ao teatro de operações" (BRASIL, 2008, p. 11), ou ao nível tático, entendida como "a aptidão para se mover dentro daquele teatro." (BRASIL, 2008, p. 11). Dessa forma, tanto para chegar à porção do território que demandar por ações de defesa, quanto para operar neste espaço, há uma intrínseca necessidade da obtenção, de tratamento e de armazenamento de informações, logo de comando/controle, em escala temporal que permita se tornar efetiva e eficaz determinada operação.

Da mesma forma é a *presença*, que por sua vez depende da *mobilidade*. Assim, logo pela diretriz de nº 2, a Estratégia anunciou a opção pelo uso de recursos tecnológicos, sejam informacionais e de comunicações, sejam ligados à capacidade de transporte, em detrimento da presença permanente de tropa em todo o território nacional, o que seria, neste último caso, inviável, tendo em vista sua dimensão de mais de 8.500.000 Km^2, sem contar o espaço abrangido pela Amazônia Azul.

Inicialmente, havia a previsão de implementação de cerca de mais vinte e cinco pelotões especiais de fronteiras (PEF), organizações militares localizadas, como o nome indica, em regiões fronteiriças inóspitas e de difícil acesso.

Após a aprovação da END, entretanto, essa intenção foi alterada, em parte, pelos esforços feitos pelo SisFron [8], isto é, os cerca de 25 Pelotões Especiais de Fronteira foram preteridos por projetos que priorizaram tecnologias informacionais.

Esse ponto foi bastante reforçado na diretriz de nº 9 também desse documento, quando tratou da relação entre presença de unidades militares na região de fronteira via monitoramento/controle e mobilidade, e não de forma onipresente.

tema discutido e apreciado pela sociedade, como um todo.

[7] Ao todo, são enunciados 10 (dez) objetivos e respectivas explicações pela Marinha do Brasil, 11 (onze) pelo Exército Brasileiro e 5 (cinco) pela Força Aérea Brasileira.

[8] Isso aliado ao já existente Centro Gestor e Operacional do Sistema de Proteção da Amazônia (Censipam), logo ao Sipam/Sivam, o qual "deverá atuar integradamente com as FA, a fim de fortalecer o monitoramento, o planejamento, o controle, a logística, a mobilidade e a presença na Amazônia." (BRASIL, 2012, p. 54). Para isso o Censipam foi incorporado à estrutura organizacional do Ministério da Defesa "agregando sua base de dados atualizada, conceitos de emprego dual da informação e integração de informações de órgãos civis com atuação na Amazônia brasileira." (BRASIL, 2012, p. 114). Essa foi uma novidade da END 2012 em relação à sua versão de 2008.

> Nas fronteiras terrestres, nas águas jurisdicionais brasileiras e no espaço aéreo sobrejacente, as unidades do Exército, da Marinha e da Força Aérea têm, sobretudo, tarefas de vigilância. No cumprimento dessas tarefas, as unidades ganham seu pleno significado apenas quando compõem sistema integrado de monitoramento / controle feito, inclusive, a partir do espaço. [...] Os vigias alertam. As reservas respondem e operam. E a eficácia do emprego das reservas táticas regionais e estratégicas é proporcional à capacidade de atenderem à exigência da mobilidade. (BRASIL, 2008, p. 53)

Em uma correlação com conceitos geográficos, o que se constata é uma mudança na concepção estratégica ao considerar não só a questão das distâncias espaciais, dentro de um enfoque geopolítico tradicional, mas também a de escala temporal, o que Becker (2012 [1988]) denominou cronopolítica. A questão passa a incorporar a noção de espaço-tempo, instigando, para sua resolução, portanto, além da capacidade logística, o conceito de rede e a informação. Nesse aspecto, mais uma vez, a cibernética se torna, nos tempos atuais, imprescindível, pois é relacionada diretamente à possibilidade de comando e controle, que gera consciência situacional, resultando na melhor colocação de peças no tabuleiro, ou no teatro de operações, dentro do menor tempo possível. E isso é capaz de definir resultado, tanto de concorrência comercial quanto de um conflito bélico.

– Diretriz Estratégica nº 3: trouxe a intenção de desenvolvimento de capacidades para fins de monitoramento e controle do território brasileiro em todas as suas dimensões, a partir da utilização de tecnologias que estejam sob inteiro e incondicional domínio nacional. Aqui a END reforçou a busca pelo comando e controle e também anunciou a preocupação com a origem das capacidades desenvolvidas ou atingidas. Nesse aspecto, além do sentido estrito de cibernética, correspondente a computadores, abre-se debate para a conexão entre os sistemas de monitoramento e controle do território. [9]

– Diretriz Estratégica nº 6: tratou do anúncio dos três setores estratégicos – o espacial, o cibernético e o nuclear. É por meio do fortalecimento desses setores, anunciou a Estratégia, que se contribui para a capacitação dos recursos humanos no conceito de *flexibilidade*[10], este entendido de forma ampla, abrangendo previsão de capacidade para operar em ambiente de guerra convencional ou não convencional, em operações de amplo espectro, que envolvam conflito, crimes, defesa civil e assistência humanitária em um único recorte espacial, por exemplo[11]. O próprio uso de tecnologias que permitam atender aos requisitos do *monitoramento e controle*, *mobilidade* e *presença* favorecem ao desenvolvimento da *flexibilidade*.

> *Flexibilidade* é a capacidade de empregar forças militares com o mínimo de rigidez preestabelecida e com o máximo de adaptabilidade à circunstância de emprego da força. Na paz, significa a versatilidade com que se substitui a presença – ou a onipresença – pela capacidade de se fazer presente (*mobilidade*) à *luz da informação (monitoramento e controle)*. (BRASIL, 2008, p. 23, *grifo do autor*)

[9] Como o Satélite Geoestacionário de Comunicações Estratégicas (SGDC-1).

[10] Considerado como um imperativo estratégico, no título da subseção referente aos objetivos estratégicos do Exército: "O Exército Brasileiro: os imperativos de flexibilidade e de elasticidade" (BRASIL, 2008, p. 23). A END (2012) não trouxe esse título da subseção, mas repetiu a redação na íntegra.

[11] Esse cenário também é denominado "guerra em três quarteirões", onde em um único teatro de operações tem-se áreas (quarteirões) com demandas distintas. Em cada quarteirão a tropa no terreno teria atribuições de perfis diferentes: guerra convencional, ação humanitária e segurança de instalações ou de pessoas, por exemplo. Isso é largamente vivenciado por militares que participam de operação de manutenção da paz das Nações Unidas. Ainda, essa descrição pode ser vista como resposta ao conceito de segurança e sua ampliação, conforme a própria END (2012) e PND (2012) trouxeram.

> [...] Cada combatente deve ser treinado para abordar o combate de modo a atenuar as formas rígidas e tradicionais de *comando e controle*, em prol da *flexibilidade*, [...] no campo de batalha.
>
> Ganha ascendência no mundo um estilo de produção industrial marcado pela atenuação de contrastes entre atividades de planejamento e de execução e pela relativização de especializações rígidas nas atividades de execução. Esse estilo encontra contrapartida na maneira de fazer a guerra, cada vez mais caracterizada por extrema *flexibilidade*. (BRASIL, 2012, p. 57, *grifo do autor*)

Ainda quanto aos setores estratégicos, a END (BRASIL, 2012) traz uma seção específica para esses, na parte "Formulação Sistemática". Já na primeira parte relativa ao setor cibernético, a Estratégia anunciou que deve ocorrer capacitações no mais amplo espectro de usos, não só militar, incluindo também as industriais e de educação. Como inferência, conclui-se que em mais essa parte do documento é evocada a preocupação com o uso dual. Além disso, a END (BRASIL, 2012) acenou para a necessidade de se atuar em rede, que, como exposto, é relacionada com a mudança na forma de se planejar e executar os novos espectros de conflitos, nos quais a variável *tempo* pode superar os óbices ligados ao *espaço*.

Como a Estratégia Nacional de Defesa é, precipuamente, destinada ao Ministério da Defesa, a prioridade foi dada à possibilidade de integrar, via tecnologias de comunicação, todo o contingente das Forças Armadas. Todavia, após análise e avaliação da PND e END como um todo, tem-se que não é só para as Forças Armadas que este setor vem sendo pensado – e executado. Abaixo, no Quadro 2, são listadas, resumidamente, as prioridades do setor cibernético constantes na END (BRASIL, 2012)[12] e que consistem em avanços com relação à de 2008, que se expressava ainda de forma bem genérica:

> As capacitações cibernéticas [...]. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. (BRASIL, 2008, p. 33)

Quadro 2: Prioridades do Setor Cibernético na END – 2012

Prioridades	
(a)	Fortalecer o Centro de Defesa Cibernética (do Exército) 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 de 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**, e **Elaborar, com participação de outros Ministérios, 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**.
(f)	Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos em prol das operações conjuntas e da **proteção das infraestruturas estratégicas**.[13]
(g)	Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas.

[12] Grifou-se aquelas prioridades que, em princípio, transbordam a esfera das Forças Armadas.

[13] A literatura e os documentos oficiais no recorte temporal da pesquisa trouxeram os termos *infraestruturas críticas*, *infraestruturas estratégicas* e *estruturas estratégicas* com o mesmo significado, referindo-se a estruturas sensíveis ao poder nacional, tais como rede de energia elétrica, de telecomunicações e de transporte.

(h)	Estruturar a produção de conhecimento oriundo da fonte cibernética.

Fonte: END (2012, pp. 93-95, **grifo do autor**).

Portanto, da END 2008 para a de 2012, houve um detalhamento maior dos objetivos acerca das capacitações cibernéticas necessárias e também ocorreram de forma mais nítida ações localizadas na interseção dos subportfólios apresentados pelo EPEx. Como exemplo, enquanto na versão 2008 constou a previsão de uma organização para desenvolver a capacitação cibernética, a de 2012 já tratou nominalmente dessa organização, vislumbrando a possibilidade de sua alçada a um nível que envolvesse todas as Forças Armadas, em conjunto, o que ocorreu, de fato, em 2016, com a criação do Comando de Defesa Cibernética (ComDCiber), e ainda previu a ampliação da relação entre este Comando e a segurança de estruturas estratégicas nacionais.

No tocante ao Quadro 2, conforme identificação das prioridades, ainda se destaca o seguinte:

(a) o que fora antes um incipiente Núcleo de Defesa Cibernética (NuDCiber), em 2009/2010, localizado de forma provisória em instalações do Quartel-General do Exército em Brasília, que, depois, foi transformado em Centro, abrangendo apenas o âmbito do Exército, hoje perfaz um Comando, abarcando todas as Forças Armadas e com instalações específicas localizadas no Forte Marechal Rondon, em Brasília-DF, organização militar ligada intrinsecamente à Arma de Comunicações do Exército. Nessa unidade militar, também fruto de uma previsão da END, servem profissionais das Três Forças, de forma integrada, cooperativa.

(b) essa prioridade tratou da segurança das informações e das comunicações, baseadas em ferramentas cibernéticas, como por exemplo o uso de certificações digitais, de criptografia e de padronização de normas técnicas não só âmbito Exército, e sim das Três Forças. [14]

(c) Nesse ponto, houve evidências que comprovam os esforços do fomento de pesquisa nesse setor, envolvendo sobretudo a comunidade acadêmica nacional, civil e militar. Houve parcerias entre os institutos de tecnologia das Forças e instituições de ensino superior civis, e entre as Forças e Ministérios e órgãos, como por exemplo entre MD e Ministério da Ciência, Tecnologia e Inovação, e MD e Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, o primeiro com o Programa Amazônia Conectada, este último com os programas de fomento à pesquisa Pró-Defesa e Pró-Estratégia. Deve-se salientar, ainda, a criação da Escola Nacional de Defesa Cibernética como uma das prioridades também consideradas e atendidas. Nessa Escola, há participação de militares das três Forças e de civis, agentes públicos federais e outros convidados, envolvidos diretamente com ações que envolvem defesa ou segurança cibernética. [15]

(d) (e) (f) Muitas foram as realizações que abrangem essas três prioridades. Talvez a de maior vulto foi o desenvolvimento de um simulador autóctone de defesa cibernética, o Simulador de Operações de Guerra Cibernética – Simoc, idealizado pelo Centro de Instrução de Guerra Eletrônica – CIGE, e desenvolvido com participação de empresas nacionais, como a Rustcon. Também se destaca a parceria feita entre o EB e a empresa Itaipu Hidrelétrica, a respeito da proteção cibernética daquela estrutura estratégica para o Estado. Nesse aspecto específico, a END 2012 inseriu mais uma diretriz estratégica em relação à de 2008 – a de nº 24 – "Participar da concepção e do desenvolvimento da infraestrutura estratégica do País, para incluir requisitos necessários à Defesa Nacional." (BRASIL, 2012, p. 63). Essa diretriz está concretizada por meio do Programa de Proteção de Estruturas

[14] A *expertise* nessa área se mostrou importante quando da aproximação institucional entre o Exército e a Itaipu Binacional, e o Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro).

[15] Oficialmente inaugurada em 7 de fevereiro de 2019, a ENaDCiber funcionava como núcleo de capacitação desde 2015.

Estratégicas (Proteger), que visa ampliar a segurança de estruturas estratégicas do País e da condução de grandes eventos. Além de estruturas terrestres, a intenção é que o Proteger se articule com outros sistemas, como o SisFron e o da Defesa Cibernética.

(g) No tocante à produção e ao tratamento oriundo da fonte cibernética, essa prioridade anunciou que esse setor também é considerado na utilização para fins de atividade de inteligência. Nesse ponto, mais uma vez, resta evidenciado o uso da cibernética como mais um recurso de poder, a partir da captação e tratamento da informação em tempo hábil. Se as prioridades (a) e (b) se referem mais à cibernética vista como um espaço, isto é, com preocupações voltadas para máquinas processadoras e respectivas infovias, demandando procedimentos a fim de se territorializar essa dimensão, a prioridade (g) é, de fato, para o uso na manutenção de *status quo* ou, ainda, na projeção de poder.

Além das prioridades listadas acima, que são explicitamente relativas à cibernética, há outras referentes aos setores espacial e nuclear que são profundamente ligadas à necessidade de desenvolvimento de equipamentos, de programas e de tratamento da informação digitalizada, como indica a END ao elencar prioridades do setor espacial:

> No setor espacial, as prioridades são as seguintes: [...] (c) Desenvolver **tecnologias de comunicações, comando e controle** a partir de satélites, com as forças terrestres, aéreas e marítimas, inclusive submarinas, para que elas se capacitem a **operar em rede e se orientar por informações** deles recebidas. (BRASIL, 2012, p. 93, **grifo do autor**).

Isso se justifica pela capacidade de transversalidade inerente à cibernética. Ademais, a ideia de Becker (2012), no tocante à existência de uma cronopolítica, também é evidenciada e, mais que isso, passa a ser buscada como elemento-chave para o êxito das operações.

Após mostrados os setores estratégicos anunciados na diretriz de nº 6, com ênfase na cibernética, continua a END (2008), no que diz respeito ao objeto desta pesquisa:

– Diretriz Estratégica nº 9: tratou sobre a necessidade de adensamento do papel do Estado nas fronteiras, mas não forma tradicional, de onipresença física, mas sim do uso de tecnologias que permitam o monitoramento/controle e a mobilidade. Essa diretriz tem sinergia com as de nº 2 e 3 já apresentadas.

– Diretriz Estratégica nº 10: atribuiu prioridade à região amazônica; enfatizou a importância do trinômio monitoramento/controle, mobilidade e presença; registrou no documento de Defesa a ideia de desenvolvimento sustentável para essa região e rechaçou qualquer tentativa externa de tutela *vis a vis* a soberania do País nessa porção territorial: "Quem cuida da Amazônia brasileira, a serviço da humanidade e de si mesmo, é o Brasil." (BRASIL, 2008, p. 14; BRASIL, 2012, p. 54). A diferença da END versão 2008 para a de 2012 é que nesta última há previsão expressa do uso do Censipam de forma integrada com as Forças Armadas, para viabilizar e fortalecer "o monitoramento, o planejamento, o controle, a logística, a mobilidade e a presença na Amazônia brasileira." (BRASIL, 2012, p. 54). Aqui foi reforçada, portanto, a ideia da cibernética e de suas possibilidades, tanto como mais uma dimensão espacial quanto recurso de poder.

– Diretriz Estratégica nº 13: versou sobre a necessidade de desenvolvimento de um combatente com práticas e conhecimentos capazes de atender aos requisitos de monitoramento e controle, mobilidade e presença, que, por sua vez, exigem a capacidade de atuar em rede,

> não só com outros combatentes e contingentes de sua própria Força, mas também com combatentes e contingentes das outras Forças. As tecnologias de comunicações, inclusive com os veículos que monitorem a superfícies da terra e do mar, a partir do espaço, devem ser encarados como instrumentos

> potencializadores de iniciativas de defesa e de combate. (BRASIL, 2012, p. 56).

Nesse ponto a END ratificou, novamente, a transversalidade da cibernética e suas possibilidades no uso como recurso de poder nacional.

– **Diretriz Estratégica nº 18**: esta diretriz anunciou o intento de fomentar na América do Sul uma cooperação regional utilizando-se da integração das bases industriais de defesa. Assim, além de ganhos econômicos e de Defesa para a região, a intenção foi minimizar suposições relacionadas ao dilema de segurança sob a bandeira de uma cooperação regional voltada para uma dissuasão extrarregional (MEDEIROS FILHO, 2010). Nesse sentido, em uma das direções assumidas no período entre 2008 e 2018, o Conselho de Defesa Sul-americano (CDS) atuaria como um dos órgãos fomentadores. Houve elaboração de planos de ação sobre a defesa cibernética sul-americana, feitos pelo CDS, contudo permaneceram apenas na intenção dos escritos.

– Diretriz Estratégica nº 22: relativa à Base Industrial de Defesa e à busca da autonomia em tecnologias indispensáveis à defesa, esta diretriz tratou de: a) prever regimes jurídico, regulatório e tributário especiais, para fins de proteção de empresas nacionais de produtos de defesa "contra risco do imediatismo mercantil" (BRASIL, 2012, p. 60) e para assegurar compras públicas (garantia de demanda efetiva); b) estipular o papel do setor estatal acerca dos produtos de defesa, com missão de operar no teto tecnológico, complementando o que o setor privado não conseguir produzir no curto ou médio prazo de forma rentável; c) incentivar parcerias com países com o propósito de desenvolvimento de capacidades, a fim de diminuir a dependência de importados; d) estimular o desenvolvimento de material de uso dual.

Há uma diferença no tocante a essa diretriz da END de 2008 para as sucessoras. A previsão de uma secretaria do MD para formulação e execução da política de obtenção de produtos de defesa concretizou-se por meio da criação da Secretaria de Produtos de Defesa (Seprod) no âmbito desse Ministério.

Nas páginas seguintes as da Diretriz nº 22 há detalhamento no que diz respeito à reorganização da BID e a algumas características esperadas. Logo em seu subtítulo consta a aspiração de um desenvolvimento tecnológico independente. Na sequência, há o reforço da subordinação das considerações comerciais aos imperativos estratégicos do País, para isso contemplando previsão de marco regulatório especial. Uma passagem, nesse sentido, é bastante interessante na Estratégia:

> O Estado ajudará a conquistar clientela estrangeira para a Base Industrial de Defesa. Entretanto, a continuidade da produção deve ser organizada para não depender da conquista ou da continuidade de tal clientela. Portanto, o Estado reconhecerá que, em muitas linhas de produção, aquela indústria terá de operar em um sistema de "custo mais margem" e, por conseguinte, sob intenso escrutínio regulatório. (BRASIL, 2012, p. 101)

Aqui, mais uma vez, a visão de List (PADULA, 2007) sobre a economia nacional é inspiradora, ao mesmo tempo em que contempla o viés realista das relações entre Estados ou de uma Economia Política Internacional nacionalista ou neomercantilista.

Também nas páginas seguintes da END que se referem à BID, há maiores especificações sobre a competência da Seprod/MD, prevendo inclusive a busca de integração entre os institutos de pesquisa militares e entre esses e os institutos civis, algo que se vislumbra como embrião ou tentativa bem próxima do que apontou Brustolin (2014) sobre a interação entre os entes do complexo militar e industrial-acadêmico dos Estados Unidos e sua forma de sinergia. Sobre esse ponto, destaca-se o trecho contido na própria END:

> A Política de Ciência, Tecnologia e Inovação para a Defesa Nacional tem como propósito estimular o desenvolvimento científico e tecnológico e a inovação em áreas de interesse para a defesa nacional.

> Isso ocorrerá por meio de um planejamento nacional para desenvolvimento de produtos de alto conteúdo tecnológico, com envolvimento coordenado das instituições científicas e tecnológicas (ICT) civis e militares, da indústria e da universidade [...] e a criação de instrumentos de fomento à pesquisa de materiais, equipamento e sistemas de emprego de defesa ou dual [...]. (BRASIL, 2012, pp. 103-104)

Essa mesma concepção foi ratificada posteriormente, já intitulada e orientada: "[...] O objetivo será fomentar o desenvolvimento de um **complexo militar universitário-empresarial** capaz de atuar na fronteira de tecnologias que terão quase sempre utilidade dual, militar e civil." (BRASIL, 2012, p. 105, **grifo do autor**).

O LBDN (2012), mencionando como base a END (2008), também reforçou essa perspectiva:

> A interação entre instituições de pesquisa civis e militares, universidades e empresas é fundamental para integrar os esforços empresariais na criação de polos de alta tecnologia em variadas áreas. No Brasil, os polos tecnológicos estão diretamente ligados a processos de planejamento que envolvem o governo, universidades e empresas, com destaque especial para os incentivos do Estado ao desenvolvimento tecnológico. (BRASIL, 2012, p. 219)

E elencou cinco iniciativas adotadas pela Seprod/MD como principais:

a) Criação do Núcleo de Promoção Comercial: instituído pela Diretriz nº 1.116/2012, do MD, com a finalidade de "elaborar ações voltadas para o incentivo ao desenvolvimento e a promoção comercial de produtos de defesa brasileiros e para a atração de capital e tecnologias que possam ser empregados no desenvolvimento de produtos de defesa ou de uso dual." (BRASIL, 2012, p. 189).

b) Levantamento da Base Industrial de Defesa e incentivo ao aumento das exportações: por meio de parceria entre o MD e a Agência Brasileira de Desenvolvimento Industrial (ABDI), o Livro Branco estipulou o levantamento completo da BID para fins de integração com a indústria nacional, na busca de capacidades e potencialidades com transbordamento econômico-social.[16]

c) Marcos regulatórios para o fortalecimento da indústria de defesa: pautada na Diretriz nº 22 das END (2008; 2012), esta iniciativa buscou evitar sazonalidades mercantis para o setor industrial da defesa, ao mesmo tempo que incentivou a indústria nacional a participar desse esforço, apontando segurança no sentido de carga tributária e de garantia de demanda. Além da Lei nº 12.598/2012, que trata de regime especial para produtos de defesa, duas normatizações foram daí derivadas: a Política Nacional da Indústria de Defesa (PNID), que serviu de norteadora para as ações da Seprod/MD, e a Política Nacional de Exportações de Produtos de Defesa (Pneprode). Esses documentos passaram a ser referências na atuação de adidos militares brasileiros, por exemplo, quando em missão em outros países, com apoio do Itamaraty.

d) Desenvolvimento de Ciência e Tecnologia: por meio da parceria entre MD e o MCTI, a tentativa foi a maximização de esforços de pesquisa nas instituições científicas e tecnológicas militares para fins de desenvolvimento de tecnologia de ponta na área de Defesa.

e) Interlocução com as empresas brasileiras voltadas para o setor de defesa: quanto a esta iniciativa, cabe registrar o papel crucial do Conselho Nacional de Desenvolvimento Industrial como canal de acesso à Presidência da República com relação a políticas nacionais para esse setor. Ainda nesse sentido, teve destaque a Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (Abimde) e as federações das indústrias, por meio do Comitê da Cadeia Produtiva da Indústria de Defesa

[16] Essa iniciativa que consta no LBDN (2012), como é assinalada, foi concretizada parcialmente em 2016. O Instituto de Pesquisa Econômica Aplicada (IPEA) publicou o resultado desse levantamento, em parceria com a ABDI, com os Ministérios do Planejamento, Desenvolvimento e Gestão, e da Indústria, Comércio e Serviços. O título dado foi "Mapeamento da Base Industrial de Defesa" (IPEA, 2016).

(Comdefesa), como foi o caso de São Paulo e de Santa Catarina.

– **Diretriz Estratégica nº 24**: alertou para a ligação entre estruturas estratégicas do País e a Defesa, prevendo a inclusão de elementos desta naquelas, com previsão do teor dual. Aparentemente sucinta e despretensiosa, esta diretriz se tornou de grande importância, quando se deparou com parcerias, convênios e acordos feitos entre algumas dessas estruturas e o MD, no tocante ao setor cibernético, como foi o caso da Itaipu Binacional e o Exército, contido no Proteger.

3. O setor estratégico da cibernética no Brasil

O termo *cibernética*, apesar de um tanto quanto novo na seara acadêmica, pelo menos atrelado ao significado de ciberespaço, de informação digitalizada e de infovia, ou de informacional, como abordou Castells (2006 [1999]), esteve inserido no pensamento geopolítico de militar brasileiro, como foi o caso do General Carlos de Meira Mattos, ainda na década de 1970, quando comparando o grau de "cibernetização" dos Estados Unidos em relação ao do Brasil.[17]

Notadamente, a preocupação desse militar diz respeito ao nível do desenvolvimento tecnológico e ao uso deste como instrumento garantidor, ou ampliador, de assimetria entre os países no sistema internacional. Porém há algo mais: existe a ideia do computador como ferramenta que permite esse aumento de capacidade, por meio, à época, do que Mattos (2011 [1977]) verificou como a capacidade das memórias dessas máquinas na realização de cálculos de forma rápida, isto é, na capacidade de alterar a variável *tempo*. Também pode ser inferida a associação entre o nível de tecnologia da sociedade, os complexos empresariais e a qualidade dos recursos humanos (complexos educacionais), assim como seus produtos.

Antes da utilização do termo *cibernética*, havia políticas públicas no Brasil ligadas à área hoje assim tratada, porém eram chamadas por outros termos, como é o caso de *segurança da informação*. Ainda que mais amplo, esse termo serviu durante muito tempo para também se referir à segurança no que diz respeito ao uso dos computadores na produção, no armazenamento e na circulação da informação. Como exemplo, antes da END (2008), houve o Decreto Nr 3.505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal (APF) e a Lei Nr 10.683, de 2003, que estabeleceu atribuições ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), no que diz respeito aos assuntos de inteligência federal e de segurança da informação. Também como referência nessa área, antes do *status* estratégico e da implantação do setor cibernético, houve a criação do Departamento de Segurança da Informação e Comunicações (DSIC) no âmbito do GSI/PR, como bem recordou o Coronel Arthur Pereira Sabbat, em audiência pública e interativa.[18]

No nível político, a atribuição na área cibernética ficou sob o encargo do Gabinete de Segurança Institucional da Presidência da República. Assim apresentou o Departamento da Segurança da Informação e Comunicações do GSI/PR quanto ao tema, em publicação intitulada *Livro Verde de Segurança Cibernética*:

> Dentre as motivações do Gabinete de Segurança Institucional, órgão essencial da Presidência da República, para esta obra, tem-se a própria prerrogativa do Gabinete de coordenar a atividade de Segurança da Informação, mantendo o compromisso com o Estado. Assim, motivado por esta missão e considerando a necessidade de assegurar dentro do

[17] "O grau de cibernetização indica, atualmente, o padrão tecnológico da sociedade. As atividades dos grandes complexos empresariais ou educacionais estão relacionadas, hoje, com os computadores, cujas memórias realizam cálculos […]. Os números - 70 mil computadores nos EUA e 1.500 no Brasil - revelam o profundo gap, em termos de avanço tecnológico entre ambos os países." (MATTOS, 2011 [1977], p. 310)

[18] 1ª Audiência Pública e Interativa sobre o tema "O Programa de Defesa Cibernética", datada de 5/9/2019, solicitada pelo senador Espiridião Amin, por meio do requerimento nº 24/2019, da Comissão de Relações Exteriores do Senado Federal do Brasil.

> espaço cibernético ações de segurança da informação e comunicações como fundamentais para a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação; a possibilidade real e crescente de uso dos meios computacionais para ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade; foi instituído Grupo Técnico para estudo e análise de matérias relacionadas à Segurança Cibernética. (BRASIL, 2010, p. 5)

De maneira geral, visualiza-se as competências relacionadas ao setor cibernético e respectivas instituições responsáveis conforme o Quadro 3:

Quadro 3: atribuições no ambiente cibernético, por nível de atuação

NÍVEL	ATRIBUIÇÕES
Nível Político	Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, coordenadas pela Presidência da República (PR) e abrangendo a Administração Pública Federal (APF) direta e indireta, bem como as infraestruturas críticas da informação dos setores público e privado.
Nível Estratégico	Defesa Cibernética, a cargo do MD, em interação com PR e APF.
Níveis Operacional e Tático	Guerra Cibernética, denominação restrita ao âmbito interno das Forças Armadas.

Fonte: Cerávolo; Ferreira Neto (2015, p .82)

No nível estratégico é onde ocorre a interface entre o comando político e o planejamento e implementação de ações de defesa propriamente dito, conduzidas pelo Ministério da Defesa e pelas Forças Armadas.

Já nos níveis operacional e tático são executadas ações reais estipuladas no nível estratégico, como ocorreu na Copa das Confederações, em 2013, na Copa do Mundo Fifa 2014 e nas Olimpíadas 2016. No relato de quem participou em tais situações encontra-se o seguinte:

> A atuação do CDCiber materializou o vetor Defesa Cibernética do planejamento das ações de segurança previstas para a Copa das Confederações. Este planejamento foi elaborado pelo MD em coordenação com a Secretaria Especial para Grandes Eventos (SESGE), vinculada ao Ministério da Justiça, contando com as FA, com a Polícia Federal e as Polícias Estaduais e Municipais, além de uma miríade de agências governamentais. Foi, portanto, uma Operação Interagências, com toda a sua complexidade, diferenças de cultura e nível de complexidade em segurança cibernética entre as organizações envolvidas e uma necessidade intrínseca de grande coordenação de esforços. (CAMELO; CARNEIRO, 2014, pp. 150-151)

A execução nesses níveis se deu por meio de células menores, denominadas destacamentos, no caso Destacamento de Defesa Cibernética (Dst Def Ciber). Assim ocorreu na Copa das Confederações, por exemplo:

> O Destacamento de Defesa Cibernética foi composto por um Dst Def Ciber Central, localizado em Brasília, e mais seis Dst Def Ciber Remotos (Rmto), localizados em cada uma das sedes da Copa das Confederações, a saber: Belo Horizonte, Brasília, Fortaleza, Recife, Rio de Janeiro e Salvador. A cidade de Brasília abrigou, portanto, o Dst Def Ciber Central e um Dst Def Ciber Rmto.
> Todos os Dst Def Ciber Remotos foram conjuntos, ou seja, compostos por militares das três Forças Armadas. O Dst Def Ciber Central também foi conjunto, além de ser integrado por parceiros institucionais e empresas contratadas. (CAMELO; CARNEIRO, 2014, p. 153)

Dentre o rol de atribuições desses Destacamentos, teve-se a

> montagem de um "sistema de consciência situacional", por meio de um conjunto de sistemas para obter e concentrar informações sobre: sistemas de TIC e

> ativos críticos para a Copa das Confederações; diagnósticos de riscos dos ativos analisados, no que foi considerado pertinente; inteligência cibernética; incidentes nas redes envolvidas; eventos de segurança da informação de interesse; gerência de redes de interesse; [...]. (CAMELO; CARNEIRO, 2014, p. 155)

Em linhas gerais, portanto, assim funcionou a distribuição de atribuições no tocante à segurança e defesa cibernética, e respectivos planejamento e execução. A seguir constam projetos e programas desse setor.

3.1 Projetos e Programas Inseridos no Setor Cibernético

Para compreensão dos esforços do MD, via EB, no tocante ao setor cibernético, também é importante entender o contexto em que a Força Terrestre se propôs. Tratou-se do Processo de Transformação do Exército (2010). Nesse sentido, as ações e os planejamentos oriundos do EB tiveram como pressuposto esse processo, que não buscou apenas modernização, adaptação ou reaparelhamento, mas também, e com maior ênfase, uma transformação na própria concepção da Força, incluindo sua doutrina. Esse processo data de 2010 e repercutiu em projetos e programas, dentre outras ações. Por exemplo, assim mencionou a versão da Estratégia Nacional de Defesa de 2016, a respeito do Processo de Transformação e dos sistemas daí derivados, submetida ao Senado Federal, via proposta de Decreto Legislativo nº 847/2017, e aprovada pela Comissão Mista de Controle das Atividades de Inteligência, em 19/10/2017:

> Dos *sistemas indutores da transformação*, alguns colaboram diretamente para a capacidade de dissuasão, em conjunto com as demais Forças Singulares. O Sistema Integrado de Monitoramento de Fronteira – SISFRON, o Sistema de Mísseis e Foguetes, o Sistema de Defesa Antiaérea, *o Sistema de Defesa Cibernética* e a Mecanização do Exército atuam por meio do incremento da mobilidade, da *atividade de monitoramento e controle* das fronteiras e da capacidade de *atuar na negação de acesso* indesejado a áreas ou a sistemas estratégicos de interesse da Defesa Nacional. (BRASIL, 2017, p. 46, *grifo nosso*)

O Processo de Transformação do Exército vem sendo conduzido pelos vetores da ciência e tecnologia, doutrina, educação e cultura, engenharia, gestão, logística, orçamento e finanças, preparo e emprego, e recursos humanos. Em todos esses, a Força Terrestre buscou – e ainda busca – sair de uma estrutura e concepção calcadas na Era Industrial para uma condizente com a Era do Conhecimento. Esse ponto é importante, uma vez que torna mais fácil a compreensão das mudanças apontadas na END, sobretudo quanto aos imperativos elencados da flexibilidade, adaptabilidade e mobilidade, como se viu anteriormente expressos nas diretrizes estratégicas. Ainda no que diz respeito aos documentos ligados ao Processo de Transformação, esses contemplam de forma explícita o objetivo de fortalecimento do setor estratégico cibernético.[19]

A partir da definição, por parte do Ministério da Defesa, sobre a responsabilidade pela condução dos setores estratégicos no País[20], o Exército, a que coube a cibernética, criou o Núcleo de Defesa Cibernética (NuDCiber), ainda em 2010, que se transformou na sequência em Centro de

[19] Ver Portaria nº 1.253, de 2013, do Comandante do Exército e livreto publicado pelo Estado-Maior do Exército. Disponível em: http://www.ceeex.eb.mil.br/manuais/livreto_transformacao(2).pdf. Acesso em: 18 nov. 2019.

[20] A definição da Força-líder para cada setor não ocorreu no texto originário da END (2008), mas sim posteriormente. Pelo que se investigou, em 3/7/2009 um documento (Ofício Nr 035) do Comandante do Exército, então General de Exército Enzo Martins Peri, foi expedido ao MD, apresentando uma exposição de motivos pelos quais o setor cibernético deveria ficar a cargo do Exército Brasileiro. Até a presente data não se conseguiu acesso ao texto do ofício, pois foi classificado como de natureza *reservada*. Contudo, no dia 9/11/2009, por meio da Diretriz Ministerial Nr 14, o MD aceitou tais argumentos e definiu o EB como Força condutora desse setor. Essa mesma Diretriz também previu a possibilidade da criação de um centro que englobasse esforços de militares e civis das outras Forças Armadas.

Defesa Cibernética (CDCiber)[21], órgão funcionando dentro da estrutura do próprio Exército. Esse primeiro esforço, criado com certa brevidade, visava, além da segurança e defesa de organizações militares, à preparação para os compromissos internacionais assumidos pelo Brasil, como foi o caso da Rio+20, da Copa das Confederações (2013), do Mundo FIFA de Futebol (2014) e das Olimpíadas no Rio (2016).[22]

O EB delineou – visando a atender a cinco áreas de interesse ou vetores fundamentais[23]: educação/recursos humanos, doutrina, operações, ciência e tecnologia, e inteligência – oito projetos estruturantes para o setor, que orbitariam em torno das *expertises* obtidas pelo CDCiber. Foram esses: 1) Estrutura de Capacitação e de Preparo e Emprego Operacional; 2) Estrutura de Apoio Tecnológicos e Desenvolvimento de Sistemas; 3) Organização do CDCiber; 4) Estrutura para a Produção do Conhecimento Oriundo da Fonte Cibernética; 5) Gestão de Pessoal; 6) Arcabouço Documental; 7) Estrutura da Pesquisa Científica na Área Cibernética; 8) Planejamento e Execução da Segurança Cibernética.

Um dos fatos que chamou atenção nesse processo de investigação foi a velocidade e a quantidade de ações que foram derivadas desses projetos estruturantes, as quais são apresentadas a seguir. Além disso, outros órgãos, estruturas e sistemas foram desenvolvidos na busca de implementação de ações e de soluções decorrentes da natureza do setor, como foi a dificuldade de recurso humano com nível de especialização específica e a dependência de equipamentos e acessórios não nacionais, além dos desafios de garantia de segurança nessa área.

O Quadro 4 a seguir, ainda que de forma resumida, passa a ter grande valia para o entendimento das intenções e da forma como foram divididas as tarefas pela Força, assim como demonstradas as principais preocupações e objetivos.

Como organizações militares do Exército que foram incluídas nos esforços desse setor, tem destaque o Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx), o Centro Integrado de Telemática do Exército (CITEx), o Instituto Militar de Engenharia (IME), o Centro de Tecnológico do Exército (CTEx), além do próprio CDCiber.

Concomitantemente à implementação de ações vinculadas aos projetos estruturantes, a cibernética ensejou a elaboração de um arcabouço normativo, incluindo estratégia, política e doutrina específicas para a defesa cibernética do País, como foi a Política Cibernética de Defesa (2012) [24] e a Doutrina Militar de Defesa Cibernética (2014) [25] [26], essas mais estritas às ações e procedimentos em operações militares propriamente ditas.

Além das ações descritas, da distribuição de competências e

[21] Por meio das Portarias nº 666 e 667, de 4/8/2010, do Comandante do Exército Brasileiro.

[22] Interessante foi assistir em Audiência Pública e Interativa, conduzida pelo Senado Federal, a apresentação do General de Divisão Guido Amin Naves, quanto à rapidez necessária na implantação do setor, tendo em vista o compromisso assumido pelo País junto à sociedade internacional. Essa foi exatamente a percepção que se teve enquanto se acompanhou esse processo inicial de planejamento e de implementação pelo EB.

[23] Esta última terminologia "vetores fundamentais" foi usada pelo General José Carlos dos Santos, quando em audiência pública relacionada à CPI da espionagem, derivada do Caso Snowden. Ver "CPI da Espionagem: relatório final", precisamente nos termos registrados na 6ª reunião, em 2 de outubro de 2013. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco. Acesso em: 13 nov. 2018.

[24] O Decreto nº 7.364 serviu de base para a formulação dessa Política, que foi aprovada pela Portaria Normativa nº 3.389, hoje consistindo na publicação MD 31 – P – 02, 1ª edição, de 21/12/2012.

[25] Aprovada pela Portaria Ministerial nº 3.010/MD, de 18/11/2014.

[26] As iniciativas para esse setor não cessaram após o recorte temporal da pesquisa. Dia 5 de fevereiro de 2020 foi aprovada, pelo Decreto nº 10.222, a Estratégia Nacional de Segurança Cibernética, a E-Ciber, como foi denominada. Esse documento veio cumprir o estabelecido na Política Nacional de Segurança da Informação, em vigor desde 26 de dezembro de 2018 (Decreto nº 9.637). Por este documento, a segurança cibernética, como um subconjunto, está contida na segurança da informação.

responsabilidades, e de arcabouço normativo, surgiu a preocupação de configurar separadamente os objetivos a que se propunha o Exército perante o ordenamento da END. O setor estratégico da cibernética foi dirigido para abarcar toda a estrutura da Defesa, e não apenas da Força Terrestre. Isso ensejou o desmembramento dos esforços da cibernética em dois grandes programas, um voltado para a própria Força – o Programa Estratégico da Defesa Cibernética – e outro abrangendo toda a Defesa – Programa Defesa Cibernética na Defesa Nacional, ambos contidos no Projeto Estratégico Defesa Cibernética (PEDCiber), previsto pela Ação Orçamentária (AO) 147F.[27]

3.1.1 Programa Estratégico da Defesa Cibernética

Do anteriormente denominado Projeto Estratégico Defesa Cibernética, restrito às atribuições âmbito Exército apenas, a partir de 2016 houve sua transformação em Programa Estratégico do Exército Defesa Cibernética, permitindo que parcela dos esforços na área de segurança e defesa cibernética fossem divididos entre a garantia do funcionamento de sua própria estrutura de redes e equipamentos informacionais, e a do Ministério da Defesa, tendo em vista a designação do Exército para tal responsabilidade.

O Programa Estratégico Defesa Cibernética apresentou os seguintes projetos e respectivos objetivos:

Quadro 4: Projetos do Programa Estratégico da Defesa Cibernética

PROJETOS	DESCRIÇÃO/OBJETIVOS
1. Centro de Defesa Cibernética	Visa implantar a estrutura organizacional e a infraestrutura do Centro de Defesa Cibernética como organização militar diretamente subordinada ao Comando de Defesa Cibernética (ComDCiber).
2. Escudo Cibernético	Tem o propósito de dotar o Exército Brasileiro da infraestrutura necessária para realizar a proteção cibernética dos ativos de informação da Instituição.
3. Apoio Tecnológico	Tem por objetivo fomentar as estruturas de apoio tecnológico e de desenvolvimento de sistemas para atender às necessidades do setor cibernético.
4. Força Cibernética	Visa à criação de estruturas de capacitação e de preparo e emprego operacional voltadas para atividades de segurança, defesa e guerra cibernéticas, que garantam à Força Terrestre a capacidade de atuar em rede de forma segura e integrada ao Sistema Militar de Comando e Controle do Ministério da Defesa.
5. Inteligência Cibernética	Visa à criação de estruturas voltadas para a produção do conhecimento a partir de dados oriundos da fonte cibernética.
6. Pesquisa Cibernética	Destina-se à supervisão e ao fomento da capacitação de recursos humanos de nível superior, à pesquisa científica tecnológica em instituições de ensino civis e militares, e à extensão universitária do instituto Militar de Engenharia (IME), todos voltados para o setor cibernético.
7. Gestão de Talentos	Visa a estruturar e a consolidar a gestão de recursos humanos de modo a suprir as necessidades da Força Terrestre. As ações envolvidas nessa gestão incluem selecionar, gerir capacidades e realizar administração do pessoal.
8. Ações comple-mentares	**Capacitação:** visa formar profissionais competentes nas áreas de conhecimento afetas a cibernética por meio da capacitação em cursos no meio civil e militar.
	Doutrina: tem como foco a elaboração e a atualização de

[27] A AO 147F é subdividida em dois Planos Orçamentários (PO), o 001, destinado ao Exército especificamente, e o PO 002, para âmbito Defesa como um todo. Essa AO estava contida no Programa 2058 – Defesa Nacional – do Plano Plurianual (PPA) 2016–2019.

	publicações doutrinárias e normativas relativas ao setor cibernético, visando assim à consolidação da sistemática e dos processos de elaboração, revisão, atualização, divulgação e prospecção de novos conhecimento, bem como a verificação da aplicação das normas doutrinárias relativas ao setor.

Fonte: o autor com base no *site* do EPEx (2019).

Percebe-se que o rol dos objetivos realmente dá preferência à manutenção do funcionamento seguro da estrutura informacional do Exército: suas redes/infovias internas, entre suas organizações militares, a capacitação de pessoal para essa área, a contratação e retenção de talentos, o desenvolvimento de pesquisa e de tecnologia, o emprego nos níveis estratégico, operacional e tático, âmbito EB etc.

3.1.2 Programa da Defesa Cibernética na Defesa Nacional

Fruto do desenvolvimento do Programa Estratégico da Defesa Cibernética, que funcionou basicamente voltado para atender à Força Terrestre, e das demandas das outras Forças e órgãos relacionados à segurança, *lato sensu*, e da defesa civil, o Ministério da Defesa criou o Programa Defesa Cibernética na Defesa Nacional para

> incrementar as atividades de capacitação, doutrina, ciência, tecnologia e inovação, inteligência e operações, visando assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) **pelo MD e pelas Forças Armadas** e impedir ou dificultar sua utilização contra os interesses nacionais. (EPEX, 2019, **grifo do autor**)

A diferença crucial entre os dois Programas – este e o Programa Estratégico da Defesa Cibernética visto anteriormente – baseou-se no nível de atuação: enquanto o primeiro visa, sobretudo, atender às demandas do Exército, o segundo vai além, buscando, de forma integrada entre as Forças e outras instituições, a segurança do ciberespaço. Contudo, em última instância, foi a Força Terrestre que os conduziu. O objetivo foi dotar a Defesa Nacional com uma estrutura de desenvolvimento conjunto de Defesa Cibernética.

Como iniciativas para consolidar esse Programa, destacam-se a criação do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber). Essas duas ações, por sinal, foram anunciadas na END (2012) como prioridades para esse setor.

Constatou-se que o nível de atuação realmente foi além do Exército, englobando todo o MD e mais órgãos da Administração Pública Federal, como ocorreu na implantação de banco de dados visando ao incentivo em projetos de pesquisa, desenvolvimento e inovação (P&D&I) nacionais no setor cibernético.

Aparentemente algo visto como consequência natural, a criação do ComDCiber, após a estruturação do CDCiber, não foi tão simples assim. A questão, além do orçamento, evidentemente, envolveu a condução da atividade, isto é, a afirmação (ou reafirmação) de que mesmo contemplando a implantação do um Comando de Defesa nível MD, que visa à interoperabilidade entre as Forças Armadas, a condução dos esforços para esse setor continuaria sob a competência do EB. Isso foi feito, pois o ComDCiber, apesar de possuir uma rotatividade na direção de suas atividades entre militares das Três Forças, ficou vinculado à estrutura regimental do Comando do Exército.

A ENaDCiber, como os objetivos indicam, contempla discentes civis e militares, componentes das Forças Armadas e de outros órgãos públicos, o que indica investimento em "espadas", porém para além da guerra.

No Quadro 5 constam as principais entregas desse programa até o final do recorte temporal desta pesquisa:

Quadro_5: Programa Defesa Cibernética na Defesa Nacional – entregas

– Ativação do ComDCiber nas instalações do Forte Marechal Rondon (Brasília-DF).
– Realização de Operações Conjuntas com a utilização de um simulador de operações cibernéticas.
– Ativação do Núcleo da ENaDCiber em instalações no Comando Militar do Planalto (Brasília-DF).
– Parcerias com instituições de pesquisa público e privadas, para desenvolvimento de projetos de interesse para a Defesa Cibernética.
– Especialização de militares das três Forças Armadas em instituições públicas e privadas, no Brasil e no exterior.
– Implantação de soluções tecnológicas para uso das Forças Armadas.

Fonte: o autor com base no *site* do EPEx (2019).

Pelo Quadro 5 percebe-se o alinhamento das entregas aos objetivos propostos pelo programa. A direção dada foi no sentido de expandir o alcance da Defesa cibernética para além do Exército, abrangendo as três Forças, relacionando-a com a interoperabilidade, e instituições civis, tanto ligadas à pesquisa como à empresarial. O uso de um simulador de operações cibernéticas autóctone, por exemplo, permitiu a interação entre essas instituições, a partir de esforços no desenvolvimento de tecnologias da área cibernética próprias. A questão da homologação e certificação de produtos dessa área também foi buscada, assim como a criação de laboratórios voltados tanto para segurança quanto para pesquisa cibernética foi concretizada.

4. Considerações finais

O presente texto apresentou a estruturação do setor cibernético, a partir do *status* de estratégico para o País, em 2008, com a publicação da END.

Esse documento, basilar para as iniciativas do setor de Defesa e de outros afins, foi dividido em duas grandes partes, uma tratando da formulação sistemática e outra das medidas de implementação. No tocante à primeira, foram anunciados: três eixos estruturantes, 25 diretrizes e três setores estratégicos, dentre os quais o cibernético. Como elemento norteador de todos, o documento afirmou a intenção em conciliar o binômio Defesa–Desenvolvimento.

Reforçando o suporte normativo que deu sustentação a este estudo, foram utilizados a Política Nacional de Defesa e o Livro Branco da Defesa Nacional. Esses ratificaram a END e foram além. Aquele promovendo os eixos, as diretrizes e os setores estratégicos ao mais alto nível do Estado; este explicitando de forma detalhada as intenções contidas na Estratégia, até por questões evocadas pelo ordenamento construído para a segurança internacional, como no caso de promoção da transparência nas ações ligadas a setores como o bélico-militar e, assim, evitar uma corrida armamentista.

De volta ao binômio Defesa-Desenvolvimento, as ações e, logo, os investimentos nesse setor são considerados como uma das falhas de mercado, por serem bem público. Mais que isso, economicamente tratando, Defesa é um bem público puro, tendo em vista a particularidade concedida aos Estados nacionais pelo princípio da soberania. Por esse princípio, ao Estado cabe o monopólio do uso da força *weberiano*, isto é, dos mecanismos legais e legítimos de coerção e coação, para seu âmbito interno e externo.

Também vista como uma falha de mercado, a externalidade, ou a sua busca, pode ser uma das soluções para mitigar os reflexos dos investimentos públicos em Defesa. Aqui trata-se de benefício marginal social e do efeito multiplicador que algumas ações estatais podem gerar. Em outras palavras, trata-se da conciliação do dilema entre investimento em "espadas ou em arados". A alternativa para esse aparente impasse está no próprio binômio instituído pela END. Por isso propõe-se ir além: a Defesa não serve apenas de escudo para o Desenvolvimento, como consta na END – pelo menos não na experiência norte-americana. Esse setor é, também, um fator do próprio Desenvolvimento, por meio de transbordamentos, externalidades ou benefícios marginais sociais advindos da tecnologia produzida para fins de dissuasão

ou, porventura, de guerra. Nesse caso, o gasto com a preparação para guerra deixa de ser mais um encargo para resultar em – além do aumento da capacidade de monitoramento e controle – instrumento potencial de desenvolvimento.

Nesse sentido, a END e a PND previram como necessidade o papel do Estado como garantidor da demanda efetiva *keynesiana*, só que voltado para produtos de defesa. Pode-se registrar que muitas dessas diretrizes foram realizadas, como o levantamento da base industrial de defesa e a lei do Prode ou Retid, como ficou conhecida a Lei nº 12.598, de 2012, que concedeu tratamento tributário especial a indústrias dessa natureza. Além dessas ações, foi criada uma secretaria no Ministério da Defesa – a Secretaria de Produtos de Defesa (Seprod) – para aprimorar processos ligados à pesquisa e ao desenvolvimento de tecnologias de interesse da Defesa e a articulação entre as Forças e entre essas e instituições civis científicas, tecnológicas e industriais, ou seja, dentro da concepção do sistema hélice tríplice, tal qual o Sisdia de Inovação do Exército.

O setor cibernético desenvolveu produtos de forma autóctone, como foi o caso do simulador de operações cibernéticas, o Simoc, e um antivírus, da empresa Bluepex, mas esses, em última análise, não se constituíram em tecnologias disruptivas, e sim em uma opção nacional para uma tecnologia que já funcionava em países de capacidade militar-tecnológica nesta área.

Em se tratando da formação de um complexo militar, industrial-acadêmico ou de um complexo militar-universitário industrial, consoante a END, pelo lado do Exército verificou-se esforços nesse sentido.

No tocante ao setor cibernético, houve um notório aprimoramento de sua estrutura, tanto pela criação de um núcleo, que logo se tornou um centro, o Centro de Defesa Cibernética, âmbito Exército, que operou durante os grandes eventos internacionais que ocorreram no Brasil, entre 2011 e 2016, e que depois deu origem ao ComDCiber, englobando toda a Defesa, isto é, no nível político-estratégico do País, bem similar ao que aconteceu na estruturação do setor cibernético nos Estados Unidos e a função do seu USCYBERCOM. Também se pode afirmar que houve uma normatização de atribuições e competências para ações desse setor.

Além disso, foi criada a Escola Nacional de Defesa Cibernética, local de formação de recursos humanos para este fim, mas não só isso: por fomentar a integração de civis e militares, e do setor público com o privado, esta escola tornou-se um centro de referência com possibilidade de aglutinar *expertise*, interesses e inovação sob vários prismas e assim gerar transbordamentos, externalidades positivas, tangíveis e intangíveis, como a formação de uma cultura de defesa e de uma mentalidade em prol da consecução do binômio Defesa-Desenvolvimento.

Referências

BECKER, Bertha. “A Geografia e o Resgate da Geopolítica”. In: *Espaço Aberto*, PPGG – UFRJ, v. 2, n.1 2012 [1988]. pp. 117-150.

BLACKWILL; Robert D.; HARRIS, Jennifer M. *War by Other Means*: geoeconomics and statecraft. Introduction e Cap. I. pp. 2-24. Cambridge Massachususetts: The Belknap Press of Harvard University Press, 2016.

BRASIL. *Estratégia Nacional de Defesa*. Brasília, DF, 2008.

_____. *Livro Verde: Segurança Cibernética no Brasil*. Brasília: Gabinete de Segurança Institucional da Presidência da República, 2010. Disponível em:

<http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 8 ago. 2011.

_____. Política Nacional de Defesa. Brasília, DF, 2012.

_____. *Livro Branco de Defesa Nacional*. 2012.

_____. Senado Federal. *Comissão Parlamentar de Inquérito da Espionagem*. Relatório Final. 2014. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco. Acesso em: 20 jan. 2017.

_____. Exército Brasileiro. Portaria n. 1701, do Comandante do Exército. *Cria o Sistema Defesa, Indústria e Academia de Inovação (SisDIA) de Inovação*. 2016.

_____. Senado Federal. Projeto de Decreto Legislativo n. 847. *Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional*, [...]. Brasília, 2017.
BRAUDEL, Fernand. *Dinâmica do Capitalismo*. Rio de Janeiro: Rocco, 1987 [1985].

BRUSTOLIN, V. M. *Inovação e Desenvolvimento via Defesa Nacional nos EUA e no Brasil*. Tese (Doutorado em Ciências, em Políticas Públicas, Estratégias e Desenvolvimento) – Universidade Federal do Rio de Janeiro, Centro de Ciências Jurídicas e Econômicas, Instituto e Economia, Rio de Janeiro, 2014.

CAMELO, José R. de S.; CARNEIRO, João M. E. "A Atuação do Centro de Defesa Cibernética na Copa das Confederações FIFA 2013". In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONÇALEZ, Selma L. de M. (org.) *Segurança e Defesa Cibernética*: da fronteira física aos muros virtuais. Recife: Editora UFPE, 2014.

CASTELLS, Manuel. *A Sociedade em Rede*. 6. ed. São Paulo: Paz e Terra, 2006 [1999].

CERÁVOLO, Luiz E. S.; FERREIRA NETO, Walfredo B. "Defesa Cibernética no Brasil: distribuição de competências nas operações interagências". In: *Defesa Nacional*. Ano CIII, n. 828, 3. quadrimestre, 2015. pp. 65-90.

CHANG, Ha-Joon. *Chutando a Escada*: a estratégia do desenvolvimento em perspectiva comparada. São Paulo: Unesp, 2004.

FIORI, José L. da C. (org.). *O Poder Americano*. Coleção Zero à Esquerda. Petrópolis: Vozes, 2004.

GABRIEL, Pedro H. L. *Pensamento Geopolítico dos Militares Brasileiros no Século XX*. Curitiba: Editora Prismas, 2015.

KRUGMAN, Paul; WELLS, Robin. *Introdução à Economia*. Rio de Janeiro: Elsevier, 2007.

LIMA, Maria R. S. *Tradição e Inovação na Política Externa Brasileira*. Working Paper n. 3, 2010. Disponível em: http://www.plataformademocratica.org/Arquivos/Tradicao%20e%20Inovacao%20na%20Politica%20Externa%20Brasileira.pdf. Acesso em: 20 set. 2016.

MATTOS, Carlos de M. "A Geopolítica e as Projeções de Poder". In: *Geopolítica.* vol I. Rio de Janeiro: Editora FGV, 2011 [1977].

MAZZUCATO, Mariana. *O Estado Empreendedor*: desmitificando o mito do setor público vs. o setor privado. São Paulo: Portfolio/Penguim, 2014.

MEDEIROS, Carlos Aguiar "O Desenvolvimento Tecnológico Americano no Pós-Guerra como um Empreendimento Militar". In: FIORI, José Luís. *O Poder Americano*. 2. ed. Petrópolis, RJ: 2004. pp. 225-252.

MEDEIROS FILHO, Oscar. *Entre a cooperação e a dissuasão: políticas de defesa e percepções militares na América do Sul*. 2010. 240 f. Tese (doutorado). Faculdade de Filosofia, Letras e Ciências Humanas. Universidade de São Paulo. São Paulo, 2010.

MORAES, Gloria. "Telecomunicações e o Poder Global dos Estados Unidos". In: FIORI, José Luís. *O Poder Americano*. 2. ed. Petrópolis, RJ: 2004. pp. 347-392.

OLIVEIRA, Eliézer R. "A Estratégia Nacional de Defesa e a Reorganização e Transformação das Forças Armadas". In: *Interesse Nacional*, abr-jun., 2009. pp. 71-83.

PADULA, Raphael. *Friedrich List* – nota introdutória. Oikos. Rio de Janeiro, v. 8, 2007.

ROSSETTI, José P. *Introdução à Economia*. 21 ed. São Paulo: Atlas, 2016.

RUTTAN, Vernon W. *Is war necessary for economic growth?* Saint Johns University Collegeville, Minnesota, oct. 2006.

VASCONCELLOS, Marco A. S. *Economia*: micro e macro. 6. ed. São Paulo: Atlas, 2015.

WU, Tim. *Impérios da Comunicação*: do telefone à internet, da AT&T ao Google. Rio de Janeiro: Zahar, 2006.