UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ECONOMIA POLÍTICA INTERNACIONAL

WALFREDO BENTO FERREIRA NETO

UMA ESTRATÉGIA NACIONAL DE DEFESA PARA ALÉM DA GUERRA: *GEOPOLÍTICA CIBERNÉTICA E SEU TRANSBORDAMENTO ECONÔMICO-TECNOLÓGICO NO BRASIL (2008-2018)*

RIO DE JANEIRO
Agosto – 2020

WALFREDO BENTO FERREIRA NETO

UMA ESTRATÉGIA NACIONAL DE DEFESA PARA ALÉM DA GUERRA: *GEOPOLÍTICA CIBERNÉTICA E SEU TRANSBORDAMENTO ECONÔMICO-TECNOLÓGICO NO BRASIL (2008-2018)*

Tese de doutorado apresentada junto ao Programa de Pós-graduação em Economia Política Internacional, da Universidade Federal do Rio de Janeiro (Pepi/IE/UFRJ).

Orientador: Prof. Dr. Pedro Henrique Pedreira Campos

RIO DE JANEIRO

Agosto – 2020

FICHA CATALOGRÁFICA

F383 Ferreira Neto, Walfredo Bento.

Uma estratégia nacional de defesa para além da guerra: geopolítica cibernética e seu transbordamento econômico-tecnológico no Brasil (2008-2018) / Walfredo Bento Ferreira Neto. – 2020.

318 f.; 31 cm.

Orientador: Pedro Henrique Pedreira Campos.

Tese (doutorado) – Universidade Federal do Rio de Janeiro, Instituto de Economia, Programa de Pós-Graduação em Economia Política Internacional, 2020.

Bibliografia: f. 287 – 307.

Ficha catalográfica elaborada pela bibliotecária: Bruna Amarante Oliveira CRB 7 – 6602
Biblioteca Eugênio Gudin/CCJE/UFRJ

WALFREDO BENTO FERREIRA NETO

UMA ESTRATÉGIA NACIONAL DE DEFESA PARA ALÉM DA GUERRA*: GEOPOLÍTICA CIBERNÉTICA E SEU TRANSBORDAMENTO ECONÔMICO-TECNOLÓGICO NO BRASIL (2008-2018)*

Tese de doutorado apresentada junto ao Programa de Pós-graduação em Economia Política Internacional, da Universidade Federal do Rio de Janeiro (Pepi/IE/UFRJ).

BANCA EXAMINADORA

_____

Prof. Dr. Pedro Henrique Pedreira Campos – Orientador

_____

Prof. Dr. Eduardo Alberto Crespo – Membro Interno

_____

Prof. Dr. Cristina Soreanu Pecequilo – Membro Interno

_____

Prof. Dr. Pablo Ibañez – Membro Externo

_____

Prof. Dr. Oscar Medeiros Filho – Membro Externo

RIO DE JANEIRO

Agosto – 2020

A meus Anjos da Guarda:

Francisco (em memória) e Helena;

Francisco Neto, Maria Helena e Antônio;

Suzy, que, além de Anjo, é meu bastião, fonte de força, de luz e de amor,

com muito carinho, gratidão e emoção. Sem esses Anjos, eu nada seria.

AGRADECIMENTOS

A palavra que utilizo como registro de meus agradecimentos é GRATIDÃO. Em todo decurso temporal desta pesquisa, ou mesmo antes, sou GRATO,

A Deus, fonte de inspiração e de vida;

Ao meu professor e orientador, Pedro Campos, primeiro por acreditar em mim, depois pelo profissionalismo acadêmico com que conduziu sua meticulosa orientação e, principalmente, pelo respeito, pela generosidade e pelo ser humano que é;

Aos professores Eduardo Crespo e Pablo Ibañez que, além de participarem da qualificação desta pesquisa, indicaram-me caminhos e referências de muita valia para a continuidade de minha investigação e, ainda, prontificaram-se, literalmente de imediato, a serem membros da banca de avaliação final;

Ao meu amigo Marcos Mendonça, ser humano e geógrafo na essência, não só assumindo missões administrativas e cotidianas da seção de ensino onde lecionamos, para permitir que eu continuasse minha pesquisa, como na função que arrumei para ele, no final do trabalho, de revisor de texto. A você, meu amigo Mendonça, MUITO OBRIGADO!

Ao também amigo e geógrafo Oscar Filho, fonte de longínquas inquietações, no – e acerca do – espaço-tempo, incluindo as de natureza multidimensionais, sejam geopolíticas, sejam do conceito de segurança;

Ao professor e pesquisador geógrafo Hélio Farias, responsável por me indicar o Pepi/UFRJ para a continuidade e aprimoramento da minha pesquisa de mestrado, o que resultou nesta tese;

Ao meu chefe de seção de ensino, Tenente-Coronel Carlos Eduardo Luz Gabriel, que me apoiou nesse mundo das pesquisas desde o curso de mestrado;

Ao Cel Cavalieri, Professor e um do precursores da Cadeira de Relações Internacionais da AMAN, pelas palavras – e ações – de reconhecimento de nosso trabalho e por apontar rumos;

Aos amigos docentes da Cadeira de Economia da AMAN, Augusto Melo, Gustavo Imbiriba e Alex Hummel, pelos esclarecimentos acerca de conceitos e teorias econômicas, que me serviram de sólido suporte para esta tese;

Aos professores do Pepi/UFRJ, Daniel Barreiros, Raphael Padula, Mauricio Metri e Numa Mazat, pelo respeito e compartilhamento de conhecimento que possuem;

Aos Comandantes da Academia Militar das Agulhas Negras (AMAN), generais André Luís Novaes, Ricardo Augusto Ferreira Costa Neves e Gustavo Henrique Dutra de Menezes, por terem não só autorizados meus deslocamentos para fins desta pesquisa, como pela atribuição de tempo para reflexão e registros dos resultados;

Ao senhores chefes da Divisão de Ensino da AMAN, Coronel Claudio Magni Rodrigues, hoje meu amigo de tablado na Cadeira de Geopolítica e com quem aprendo todos os dias, acerca da geopolítica e da vida; Coronel João Augusto Vargas Ávila e Messias Coelho Mendes, pelo constante apoio e – nem sei se eles sabem – por proporcionarem momentos de descompressão para mim, quando marcavam o querido "futebol da DE";

À Associação Educacional Dom Bosco, nas pessoas dos professores Antonio Carlos e Mario Esteves, das senhoras Julia Beatriz Esteves e Gisele Mendes, e dos coordenadores do Curso de Administração, Washington Lemos, e de Economia, Alex Hummel e Marcos Machado, pela confiança e pelo auxílio anímico e financeiro para a pesquisa;

Aos meus amigos de turma do Pepi/UFRJ, com quem compartilho, carinhosamente, a denominação "*pepitos*";

Ao Inest/UFF, nas pessoas dos professores Eurico Figueiredo, Frederico Sá Costa e Vagner Camilo, à senhora Graça e meus amigos *inestianos*, onde minha caminhada acadêmica da pós *stricto sensu* começou e logo na forma bem intensa com o aprender sobre o "pensar estratégico e nacional", uma vez que os "jogos não estão feitos";

Ao funcionário Fabio, da Secretaria do Pepi, que com muita paciência me orientou nos trâmites administrativos da vida acadêmica na UFRJ;

Por fim, registro que o uso da primeira pessoa do plural na redação foi feito de forma intencional, uma vez que eu não teria, de maneira alguma, a capacidade para elaborar esta tese de forma solitária. Pelo contrário, essa realização só foi possível graças a inúmeras contribuições, como mencionei nestes agradecimentos, certo da injustiça de não ter registrado todos. Contudo, também grifo que os equívocos, falhas e outros senões ao longo do trabalho são de inteira responsabilidade deste autor.

"Contemporaneamente, o poder tecnológico moderno, calcado na velocidade acelerada, se firma associado a uma estratégia de controle não só do espaço, mas também do tempo, isto é, do espaço-tempo, que produz um espaço de fluxos. A logística parece estar na base do poder e da Geopolítica hegemônicos: a descoberta e a inovação permanentes, apoiados na concepção e gestão, acionam a economia, antes do que a produção em si, e a guerra permanente, antes do que a batalha em si."

Bertha Becker

"Para os Estados poderosos, nada é mais real e nacional do que a sua Defesa. Para os países menos aquinhoados pelo poder, nada é mais ideal e menos nacional do que a sua própria Defesa."

Eurico de Lima Figueiredo

RESUMO

A presente pesquisa tratou das políticas ligadas ao setor cibernético no Brasil, após a publicação da Estratégia Nacional de Defesa. Os objetivos foram verificar: 1) em que consistiu essa política no período 2008-2018; 2) como se inseriu no panorama internacional; 3) e a que procurou responder. A preocupação condutora desta investigação disse respeito às chances de continuidade dessa política em um País que, tradicionalmente, não se envolve em conflito interestatal. Mais que isso, a pretensão foi de verificar se, a partir desta política, haveria oportunidade de fornecimento de um bem público – Defesa – com transbordamento econômico-tecnológico para outros setores, uma vez que o núcleo da cibernética baseia-se em ferramentas de tecnologia da informação e comunicação, o que permitiria a formação de um circuito virtuoso entre coerção e riqueza, dirimindo o dilema acerca dos investimentos "em espadas ou em arados". Constatamos que Estados estão se movimentando para comporem sistemas de defesa especializados para o ciberespaço, a fim de garantirem suas respectivas seguranças nessa nova dimensão, o que conduz o sistema internacional a uma nova delimitação, a da *fronteira-ponto*, como consequência da capacidade de monitoramento e controle por parte de alguns atores. A cibernética, assim, é tratada como um espaço em si e como mais um recurso, capaz de territorializar as dimensões geográficas tradicionais. Contudo, além desse uso, a cibernética é capaz de acionar a economia, o que exige um olhar a partir de instrumentos disponibilizados pela Economia Política Internacional, por relacionar, mutuamente, instrumentos de coerção e de oportunidades econômicas, e por considerar as características do sistema, que é capitalista. Foi nesse sentido que o setor estratégico da cibernética no Brasil foi conduzido, com resultados para o setor Defesa e com transbordamentos científico-tecnológicos para outros setores, a título de externalidades positivas. A intenção foi de compor, no Brasil, um complexo militar universitário-industrial nos moldes do sistema tríplice hélice. Dessa forma, a preparação da Defesa pode trazer dividendos para além da guerra. Para essa conclusão, investigamos precipuamente documentos, discursos e ações oficiais do Executivo e do Legislativo, do nível federal e estadual, reportagens e instrumentos do *e-Gov*, e os confrontamos com a realidade.

Palavras-chave: Estratégia Nacional de Defesa. Setor cibernético. Preparação para a guerra. Transbordamento econômico-tecnológico.

ABSTRACT

The present research dealt with policies related to the cyber sector in Brazil, after the publication of the National Defense Strategy. The objectives were to verify: 1) what this policy consisted of in the 2008-2018 period; 2) how it was inserted in the international panorama; 3) and the one you tried to answer. The guiding concern of this investigation was related to the chances of continuing this policy in a country that, traditionally, is not involved in interstate conflict. More than that, the intention was to verify if, from this policy, there would be an opportunity to supply a public good – Defense – with economic-technological overflow to other sectors, since the core of cybernetics is based on technology tools of information and communication, which would allow the formation of a virtuous circuit between coercion and wealth, resolving the dilemma about investments "in swords or plows". We note that States are moving to compose specialized defense systems for cyberspace, in order to guarantee their respective security in this new dimension, which leads the international system to a new delimitation, that of the border-point, as a consequence of the monitoring capacity. and control by some actors. Cybernetics, therefore, is treated as a space in itself and as another resource, capable of territorializing traditional geographical dimensions. However, in addition to this use, cybernetics is capable of triggering the economy, which requires looking at instruments made available by the International Political Economy, for mutually relating instruments of coercion and economic opportunities, and for considering the characteristics of the system, which is capitalist. It was in this sense that the strategic sector of cybernetics in Brazil was conducted, with results for the Defense sector and with scientific-technological spillovers to other sectors, as positive externalities. The intention was to compose, in Brazil, a military university-industrial complex along the lines of the triple helix system. In this way, the preparation of the Defense can bring dividends beyond the war. To this conclusion, we investigated documents, speeches and official actions of the Executive and Legislative, at the federal and state level, reports and instruments from e-Gov, and confronted them with reality.

Keywords: National Defense Strategy. Cyber sector. Preparation for war. Economic-technological overflow.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

A inspiração desta pesquisa de tese começou ainda nos bancos universitários do curso de mestrado, entre 2011 e 2013, no Programa de Pós-graduação em Estudos Estratégicos da Universidade Federal Fluminense, campus Valonguinho, em Niterói-RJ. Naquela ocasião, debruçamo-nos sobre o mesmo objeto da atual investigação – a cibernética e o ciberespaço – e a forma como estava sendo conduzido esse setor estratégico no Brasil, *status* atribuído à cibernética pela Estratégia Nacional de Defesa de 2008 e em documentos de Defesa[1] sucessores.

À época, em comparação com informações acerca da estruturação desse setor em outros países, como os Estados Unidos, membros da União Europeia e a China, e em organizações internacionais, como a União Internacional de Telecomunicações da Organizações das Nações Unidas (UIT/ONU), notamos que o movimento nacional era muito similar, no que dizia respeito à formação de centros ou núcleos especializados em defesa para esse novo espaço e recurso de poder e a discussão sobre provável criação de uma quarta Força, além das já existentes para os domínios espaciais geográficos tidos como tradicionais: terrestre – Exército; marítimo – Marinha; aéreo – Força Aérea ou Aeronáutica, além de exercícios de simulação de ataque e defesa nesse ambiente. Dessa forma, naquele trabalho, uma das conclusões foi que a cibernética estava sendo empregada, também, para fins de coerção no sistema internacional, em conflitos, alguns com características de guerra, e outras ações que demandavam o uso da força. Esse processo por nós apreendido pode ser enquadrado no fenômeno da territorialização-desterritorialização-(re)territorialização, T-D-R, observado pelo geógrafo suíço Claude Raffestin (1993). A cibernética e o seu espaço consubstanciavam novos instrumentos nessa busca de ocupação, gestão e aproveitamento de territórios, em suas várias dimensões.

[1] Para fins de padronização, utilizamos Defesa com inicial maiúscula, da mesma forma que Desenvolvimento, quando nos referimos a esses como instituições nacionais, contempladas em políticas públicas setoriais, ou seja, em um nível macro, diferenciando-os de defesa e desenvolvimento vistos como ações pontuais.

Contudo, da metade para o final daquela nossa pesquisa de mestrado, com base na literatura e em documentos disponíveis, e nos fatos, percebemos que as ações voltadas para a cibernética iam além da utilização deste instrumento para fins de coerção. Não foram poucos os livros, periódicos, documentos e reportagens que trouxeram a relação entre pesquisas para desenvolvimento de ferramentas de tecnologia da informação e comunicações, logo ferramentas relacionadas à cibernética e seus ganhos econômicos e, portanto, sociais. A tecnologia, nesses casos, inserida em ambiente que contemplava a competição e a concorrência, em várias áreas, serviu, de forma ambivalente, de força-motriz para o desenvolvimento econômico-social e para a preparação para o conflito. Esse ponto nos despertou muita atenção, sobretudo para o Brasil, por um lado, por ser um país inserido no rol dos "em desenvolvimento", com todas as características que lhe são peculiares e, por outro, por possuir recursos naturais de cunho estratégico no presente e do futuro.

Até então, em disciplina eletiva do mestrado que contemplava a relação entre ciência, tecnologia e poder, conduzida pelo professor José Carlos Albano do Amarante, general da reserva do Exército Brasileiro, antigo diretor do Instituto Militar de Engenharia, nosso entendimento era de que o poder provinha, em última instância, da capacidade do uso da força, ou, como disse John Mearshimer (2007), do uso da força bélica-militar, acompanhando os princípios de um realismo de poder ofensivo. Hoje, não temos mais tanta certeza dessa posição. Pelo visto, pode até ser realmente o uso da força, porém, para se possuir esta capacidade, cada vez mais são o *gap* tecnológico e a busca da construção de um circuito virtuoso gerado pela pesquisa, desenvolvimento e inovação os pontos-chave, tanto para coerção quanto para riqueza de um país. Por conseguinte, além da política, concordamos que, de forma mútua e interdependente, temos que considerar a gestão dos recursos, da riqueza, como parte desta preparação, para o desenvolvimento econômico e para a guerra. Daí nossa opção pelas reflexões citadas na epígrafe deste trabalho, inclusive para somarmos esforços na transformação do ideal em real e nacional.

Que a guerra é um fenômeno social, cremos que não resta dúvida e, como tal, é certo contar com os imponderáveis, intrínsecos à própria natureza humana. Entretanto, devido a esses argumentos, entregar à sorte a condução da preparação para esse fenômeno não parece ser uma medida assertiva, tal como já observara Tucídides em seu famoso "Diálogo de Melos" (2001 [V a.C.]), sobretudo ao nos depararmos, com base na história e buscando sistematizar os fatos, com a conclusão de que se preparar para a guerra pode ser uma estratégia para além de si mesma.

Não foram poucos os casos em que tecnologias, tanto na forma de produtos quanto de processos, geradas para responderem a ameaças, terminaram por transbordar outros benefícios para a sociedade, o que na literatura econômica pode ser encontrado com as denominações *externalidade*, no caso positiva, *benefício marginal social*, *spin in* ou *spin off*, possibilidade de gasto ou de *investimento bivalente*, ou, ainda, em se tratando de investimento do ator estatal, em termos *keynesiano*, da capacidade de criar um *efeito multiplicador*. Esse é o pretérito do GPS e da *internet*, por exemplo. Parece-nos que o famoso provérbio latino "se queres paz, prepara-te para a guerra", atribuído a Publius Flavius Vegetius Renatus, ainda no século IV d.C., contém muito mais ensinamentos do que podemos imaginar.

Não queremos de forma alguma apontar que o fenômeno guerra é algo salutar, profícuo ou que traz benefícios. Não é isso. Caso sigamos essa linha de pensamento, podemos correr o risco pelo qual passou Yves Lacoste (1989 [1976]), ao mencionar que a geografia serviria, antes de mais nada, para fazer a guerra. Não é dizer que a geografia serve apenas para a guerra, da mesma forma que não é dizer que a guerra traz a paz. Se prestarmos bastante atenção na própria construção dessas expressões e dos ensinamentos contidos nos pensamentos de seus autores, a questão passa a ser, para o primeiro, a atribuição da devida importância às condicionantes geográficas para outros ramos científicos e sociais, além de ser um fator de extrema relevância no pensamento dos estados-maiores dos exércitos e, para outro, ao potencial advindo dos atos de *preparação* para o conflito para além da guerra, e *não de fazer* a guerra propriamente; e essa diferença de interpretação, aparentemente simples, é capaz de gerar complexas e severas consequências ou externalidades, positivas ou negativas, dependendo da maneira como é conduzida. A ideia pode ser concebida no propósito de que o ato de se preparar para a guerra pode ser útil para a dissuasão político-estratégica e também para o desenvolvimento econômico, científico-tecnológico e social, podendo ainda ser quanto a este último um fator de convergência e de aglutinação de valores comuns internos perante alguma ameaça externa, o que acarreta coesão via a também almejada cultura de Defesa. Esse processo de reflexão e de condução configuraria, assim, fenômeno intitulado "uma ação e dois (ou mais) movimentos".

O Brasil, por meio de seus documentos de Defesa, apontou nessa direção, no recorte temporal desta pesquisa (2008-2018), não se esquecendo de seus compromissos assumidos perante a sociedade internacional e de sua tradição diplomática. Além disso, outro viés pode ser inferido desses documentos e das ações resultantes: os setores definidos pela Defesa como estratégicos para o País são intrinsecamente objetos de possíveis transbordamentos positivos, pelo seu uso dual. Essa é a realidade do setor cibernético, que cada vez mais ganha espaço nos fóruns políticos e acadêmicos, nacionais e globais, por se reconhecerem, todos os dias, novas

possibilidades advindas do desenvolvimento desse setor: Indústria e Educação 4.0, aí compreendidos o *Big Data*, a robótica, a inteligência artificial, as "cidades inteligentes", a *internet* das coisas (IoT) e a 5G, por exemplo, esta inclusive sendo objeto de intensas disputas entre, pelo menos, Estados Unidos e China, por se tratar de tecnologia disruptiva, o que, por conseguinte, pode alterar o equilíbrio de poder político e econômico do sistema internacional.

Em 2013, sob o ponto de vista político, apontamos a importância do núcleo duro do que denominamos cibernética, que vem ser a informação na sua forma digital, isto é, sob uma abordagem que visava entender o papel da informação, sobretudo, em um processo decisório, inclusive nos casos de conflitos que alcancem o extremo do uso da força. De lá para cá, por meio de observações mais aproximadas deste objeto e de leituras especializadas quanto às capacidades advindas desse elemento, chegamos a outras conclusões, que não necessariamente excluem aquela; pelo contrário, somam-se, na medida em que reforçam a relação entre *informação* e *poder*, englobando outros componentes ou fatores, como é o caso do papel da economia no jogo decisório, no jogo do poder.

Quanto ao poder, inúmeras definições foram formuladas e são usadas para conceituá-lo. Talvez, em termos de política, o mais importante é que poder é relacional, o que, *per se*, demanda conexão entre as partes envolvidas em uma relação. A capacidade de influenciar outrem ou de fazer com que outrem realize aquilo que você deseja necessita, *a priori*, para se concretizar, de uma conexão, o que nos remete, em seu núcleo, à informação. Esse apontamento pode ser encontrado, com maior ou menor ênfase, em Robert Dahl (1957), Claude Raffestin (1993), José Fiori (2004) e, ainda mais distante no tempo, em Harold Lasswell (1936 *apud* HUNTINGTON, 1996 [1957]).

No tocante à informação, núcleo do objeto deste estudo, física e filosoficamente tratando, não há ainda um consenso de sua natureza, nem mesmo se este elemento é singular, isto é, um elemento em si, um componente independente na natureza e no universo, além da matéria e da energia. De nossa parte, pelo que pesquisamos, inferimos e refletimos, acreditamos fortemente ser a informação não só um elemento em si como também o de maior importância. É a informação que dá sentido a um processo decisório, por exemplo, em qualquer nível de análise e em qualquer escala, seja geográfica, seja temporal. Isso, no atual momento – na verdade, desde o final do século XX (CASTELLS, 1999) e até mesmo antes – é crucial, uma vez que assistimos a um deslocamento da preponderância de fatores de produção tradicionais como matéria e energia, para os que se baseiam na informação, como é o caso das ferramentas de tecnologia da informação e comunicações (TIC), da informática e das telecomunicações.

Essa tendência também é constatada, e com maior ênfase, por Yuval Harari (2016) para o século XXI, e, por meio de uma arqueologia do papel da informação, por James Gleick (2013).

Ainda quanto à informação e à sua existência de forma autônoma, várias ações praticadas por nós, sejam indivíduos, sejam Estados, apesar de despercebidamente, só são consideradas ações por derivarem de um gasto de energia para uma determinada finalidade. E é esta determinação sobre qual finalidade e o como agir que nós entendemos como sendo a residência da informação. Como exemplo, no início da formação militar, por meio da denominada instrução individual básica, aprendemos a como nos orientar no caso de ficarmos perdidos espacialmente. A sigla, ou o processo mnemônico, constante do manual e que memorizamos consiste no "ESAON", cujo significado nos remete a: E – estacione, S – sente, A – alimente-se, O – oriente-se, e N – navegue.

Com relação as duas primeiras ações – estacione e sente – estas indicam a necessidade de não gastarmos energia em vão, ou seja, a preocupação com a economia de energia para a manutenção da sobrevivência. A terceira ação, que reforça a preocupação das primeiras, acena para a necessidade de buscarmos aumento e acúmulo de energia, o que indica a noção de previsibilidade entre meios e fim. Em todas essas constatamos o objeto *informação*, no momento da tomada de decisão ponderada acerca do que fazer. No entanto, é a partir da fase "oriente-se", a quarta, que a informação passa a ser mais facilmente vista, eis que trata de indicar as bases para a próxima fase, que é a navegação, o deslocamento de um ponto a outro, de maneira sistematizada e para atender também a um fim, que no exemplo trazido corresponderia a nos situarmos espacialmente.

Esse processo, embora não acompanhado desta sigla, pode ser inferido a partir da análise do planejamento estatal, tanto para fins de desenvolvimento econômico, quanto para uma política de poder. Quando William Petty publicou *Aritmética Política* (1690), sua preocupação maior era a de como transformar uma sociedade (a inglesa), a partir de um território e sua geografia (ilhas britânicas), em potência mundial, em partícipe ou até mesmo definidora da ordem global. Primeiramente Petty analisou pontos fortes – forças – e fracos – fraqueza, vulnerabilidades – de seu Estado, para depois delinear um caminho visando a um fim. Para isso ele sabia – embora não explicitasse, pois não era seu objeto de estudo à época – da necessidade de se possuir energia para fins de se orientar e, só então, navegar. E isso foi o que literalmente a Inglaterra fez a partir do fim do século XVII, como bem descreveu Alfred Mahan (1890), e que posteriormente serviu de lição para seus irmãos anglo-saxões nas Américas.

Todavia, não foi só a Inglaterra que se planejou para o intento de se tornar potência. Antes mesmo, Portugal e Espanha se destacaram no cenário mundial por possuírem

conhecimento sobre a geografia do globo e as ferramentas tecnológicas que permitiriam explorar as possibilidades daí advindas. As chamadas Grandes Navegações só foram possíveis graças à existência de poder, ou seja, de energia e informação, elementos capazes de deslocar matéria de forma intencional, para uma finalidade. Esse relato é muito bem descrito por Celso Furtado, na introdução do célebre *Formação Econômica do Brasil* (2005 [1959]), ao abordar o tratamento dado pelas potências ibéricas às suas "novas terras" americanas e o planejamento em face das ameaças representadas pelas outras potências europeias, o que demandou articulação entre Defesa e Desenvolvimento, seguramente com o fito de não onerar os respectivos cofres públicos.

Mais tarde, quando Sir Halford Mackinder (MELLO, 1999) procurou desenvolver sua teoria acerca dos espaços geográficos e do poder, que resultou na identificação de um *heartland*, indubitavelmente buscou no elemento *informação* a chave para superar as dificuldades impostas pela localização inglesa *vis a vis* à tradicional potência russa e à crescente e já unificada Alemanha. Não foi à toa que um dos requisitos para se definir a terra-coração foi a existência de vastas reservas de fontes de energia. Na sequência histórica, consoante demonstrou Mello (1999), Nicholas Spykman (1942) daria outra opção estratégica para essa questão.

Ao escrever sobre *A Grande Ilusão*, Norman Angell (1910), de forma bastante convincente, alertou para o papel que a informação possuía no sistema econômico mundial, tornando-se global, via financeirização. As conexões entre bancos e países, e a respectiva interdependência, para esse autor, seriam capazes de impedir o surgimento de novos conflitos, o que dispensaria os gastos militares. Todavia, com um pouco mais de atenção, pode ocorrer que o nível de análise em que o debate e o referencial teórico estejam ocorrendo não correspondam, verdadeiramente e de fato, a esses. Por exemplo, quando Angell abordou a importância das comunicações para o comércio e para o desenvolvimento e que, a partir desta, não seria mais interessante fazer a guerra, ele não mencionou a quem pertencia a estrutura e o controle daquelas redes de informação, e isso, em termos de poder, tem grande importância, uma vez que perfaz a própria estrutura do sistema. Por isso é mister identificarmos sobre qual camada estamos refletindo, escrevendo, planejando, da mesma forma que fez Braudel (1987), ao apontar o diferente funcionamento nas camadas da vida material, da economia de mercado e do verdadeiro capitalismo, bem como a relação entre essas. O "jogo da guerra" (ELIAS, 1994 [1939]; FIORI (2004), ao que tudo indica, está muito mais próximo desta última camada, que dirige, ou no mínimo influencia, as demais.

A pergunta que permeou as experiências das potências exitosas certamente não foi a de se investir ou não em Defesa, ou, para a linguagem da época, na preparação constante para a guerra. A questão pautava-se no *como* investir na preparação para a guerra e ainda obter ganhos econômicos e, assim, tanto impulsionar o desenvolvimento do país quanto manter um processo de retroalimentação entre preparação da Defesa e Desenvolvimento, e deste para a Defesa, sucessivamente. Em suma, esse foi um dos argumentos contidos na tese defendida por Paul Kennedy (1989) acerca da ascensão e queda das grandes potências. Nesse processo, evidentemente, quanto menor os custos para se obter poder, capacidades e domínio melhor. É nessa esteira que foram aplicadas as formas de poder recentemente denominadas *soft* (poder brando) e *smart* (poder inteligente) por Joseph Nye (2012). Todavia, nem sempre foram apenas essas formas as infalíveis. O poder em sua vertente *hard* (poder duro), ainda que latente, também era – e é – usado para esses fins.

Nos últimos anos, no Brasil, principalmente após a publicação da Estratégia Nacional de Defesa, em 2008, essa relação entre Defesa e Desenvolvimento parece novamente ter sido trazida à tona. Inúmeros segmentos da sociedade surgiram ou ganharam espaço nas discussões acerca desse tema e na proposição de questões para a agenda política. Universidades, institutos de pesquisa, associações, indústrias, além do segmento militar, debruçaram-se cada vez mais sobre as possibilidades advindas dessa relação para o País. Os documentos oficiais, as audiências públicas e interativas no Senado Federal e na Câmara dos Deputados, os simpósios, *workshops*, painéis e congressos apontaram cada vez mais para a necessidade de se ir além da questão de investir ou não em Defesa e passaram a encarar a fase posterior, uma outra etapa, compatível com um País de dimensão continental, rico, de grande população e que aspira, por tudo isso, participação crescente nos processos decisórios mundiais.

Diante disso, o problema central e norteador que formulamos para esta pesquisa diz respeito a como o Brasil tem se utilizado da Defesa cibernética enquanto oportunidade de desenvolvimento e de acúmulo de poder? Relacionadas com este problema há as seguintes inquietações: em que consiste a política de defesa cibernética brasileira correspondente ao período 2008-2018? Como ela se insere no panorama internacional e a que ela procura responder?

Inseridas nessas inquietações, as questões seguintes também moldaram o arcabouço do problema desta pesquisa: quais as chances de continuidade dessa política em um País que, tradicionalmente, não se envolve em conflito interestatal? Haveria, por meio dessa política em específico, oportunidade de fornecimento de um bem público, considerado, economicamente, puro (Defesa), com transbordamento econômico-tecnológico positivo, tendo em vista se tratar

de um setor estratégico baseado em ferramentas de tecnologia da informação e das comunicações, logo instrumentos de utilidade dual e transversal, tanto para (e no) uso militar quanto para (e no) civil?

Como hipótese central da pesquisa, acreditamos que por trás do atual conceito de *cibernética*, e das políticas que a conduzem a partir da publicação da Estratégia Nacional de Defesa (2008), existem empreendimentos, estatais e privados, nacionais e internacionais, no sentido de uma *territorialização* do "novo" domínio espacial – o ciberespaço – e, também e a partir deste "novo" recurso de poder, uma *(re)territorialização* dos domínios geográficos tradicionais – o terrestre, o marítimo e o aeroespacial – que porventura estejam ou venham sendo submetidos ao denominado fenômeno globalização.

Como hipóteses secundárias, mas extremamente vinculadas à primeira, temos que, historicamente: 1) a pressão competitiva pelos espaços geográficos e, consequentemente, pelo aumento de capacidade de segurança (abrigo) e de oportunidades econômicas (riqueza) é fenômeno comum, que pode ser visto tanto aplicado na dimensão terrestre, quanto nas demais dimensões espaciais geográficas; 2) os Estados, juntamente com o grande capital privado, são os atores principais dessa empreitada, buscando conciliar coerção e capital; 3) nem todos os atores são capazes de participar desse jogo competitivo, que envolve tanto o "jogo das trocas" *braudeliano*, quanto o "jogo das guerras", de Elias (1994 [1939]), como abordados por Fiori (2004).

Nesse sentido, em se tratando de Brasil, a Estratégia Nacional de Defesa de 2008 foi um passo importante na direção de esforços para a formação de uma espécie de "complexo militar-industrial-acadêmico" não só nacional, mas sim na tentativa de envolver países sul-americanos, no que diz respeito ao setor cibernético e às áreas por este tangenciadas, o que vem sendo denominado base industrial de defesa regional, dentro do que Medeiros Filho (2010) denominou "cooperação regional para uma dissuasão extrarregional".

Esse processo, estruturalmente e em resposta à questão de fundo, está relacionado à tentativa de formação ou consolidação de um Estado-economia nacional (FIORI, 2004; 2008). A própria Estratégia Nacional de Defesa explicitou a necessidade do binômio *Defesa-Desenvolvimento*, pois tenta fomentar a sustentabilidade da Defesa Nacional, por meio do início de um ciclo virtuoso, visando ao fornecimento, em última instância, de um bem público puro – Defesa – sem que isso ocasione reflexos deficitários no orçamento e, simultaneamente, garantindo perenidade às demandas por produtos dessa natureza, que no caso das ferramentas de tecnologia da informação e comunicação se torna mais fácil. Contudo, há ainda inúmeras

oportunidades de melhoria do processo, no campo político, econômico, científico-tecnológico e social, e no intercâmbio entre esses campos, visando ao pleno desenvolvimento dessa política.

O arcabouço teórico da pesquisa utilizou lentes e variáveis que buscaram ligar, mútua e reciprocamente, instrumentos da política e da economia (STRANGE, 1988), inseridos em uma visão estratégica, aí contidas as perspectivas da geopolítica e da geoeconomia (BLACKWILL; HARRIS, 2016). Essa visada em muito se assemelha – apesar do grande lapso temporal – à forma de se pensar e fazer política, nacional e internacional, a partir de elementos, se não determinantes, pelo menos condicionantes ou possibilitadores, como foi o pensar crítico de William Petty (1996 [1690]), conforme também anunciado por José Fiori (2005; 2012), de Alexander Hamilton e de Friederich List (EARLE, 2001; CHANG, 2004), por exemplo, e, mais recente, como registraram Jean Gottman (2012 [1975]) e Yves Lacoste (1989 [1976]).

Dessa forma, mormente foram estudados e aplicados os conceitos de espaço e poder, e sua transformação em território(s), em conjunto com o de cibernética, em seu contexto atual. Nesse sentido, a cibernética foi vista tanto como um "novo" domínio espacial (o ciberespaço e as infovias), que, embora sendo artificial, obedece a regras e a relações bem semelhantes às ocorridas nos domínios geográficos naturais ou tradicionais, e como mais um recurso de poder utilizado pelos Estados, tanto na esfera interna quanto nas relações externas. Ainda nesse sentido, a cibernética seria mais um instrumento que possibilitaria a territorialização desse "novo" espaço das infovias e uma (re)territorialização dos domínios espaciais tradicionais, como o terrestre, o marítimo e o aéreo.

Assim, uma inovação disruptiva *schumpteriana* (1997 [1911]) é capaz de gerar monopólio sobre o produto ou o processo inovador, ainda que temporário, e que depois, acompanhando o ciclo de vida do produto descrito por Vernon (1966), ramifica-se, por meio da padronização da inovação na sociedade internacional, o que gera dependência. Aqui, traduzindo para nosso cotidiano, estamos falando da necessidade de atualização constante dos sistemas operacionais informacionais de nossas máquinas, tanto por parte da inserção de novos componentes e programas, como também por uma questão que age no psicológico do indivíduo, ligado a *status*, à imagem pessoal. E esse poder é incrível, eis que é praticamente invisível e sorrateiro para o senso comum. Todavia, para os que se debruçam sobre essa problemática, isso passa a ser quase uma prisão, sobretudo no tocante à condição de país em desenvolvimento ou subdesenvolvido que não consegue vencer a barreira da economia de mercado para a de obtenção e controle de monopólios, seja por causa do cerceamento tecnológico praticado pelos que "chutam a escada" – o que deve ser visto como algo natural sob o ponto de vista realista – quanto por problemas internos ligados ao baixo índice de qualificação de recursos humanos e

de tecnologia autóctone.

Por tudo isso, acreditamos pertinentes nossa reflexão e, pelo menos em tentativa, contribuição para o País acerca da cibernética e suas possibilidades.

No tocante à metodologia, em um primeiro momento, a pesquisa foi exploratória e descritiva, visando à compreensão de como vem funcionando a estrutura das instituições ligadas à política de defesa cibernética brasileira, a partir dos principais documentos do setor, como a Estratégia Nacional de Defesa (2008) e a Política Nacional de Defesa (2012). Após isso, de forma também exploratória, porém explicativa, verificamos benefícios obtidos e pontos que dificultaram a consolidação das diretrizes contidas nesses documentos.

A pesquisa constou de revisão bibliográfica sobre o objeto de estudo – setor cibernético e Defesa – e áreas correlatas, tendo em vista a multi e interdisciplinaridade exigida pela própria natureza do tema. Essa também é uma característica marcante proporcionada pelo Programa de Economia Política Internacional da Universidade Federal do Rio de Janeiro, motivo pelo qual o procuramos como suporte a nosso intento.

A pesquisa de campo, *lato sensu* tratando, foi essencial, tendo em vista a coleta de dados de autoridades e instituições vinculadas ao setor estratégico da cibernética. Tivemos a oportunidade de participar de congressos, seminários, simpósios temáticos e *workshops* relacionados com o assunto em tela. Além disso, entre 2014 e 2018, participamos, como pesquisador, autor e organizador de coletâneas, de projetos ligados à defesa cibernética, como foi o caso do *Vigilância nas Fronteiras e Muros Virtuais*, vinculado ao Pró-Estratégia, fomentado pela Secretaria de Assuntos Estratégicos da Presidência da República e a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, e da publicação *Guia de Defesa Cibernética na América do Sul*, apoiada pelo Instituto Brasileiro de Estudos de Defesa, o Ministério da Defesa e o Conselho Nacional de Desenvolvimento Científico e Tecnológico. Assistimos também a reuniões que envolviam assuntos ligados à implementação do Comando de Defesa Cibernética e do Sistema Defesa-Indústria e Academia de Inovação, dentre as quais a ocorrida durante o *Brazil Cyber Defence Summit and Expo*, evento que se propôs a debater temas sobre defesa cibernética, comunicações e guerra eletrônica, em 2018, em Brasília. Ainda, como instrumento de coleta de informações diretas dos órgãos públicos, utilizamo-nos de ferramentas da própria cibernética, por meio do sistema *e-Gov* e da Plataforma Integrada de Ouvidoria e Acesso à Informação – Fala.BR.

Os resultados colhidos e elaborados por nós foram agrupados em quatro capítulos distintos, porém conexos, além desta introdução e das considerações finais. A ideia, mas não de forma taxativa ou inflexível, foi irmos do geral para o particular e do teórico para o empírico.

No primeiro capítulo, com as devidas atualizações, resgatamos os ensinamentos colhidos a partir de nossa pesquisa de mestrado acerca do enfoque geopolítico dado à cibernética e ao ciberespaço. Nessa parte, revisitamos os processos de ocupação de outras dimensões espaciais para concluir sobre a territorialização do ciberespaço, que nos conduziu à formulação de um novo tipo de delimitação: a *fronteira-ponto*. Além disso, verificamos que a cibernética é vista como um espaço em si mesmo, o ciberespaço, e como um recurso de poder, sobretudo pela sua transversalidade.

No segundo capítulo, ampliamos a discussão teórica para além da geopolítica, com alguns adendos empíricos, para fins de obter maior capacidade de explicação dos fenômenos que ocorreram no período estudado – mas não só nesse – acerca da composição de estruturas de Defesa voltadas para o ambiente cibernético. Nessa parte, procuramos verificar os "porquês" desse movimento, isto é, a que eles procuraram responder e de que forma. Precisamos, para isso, ir além das correntes teóricas do realismo, do liberalismo e do marxismo das relações internacionais, encontrando no campo da economia política internacional respostas mais completas para nossos questionamentos e para a realidade, sobretudo pela busca de conexão entre coerção e riqueza e o papel da tecnologia nesse movimento.

No terceiro capítulo, expomos a estruturação da Defesa brasileira a partir da elevação da cibernética a um dos setores estratégicos do País. Nesta parte, muito do que apreendemos também de nossa pesquisa de mestrado se mostrou significativo, tendo em vista a possibilidade que nos proporcionou em comparar o movimento inicial da administração legal e legítima da violência para esse setor e sua continuidade. Assim pudemos nos deparar com a criação de um núcleo, que logo em seguida foi transformado em um centro, de defesa cibernética, âmbito Exército, que depois foi alçado ao nível de comando conjunto, envolvendo as Três Forças Armadas nacionais. Também nesse capítulo vimos esforços no sentido de atender às diretrizes e aos eixos estruturantes da Estratégia Nacional de Defesa, principalmente, no que tange à cibernética, no aprimoramento dos conceitos, denominados pelo documento imperativos, de controle/monitoramento, mobilidade e presença, e a busca pelo binômio Defesa-Desenvolvimento como premissa, este último materializado na criação de um escritório específico, o Escritório de Projetos do Exército, e de um sistema de inovação que conjuga, além da Defesa, a indústria e a academia, inspirado no modelo estadunidense de complexo militar-industrial-acadêmico ou no que a própria estratégia nacional brasileira chamou de complexo militar-universitário empresarial. Nesse capítulo, portanto, focamos nas ações, projetos e programas com origem na estrutura de Defesa para o setor cibernético.

Por fim, no quarto e último capítulo de nosso relatório de pesquisa, escrevemos os resultados de nossa investigação sobre os efeitos que o setor cibernético, após ter sido elevado ao *status* de estratégico, ocasionou para além da Defesa *stricto sensu*. Por conseguinte, analisamos ações e normas ministeriais, projetos e programas que, muito embora não fossem ligados originariamente à Defesa, ou passaram a ser inseridas por esta ou passaram a considerar o previsto na Estratégia Nacional de Defesa para sua consecução. Assim, este capítulo nos permitiu organizar os resultados para o setor cibernético a partir de outros atores não situados especificamente no setor Defesa. Esses foram os casos, por exemplo, do Programa Nacional de Banda Larga, capitaneado pelo então Ministério da Ciência, Tecnologia e Inovação e pelo das Comunicações, e da Estratégia para Transformação Digital do Brasil, a E-Digital. Essa também foi a realidade do Programa Amazônia Conectada e do Satélite Geoestacionário de Defesa e Comunicações Estratégicas. Ainda como um desses intentos, mas que não atingiu êxito, a iniciativa de construção do cabo submarino Brasil-Europa. Em todas essas iniciativas, o caso de espionagem denunciado por Edward Snowden criou, em maior ou menor grau, uma janela de oportunidade para políticas públicas que se propuseram a aumentar a confiabilidade do ambiente cibernético por parte do Brasil, mas, ao que tudo indica, não apenas para isso.

Após esta introdução, desejamos uma ótima e profícua leitura!

CAPÍTULO 1

GEOPOLÍTICA CIBERNÉTICA

O objetivo desse capítulo visa definir, principalmente, *cibernética*, conceito-guia desta pesquisa. O enfoque dado é geopolítico, apesar de serem, a seguir, apresentados diversos significados de "cibernética" ao longo da história. Para tanto, a cibernética, que em essência, hoje, trata da informação digitalizada e o meio em que esta circula (infovias), é considerada aqui como: 1) um espaço em si mesmo, o denominado ciberespaço, e 2) mais um recurso de poder, inserido no relacionamento entre os principais atores do sistema interestatal.

Não é nosso intento, neste momento, fazer um histórico ou resumo das teorias geopolíticas clássicas e contemporâneas, mas sim extrair delas seus principais conceitos e, sobretudo, a forma de como esses eram – e são – teorizados e aplicados. Por isso, conceitos de natureza geográfica e política são manuseados, como é o caso de *espaço*, *rede*, *poder* e, com destaque, *território*, por ser este, por ora, conceito-síntese da discussão, o *locus* resultante dos mais variados e complexos feixes de forças. Junto a isso, inferida de quase a totalidade das teorias geopolíticas, utilizamo-nos da ideia de que aquele que domina ou controla um determinado território consegue projetar poder sobre os demais. Esse é um ponto importante, principalmente ao considerarmos que o ciberespaço já se perfaz um território – para alguns atores – e que é disposto de forma transversal e com acesso a todas as outras dimensões espaciais.

Essa visão ensejada também não é no sentido de ir de encontro à tese de Kaplan (2013). Pelo contrário, "A Vingança da Geografia" realmente, para nós, faz-se presente no sistema internacional, porque é e compõe, antes de qualquer coisa, a estrutura. Contudo, entendemos que o homem, historicamente, cria possibilidades, visando à superação de alguns relativos óbices dessa mesma estrutura. Esse é exatamente um dos mais importantes papéis exercidos

pela informação e sua circulação – as comunicações. É isso, exatamente, que constitui o núcleo duro do que hoje denominamos *cibernética*, permitindo um encurtamento de distâncias e uma compressão temporal cada vez maior, mas, todavia, não deixando de ter, de pertencer ou de estar, em última instância, em um determinado *locus*: no território.

Decidimos por esse enfoque, metodologicamente tratando, tendo em vista o objeto da pesquisa: a cibernética vista como um setor estratégico do Brasil, a partir de seus principais documentos de Defesa. Como exemplo, constando do nível político mais elevado do País, debruçamo-nos sobre a Estratégia Nacional de Defesa (END), a Política Nacional de Defesa (PND) e o Livro Branco de Defesa Nacional (LBDN), constituindo o primeiro desses documentos na fonte primária oficial de referência precípua dessa pesquisa.

Entendemos, assim, que a END, por si, representa um documento elaborado por um Estado, para fins de Defesa, considerando a relação de poder entre este e outros atores do sistema internacional. É por isso, também, que decidimos pela Geopolítica, por se tratar, a princípio, de um ramo da ciência ou até mesmo de um campo multidisciplinar (VESENTINI, 1989), que se situa, tradicionalmente como nível de análise, na relação entre Estados soberanos e, mais recentemente e de forma ampliada, entre esses e outros atores do sistema interestatal, como é o caso das grandes corporações empresariais e dos organismos internacionais.

Todavia, convém registrar que os conceitos que conformam a Geopolítica e que lhe atribuem *status* de ramo científico podem ser encontrados na relação entre elementos em outra escala geográfica, como no relacionamento entre indivíduos. Para ilustração, a título de exemplo, imaginemos uma sala de aula, com diversas cadeiras colocadas no interior daquele espaço (geográfico). Ao entrar na sala e sentar em uma das cadeiras disponíveis, o indivíduo está, na verdade, ocupando um espaço específico, e, para tanto, ele precisou projetar poder sobre esse objeto, necessitando até mesmo ocupá-lo. Nessa cena, podemos inferir o movimento que contém conceitos básicos dos estudos geopolíticos: primeiramente o *espaço geográfico*, que em seguida é transformado em *território*, eis que foi objeto de relação de *poder* em um determinado *tempo*. A intenção de mais um ator no sentido de ocupar o mesmo espaço (território) ao mesmo tempo, pode ocasionar conflito. Portanto, para fins didáticos, dentre outros, podemos usar essas ilustrações, metáforas ou casos para facilitarmos o entendimento dos conceitos-chave ligados à Geopolítica. Contudo, como delimitação mais precisa, há que se frisar que o nível de análise pretendido ou a escala geográfica trabalhada *a priori* pela Geopolítica deve considerar a relação de poder entre Estados, ou entre esses e outros atores no nível do sistema internacional.

Por meio não só de documentos oficiais, mas também de leitura de bibliografia especializada na área de relações internacionais, de política e economia internacional, e de geopolítica; de notícias a partir de mídias de diferentes matizes teóricas e ideológicas, da movimentação burocrática, interna e externa, de alguns atores do sistema interestatal, inclusive do Brasil, e do método empírico, podemos verificar um profundo relacionamento entre a forma de se pensar a Geopolítica e a conotação que vem sendo dada à cibernética ou ao poder cibernético atualmente.

Assim, a cibernética é vista como um espaço em si mesmo, o ciberespaço, a partir das redes formadas e que interligam países e continentes. Esse mesmo espaço, apesar de ser usualmente definido como um espaço de uso comum e até mesmo livre, tal qual preconizado na declaração de independência do ciberespaço, de John Balow, ou um *global common* (POSEN, 2003), vem sofrendo pressão fruto da competição entre vários atores do sistema internacional, principalmente dos Estados. Em consequência, a disputa pelo domínio desse novo espaço aparenta ter relação e obedece às mesmas estratégias do domínio dos espaços tradicionalmente estudados pela Geografia, como a dimensão terrestre, a marítima e a aeroespacial. Por conseguinte, percebemos um movimento no sentido de territorialização desse "novo" espaço, pois sabemos que a partir do domínio do ciberespaço haverá uma maior probabilidade de se dominar ou de ampliar o domínio sobre as dimensões tradicionais, cada vez mais dependentes do conteúdo informacional e da forma reticular de gestão (SANTOS, 1996).

Esse movimento também permite a alguns atores a possibilidade de expandir suas capacidades econômicas, como a construção de redes de telecomunicações e de transporte, o que Gottmann (2012 [1975]) chamou de oportunidades econômicas[2]. Dessa forma, um movimento político parece estar completamente imbricado às possibilidades de ganhos econômicos e de reprodução do capital, com a transformação do espaço cibernético em mais um território, *locus* de confronto de "poderes", no "jogo das trocas" (BRAUDEL, 1987) e no "jogo das guerras" (FIORI, 2004), ao serem associados às necessidades de domínio de recursos e de busca por segurança.

Por fim, associamos esse fenômeno recente, que tem como objeto a cibernética, ao fenômeno da territorialização-desterritorialização-(re)territorialização (T-D-R) apontado por Raffestin (1993). Para esse autor, alguns instrumentos à disposição do poder, como agora ao que tudo indica parece incluir os instrumentos ligados à cibernética, permitem a prática desse

[2] No sentido de ampliação das possibilidades advindas de instrumentos econômicos para fins de aumento da capacidade de poder, BlackWill e Harris (2016) também trazem essa concepção, dentro de um enfoque que insere na geoeconomia um ingrediente estratégico.

jogo, onde se territorializa uma determinada área, ao mesmo tempo em que se tenta desterritorializar outras, a fim de se (re)territorializar sob seus objetivos e interesses, o que apresenta grande semelhança com o movimento de expansão do poder e suas consequências nas outras dimensões territoriais.

As ideias e discussões contidas nesse capítulo servirão de embasamento conceitual e teórico para a continuação do *constructo* da tese, partindo-se, assim, do geral para o particular, e do teórico para a aplicação prática, pois o entendimento desses conceitos e o como esses estão sendo empregados vêm refletindo na forma como está sendo implementado o setor estratégico da cibernética no Brasil e seus projetos derivados, foco principal desta tese.

No primeiro momento este capítulo traz a definição de cibernética, buscando-se em textos e significados pretéritos o entendimento do atual uso desse termo. Na sequência, antes de dividirmos a cibernética sob os dois enfoques anunciados, trazemos uma discussão acerca do conceito de território, na intenção de mostrar como ocorreu o movimento de territorialização das dimensões espaciais ao longo do tempo, e como essas dimensões foram expostas, primeiro, ao jogo de forças do poder, para depois serem delimitadas, via normatização. É nesse ponto que encontramos grandes semelhanças com os acontecimentos que circundam ou têm como temática a cibernética e seu espaço hoje. Por fim, expomos o que entendemos por ciberespaço e como enxergamos a cibernética como mais um recurso de poder, inclusive com suas aplicações na e para a guerra.

1.1 DEFININDO CIBERNÉTICA

1.1.1 Cibernética: origens do termo

A palavra *cibernética*, em sua origem grega, significava a arte de pilotar uma embarcação. Platão relacionou o termo à arte de governar (MOREIRA, 1980). O significado moderno da palavra, entretanto, relaciona-se ao uso do termo *governator* (do inglês) em Mecânica. Em 1790, James Watt usou a expressão para designar um mecanismo que estabilizasse a velocidade de rotação do motor a vapor. Em 1868, o físico escocês James Clerk Maxwell descreveu certo tipo de mecanismo de controle no ensaio *The Theory of Governors*.

Foi nesse ensaio de Maxwell que o professor de matemática do Instituto de Tecnologia de Massachusetts (M.I.T), Norbert Wiener, diz ter-se inspirado para, em 1948, escrever a obra

Cybernetics, or Control and Communcation in the Animal and the Machine.[3] Contudo, admitiu Norbert Wiener que, mais tarde, casualmente, descobriu que esta palavra já tinha sido empregada, nos primórdios do século XIX, tanto por Ampère, no contexto da ciência política, quanto por um cientista polonês (WIENER, 1973). Em 1950, Wiener publicou "*Cibernética e Sociedade*: O uso humano de seres humanos", cujo texto revisado pelo autor, em 1954, foi traduzido para o português e publicado em 1973. Por meio desta obra, o matemático do M.I.T. tornou acessível a um público maior os conceitos fundamentais acerca da *cibernética* e algumas de suas implicações.

Ao contrário do que se poderia imaginar, as aplicações dessa ciência, assim considerada por Wiener, vão desde o campo da Filosofia, inserindo-se na Sociologia e na Psicologia, e alcançando o da Tecnologia (Engenharia). A obra de Wiener acerca da *cibernética* vai muito além de questões ligadas a mecanismos e a autômatos. Pela *cibernética*, disse esse autor, o homem seria capaz de compreender o que acontece com qualquer organismo, por meio da análise de seu sistema de funcionamento, principalmente no que concerne à informação e à reação do sistema a esta. Tanto o organismo dos seres humanos, por meio dos sentidos, quanto na estrutura de uma máquina (por sensores artificiais), o papel que a informação exerce é a chave de seu entendimento e de sua prospecção. O professor Wiener transporta, inclusive, a *cibernética* para a condução do corpo social, tanto por meio das leis, que para o autor exercem papel de emissoras de informações – mensagens do que fazer e não fazer – que formatam o comportamento da sociedade, como por meio do papel da comunicação, que para ele "cimenta a estrutura da sociedade" e, ao mesmo tempo, expande cultura (WIENER, 1973, p. 27). Assim chegou a afirmar esse matemático: "A minha tese é a de que o funcionamento físico do indivíduo vivo e o de algumas máquinas de comunicação mais recentes são exatamente paralelos no esfôrço [sic] análogo de dominar a entropia através da realimentação." (WIENER, 1973, p. 26). [4]

O ponto da questão para Wiener são as ramificações possíveis da *Teoria das Mensagens*, cujo conteúdo consiste na *informação.* O interesse do matemático por esse tema tem origem em um projeto de pesquisa iniciado nos primeiros anos da década de 1940, quando, como parte do esforço de guerra norte-americano, ele recebeu a incumbência de desenvolver um "sistema de

[3] Cremos interessante destacar que o geógrafo Milton Santos também conhecia esse termo, seu significado atual e o pensamento de Norbert Wiener. Ao apresentar discussão sobre a era da informação e do surgimento de uma "era das telecomunicações", Santos disse que "esta teria começado nos Estados Unidos no século XIX, mas seu desenvolvimento teve de esperar pelo advento das tecnologias do microprocessamento, isto é, pelo amadurecimento da **ciência cibernética**, como em 1940 chamou Wiener a essa nova disciplina, incubida do estudo da 'comunicação e controle no animal e na máquina'." (SANTOS, 1996, p. 147, **grifo nosso**)

[4] A entropia, para esse autor, fisicamente tratando, significa uma medida de desordem.

controle de baterias antiaéreas que fosse capaz de acompanhar a trajetória em que se movia um avião, predizer sua posição futura e disparar fogo levando em conta, senão só os hiatos humanos do canhão e do avião envolvidos." (MOREIRA, 1980, p. 32). O próprio N. Wiener explicou que, por meio desse poder de comando e controle, as máquinas atuais seriam capazes de interagir com o ambiente externo por meio de sensores.

Desta forma, de um sistema fechado, comum nas máquinas pretéritas, as máquinas modernas se caracterizariam por um sistema aberto[5], pelo qual a troca de informações/mensagem serviria como fenômeno de realimentação *(feedback)* constante, como ocorre em um monitoramento e uma reflexiva ação. Os exemplos, aponta o matemático do M.I.T., podem ser encontrados nos mísseis controlados, na espoleta de proximidade, no abridor automático de portas, no elevador, dentre outros. Tudo isso se torna possível, uma vez que essas "novas" máquinas possuem partes responsáveis pelo sensoriamento, verdadeiros órgãos sensoriais. São esses órgãos que permitem à máquina receber mensagem do exterior, como uma espécie de receptores e atualizadores de informação, a fim de evitar a entropia. Daí também advém a conhecida nomenclatura utilizada pela teoria do sistema, como o *input* (entrada) e o *output* (saída), além do *feedback*.

Segundo o próprio Wiener, a *cibernética* envolveria "o estudo do que em contexto humano é às vezes descrito genericamente como o ato de pensar e o que em engenharia é conhecido como controle e comunicação" (MOREIRA, 1980, p. 33). Em suma, pretendia-se estudar, compreender e dominar uma *trilogia*: *transmissão, entendimento* (processamento), e respectiva *obediência* (retorno/resultado), cujo objeto interior é a *mensagem* e, por conseguinte, a *informação* nesta contida. Desta forma, Norbert Wiener configuraria uma teoria sobre a comunicação e o controle. Para ele, o propósito da *cibernética* seria o de desenvolver uma linguagem e técnicas que fossem capazes, de fato, de habilitar os homens no tratamento dos problemas relacionados ao controle e à comunicação em geral (WIENER, 1973).

Assim, os primeiros projetos em que o termo *cibernética* foi utilizado com esse significado tratavam do desenvolvimento de mecanismos destinados a regular automaticamente determinados artefatos industriais e bélicos, capazes de substituir o homem na tarefa de corrigir desvios dos sistemas projetados por dispositivos reguladores programados especificamente para esta finalidade (WIENER *apud* EPSTEIN, 1986). De forma geral, *cibernética*, no século XX,

[5] *Sistema fechado*: aquele que não sofre influência do ambiente no qual está inserido. Por isso, basicamente, seu funcionamento depende de si mesmo. É, por si, um sistema isolado. Por sua vez, *sistema aberto* caracteriza-se por estar exposto a interações com o ambiente onde está inserido. Desta forma, essa interação gera realimentações que podem ser positivas ou negativas. Neste caso, há maior chance de entropia.

passou a sugerir o estudo das funções humanas de controle e dos sistemas mecânicos e eletrônicos que se destinam a substituí-las (THEOPHILO, 2011). É também essa ideia registrada na *American Society for Cybernetics*: “o termo foi criado em 1948 pelo matemático Norbert Wiener para abranger todo o campo da teoria do controle e comunicação, seja na máquina ou no animal.” (AMERICAN SOCIETY FOR CIBERNETICS FOUNDATIONS, 2008). O sentido atual, que é também o utilizado neste trabalho e que justifica a elaboração e implementação de uma política de Defesa específica para esse setor, versa, de maneira geral, sobre o controle e a comunicação por meio de uma máquina processadora de mensagem: o computador.

1.1.2 Cibernética: definição e emprego atual

Com o advento das redes de computadores, especialmente a *internet*, a conotação da *cibernética* se aproximou cada vez mais da ideia de *infovias* (sistemas de informação interligados). Nesse sentido, o controle dos sistemas de comunicação passou a dominar a “agenda cibernética”. Temas como Segurança, Defesa e Guerra Cibernética passam a fazer parte do dia a dia, indo justamente ao encontro da tese de Alvim e Heidi Toflller de que a forma do homem combater está, em muito, atrelada à forma como ele produz e a como são tratados os meios de produção (TOFFLER, 1995). É nesse sentido que acompanhamos cerca de três décadas a desmassificação da produção, o incremento na velocidade das inovações, a maior necessidade da integração dos sistemas e de sua infraestrutura, a diminuição do tamanho dos componentes eletroeletrônicos, simultaneamente ao aumento da precisão, e o deslocamento do trabalho calcado na força bruta para o que demanda profunda qualificação técnica; é também nesse sentido que observamos mudanças na forma de se combater.

Em abril de 2007, foram divulgados ataques maciços do tipo “ataque a redes de computadores”, a instituições públicas e privadas da Estônia; em agosto de 2008, ocorreram ações cibernéticas em setores estratégicos da Geórgia; em 2010, foram noticiadas ações nos complexos industriais da China, da Indonésia e do Irã – incluindo neste seu setor nuclear –, e, também, tornou-se público o caso *WikiLeaks*, que divulgou cerca de 250.000 mensagens confidenciais envolvendo o governo dos Estados Unidos da América. Em 2011, empresas brasileiras, como a Petrobras, e até a Administração Pública Federal (APF), pelo *website* da Presidência da República, sofreram alguma forma de tentativa de “intrusão cibernética”, com ou sem êxito. Em 2013, pelo caso Snowden, a utilização da cibernética como recurso de poder foi exposta ao público, demonstrando a participação direta de agências governamentais na

manipulação desse meio como forma de monitorar ou de projetar poder, alcançando a meticulosidade de se espionar computadores específicos, dependendo do cargo ou função de seu usuário.

Da mesma forma que pode ser usada na relação entre Estados, em tom alarmante um artigo publicado na Revista Info Exame sugeriu que qualquer computador pessoal pode estar sendo utilizado por *hackers* em ações criminosas. Esse texto apresentou uma tabela contendo a cotação de trabalhos no mercado negro das fraudes: com aproximadamente US$ 1 podemos adquirir dados pessoais roubados para abrirmos uma conta bancária; com o valor de US$ 150 compramos o envio de *spams* para 1 milhão de *e-mails*; e que com um pouco mais de investimento, aproximadamente US$ 300, podemos infectar uma centena de máquinas (MACHADO; MONTEIRO, 2011). Em episódio bem recente, em maio de 2017, algumas máquinas de mais de 74 países, inseridas aí as máquinas de empresas e de órgãos públicos, foram infectadas pelo vírus *wannacry*, uma espécie de ataque em que um banco de dados alvo é "sequestrado", via criptografia, e é cobrado resgate para sua "devolução". Tecnicamente, esse vírus é do tipo *ransomware*. Ver Quadro 1.1:

Quadro 1.1 – Tipos de ataques cibernéticos do tipo sabotagem

TÉCNICA(S)	TÁTICA(S)	EXEMPLO(S)
Vírus, *Worm* (armas inequivocamente ofensivas)	Contaminação de arquivos executáveis	Stuxnet (2010)
DoS, DDoS	Ataques de *Denial of Service* simples ou distribuídos	Spamhaus vs CyberBunker, 300Gbps (2013)
Invasão	Invasão de máquina e execução de código não autorizado	Anonymous vs Coreia do Norte (2013)
SQL Injection	Alteração de comandos de acesso a bancos de dados	hospital israelense em SP (2011)
Ataque a Redes de Computadores (ARC)	prejudicar, negar, degradar ou destruir redes de computadores, as informações nelas contidas ou os sistemas por elas controlados	Estônia (2007), Geórgia (2008) e Irã (2010)

Fonte: adaptado de Lopes e Gama Neto (2014, p. 37).

Como resposta, vários atores do sistema internacional vêm organizando seus respectivos sistemas de Segurança e de Defesa nessa área, como é o caso dos EUA; da UE, por cada um de seus membros e por meio da OTAN; da Rússia; da China; de Taiwan, da Coreia do Norte e do Irã, alguns, inclusive, constituindo uma nova Força Armada, além das três convencionais –

Exército, Marinha e Aeronáutica –, como apontou, em 2011, o general de divisão do Exército Brasileiro José Carlos dos Santos, então comandante do Centro de Defesa Cibernética do Exército, em entrevista à Revista Época (SANTOS, 2011).

Nessa linha, Richard Clarke e Robert Knake (2010), no que seguiu o pesquisador francês sobre segurança da informação Daniel Ventre (2012), informam que a China anunciou, ainda em 2003, a criação de unidades de guerra cibernética alojadas na base naval da Ilha de Hainan, sul da Província de Cantão. Os autores também relatam que os chineses treinam o emprego de "armas" técnicas nesse setor para dez objetivos possíveis: 1) plantar minas de informação; 2) realizar reconhecimento de informações; 3) alterar dados da rede; 4) liberar bombas de informações; 5) difundir lixo de informações; 6) difundir propaganda; 7) liberar informações enganosas; 8) liberar informações de clones; 9) organizar defesa de informações; 10) estabelecer estações de espionagem de rede.

Também quanto à China, com relação às ações de ciberespionagem, o presidente dos Estados Unidos, Barack Obama, discursando para o Congresso em 12 de fevereiro de 2013, anunciou a preocupação que vem tendo, a fim de evitar os ciberataques: "Sabemos que empresas e países estrangeiros furtam nossos segredos industriais. Agora, nossos inimigos estão tentando se capacitar para sabotar nossa rede de energia elétrica, instituições financeiras e controle de tráfego aéreo" (CIO, 2013)[6]. Todavia, por outro lado, os mesmos Estados Unidos, em ação conjunta com Israel, foram acusados de sabotarem o sistema referente ao enriquecimento de urânio do Irã, em 2010, o que veio a ser comprovado em 2012.

Os Organismos Internacionais (OI) também vêm demonstrando grande interesse na exploração e na segurança ligadas à cibernética. No final de 2011, a ONU, por meio da União Internacional da Telecomunicação (UIT), realizou um exercício de simulação contra ataques cibernéticos, contando com a participação de países do sudeste asiático, entre esses o Laos, o Camboja e o Vietnã. Para o responsável pela condução da simulação, Hamadoun Touré, Secretário Geral da UIT: "Ataques cibernéticos não têm fronteiras, por isso é vital cada país compartilhar informações e experiências." (TOURÉ, 2011).

Por essa declaração, dois pilares básicos para o ente estatal e seu sistema são postos em questão: primeiro, a alegação sobre a inexistência de fronteiras nesse espaço, consoante H. Touré; depois, a abordagem sobre a necessidade do compartilhamento de informação, esta como um dos principais recursos do poder estatal (GIDDENS, 2001). Nesses termos, assim também

[6] Disponível em: https://cio.com.br/nova-politica-de-ciberseguranca-para-os-eua-pode-gerar-padroes-seguidos-por-todos/. Acesso em: 20 mai. 2018.

lembra Ron Deibert: “Informação (seu sigilo), disse o Cardeal Richilieu, em 1641, é o assunto mais fundamental do Estado” (DEIBERT, 2012, p. 18, tradução nossa).

Para ilustrar o enorme potencial que traz essa nova dimensão, tem-se o caso ocorrido na Geórgia, em agosto de 2008, no qual, pela primeira vez, uma operação de Ataque Contra Redes de Computadores (ARC) de grande escala foi executada em conjunto com importantes operações de combate terrestres. Apesar de o ataque cibernético não ter sido admitido pelo governo russo, este foi o maior beneficiário, pois conseguiu “isolar e silenciar” os georgianos, produzindo efeitos psicológicos e de informações, reduzindo a capacidade de comunicar-se com o mundo externo, não apenas pela mídia e pelo governo, mas também pela população local. Para Paul Shakarian, professor assistente no Departamento de Engenharia Elétrica e Ciência da Computação da Academia Militar dos EUA (USMA), “independentemente do Kremlin estar ou não envolvido nos ataques cibernéticos […] talvez devamos passar a considerar as capacidades cibernéticas como um sistema operacional do campo de batalha, assim como o são a manobra, a artilharia, a defesa antiaérea, etc.” (SHAKARIAN, 2011, p. 72).

Do ponto de vista militar, ameaças cibernéticas se relacionam a um grande espectro de temas, que envolvem desde tópicos de guerra eletrônica até segurança de sistemas de informação, conforme inferimos do Quadro 1.2, a seguir.

Quadro 1.2 - Temas Relacionados à Cibernética

GUERRA ELETRÔNICA – Conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas.
GUERRA CENTRADA EM REDES – Guerra que reúne em rede os mais diversos elementos das forças armadas de um país, permitindo-lhe administrar diversas tarefas que vão desde a coleta até a distribuição de informações críticas entre esses muitos elementos. Outorga-lhe maior capacidade de combate ao ligar em rede os elementos de sensoriamento, de combate e de comando. Visa obter melhor sincronismo entre aqueles elementos e os efeitos que podem proporcionar, assim como o incremento na velocidade das operações bélicas e do processo decisório de comando.
GUERRA DE INFORMAÇÃO – Conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos.

Fonte: BRASIL (2015).

O envolvimento militar, tanto defensivo quanto ofensivo, em uma guerra cibernética, sugere **d**etecção (sensoriamento, monitoramento), **p**rocessamento e **a**tuação (D-P-A) (AMARANTE, 2010). Nesse aspecto, o circuito D-P-A apontado por José Amarante (2010) corresponderia à ideia de Guerra Centrada em Redes (*Network Centric Warfare*), que, para Libicki (1995 *apud* FONTENELLE, 2008, p. 16; SILVEIRA, 2011, p. 33), busca a *consciência situacional*, isto é, o fato de que "a otimização do fluxo informacional numa rede de computadores e comunicações provê informações mais consistentes para tomadas de decisão mais adequadas e oportunas." (FONTENELLE, 2008, p. 16).

Faz-se ainda necessário diferenciar o campo eletromagnético (telecomunicações e ondas *hertz*), das redes de computadores e do controle da informação (sistema de informação), que, consoante Pierre Lévy, compõem o ciberespaço:

> Eu defino o ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. Essa definição inclui o conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de redes *hertzianas* e telefônicas clássicas), na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização. (LÉVY, 1999, pp. 94-95)

Ainda para Pierre Lévy, a palavra "ciberespaço" foi inventada por William Gibson, em 1984, no romance de ficção científica *Neuromancer*. Nesse sentido, Ron Deibert denomina o canadense William Gibson como o "pai" do ciberespaço (DEIBERT, 2012). Para W. Gibson, o ciberespaço designa o universo das redes digitais, descrito como campo de batalha entre empresas multinacionais, palco de conflitos mundiais e nova fronteira econômica e cultural. Esse espaço criado por Gibson torna sensível a geografia móvel da informação, normalmente invisível, pois, pela sua criação, alguns heróis tornam-se capazes de entrar "fisicamente" nesse espaço de dados e lá viverem todos os tipos de aventura.

Dessa forma, *cibernética* envolve muito mais temas que o simples controle de sistemas computacionais de informação via *internet*, como sugere o senso comum. Oliveira prefere não definir o termo, por considerar um tanto quanto prematura a apresentação de conceito, sobretudo de uma área extremamente dinâmica, apenas falando em entendimento acerca de um "ambiente ou espaço cibernético, que contém a interação de pessoas, empresas e instituições públicas e privadas, nacionais e internacionais, utilizando modernos recursos de Tecnologia da Informação e das Comunicações (TIC)." (OLIVEIRA, 2011, p. 108).

Nessa linha segue também Raphael Mandarino Jr., que optou por não conceituar *cibernética*, mas sim o seu espaço, o ciberespaço, como "conjunto de pessoas, das empresas,

dos equipamentos e suas interconexões, dos sistemas de informação e das informações que por eles trafegam [...].” (MANDARINO JÚNIOR, 2011, p. 43).

As iniciativas estratégicas do Departamento de Defesa norte-americano reforçam o entendimento acerca do ciberespaço e suas possibilidades de uso para fins militares considerando, logo em primeiro plano, tratar esse espaço como mais um domínio operacional, tornando-se mister prever e prover organização, treinamento e equipamentos que permitam tirar proveito potencial nesse (e desse) ambiente (REVERON, 2012).

1.1.3 Cibernética: restringindo o termo

No VI Congresso de Relações Internacionais da *Universidad Nacional de La Plata*, em novembro de 2012, os pesquisadores Sergio Eissa, Sol Gostaldi, Iván Poczynok e Maria Di Tullio, da *Universidad de Buenos Aires*, também demonstraram preocupação em diferenciar os termos ligados à *cibernética*. Em seu artigo, esses pesquisadores expõem a confusão geralmente feita sobre os termos *operações cibernéticas* e *ataques cibernéticos*; *ciberguerra* e *guerra de informação*.

Tal perturbação incide, segundo esses autores, sobretudo na forma como serão definidas as responsabilidades e a tomada de decisões, mais precisamente com a preocupação em separar questões voltadas para a Segurança (*Seguridad Interior*) das questões que envolvem diretamente o instrumento militar (*Defensa Nacional*). Apesar disso, em um ponto os pesquisadores da *Universidad de Buenos Aires* concordam: o núcleo do ciberespaço se constitui da produção e da transferência de informação (EISSA *et al.*, 2012, pp. 2-3).

Mais adiante, neste mesmo artigo, Sergio Eissa define *operações cibernéticas* como aquelas “ações contra um computador, ou através de um computador ou um sistema de computador, utilizando fluxo de dados” (EISSA *et. al.*, p. 8, tradução nosssa), assumindo como cerne da questão, além da informação, o uso de computador e assim vinculando-se à ideia de rede. Esse teor também pode ser encontrado na publicação do Conselho de Pesquisa Nacional dos EUA *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities on Offensive Information Warfare*: “[…] ciberataque refere-se a deliberar ações para alterar, interromper, enganar, degradar ou destruir sistemas de computador ou redes ou programa de informação residente ou em trânsito nesses sistemas ou redes.” (*apud* SALES, 2010).

Em todos esses estudos há um elemento em comum: a *informação*, o seu uso ou negação de uso. Dessa forma, diante dos objetivos do trabalho, estabelecemos um recorte na abrangência

que o termo sugere, levando em consideração os aspectos que dizem respeito à comunicação e ao controle de sistemas de informação pautados em rede de computadores. Essa é a definição adotada pelo Exército Brasileiro (EB), por meio da utilização da sigla *C⁴I*, que engloba Comando, Controle, Comunicações, Computação e Inteligência[7]. Segundo Paulo Carvalho, oficial general do Exército Brasileiro (EB), oriundo da Arma de Comunicações, *cibernética* é um

> termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC), bem como os sistemas de armas e vigilância. (CARVALHO, 2011, p. 17)

Para o general de divisão João Roberto de Oliveira (2011), dentro desse entendimento é que, utilizando-se dos recursos de tecnologia da informação e comunicações (TIC), as Forças Armadas devem buscar o aperfeiçoamento de sua capacidade de *C⁴I* , de modo a atenderem o imperativo de atuação em rede, como preconiza a Estratégia Nacional de Defesa (END), de 2008, de 2012 e a de 2016.

Abordando especificamente a segurança nessa dimensão espacial, isto é, a segurança no espaço cibernético, o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação, do Departamento de Segurança da Informação e Comunicação, do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR), traz que S*egurança Cibernética* é a "arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2010).

Desse modo, de timoneiro ou de governo, pelo sentido empregado na Grécia Antiga, passando pelo estudo que visava à substituição das funções humanas de controle por sistemas mecânicos e eletrônicos, a *cibernética* alcança, hoje, uma conotação que compreende as ideias mestras de informação e de comunicação, daí o termo *infovias* utilizado para representar os meios pelos quais as informações digitalizadas circulam. A segurança dessas *infovias* – estas constituídas por ferramentas de TIC – passa a ser mais uma meta perseguida pelo Estado, mas não só por esse, a fim de garantir o fluxo de suas mensagens e de impedir ou negar acesso ao conteúdo que por essas vias transitam: a informação digitalizada.

---

[7] Internacionalmente emprega-se, hoje, a sigla C4ISR (Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento). Na Argentina, C4IVR (EISSAR et. al., 2012, p. 9).

Apesar dessa estrutura física ou dos meios de comunicação serem, por muitos, considerados *global commons*, sobretudo a mais conhecida – a *internet* –, a informação que trafega nesse espaço não o é. Talvez por isso Ron Deibert, Diretor do Centro de Estudos de Segurança Global, da *Munk School of Global Affairs*, da Universidade de Toronto, em documento publicado pelo *Canadian Defence & Foreign Affairs Institute* afirme que o

> Ciberespaço se tornou um objeto de intensa contestação, não só entre os diferentes sistemas de governo, mas entre uma multidão do setor privado e da sociedade civil, vez que todos usam e dependem desse domínio, e tem interesse em moldar a sua vantagem estratégica. (DEIBERT, 2012, *Executive Summary*, tradução nossa)

Segundo Deibert, o modo como solucionar ou evitar conflito nesse novo espaço depende em grande parte do regime de governo de cada país. Para ele, Rússia, China e outros países em ascensão defendem um maior controle desse espaço por parte do ente estatal[8], enquanto os países democrático-liberais, como os Estados Unidos e seus aliados, entre esses o Canadá, são favoráveis a manterem o ciberespaço como um "espaço de uso comum" (DEIBERT, 2012, p. 21).

Deibert conclui seu raciocínio dizendo que o momento em que vivemos é bastante decisivo com relação ao ciberespaço (DEIBERT, 2012, p. 23) e que a visão mais territorializante desse espaço vem atraindo e formando uma rede com vários atores, inclusive dentro dos organismos internacionais. O Canadá, segundo ele, é favorável à garantia do ciberespaço como um *global common*, defendendo sim uma normatização, mas não o cerceamento dos serviços possibilitados por esse meio.

Nessa visada, notamos que há traços que coincidem bastante com as discussões acerca de princípios ligados a teorias das relações internacionais: de um lado, a visão realista da anarquia do sistema e de sua condução inexorável ao dilema de segurança, sendo o poder mensurado principalmente em termos de capacidades militares; do outro, os liberais, idealistas ou neoliberais, que veem a discussão sob o enfoque da interdependência, da pluralidade de atores internacionais e do papel das organizações/instituições no regramento de comportamento do sistema, procurando, dentre outros, no Direito Internacional a fonte de solução de conflitos.

Porém, ao que tudo indica, os mais aptos hoje na utilização desse espaço como recurso não pretendem ceder a uma regulamentação mais profunda, ou até mesmo à sua delimitação, sobretudo no tocante ao uso para a guerra. Permanecendo formalmente como *global common*,

[8] Mais à frente nesse trabalho, chamamos esse movimento de "*territorialização*" do ciberespaço.

o espaço cibernético, para uns, já significa, materialmente, um espaço territorializado, apesar de considerado "ilimitado" ou "incontrolável". Cabe frisar que, em não poucas ocasiões, o discurso é um e as práticas são outras, sobretudo quando se detém o controle (domínio) sobre grande parte da infraestrutura cibernética do globo, como é o caso dos Estados Unidos, diretamente por órgãos do Estado, ou por meio de grandes empresas.[9]

1.2 TERRITÓRIO: PARA ALÉM DE ESPAÇO COMUM, UM ESPAÇO DE PODER

O conceito de território é muito caro aos geógrafos, mas não só a esses. Ora visto em sua forma tradicional – o espaço físico geográfico –, que contempla, hoje, as dimensões marítima e aérea, além da terrestre, ora sob uma ótica que privilegia uma ampliação, na qual se inserem "territórios", econômicos e virtuais, por exemplo, o certo é que o debruçar sobre esse conceito inspira, ainda que não de forma explícita, muitas das estratégias de poder inseridas no sistema interestatal.

Do primeiro ponto de vista, o conceito de território serviria apenas para enquadrar o espaço geográfico que fosse sentido e exercido pelo homem, isto é, objeto de estudo que pudesse ser visto, tateado e organizado, por exemplo. Sob a segunda ótica, o estudo acerca do conceito de território – ou sobre "territórios" – incluiria muito mais variáveis que, embora em um primeiro momento não fossem contempladas em um espaço físico perceptível, trazem certamente reflexos para este e para o homem. Neste aspecto ganha importância a associação entre os conceitos de território, poder e jurisdição.

Na tentativa de seguir pistas que levaram a essa discussão e à investigação da evolução do conceito de território, Jean Gottmann (2012 [1975]) trouxe contribuições bastante instigantes. A percepção desse autor, à época que escreveu "*The evolution of the concept of territory*", era de que o conceito *território* não se enquadrava mais apenas na relação com o espaço terrestre. Abrangia muito mais espaços, derivados da competição por mais poder, segurança (abrigo) e recursos (oportunidades econômicas), como foi o caso do domínio humano sobre os espaços marítimo e aéreo. Além disso, para Gottmann, território era muito mais do que geografia ou espaço geográfico. Representava uma categoria de estudo na qual convergiam, também, tempo, poder e riqueza, todas consideradas por um planejamento central, atendendo às estratégias de um Estado nacional.

[9] A cibernética sob o enfoque de teorias das Relações Internacionais é tratada no próximo capítulo, assim como a distribuição pelo globo das redes de fibra ótica e de outros meios pelos quais a informação digitalizada navega.

Foi com a sedentarização do homem que podemos apontar o início da tradição da ideia de *território*. Foi por buscar espaços geográficos para seus assentamentos que comunidades politicamente organizadas iniciaram, também, uma espécie de "sedentarização do poder". (FIORI, 2004). Nesse aspecto, a identidade entre território e abrigo, e território e oportunidades econômicas (GOTTMANN, 2012 [1975]) tornou-se algo intrínseco ao movimento humano no planeta.

Fruto desse movimento derivou-se a pressão competitiva por "territórios", e, consequentemente, uma corrida por melhor abrigo e por maior capacidade de recursos. Vários podem ser os recortes históricos e geográficos que traduzem esse movimento; contudo temos como base o sistema interestatal pós-*Westphália* e como referencial o conceito de Gottmann acerca do território:

> Território é uma porção do espaço geográfico que coincide com a extensão espacial da jurisdição de um governo. [...] é um conceito político e geográfico, porque o espaço geográfico é tanto compartimentado quanto organizado através de processos políticos. Uma teoria que ignora as características e a diferenciação do espaço geográfico opera no vácuo. [...]. (GOTTMANN, 2012 [1975], pp. 523; 526).

Dessa forma, inseridos no conceito de território estão dois outros: o de espaço geográfico e o de poder. É por meio deste poder, na sua forma política ou jurisdicional, como afirma Gotmann, que o espaço geográfico é definido, delimitado, demarcado e organizado, surgindo, assim, no sistema interestatal, a importância das fronteiras, para as várias dimensões territoriais. Pois é, em um primeiro momento, dentro dessas fronteiras, que o ente político organizado busca ampliar sua capacidade de abrigo, de obtenção de recursos e, consequentemente, de segurança e bem-estar para sua população.

Todavia, o próprio Gottmann já assinalara para outras possibilidades que não apenas um "isolacionismo platônico", como é o caso da opção pelo modelo de "cosmopolitismo alexandrino", com uma nova roupagem, pela qual, no uso de "territórios", o corpo político dependeria de "expansão que não envolve necessariamente alargamento territorial, mas pressupõe confiar política e economicamente numa vasta rede de relações externas." (2012 [1975], p. 532) [10]. Essa expansão seria, para Gottmann, propiciada pela tecnologia de transporte

[10] Nesta passagem, além dos escritos contidos nas páginas 532-535, Gottmann (2012 [1975]) transpareceu um pensamento bem similar ao de William Petty (1690) ao questionar, estrategicamente, como um Estado de pequena superfície territorial e pouca população poderia manter-se como bom abrigo e com muitas oportunidades econômicas frente a outros maiores. A ideia de poder relacional também é inferida. Uma das alternativas, assim, era de expandir-se para além do território físico. Ir para outra dimensão espacial – a marítima, à época – ou usar

e de comunicações. Nesse ponto, este autor abre discussão, embora não citando, para várias abordagens sobre o conceito de território, incluindo o de "territórios econômicos", de Hilferding (1985 [1910]), e seu respectivo capital financeiro. Mais que isso, outros mecanismos de enquadramento podem ser utilizados para este fim de apropriação do espaço, como foi – e é – a tributação direta, a moeda e a dívida pública. Indo além, Gottmann cita Raymond Vernon e a possibilidade do uso da "grande corporação multinacional" para este intento (VERNON, 1971 *apud* GOTTMANN, 1975, p. 531) [11], no que seguiu Dreifuss (1997) e Harvey (2003).

Assim, como um dos elementos essenciais do Estado moderno, o território recebeu, ao longo da história, diversas conotações. Sob a ótica *westfhaliana*, o território possuía o significado do local (espaço físico) em que o Estado exercia sua jurisdição, sua autoridade política. O território era um objeto que fazia parte das relações de poder, dentro e para fora de um ente soberano, e que possuía, como um dos princípios, a impenetrabilidade, isto é, a exclusividade em seu uso, um monopólio de ocupação, tornando-se impossível duas ou mais soberanias, no mesmo espaço e ao mesmo tempo, conviverem. Apreendemos, pois, que o *território*, visto nessa perspectiva, apresenta dois significados jurídicos: um negativo, pois exclui outras soberanias, e outro positivo, "enquanto assegura ao Estado a possibilidade de agir soberanamente no seu campo de ação." (DALLARI, 1995, pp. 76-77).

Hans Kelsen, jurista austríaco tido como principal nome da positivação do Direito, apesar de considerar a delimitação territorial uma necessidade do Estado moderno, face à noção de exclusividade, é um dos poucos que não vincula o território ao Estado, como um componente meramente físico. Acredita Kelsen que o território é um espaço ao qual se circunscreve a validade da ordem jurídica estatal, mas que essa ordem, isto é, a eficácia das normas face ao interesse do Estado, pode ir além desses limites, uma espécie de "território-competência", na apreensão feita por Paulo Bonavides, em detrimento da concepção de patrimônio ou de mero espaço substrato físico.

Para Bonavides (1967 *apud* DALLARI, 1995), assim podem ser entendidas essas concepções:

---

de outros artifícios econômicos, para fins de obtenção de riqueza ou como mais um instrumento de coerção, por exemplo.

[11] Sobre os trabalhos de Raymond Vernon (1966 e 1971), citados por Jean Gottman (1975), tomamos ciência deste na disciplina de Economia Política Internacional I, conduzida pelo professor Maurício Metri, no Pepi, em 2016, ao mesmo tempo em que fomos convidados para lecionar na Associação Educacional Dom Bosco, em Resende-RJ, a disciplina de Gestão de Negócios Internacionais para a turma do 4º Ano de Administração. As referências desta área do conhecimento, quando abordam o comércio internacional, também tratam da teoria do ciclo de vida dos produtos e registram a capacidade de explicação que esta possui, no que diz respeito à inovação, ao monopólio temporário e à padronização do produto de forma sistêmica, e os ganhos daí advindos, para a empresa e para o país a quem esta responde. Nesse momento tivemos mais certeza do quadro teórico e da realidade para conduzir esta pesquisa, a fim de melhor interpretar o objeto ora em estudo.

a) *território-patrimônio*: uma característica do Estado Medieval, que não diferenciava o *imperium* do *dominium,* concebendo o poder do Estado sobre o território exatamente como o direito de qualquer proprietário sobre um imóvel;
b) *território-espaço*: considerava o território a extensão espacial da soberania do Estado e o incluía como parte da personalidade jurídica do Estado;
c) *território-competência*: teoria defendida por Hans Kelsen, que considera território o âmbito de validade da ordem jurídica do Estado (BONAVIDES, 1967 *apud* DALLARI, 1995). Estas duas últimas ideias são interessantes por permitirem a projeção do conceito de território e o entendimento acerca do princípio da extraterritorialidade, que adiante, quando do estudo acerca da tentativa de controle e de normatização do espaço cibernético, e de configuração e delimitação de uma fronteira, será abordado e empregado.

Dessa forma, território não é sinônimo de espaço, é algo mais elaborado, uma construção a partir do espaço. Para Hasbaert, "o território é o produto de uma relação desigual de forças, envolvendo o domínio ou o controle político-econômico do espaço e sua apropriação simbólica, ora conjugados e mutuamente reforçados, ora desconectados e contraditoriamente articulados." (HASBAERT, 2002, p. 121). Para Claude Raffestin,

> É essencial compreender bem que o espaço é anterior ao território. O território se forma a partir do espaço, é o resultado de uma ação conduzida por um ator sintagmático (ator que realiza um programa) em qualquer nível. Ao se apropriar de um espaço, concreta ou abstratamente (por exemplo, pela representação), o ator "territorializa" o espaço. Lefebvre mostra muito bem como é o mecanismo para passar do espaço ao território: "A produção de um espaço, o território nacional, espaço físico, balizado, modificado, transformado pelas redes, circuitos e fluxos que aí se instalam: rodovias, canais, estradas de ferro, circuitos comerciais e bancários, auto-estradas e rotas aéreas etc.". O território, nessa perspectiva, é um espaço onde se projetou um trabalho, seja energia e informação, e que, por consequência, revela relações marcadas pelo poder. O espaço *é* a "prisão original", o território é a prisão que os homens constroem para si. (RAFFESTIN, 1993, p. 143)

Foi por isso que Robert Sack afirmou ser a territorialidade humana uma estratégia geográfica poderosa. É por meio do processo de *territorialização* que o homem busca se relacionar com o espaço geográfico, tentando afetá-lo, influenciá-lo e controlá-lo (SACK, 1986 *apud* BECKER, 2009, p. 156).

Yves Lacoste (1989 [1976]), em sua obra "*A geografia serve, antes de mais nada, para fazer a guerra*", propôs uma ruptura na maneira tradicional de se pensar o espaço, corroborando a importância de maior valorização do estudo desse conceito, pois, para ele, além de uma ideia

superficial do título de seu livro, a função básica e mais antiga dos estudos a respeito de conceitos geográficos – dentre esses o de território – foi a de elaboração de estratégias militares. Assim afirma J. W. Vesentini, ao apresentar as ideias desse geógrafo francês:

> […] isto – a geografia – serve em primeiro lugar (embora não apenas) para fazer a guerra, ou seja, para fins político-militares sobre (e com) o espaço geográfico, para produzir/reproduzir esse espaço com vistas (e a partir) das lutas de classes, especialmente como exercício do poder. O fundamental, a seu ver, é que, malgrado as aparências mistificadoras, os conhecimentos geográficos sempre foram, e continuam sendo, um saber estratégico, um instrumento de poder intimamente ligado a práticas estatais e militares. (VESENTINI, 1989, p. 7)

É esse conhecimento geográfico sobre o espaço um objeto-chave, de significado capital não só para estados-maiores de exércitos, como também para outros aparelhos do Estado e até mesmo para as grandes empresas privadas. Para Lacoste, é preciso saber pensar o espaço para nele agir de forma mais eficiente. Nisso consiste sua estratégia espacial.

Apesar da função espacial, hoje, não corresponder apenas àquela voltada para os estados-maiores, estrategistas – que enxergam o conflito militar como pano de fundo constante, cujas importâncias a serem realçadas são: o controle de determinados territórios ou de sua expansão, a forma de fortalecimento do Estado e o meio de alcançar a hegemonia –, não deixa de ser esta uma das funções, talvez a principal, apesar do conjunto de atores que participa da cena internacional e das faces de como se apresenta o poder. A busca por espaços e por recursos, mesmo em um ambiente tão difuso, parece ser uma constante. É nesse sentido que lembra Lacoste:

> A Geografia, enquanto descrição metodológica dos espaços, tanto sob os aspectos que se convencionou chamar "físicos", como sob suas características econômicas, sociais, demográficas, políticas (para nos referirmos a um certo corte do saber), deve absolutamente ser recolocada, como prática e como poder, no quadro das funções que exerce o aparelho de Estado, para o controle e a organização dos homens que povoam seu território e para a guerra. (LACOSTE, 1989 [1976], p. 10)

É, portanto, dessa forma, que o saber sobre o espaço e a respectiva forma de apropriação desse elemento se amplia, alcançando suas variadas dimensões.

1.2.1 Espaço, território e limites nas diferentes dimensões

Como consequência de *Westphalia* (1648), e do reconhecimento recíproco de não interferência nos assuntos internos do Estado, houve a necessidade de se delimitar bem

nitidamente até aonde se aplicaria esse reconhecimento, isto é, até aonde "posso", ou "não posso" (alteridade), aplicar o poder, legal e legitimamente, o que coincide com a área ou poder de jurisdição. Nesse sentido, a fronteira, primeiramente a de natureza terrestre, funcionando como a linha epiderme do Estado territorial soberano, não mais poderia prescindir de uma teorização. A fronteira territorial passou a simbolizar o limite de uma soberania: seu início e fim. Passou a ser, por conseguinte, uma porção geopoliticamente sensível do Estado. Sua concepção e desenvolvimento não ocorreram (nem ocorrem) à toa. Segundo Meira Mattos, abordando a origem da Teoria das Fronteiras:

> Cada Estado-Nação cultiva o sentimento de soberania. A posse do território nacional, sua defesa, passa a ser dever sagrado do cidadão. A delimitação dos direitos territoriais torna-se imperativa. A fronteira adquire importância excepcional – é o limite da soberania nacional. (MATTOS, 1990, p. 15)

Disse Meira Mattos (1990) que os povos primitivos não tinham necessidade de estabelecer essa denominada limitação. Isso ocorria tendo em vista a ínfima e esparsa população que habitava o planeta, não havendo "pressões" no espaço natural. Eram povos nômades ou em vias de sedentarização e que a produção se dava em uma propriedade coletiva. Continua Mattos informando que, durante o mundo antigo, das conquistas marítimas que envolviam os sumérios, cartagineses, venezianos, sicilianos e romanos, o sentimento de posse/domínio do espaço era representado pela conquista de cidades e portos, visando às questões de logística e à submissão de governos locais. Dessa forma, não havia necessidade de fixação de uma linha, nem da faixa de fronteira. Nem no período feudal, em que houve uma extrema subdivisão do poder político, consubstanciado nos principados, grão-ducados, ducados, condados e feudos, a fronteira despertou atenção, nem foi necessária sua delimitação. Nesse tempo, o castelo e as grossas muralhas que o envolviam, além dos profundos fossos, é que simbolizavam o local a ser defendido pelo senhor e sua força militar.

Contudo, essa realidade foi alterada principalmente neste hemisfério, ocupado pela civilização ocidental. Na Europa, com o surgimento das monarquias absolutistas e com o acréscimo populacional, o que acarretou centralização política e pressão por espaço (*territorialização*), devido à contiguidade, a tendência passou a ser o estabelecimento de uma linha fronteiriça que obedecesse às etapas de *definição*, de *delimitação* e, por fim, de *demarcação*. Essas fases de ocupação e a necessidade de delimitação foram representadas por Mattos (1990), que denominou a forma dessa delimitação para cada um desses estágios como fronteira-zona; fronteira-faixa e fronteira-linha, na medida em que o processo de pressão territorial foi ampliado e os recursos tecnológicos e coercitivos permitiram (Quadro 1.3).

Quadro 1.3: Evolução das Fronteiras

FASES/ESTÁGIOS		DESCRIÇÃO
1º	Vazios de ecúmene	- característico do mundo antigo, pouco povoado, quando os núcleos geohistóricos eram separados por enormes vazios demográficos.
2º	As largas zonas inocupadas ou fracamente ocupadas	- estas zonas não abrigavam nenhum poder político capaz de perturbar os interesses dos núcleos geohistóricos de que eram separadores.
3º	Faixas relativamente estreitas, chamadas *fronteiras-faixa*	- nas áreas em que o povoamento dos países limítrofes não chega a pressionar um sobre o outro.
4º	*Fronteira-linha*, estabelecida sob vários critérios (natural, artificial, astronômica, étnica)	- nas áreas em que a densidade populacional colocou em contato permanente o *interesse* das partes.

Fonte: elaborado pelo autor, a partir de MATTOS (1990, p. 17).

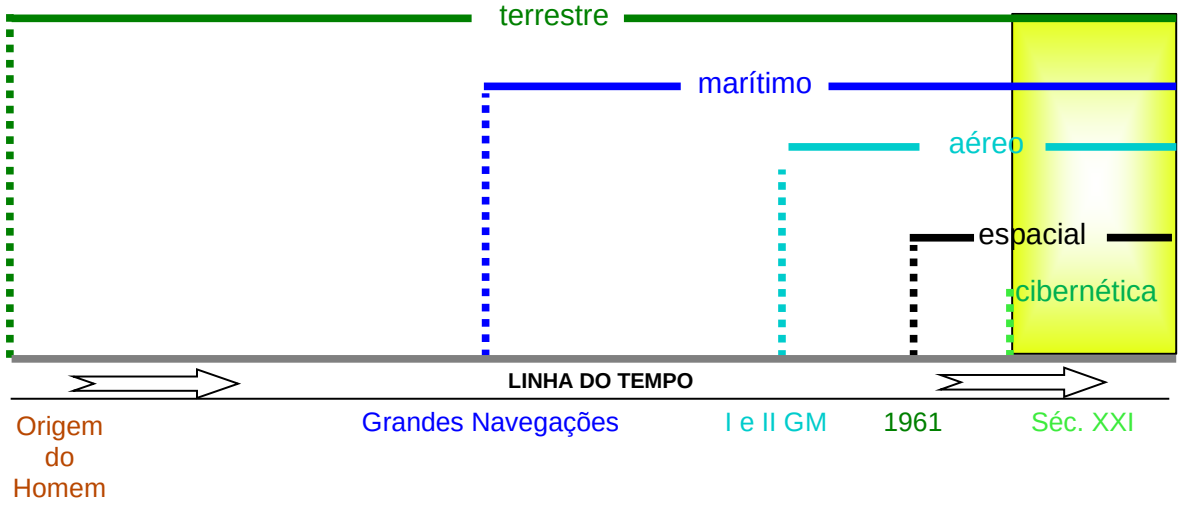
Essas transformações no formato da delimitação, em resposta às pressões competitivas por território, dizem respeito não apenas à fronteira do espaço terrestre. Junto, e em resposta a essa pressão, e até mesmo às guerras de eliminação (ELIAS, 1994 [1939]; FIORI, 2004), outros domínios espaciais foram objeto do poder. É dessa forma que podemos falar no empoderamento das dimensões marítima, aérea, extra-atmosférica e, mais recentemente, da dimensão cibernética – isto é, em suas transformações de espaços comuns (*global commons*), ou "espaços internacionais", em dimensões territoriais.

Enquanto as três primeiras dimensões são "nítidas", pelo menos possíveis de serem sensoreadas e monitoradas, e, atualmente, passíveis de plena utilização pelo homem, as duas últimas apresentam algumas restrições. Nesse sentido é que entendemos o território "antes relações sociais projetadas no espaço que espaços concretos" (SOUZA, 2003, p. 87).

De certo é que todas essas dimensões territoriais coexistem[12] (Figura 1.1), apenas variando no tempo o seu momento de descoberta pelo homem e sua conseguinte utilização, que sempre se vinculou às capacidades tecnológicas de cada época.

[12] E coexistem ou foram objeto de utilização não em um sentido linear ou de um "evolucionismo". A Figura 1.1 busca ilustrar apenas alguns dos marcos temporais acerca de conflitos ou de tentativas de normatização das dimensões espaciais, na medida em que se aumentava a pressão competitiva pelo espaço e suas várias dimensões.

Figura 1.1: Espaço Geográfico e Tempo Histórico – interação homem-natureza



Fonte: Ferreira Neto (2013, p. 42).

Para o Estado, ente que possui a prerrogativa de controle sobre seu espaço e o poder de planejamento das mais variadas formas de articulação – o que Bertha Becker chama de gestão territorial ou prática estratégica (BECKER, 2009, p. 156) – essa apreensão se torna essencial. Contar apenas com o que possa ser visto ou tateado é excluir muitas outras ações e funções do espaço. E essa simplificação para apenas o que é perceptível pode alcançar um insucesso. Sobre esse aspecto, Claude Raffestin chama atenção:

> O "estrategista" não vê o terreno; mais ainda, só deve vê-lo conceitualizado, senão não agiria. É à distância que sua ação é possível e, desde então, essa distância é a única a criar o espaço: O espaço estratégico não é uma realidade empírica. É, de fato, criado pelo conceito de ação, que pode ser a guerra, mas que também pode ser qualquer tipo de organização, de distribuição, de malha ou de corte. O estrategista não vê o terreno, mas a sua representação. (RAFFESTIN, 1993, p. 25)

Também nesse sentido trabalhou Clausewitz com o conceito de estratégia, discordando de Dietrich von Bülow, a quem acusava de intensas tentativas de matematizar o campo de batalha, sem levar em consideração outros fatores que, embora não quantificáveis empiricamente e até mesmo de natureza imponderável, existiam de fato e serviam como recurso de poder na ocasião do conflito (PARET, 2001).

Para além da sua forma tradicional, a terrestre, o território cada vez mais veio sendo associado à ideia de jurisdição. Assim, mesmo enquanto não ocupado ou habitado pelo homem, fruto de relações políticas, o território pode ser objeto de apropriação de recursos e, por conseguinte, de aumento de probabilidade de segurança. Esse é um movimento mútuo e

recíproco. De forma breve, atendendo aos objetivos desta pesquisa e à abertura do debate feito por Gottmann (1975) acerca da ampliação do conceito de território, abordamos a seguir as construções territoriais e seus limites nas outras dimensões que não a terrestre, criando suporte para a discussão sobre o mais novo desafio: o território cibernético e o poder advindo deste.

1.2.1.1 O Território Marítimo e sua Fronteira

No tocante à definição da fronteira marítima, foi a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), assinada no dia 10 de dezembro de 1982, em *Montego Bay* (Jamaica), e em vigor, internacionalmente, desde 16 de novembro de 1994, que trouxe o grande embasamento jurídico, estabelecendo os limites políticos dos Estados costeiros e, assim, minimizando a possibilidade de conflitos. Para o Estado nacional, os conceitos mais importantes criados pela CNUDM, com relação à delimitação da jurisdição nessa porção geográfica, foram os de *Mar Territorial*, *Zona Contígua*, *Zona Econômica Exclusiva* e *Plataforma Continental* (inclusive sua versão estendida) (Figura 1.2). Destacamos, brevemente, tais definições:

- *Mar Territorial* – segundo J. F. Rezek (2005, p. 307) "é a extensão da soberania do Estado costeiro além de seu território e de suas águas interiores" (arts. 2º e 3º da CNUDM). Essa ideia de soberania do Estado costeiro está intrinsecamente ligada ao imperativo de defesa do território ou, conforme Dallari (1995), aos motivos de segurança. Para se ter uma noção acerca de sua importância, ao romper do século XVIII adotava-se três milhas náuticas marítimas como Mar Territorial. Isso se justificava pelo alcance máximo da artilharia naval e costeira à época[13]. Era a utilização da consagrada fórmula "*Terra potestas finitur ubi armorum vis*"[14], primeiro critério fixado ainda no séc. XVII. Essa fixação perdurou até o século XX, quando por volta da II Guerra Mundial alguns Estados estenderam – sempre mediante atos unilaterais – a largura dessa área (4, 6, 9 e mesmo 12 milhas náuticas). A partir de 1952, diversos países da América Latina – a começar pelo Chile, Equador e Peru – decidiram estender esse limite até as duzentas milhas,

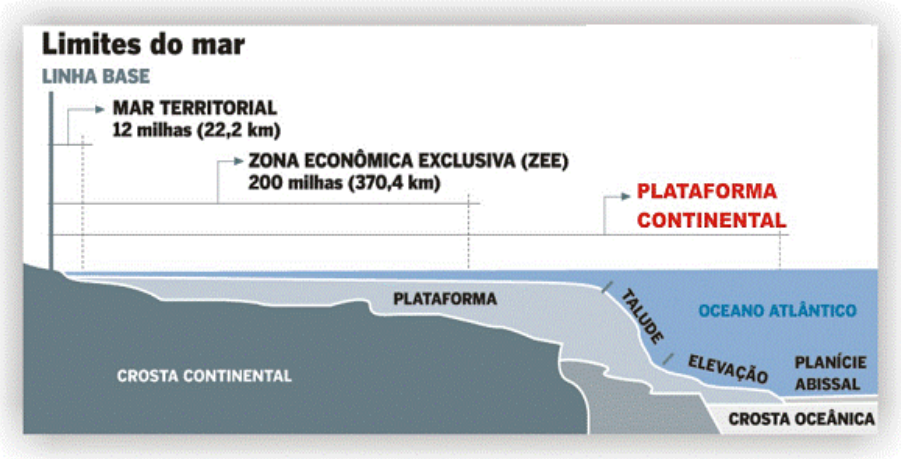
[13] Este registro é bem interessante, na medida em que se observa que o primeiro elemento capaz de fundar uma noção de alcance ou de delimitação territorial é o poder, no caso o poder bélico. Esse ponto também se torna interessante, uma vez que é mencionado por Gottmann (1975), quando da discussão sobre a delimitação do espaço aéreo e sua transformação em território estatal: "A definição e o conceito em si obviamente estiveram se alternando no espaço e no tempo, com as ferramentas tecnológicas à disposição da sociedade organizada. [...] Quando aviões U2 começaram a voar e a era dos mísseis balísticos intercontinentais despontou, eles questionaram a validez da estabelecida doutrina de soberania sobre a coluna do espaço estendida ao infinito, acima do território em terra firme. [...] A definição de 'controle' permaneceu vaga; ***deve ter sido aceita como a função da potencialidade de cada Poder destruir objetos que penetrarem no seu espaço aéreo*** [...]." (2012 [1975], p. 525).

[14] "O poder da terra acaba onde acaba a força das armas."

correspondendo a 370 quilômetros, aproximadamente. Os Estados Unidos não ficaram para trás: logo após a II GM reivindicaram o limite de 200 milhas para o mar territorial, "tendo em vista a necessidade de proteger o seu território contra armas de longo alcance" (MATTOS, 1990, p. 70). Hoje, a CNUDM estabelece 12 milhas, a partir da linha de base[15] litorânea;

- *Zona Contígua* – é uma área reservada às medidas de fiscalização, no que diz respeito à alfândega, à imigração, à saúde e, ainda, à disciplina regulamentar dos portos e do trânsito pelas águas territoriais. Essa Zona não poderá ir além das 24 milhas marítimas, contadas da mesma linha de base do Mar Territorial (art. 33 da CNUDM);

Figura 1.2: Corte Transversal e Vista do Mar Territorial, ZEE e Plataforma Continental



Fonte: Marinha do Brasil.

- *Zona Econômica Exclusiva* – é "uma faixa adjacente ao Mar Territorial e cuja largura máxima é de 188 milhas náuticas contadas a partir do limite exterior daquele, com o que perfazem 200 milhas, a partir da linha de base" (REZEK, 2005, p. 303). A utilização econômica da dimensão marítima, além das razões de segurança e defesa, passou a ocasionar uma série de conflitos, exigindo, por conseguinte, uma regulação. O art. 56, da CNUDM, expõe os direitos concernentes ao Estado costeiro: exploração e aproveitamento, conservação e gestão dos recursos naturais, vivos ou não vivos, das águas sobrejacentes ao leito do mar e seu subsolo. Também autoriza a investigação científica marinha e a produção de energia, a partir da água, das correntes e dos ventos, e atribui como um dever a proteção e a preservação do meio marinho;

[15] Linha de base: corresponde à linha intermediária entre a maré baixa (baixamar) e a maré alta (preamar) que alcança a costa.

- *Plataforma Continental e sua versão estendida* – já prevendo o aumento da capacidade de utilização como oportunidade econômica desse ambiente, por meio, sobretudo, do uso de tecnologia, a CNUDM trouxe mais essa definição. Consoante seu art. 76, a plataforma continental compreende o leito e o subsolo das áreas submarinas que se estendem além do seu mar territorial, em toda a extensão do prolongamento natural do seu território terrestre, até ao bordo exterior da margem continental, ou até uma distância de 200 milhas marítimas das linhas de base a partir das quais se mede a largura do mar territorial, nos casos em que a margem exterior não atinja essa distância. Em uma leitura mais detalhada, esse mesmo artigo traz, em seus §§ 4º e 6º, algumas exceções, possibilitando o prolongamento dessa extensão. Observa a Convenção de *Montego Bay* que o limite exterior da plataforma continental coincidirá com o limite da ZEE (200 milhas náuticas, a partir da linha de base do litoral), a menos que o bordo exterior da margem continental – isto é, o limiar da área dos fundos marinhos – esteja ainda mais distante: neste caso, o bordo será o limite da plataforma, desde que não ultrapasse a extensão total de 350 milhas náuticas [16].

1.2.1.2 O Território Aéreo e seus Limites

Com relação ao espaço aéreo, o desenvolvimento da aviação, a partir da I GM, fez com que houvesse a necessidade de uma normatização sobre esse domínio e acerca da navegação nesse espaço. Meira Mattos disse que a primeira ideia dos especialistas com relação à delimitação de uma fronteira aérea foi de aproximação ao que tinha sido feito com relação à marítima, comparando a massa atmosférica aos oceanos (MATTOS, 1990). Era premissa defender não só os territórios terrestre e marítimo; a soberania, isto é, o poder jurisdicional também nesse novo espaço deveria ser assegurado.

Podemos destacar, como primeira iniciativa quanto à regulamentação do uso desse domínio, a Convenção Internacional de Paris, em 1939, que transferiu para o ar o direito ao "uso inocente do espaço aéreo, obedecidas as restrições previstas pelas legislações de cada país" (MATTOS, 1990, p. 82). Contudo, é a Convenção de Chicago (Convenção da Aviação Civil Internacional), de 1944, que consiste na principal fonte de normatização do uso do espaço aéreo pelos Estados. Em seu preâmbulo, assim menciona essa Convenção:

> Considerando que o desenvolvimento futuro da aviação civil internacional pode contribuir poderosamente para criar e conservar a amizade e a

[16] Esse ponto muito interessa ao Brasil, devido à sua capacidade de exploração *offshore* em águas profundas.

> compreensão entre as nações e os povos do mundo, mas que seu abuso pode transformar-se em ameaça ou perigo para a segurança geral. (ONU, 1944)

Ao mesmo tempo em que indica as possibilidades de uso pelos povos e nações, e os benefícios oriundos daí[17], retrata a preocupação com a segurança no contexto internacional. Ao que nos parece, verdadeiramente, esse é o trajeto, por opção ou por necessidade, do uso e da ocupação das dimensões espaciais pelo homem: do uso pacífico, comum, acessível a todos, à possibilidade de controle e de conflito. Este último, no sistema *westphaliano*, recebe atenção especial pelos princípios internacionais que marcam o sistema *mundi* a partir de então, pois soberania e territorialidade passaram a ser os elementos norteadores que estabelecem reciprocamente a independência e a autonomia dos Estados, e alteram ou podem vir a alterar a sua capacidade de servir de abrigo (segurança) e de oportunidade econômica (recurso).

Também preocupada com isso, a Convenção de Chicago, logo em seus capítulos iniciais, fez questão de tratar de *soberania* e de *território*, apontando para esses dois pilares, tanto do Estado quanto do próprio sistema no qual este ator está inserido. Nessa visada, assim dizem os artigos I e II:

> Artigo I. Soberania. Os Estados contratantes reconhecem ter cada Estado a soberania exclusiva e absoluta sobre o espaço aéreo de seu território.
> Artigo II. Territórios. Para os fins da presente Convenção, considera-se como território de um Estado, a extensão terrestre e as águas territoriais adjacentes, sob a soberania, jurisdição, proteção ou mandato do citado Estado. (ONU, 1944)

A Convenção de Chicago também estabeleceu os procedimentos a serem adotados pela aviação civil e pela militar, esta última com bem mais restrições, algo bem semelhante ao uso do mar e o conceito e "passagem inocente". Dessa forma, por exemplo, aeronaves governamentais pertencentes a um dos Estados contratantes não poderão sobrevoar, nem aterrissar no território de outrem, sem autorização para tal feito. Há ainda a possibilidade de estabelecimento de "zonas proibidas", por razões militares ou de segurança pública (Artigo III). Cada Estado contratante pode limitar ou proibir que aeronaves de outros Estados sobrevoem certas zonas de seus territórios – terrestre ou marítimo.

[17] Interessante destacar a semelhança de como parte da teoria aborda, hoje, o ciberespaço, com o a visão idealista de Victor Hugo, ainda em 1864, escrita em uma correspondência para o balonista francês Félix Nadar, tratando da invenção do avião: "[...] a invenção do avião significaria o fim da guerra. Da ciência (aérea), sairia a paz, uma vez que o avião traria a imediata, absoluta, instantânea, universal e perpétua abolição das fronteiras." (ISAAC, 2001, p. 214).

1.2.1.3 Dos Limites do Espaço Extra-Atmosférico ou Cósmico

Em se tratando de espaço extra-atmosférico (ou cósmico)[18], ou seja, aquele localizado além do espaço aéreo, incluindo-se a lua e outros corpos celestes, e que, portanto, não consiste em território, ainda – embora territorializado[19] ou em processo de territorialização por alguns Estados[20] –, a Organização das Nações Unidas iniciou os trabalhos atinentes à regulamentação desse espaço ainda em 1957, mais precisamente em 11 de novembro, após o advento do primeiro satélite artificial *Sputnik*, colocado a bordo do foguete lançador R-7, chamado de *Semiorka*, que foi também o primeiro míssil balístico intercontinental (MONSERRAT FILHO, 2007).

As iniciativas de regulamentação partiram das duas então "superpotências", EUA e URSS, fruto de uma série de acordos bilaterais e da percepção de riscos de uma utilização militar desse então "recém-descoberto" espaço. Foi instaurado um comitê – Comitê para o Uso Pacífico do Espaço Extra-Atmosférico (COPUOS) – que produziu, ao final, uma declaração, em 13 de dezembro de 1963, por meio da Resolução 1962 (XVIII). Nesse documento, transformado, em 1966, no Tratado sobre Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Cósmico, inclusive a Lua e demais Corpos Celestes, foram formalmente elencados, além dos princípios, as competências, as responsabilidades e as finalidades com relação ao espaço cósmico. Esse tratado foi aprovado pela Assembleia Geral da ONU, em 19 dez. 1966, com entrada em vigor em 10 out. 1967.

Todavia, essa não foi a primeira, nem é a única, normatização internacional para esse ambiente. Outras iniciativas da ONU, mais específicas e que demonstram a continuidade do processo de regulamentação desse espaço (Quadro 1.4), derivadas inclusive do que propõe a sua própria Carta (art. 13), precisam ser destacadas:

[18] Em nossa pesquisa bibliográfica encontramos referências a esse espaço dessas duas maneiras (extra-atmosférico e cósmico), além das denominações "sideral" e "espaço exterior". No entanto, pelos textos das Resoluções da ONU, as duas primeiras são as mais precisas. Ver, ainda, quanto ao *espaço cósmico*, V. M. Rangel (2005, pp. 393) e em http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=118828. Com relação ao *extra-atmosférico*, Dinh; Daillier; Pellet (2003, pp. 1281).
[19] Estados Unidos, Rússia, China e União Europeia, por exemplo.
[20] Brasil, por exemplo.

Quadro 1.4: Histórico de Normatização do Espaço Cósmico pela ONU

1) Documento que estabelece um Comitê *ad hoc* sobre os usos pacíficos do espaço exterior [Resolução 1348 (XIII), de 1958];

2) Documento de criação do Comitê permanente para os usos pacíficos do espaço exterior [Resolução 1472 A (XIV), de 1959];

3) Enunciado que insiste junto aos Estados a se absterem de colocar em órbita quaisquer objetos portadores de armas nucleares ou de qualquer outro tipo de arma de destruição em massa e de instalar tais armas em corpos celestes [Resolução 1884 (XVIII), de 17 out. 1963];

4) Acordo de Salvamento dos Astronautas, o Retorno de Astronauta e a Restituição de Objetos Lançados no Espaço Extra-Atmosférico [Resolução 2345 (XXII), de 19 dez. 1967, em vigor em 22 abr. 1968];

5) Convenção sobre a Responsabilidade Internacional pelos Danos Causados por Objetos Espaciais [Resolução 2777 (XXVI), de 29 nov. 1971];

6) Convenção sobre Matrícula dos Objetos Lançados no Espaço Extra-Atmosférico [Resolução 3235 (XXIX), de 12. Nov. 1974], e

7) Acordo Regendo as Atividades dos Estados Sobre a Lua e Outros Corpos Celestes [Resolução 34/68, de 18 dez. 1979].

Fonte: elaborado a partir de documentos da ONU.

Voltando ao tratado aprovado em 1966 (em vigor a partir de 1967), este trouxe alguns princípios estampados, tais como o da *não-apropriação* e o da *liberdade*, o que diferencia, logo em um primeiro momento, esse espaço do domínio aéreo. A conclusão acima é retirada do artigo II desse tratado, que diz: "O espaço cósmico, inclusive a Lua e demais corpos celestes, não poderá ser objeto de apropriação nacional por proclamação de soberania, por uso ou ocupação, nem por qualquer outro meio." (ONU, 1966). Todavia, ainda que essa normatização tenha um enorme valor formal e funcional, a fim de se evitar o conflito, na medida em que as atividades espaciais ganharam maior intensidade e passaram a ser objeto de competição, houve a diversificação de sua utilização, tanto para fim civil, quanto militar, a partir dos satélites artificias e de outros engenhos que eram colocados em órbita. Dinh, Daillier e Pellet (2003) indicam algumas dessas utilizações:

> […] supervisão de territórios sobrevoados, localização de recursos naturais terrestres e marítimos (teledetecção), radiodifusão e teledifusão directas (*sic*), transmissões telefônicas, posicionamento dos navios, meteorologia, observações astronômicas, experiências científicas, projeto americano "guerra nas estrelas", etc. (DINH; DAILLIER; PELLET, 2003, p. 1283)

Dessa forma, ainda que o tratado indique a *não-apropriação* e a derivada *liberdade* de utilização, alguns Estados perceberam que certos tipos de exploração não estariam à disposição de todos. Primeiro, por ser difícil, na prática, diferenciar/delimitar o espaço aéreo e o extra-atmosférico, principalmente para Estados que não possuem recursos tecnológicos com essa capacidade de monitoramento. Segundo, porque alguns Estados também notaram que se encontravam em posição geográfica naturalmente beneficiada para a exploração e utilização desse espaço, como é o caso da vantagem da linha do Equador[21], no tocante à órbita geoestacionária (DINH; DAILLIER; PELLET, 2003, p. 1286).

A dimensão do espaço extra-atmosférico, pela tecnologia que demanda e pelos custos, ainda é um substrato pouco explorado, ficando seu uso mais restrito aos satélites daqueles atores que atingiram o sucesso nessa área. É exatamente esse o entendimento do general de divisão do Exército Brasileiro (EB) João Roberto de Oliveira, destacado abaixo, em resposta a uma de nossas questões sobre *Defesa*, *território* e *fronteiras* na dimensão *cibernética*:

> […] No campo militar e mesmo no político, considera-se que existem cinco dimensões no conflito moderno: o terrestre, o aéreo, o marítimo, o espacial e o cibernético. Para os três primeiros é possível estabelecer-se limites ou fronteiras físicas. Na dimensão espacial já há dificuldade de se estabelecer limites ou fronteiras, pois o espaço sideral não é regido, ainda, por regras de utilização bem delimitadas. Temos discussões em alguns órgãos internacionais sobre situações focais, como por exemplo, o uso do espaço para a localização de satélites geoestacionários e outros temas de interesse comum (por sinal, o Brasil está muito atrás nessa discussão, pois até agora o País não tem nenhum satélite próprio). (OLIVEIRA, 2012)

Procuramos destacar o depoimento desse oficial general por ter sido ele um dos responsáveis pelo planejamento e implementação do setor cibernético no Exército Brasileiro, e por ter realizado estudos acerca da implantação e do funcionamento do Sistema Integrado de Monitoramento de Fronteiras (SisFron). Adiante no trabalho esse se transformará em um dado importante, na medida em que corrobora nosso entendimento sobre os enfoques dados à *cibernética* pelo Estado brasileiro e por outros atores.

Com relação à dimensão cibernética, ponto onde queremos chegar nessa reflexão, cabe afirmar que esta está na pauta de discussões políticas e científicas há muito mais tempo. Na

[21] Por essa localização, em 3 de dezembro de 1976, por meio da Declaração de Bogotá, Brasil, Colômbia, Congo, Equador, Indonésia, Quênia, Uganda e o então Zaire proclamaram suas respectivas soberanias sobre essa área. Em seguida, aderiram Somália e Gabão. No entanto, por ter sido considerada contraditória frente aos princípios estatuídos no Tratado de 1966/1967, sobretudo o que considera o espaço cósmico um apanágio da humanidade, e o constante do artigo II, que impede a apropriação por meio de declaração de soberania, esta intenção foi rejeitada pelos demais membros da comunidade internacional. Ante a reação negativa, os países "equatorianos", em contrapartida, ficaram com alguns direitos preferenciais, em detrimento da soberania.

época do Projeto Guerra nas Estrelas, como ficou conhecida jornalisticamente a guerra espacial (MATTOS, 1986), componente da *Strategic Defense Initiative* (SDI) estadunidense, a utilização de processadores de informações em alta velocidade já era uma necessidade para o funcionamento correto daquele sistema. E mais: a garantia da continuidade do fluxo de informações e de seu processamento eram requisitos essenciais para o sucesso dessa defesa. Meira Mattos fez um relato a esse respeito:

> Todo esse sistema de armas será inútil sem a existência de subsistemas de comando e controle capazes de detectar, acompanhar, fazer pontaria e disparar as armas, bem como detectar quais os alvos destruídos a fim de concentrar a defesa nos restantes. Esse subsistema é de grande complexidade e deve ser protegido para que tudo possa funcionar. É preciso lembrar que o percurso completo de um míssil da União Soviética para os Estados Unidos dura, apenas, cerca de 25 minutos. (MATTOS, 1986, p. 56)

Para termos uma ideia da composição do sistema de armas referente à SDI, Meira Mattos classificou a variedade de tecnologias empregada em três grupos: um ligado ao mecanismo de destruição, correspondendo às armas em si (*laser*, canhões eletromagnéticos, p. ex.); outro voltado para a vigilância e o rastreamento, com um sistema desdobrado de emissores baseados em terra, ar e naves espaciais e de receptores, usando radares e meios óticos, e, por fim, um referente ao *comando e controle de comunicações e informações*, com a finalidade de operar um intenso fluxo de informações em tempo extremamente curto, envolvendo as operações de detecção, acompanhamento e destruição de mísseis balísticos e cabeças nucleares (MATTOS, 1986).

Ocorre que, diferentemente do espaço cósmico, que demanda ainda hoje gastos exorbitantes na construção de seus aparatos tecnológicos, o domínio cibernético contou com uma diminuição de custos e facilidade de obtenção em uma escala jamais vista (DIAS, 2003; NYE, 2012). Além disso, permitiu uma ampliação da interseção entre a informação e a sua forma de transporte, as comunicações.

1.3 CIBERNÉTICA COMO MAIS UMA DIMENSÃO ESPACIAL

O reconhecimento das bases territoriais, e dos direitos sobre essas, pelos integrantes do sistema torna a soberania estatal legal e legítima. Logo, na medida em que o espaço, em suas várias dimensões, torna-se objeto passível de utilização pelo homem, como fonte de recurso, por meio de inovações tecnológicas, a prática desse poder – o empoderamento, o domínio –

sobre esse espaço torna-se crucial. Se, primeiro, surgem os conflitos, às vezes alcançando o nível mais elevado da violência, em seguida, pelo fio condutor histórico, tem aparecido o Direito, a fim de manutenção do *status quo* ou como forma de tentativa de solução pacífica e de ordenamento racional, a fim de minimizar os impasses, que não deixam de ser constantes. Esse foi o ocorrido (e o que ainda ocorre) com as dimensões terrestre, marítima, aérea e extra-atmosférica.

Da mesma forma, embora já utilizado em um passado próximo, temos hoje um "novo" espaço, ou uma "nova" dimensão espacial, fruto também do aprimoramento técnico e lógico humano. É dessa maneira que o espaço cibernético emerge como objeto de discussão política, que já alcançou o extremo do uso da força, ora visto como *espaço em si mesmo*, ora como mais um *recurso do poder*. Os conflitos nesse novo domínio são, como mostramos a seguir, cada vez maiores, quantitativa e qualitativamente, à medida que o aparato estatal e outros atores descobrem suas novas possibilidades de uso. Edgar Moran assim concluiu sua colaboração para a 3ª edição do "*Strategy in the Contemporary World"*, após relacionar a Geografia com a Estratégia na construção de seus espaços de atuação: "*Conclusion*: *War by Other Means – Cyberspace*" (MORAN, 2010, p. 138).

Dessa maneira, o espaço cibernético há algum tempo deixou de ser um dos *global commons*, como denomina Barry Posen ao se referir aos "espaços internacionais de uso comum", ou aos "bens comuns globais" (POSEN, 2003, pp. 7-8), ou como argumentou o canadense Ron Deibert (2012), eis que nesse espaço já é exercido realmente um poder específico, inclusive de natureza militar:

> A força militar dos EUA possui atualmente o comando dos bens comuns globais. Comando dos bens comuns é análogo ao comando sobre o mar, ou nas palavras de Paul Kennedy, é análogo à 'naval *maestria'*. Os bens comuns, no caso do mar e do espaço (cósmico), são áreas que não pertencem a nenhum Estado. Até mesmo o acesso para grande porção do espaço aéreo global não pertence tecnicamente aos países abaixo dele, pois há poucos países que podem negar o seu espaço aéreo acima de 15.000 metros para aviões de guerra americanos. (POSEN, 2003, p. 8, tradução nossa)

Esmiuçando o sentido de comando concebido por Posen (2003), Kelly Ferreira concluiu que um país que possui o domínio sobre esses espaços "pode dificultar as operações e movimentações de Estados rivais, não bloqueando o uso, mas constrangendo os demais, de tal forma que seja necessário que o país que domina a região dê um consentimento tácito para ações na área" (FERREIRA, 2012, p. 70). Ainda reforçando a tese de Posen (2003), incluindo nesses o espaço cibernético, afirmou Alexandre Rodrigues que *global commons* são:

> espaços que não estão sob o controle direto de qualquer Estado, mas que são vitais para o acesso e ligação de quaisquer pontos do mundo. Incluem águas e o espaço aéreo internacionais, o espaço exterior e o ciberespaço. [...] Implicam uma nova e sobretudo mais alargada visão dos espaços de interesse, por forma a incluir (*sic*) as suas quatro dimensões, em vez das duas tradicionais. Aliás, o nosso atual grau de dependência em relação aos dois novos espaços (cibernético e espaço exterior) é hoje quase idêntico ao que se verifica em relação aos tradicionais (mar alto e espaço aéreo). O espaço cibernético é uma área crítica para a segurança dos Estados e para o funcionamento das economias. Amanhã, será, com grande probabilidade, também um espaço de projeção de poder. (RODRIGUES, 2012, p. 5)

Assim, o espaço cibernético, embora formalmente considerado um espaço comum internacional, na prática tem o seu uso e controle pelos mais aptos, o que termina proporcionando a esses poucos a possibilidade de *territorialização* desse "novo" espaço e, a partir deste – talvez aí o maior ganho –, uma *(re)territorialização* dos espaços tradicionais, que se encontram expostos ao que se convencionou chamar fenômeno da globalização, e que, por consequência, estariam passíveis de um processo de *(des)territorialização*. Essa é a sequência do fenômeno apontado por Raffestin (1993), por meio das siglas T–D–R.

Notamos que a *cibernética*, em si, pode ser vista para além de um espaço/território, configurando-se em outra função, a de recurso de poder, por meio, entre outros, das possibilidades proporcionadas pelas redes de comunicação e informação ligadas por processadores cada vez mais velozes, aprofundando a concepção de "território-rede". É dessa forma que também se refere o general norte-americano Robert Elder, ex-diretor do *Cyberspace Operations Task Force*: "Se você não dominar o ciberespaço, você não pode dominar os outros domínios." (CLARKE; KNAKE, 2010). Por conseguinte, sob comando dos Estados, o fenômeno da *territorialização* vem ocorrendo nesse espaço e deste se projetando aos demais domínios, ocasionando uma *(re)territorialização*. É dessa forma que os Estados acenam com uma reação, face às descobertas das inúmeras possibilidades desse novo ambiente, o que nos remete à constatação de Marcos Saquet:

> O fato é que território e rede se condicionam reciprocamente. [...] As redes de circulação e comunicação são meios na articulação interna do território e, ao mesmo tempo, são território e interligam-no a outros territórios, tornando o território 'inicial/local' um nó ou um território articulado a outros territórios, econômica, política e culturalmente. (SAQUET, 2007, p. 72)

Por isso, a partir da busca de um maior monitoramento dentro do próprio ciberespaço, será lhe proporcionado um maior controle, este no significado que lhe atribui Rodrigues:

> Controlar, nesse contexto, significa conseguir utilizar esses espaços em maior extensão do que qualquer outro país; ter meios para impedir que outros tenham sucesso em qualquer tentativa de negar o seu uso; e, finalmente, ter capacidade de interditar a sua utilização a terceiros. (RODRIGUES, 2012, p. 6)

Assim, o ente estatal encontra nas redes de informações digitalizadas (*infovias*) a projeção do poder sobre as demais dimensões espaciais. Os Estados, nesse novo cenário, respondem às alterações provocadas por essa nova variável, preparando-se para essa nova dimensão de disputa de poder. O território do Estado, que tem como epiderme suas fronteiras, deixa de ser visto apenas sob as naturezas terrestre, marítima, aérea e extra-atmosférica. Passa a ser constituído por mais esse ambiente particular, o cibernético, com características bem peculiares e diferentes das outras dimensões, como a interação com os diversos domínios; a velocidade de ações e de mudanças; a transcendência de fronteiras físicas, organizacionais, institucionais e geopolíticas; a anonimidade e a possível diminuição da assimetria. Neste contexto, lembram Clarke e Knake (2010), que o maior segredo, atualmente, sobre guerra cibernética é que nem mesmo os Estados Unidos, que se preparam há bastante tempo e com todos os recursos disponíveis, não conseguem, efetivamente, se defender de um ataque cibernético.

1.3.1 O Ciberespaço e seu Uso pelo – e para – o Poder

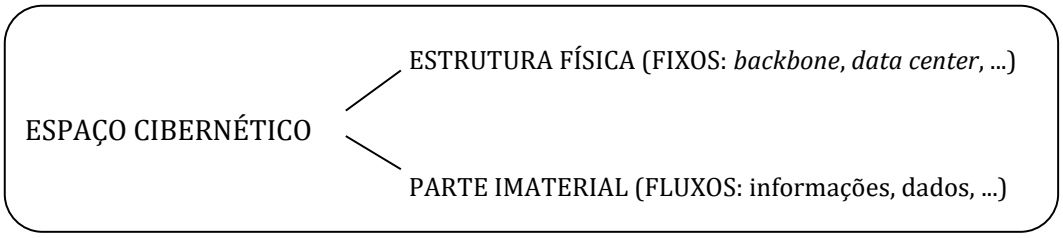
Para continuarmos nosso *constructo*, é de suma importância entendermos de forma mais detalhada o que significa, realmente, o ciberespaço.

Como vimos, para Pierre Lévy o ciberespaço corresponde a um espaço de comunicação aberto pela interconexão de computadores e das memórias dos computadores, incluindo os sistemas de comunicação tanto por meio de ondas *hertz* quanto pela telefonia clássica, a partir do momento em que essas participam do processo de transmissão de informações digitalizadas (LÉVY, 1999). Para Raphael Mandarino, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e para o General João Roberto de Oliveira, o espaço cibernético compreende também as pessoas, as empresas e os equipamentos que porventura estejam interconectados, participando, de alguma maneira, do tráfego de informações digitalizadas (Figura 1.3).

Clarke e Knake debruçaram-se sobre esse tema em um dos capítulos do "*Cyber War: The Next Threat to National Security and What to Do About It*". Iniciaram os autores investigando o que seria o ciberespaço e indicando, incialmente, que o termo mais parecia, em

um exercício de imaginação, outra dimensão, com iluminação verde e coluna de números e símbolos piscando no ar como no filme *The Matrix* (CLARKE; KNAKE, 2010). Mas, logo em seguida, atestaram que esse novo espaço é realmente bem mundano, no qual está inserido o *laptop* que nós conduzimos ou o que as crianças levam para a escola ou, ainda, um computador de nosso local de trabalho ou uma tubulação instalada sob uma rua. Para Clarke e Knake (2010), hoje o ciberespaço está em toda parte, em todo lugar em que encontramos um computador, ou um processador, ou um cabo de ligação. O ciberespaço, para esses autores, já é hoje uma zona de guerra.

Figura 1.3: Componentes do Espaço Cibernético



Fonte: Ferreira Neto (2013, p. 88).

Como conceito trazem esses norte-americanos que o ciberespaço corresponde a todas as redes de computadores, em todo o mundo, e tudo que conecte ou controle. Ciberespaço inclui outras redes de computadores além da *internet*, que, supostamente, não são acessíveis a partir desta (CLARKE; KNAKE, 2010).

Nesse sentido seguiu Derek Reveron, baseando-se na definição de ciberespaço do Departamento de Defesa dos EUA, e informando que esse espaço é "um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações, sistemas de computador e processadores embarcados, e controladores." (REVERON, 2012, tradução nossa). Prosseguiu esse autor, afirmando que o ciberespaço, assim como o ambiente físico, é muito abrangente, incluindo o *hardware*, como redes e máquinas; as *informações*, como dados e mídia; o *cognitivo*, como o processo mental das pessoas, e o *virtual*, onde as pessoas se conectam socialmente (REVERON, 2012).

Daniel Ventre, pesquisador do Centro de Investigações Científicas e secretário geral do Grupo Europeu de Pesquisa de Normas (GERN), ambos de Paris, elaborou uma proposta interessante quanto aos componentes do ciberespaço. Para Ventre, este espaço é composto por três "capas", assim denominada cada parte desse domínio. Colocando em um quadro, a proposta de Ventre fica assim ilustrada (Quadro 1.5):

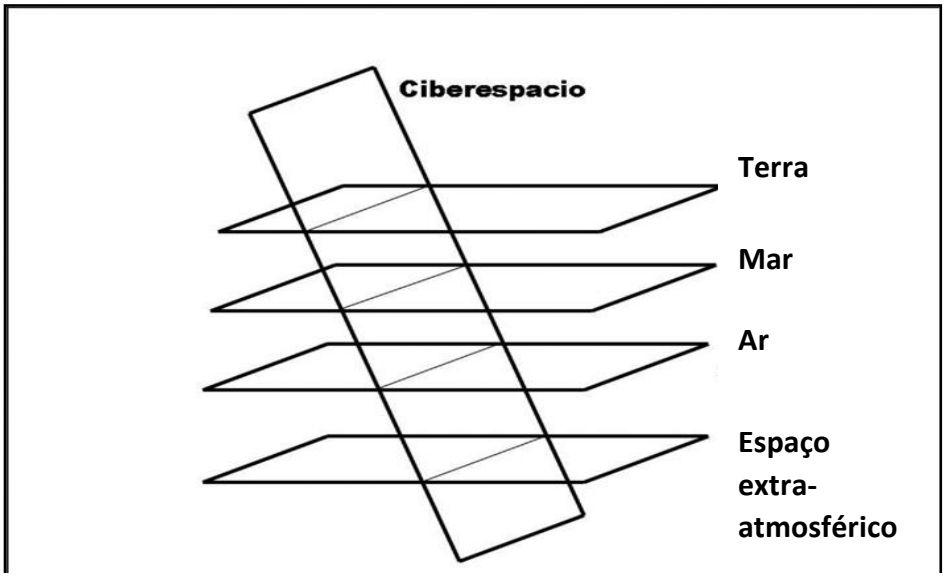
Quadro 1.5: Espaço Cibernético – "capas" e respectiva composição

"CAPA"	COMPONENTES
Inferior	- física, material, condizente à infraestrutura (*hardware*, redes, ...)
Intermediária	- *softwares* de aplicações
Superior	- cognitiva

Fonte: elaborado a partir de VENTRE (2012, p. 34).

A visão do pesquisador do GERN-Paris coaduna com a tríade formulada por especialistas das áreas de análise de sistemas e de informática, que entendem o *hardware* como a parte rígida ou os componentes do sistema; o *software* o que diz respeito à programação, e o *peopleware* referindo-se às pessoas que atuam nesse setor, por meio do conhecimento. Além disso, representando graficamente, Daniel Ventre expõe o domínio cibernético face às outras dimensões espaciais, conforme figura abaixo, afirmando que uma das características mais marcantes desse novo domínio é a sua transversalidade (VENTRE, 2012, p. 34) (Figura 1.4).

Figura 1.4: Ciberespaço e Relação com Outras Dimensões



Fonte: adaptado pelo autor a partir de Ventre (2012, p. 35).

Essa transversalidade se torna uma característica bem significativa do ciberespaço, uma vez que permite a projeção de poder e seus reflexos nos demais domínios espaciais ou, como tratamos até aqui, o fenômeno da *(re)territorialização*.

Ainda se atendo ao ciberespaço, sobretudo quanto às suas características e composição, Joseph Nye (2012) enxergou essa dimensão espacial dividida em duas partes principais: o "*intraespaço*" e o "*extraespaço*" cibernético.

Ao analisarmos essa forma de simplificação, chegamos à conclusão que muito condiz com a visão Chefe do Comando Cibernético dos Estados Unidos, General Keith Alexander, que vê o ciberespaço "sendo usado por militares no futuro (operando de dentro ou através dele) para atacar pessoal, instalações, ou equipamentos [...]." (REVERON, 2012, tradução nossa).

Dessa forma, ambos mencionam a possibilidade de operações ocorrerem *dentro* (no *intraespaço*) e *através* (no *extraespaço*) do ciberespaço. J. Nye chega a comparar o poder advindo da *cibernética* com o poder marítimo, que também se distingue em *poder naval sobre os oceanos* – o que, por sua teorização, corresponderia ao *intraespaço marítimo* –, do *poder naval sobre outros domínios*, isto é, o poder projetado do ambiente marítimo para outro domínio espacial, no caso o *extraespaço* cibernético.

Joseph Nye também aborda a utilização do poder nesse ambiente espacial com exemplificações de uso que podem ocorrer na forma branda (*softpower*) ou na forma dura (*hardpower*), tanto dentro (*intraespaço*), quanto fora (*extraespaço*) do espaço cibernético, conforme exposto no quadro abaixo (Quadro 1.6).

No "intraespaço" de Nye, na "capa" inferior e intermediária de Ventre, ou no que denominamos ao longo do trabalho *espaço cibernético considerado em si mesmo*, algumas ações são efetuadas a partir do, e com reflexos no, próprio espaço, como constam os exemplos dos ataques de negação de serviço (*Distributed Denial of Service – DDoS*[22]) do Quadro 1.6, ou do controle de companhias e empresas, no caso da estrutura física do ambiente cibernético, ambas caracterizando formas de utilização *hard* do poder.

Concomitantemente, a relação política e seus conflitos nesse espaço podem ocasionar reflexos externos, digamos no mundo sensorial humano, como no ataque ao sistema Scada [23], em 2010, nas usinas nucleares iranianas ou na possibilidade de rupturas de serviços essenciais à população, como no caso de danos às estruturas estratégicas de um Estado: energia elétrica, distribuição de água, serviço de telecomunicações, sistema financeiro, controle de tráfego aéreo, ferroviário, rodoviário, urbano etc.

[22] Ou *DoS Attack*, ocorre a partir da sobrecarga do sistema e não de uma invasão. Geralmente, um computador mestre comanda milhares de computadores denominados *zumbis*, que passam a funcionar como máquinas escravizadas. Rever Quadro 1.1.

[23] *Supervisory Control and Data Acquisition* – sistemas que utilizam *software* para monitorar e supervisionar as variáveis e os dispositivos de sistemas de controle conectados através de drivers específicos.

Quadro 1.6: Dimensões Informacional e Física do Poder Cibernético e Algumas Possibilidades

Alvos do poder cibernético		
	***Intraespaço* (cibernético)**	**(*Extraespaço*) cibernético**
Instrumentos de informação	**Duro**: ataques de negação de serviço. **Brando**: determinação de normas e padrões.	**Duro**: ataque em sistema SCADA. **Brando**: campanha de diplomacia pública para influenciar a opinião pública.
Instrumentos físicos	**Duro**: controle das companhias por parte do governo. **Brando**: *software* para ajudar ativistas dos direitos humanos.	**Duro**: roteadores de bomba ou corte de cabos. **Brando**: protestos para denunciar os provedores cibernéticos.

Fonte: elaborado e adaptado a partir de Nye (2012, p. 166).

Dessa forma, e por suas várias interpretações e possibilidades, o espaço cibernético, apesar de considerado virtual e um *global common*, há algum tempo o deixou de ser. Alguns atores empoderam-se desse espaço, delimitando-o unilateralmente, dispondo de seu controle. É nesse sentido que enxergamos o espaço cibernético não mais como um espaço comum, porém sim um território. Tentar entendê-lo e teorizá-lo, para saber "jogar", e defini-lo, delimitá-lo e demarcá-lo, com as respectivas responsabilidades advindas, é um bom começo.

1.3.2 O Território Cibernético e sua Fronteira

Compreensão exige teorização. Teoria exige abstração, que, por sua vez, exige simplificação e ordenamento da realidade (HUNTINGTON, 1996). Esse entendimento se faz necessário para a compreensão do *constructo* que fizemos até aqui. As percepções sobre a confluência da aplicação do conceito de território e da teoria das fronteiras no ambiente cibernético se, no início da pesquisa, deu-se de forma empírica, ao longo desta investigação foi-se confirmando, gradativamente, tanto pela bibliografia produzida e consultada até então, quanto pelas notícias e documentos de órgãos públicos, ligados à área em discussão, e corroborado em entrevistas com agentes, militares e civis.

Além disso, as ações planejadas e já implementadas para esse domínio seguem esse sentido. A resposta do Estado para essa possibilidade de ação no ambiente cibernético acompanha o fio condutor da *territorialização* ocorrida outrora com os demais domínios: o terrestre, o marítimo, o aéreo e o cósmico.

Nesse sentido, assim se expressou o Ministro da Defesa do Brasil, Celso Amorim, na abertura do III Seminário de Defesa Cibernética:

> A internet alterou os parâmetros de ação humana. O próprio conceito de realidade foi expandido pelo espaço digital. A cibernética emergiu como um novo domínio para a Defesa, e veio somar-se ao mar, a terra, ao ar e ao espaço. Aberto à ação humana, o domínio cibernético abre-se também ao conflito. (AMORIM, 2012)

E a Revista *The Economist*, que, de certo modo, referiu-se aos estudos de Clarke e Knake (2010) sobre a guerra cibernética: Guerra no quinto domínio: o *mouse* e o teclado são as novas armas do conflito? (THE ECONOMIST, 2010, tradução nossa).

Inúmeros países e outros atores do sistema internacional, dos diversos tabuleiros e posições do jogo do poder, participam dessa reação, tentando, ora delimitar unilateralmente esse novo espaço, ora elaborar normas para a garantia de seu funcionamento:

– os Estados Unidos, por meio do *Departament of Defense (DoD)*, da *Defense Information Systems Agency*, da *National Security Agency (NSA)*, do *Departament of Homeland Security,* da *Defense Intelligence Agency* e de um Comando específico criado em 2010 para a *cibernética* (o *USCYBERCOM*) (OLIVEIRA, 2011);

– o Reino Unido, com a primeira estratégia nacional de segurança cibernética (*Cyber Security Strategy of the United Kingdon: safety, security and resilience in cyber space*), lançada em 2009, com a previsão do *Office Cyber Security* (OCS), órgão responsável pela macrocoordenação, o *Cyber Security Operations Center* (CSOC), para monitorar o espaço cibernético e coordenar respostas aos incidentes (CANONGIA; MANDARINO JÚNIOR, 2009);

– a China, anunciando a criação de uma unidade específica de segurança e defesa na Província de Cantão (CLARKE; KNAKE, 2010), no que seguiu Ventre (2012), e até mesmo de uma Força Armada específica, "guerreiros cibernéticos", com a Coreia do Norte também seguindo esta mesma linha (SANTOS, 2011);

– o Canadá, com a *Canada's 2010 Cyber Security Strategy* (CCSS-CAN), pela qual foram enfatizados três pilares: 1) sistemas de segurança de governo; 2) parceria com o setor privado e 3) garantia da segurança aos canadenses no acesso *on-line* através de medidas de sensibilização. A estratégia canadense para o ciberespaço também atribuiu inúmeras responsabilidades entre os ógãos da Administração Pública, civis e militares daquele país (DEIBERT, 2012);

– na Europa, além da Inglaterra, destacamos a Alemanha, por meio da *Cyber Security Strategy for Germany* (CSSG-ALE) e pela criação recente (abril de 2017), do seu Comando de

Defesa Cibernética (*Germany´s Cyber and Information Comamand*), e a França, pela *Défense et sécurité des systèmes d'information: stratégie de la France*;

– com relação aos organismos internacionais, chamamos atenção para a reação da OTAN, com o *Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE), e da ONU, conforme relatado em momento anterior, que realizou, inclusive, exercícios reais entre países da região do sudeste asiático, próximos ao gigante chinês.

O fato é que esse "novo" domínio traz consigo uma série de questionamentos e, por consequência, incertezas. Para o general José Carlos dos Santos, então Comandante do Centro de Defesa Cibernética, em entrevista à Revista Época, de 18 de julho de 2011: "No espaço cibernético a fronteira não existe [...]. O inimigo é difícil de identificar." Já para Raphael Mandarino Junior, Diretor do DSIC/GSI/PR: "Aqui (no espaço cibernético), a exemplo do espaço real, também são estabelecidas relações sociais e políticas, no tempo e no espaço." (MANDARINO JÚNIOR, 2011). Essas duas afirmativas demonstram bem os pontos de vista e as discussões a respeito do ambiente que envolve a *cibernética*, sobretudo no tocante à delimitação do poder nesse espaço, por ora desafiador.

A primeira afirmativa, feita pelo Comandante do Centro de Defesa Cibernética (CDCiber) do EB, é propensa a declarar a inexistência de uma fronteira no espaço cibernético, atualmente. Contudo, *in fine*, admite o mesmo militar que há um inimigo, porém de difícil identificação. Na verdade, como uma inferência, o que o general quis indicar, mesmo ciente da existência de um poder contrário – um oponente – nesse tipo de espaço, foi a impossibilidade de um encaixe do *constructo* voltado para a fronteira terrestre, uma fronteira tradicional, no ambiente cibernético.

Isso ocorre, também, face à dificuldade de se detectar a origem, a autoria e a materialidade do ataque. Essas são, sem dúvida, algumas questões postas. De antemão, é preciso ter em conta que o espaço nesse ambiente não é natural, nem pertencente a uma geografia clássica. Esse espaço é específico, que obedece a outras regras, e não a que considera o território mero substrato físico. O território do domínio cibernético é artificial, produto do homem e fruto do nível tecnológico atual, e é, originalmente, um "território-rede".

Da segunda afirmação, de Mandarino Júnior, apreendemos uma intenção de delimitar esse espaço, face às relações sociais e políticas existentes, isto é, de poder, tal qual ocorre no espaço físico, natural. O que ocorre, então, é que esse inimigo, relembrando a afirmativa do general José Carlos, é um oponente que consegue se valer das características desse ambiente para não ser detectado, ou, pelo menos, dificultar ao máximo sua detecção. Todavia, ele está lá,

atuando e jogando com o poder, logo ocupando um espaço, interagindo e exercendo influência. É desta forma que percebemos traços e reflexos de sua existência.

Portanto, ao contrário do que possamos pensar inadvertidamente, parece haver um território cibernético, logo, havendo uma delimitação política espacial – uma fronteira – no denominado ciberespaço, ainda que por ora não regulamentada, ou não tendo todas as suas fases de regulamentação percorridas formalmente[24]. Fronteira no sentido *geopolítico* do termo, no qual se encontra a categoria *território* e, inseridos nesta, o *espaço* e o *poder.*

No ambiente cibernético do globo, os Estados definem seus territórios "nitidamente", isto é, apropriam-se de um espaço comum (*global common*) por meio do poder. Como exemplos imediatos, mas não únicos, basta-nos ver os domínios dos sítios ".br"; ".us"; ".uk"; ".it"; ..., que indicam perfeitamente os respectivos territórios no ambiente cibernético. Ainda nesse sentido, os Estados Unidos delimitaram não só o território de atuação do seu poder, como, internamente, distribuíram competências e atribuições acerca de cada domínio: o ".mil" ficou sob o encargo do comando combatente (USCYBERCOM), enquanto os ".gov" e ".com" foram atribuídos ao *Departament of Homeland Security* e às empresas privadas, respectivamente (CLARKE, 2010; ZUCCARO, 2011), ao que também segue Oliveira quanto às atribuições dos órgãos e agências norte-americanos (OLIVEIRA, 2011).

A estrutura montada e que funciona nesse ambiente também sofre influência do poder. A segurança dos *backbones*, dos *data centers;* dos *firewalls*[25] e demais elementos de filtragem, e da hospedagem de sítios são alguns dos exemplos de que há, "nitidamente", um exercício de poder no espaço cibernético, portanto havendo um território, e, por conseguinte, sua respectiva fronteira.

Ocorre que, diferentemente das fronteiras delimitadas até então (terrestre, marítima, aérea), todas perceptíveis, incluindo-se, de certo modo, a cósmica, uma nova fronteira desafia homens e Estados devido à sua virtualidade, velocidade, versatilidade, flexibilidade, ambiguidade e, porque não dizer, "volatilidade". O fluxo que "navega" por essa fronteira não é tão perceptível – pelo menos a olho nu e nem por equipamentos como luneta, binóculo, radar

---

[24] *Definição*, *delimitação* e, por fim, *demarcação* são as fases formais exigidas pelo Direito Internacional Público para o estabelecimento de uma fronteira. "A linha fronteiriça só é de fato estabelecida quando a demarcação se processa. 'De fato estabelecida' significa não estar mais sujeita à contestação por parte de um dos Estados que tivessem essa fronteira em comum. Pela demarcação, elimina-se não um conflito geral, mas um conflito do qual a fronteira pudesse ser o pretexto." (MAGNOLI, 1997, p. 240).

[25] Em uma rede de computadores, *backbone* designa o esquema de ligações/conexões centrais de um sistema mais amplo, tipicamente de elevado desempenho. Dentro de um sistema de capilaridade global, como a *internet*, há uma *hierarquia*, uma escala dessas ligações/conexões: a intercontinental, a internacional e a nacional, alcançando as empresas de telecomunicações, que representam, apenas, a periferia do *backbone* nacional. *Data centers* – centros de processamento e de armazenamento de dados. *Firewalls* – Filtros de "pacotes" de informações.

etc. – eis que o que flui nessa rede são, sobretudo, informações, por meio de caracteres simbólicos dentro de pacotes[26] que, em muitas vezes, fogem da imediata apreensão e compreensão. A delimitação de poder e de responsabilidades no espaço cibernético torna-se, doravante, a meta perseguida visando à garantia, sobretudo, da segurança, da harmonia e da paz, seja no ambiente interno, seja no internacional.

Nesse novo cenário, os conceitos geográficos de rede, de ponto e de "nós", outrora estudados nos espaços terrestre, marítimo e aéreo, são de suma importância. Sua aplicação guia os Estados e os Organismos Internacionais reguladores do Direito na formulação dos limites do espaço cibernético, ou melhor, do seu território. Se antes já existiam formas de controle e de monitoramento para as fronteiras tradicionais, nessa "nova" os contornos não se mostram muito claros, nem precisos. Entretanto, é certo que essa "nova fronteira" não existe de hoje.

1.3.2.1 Da "Fronteira-zona" à "Fronteira-ponto"

Como um dos fatores que provocaram a corrida por esse "novo" espaço, encontramos a *internet*: a instalação e a operação da rede mundial de computadores na escala global. Outro fator, como consequência deste anterior, é caracterizado pelo exponencial aumento do número de pessoas que passaram a ter acesso a esse meio e que vem, portanto, ocasionando uma "pressão" nesse espaço. Meira Mattos (1977) já apontava para esse fenômeno e seus possíveis reflexos ainda nos idos da década de 1970, denominando-o "cibernetização":

> 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)

Esse processo de pressionamento se assemelha bastante ao que deu origem à construção das fronteiras do espaço terrestre. Para ilustrá-la, também encontramos em Meira Mattos (1990) um resumo histórico sobre a Teoria das Fronteiras, relembrando o já apresentado em seção anterior, no qual agora acrescentamos mais um estágio, buscando representar o que entendemos ser hoje a nova fase dessa teoria, aplicada também ao ciberespaço, simultaneamente um território e uma rede, desde sua origem.

[26] Termo que nessa área científica indica um grupo de informações sendo transportadas unitariamente.

Se observarmos mais atentamente, além da *pressão demográfica* (MATTOS, 1990) e da *centralização do poder pelo Estado* (GIDDENS, 2001), outro fator é responsável pela evolução das fases ou estágios das fronteiras: *o fator tecnológico*. À medida que se desenvolveram instrumentos que capacitaram um maior poder de monitoramento dos espaços, por meio do controle e do armazenamento das informações, mais nítidos tornava-se sua delimitação, passando-se de uma forma de zona, para a de faixa, até chegar a de uma linha. Acreditamos que no atual estágio tecnológico os Estados são capazes de delimitar seus interesses à escala de um "ponto", alcançando-se, assim, a fase ou o estágio da "*fronteira-ponto*", como um reflexo da trajetória histórica da capacidade de monitoramento e controle do sistema de Estados, e caracterizando, desta forma, a 5ª fase ou estágio da evolução das fronteiras (Quadro 1.7).

Quadro 1.7: Evolução das Fronteiras e Nova Proposta

FASES/ESTÁGIOS		DESCRIÇÃO
1º	Vazios de ecúmene	– característico do mundo antigo, pouco povoado, quando os núcleos geohistóricos eram separados por enormes vazios demográficos.
2º	Largas zonas inocupadas ou fracamente ocupadas	– estas zonas não abrigavam nenhum poder político capaz de perturbar os interesses dos núcleos geohistóricos de que eram separadores.
3º	Faixas relativamente estreitas, chamadas *fronteiras-faixa*	– nas áreas em que o povoamento dos países limítrofes não chega a pressionar um sobre o outro.
4º	*Fronteira-linha*, estabelecida sob critérios vários (natural, artificial, astronômica, étnica)	– nas áreas em que a densidade populacional colocou em contato permanente o *interesse* das partes.
5º	*Fronteira-ponto*, acompanhando o atual estágio tecnológico	– no ciberespaço, em sua estrutura física e/ou na imaterial, onde os interesses, por meio do fluxo de informações, podem colidir e causar danos a "pontos" escolhidos no território, ou fora deste. Selecionam-se "*nós*" da rede e "*pacotes*" de informação que por esta trafegam.

Fonte: o autor, adaptado de MATTOS, 1990, p. 17. [27]

A *fronteira*, nessa visada, passa a ser *ponto* (*fronteira-ponto*), não simplesmente pelo objeto a ser defendido, pois isso já ocorria nas outras dimensões que não a *cibernética*, como no caso dos castelos, das fortalezas, dos fortes, de cidades, portos, estreitos e ilhas, ainda na

[27] O 5º estágio é proposto por nós.

Idade Média (MEIRA MATTOS, 1990; RAFFESTIN, 1993; NYE, 2012; BUZAN; HANSEN, 2012) ou pelos Estados tradicionais (GIDDENS, 2001).

Nem também estamos nos referindo à fronteira cibernética (*cyber boundary*) indicada por Clarke e Knake (2010), em seu Glossário; nem ao *ponto* que esses autores indicam dentro dessa fronteira. Para eles, *fronteira cibernética* é empregada no sentido do limite entre o mundo *cyber* e o real, e o *ponto* diz respeito ao momento em que o comandante deverá decidir se (e como) passar de uma guerra puramente cibernética para uma envolvendo forças convencionais ou com armas cinéticas.

Também não são os "pontos-fronteira" indicados recentemente por Daniel Ventre, referindo-se aos "cabos [que] chegam e saem de pontos – instalações que conectam os cabos entre si entram e saem do território, criando uma relação entre a rede interna e o resto do mundo [...] – equivalentes aos portos marítimos, aos aeroportos internacionais." (VENTRE, 2019, p. 78), apesar de enxergarmos muita proximidade com o que apontamos ainda em 2013. Todavia, acreditamos que essa capacidade de seleção e de "cortes" do espaço vai além no mundo virtual.

Pelo nosso entendimento temos o *ponto*, ou melhor, a "*fronteira-ponto*", como resultante de uma maior capacidade de controle das informações e de monitoramento, de maior precisão e velocidade de tomada de decisão entre o sensoriamento (detecção, vigilância), o processamento e a atuação (D-P-A), os quais correspondem à (ao): *Detecção* – obtenção de informação sobre possíveis ameaças; *Processamento* – trabalho da informação com vistas à tomada de decisão e implementação e *Atuação* – implementação da decisão e neutralização da ameaça (AMARANTE, 2010), que acarretam a delimitação. Portanto, para nós, esses pontos, a título de exemplo, significam: 1) as informações digitalizadas em seus "pacotes", transitando por uma rede, localizada dentro ou fora do território terrestre (pelos *backbones* e cabos, pelas ondas *hertz* e fibra ótica), sendo processadas ou armazenadas em um computador (*datacenter*) (ativos da informação [28]), 2) os "nós", isto é, os pontos de conexão da rede pelos quais trafegam esses fluxos ("pacotes"), e 3) as estruturas estratégicas (infraestruturas críticas) com interesses vitais para o Estado. Este último caracteriza o "*extraespaço*", enquanto os dois primeiros correspondem ao "*intraespaço*" ou ao *ciberespaço considerado em si mesmo*.

No caso das informações e de seus "pacotes", a abstração contida no princípio da extraterritorialidade diz respeito, por exemplo, a hipóteses em que, mesmo não estando situadas no território terrestre, no mar territorial ou no espaço aéreo do país, pessoas ou coisas são salvaguardadas. Como origem desse postulado, pode ser citada a obra de Hans Kelsen (*apud*

[28] Ativos de Informação - meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. (BRASIL, 2010b).

DALLARI, 1995), a partir do momento em que esse autor desvincula o objeto de interesse do Estado do seu *locus* de atuação de poder – seu território. Assim sendo, em alguns casos, a personalidade jurídica do Estado fica assegurada, juridicamente, para o "além-terra": o *território-competência*.

O resultado dessa construção teórica pode ser visto, de forma exemplificativa e sintetizada, no artigo 7º do Código Penal Brasileiro, quando ficam submetidos à legislação brasileira, embora cometidos no estrangeiro, crimes contra o presidente da República, o patrimônio ou a fé pública da União e demais entes federativos. Além disso, encontramos sob essa proteção, as empresas públicas, as sociedades de economia mista, as autarquias ou as fundações instituídas pelo poder público, e a própria administração pública. Em todos esses, a finalidade perseguida é a salvaguarda da personalidade jurídica estatal e seus interesses, isto é, a proteção da instituição, mesmo fora de seu território físico.

No mais, objetos ou coisas também são colocados sob essa condição, embora com algumas nuanças (extraterritorialidade condicionada), como é o caso de aeronaves e de embarcações brasileiras, mercantes ou privadas, quando em território estrangeiro. Essa é uma das soluções, a nosso ver, que o sistema de Estados pode adotar a fim de determinar fronteiras no espaço cibernético.

Semelhante a essa proposta, assim mencionou Robert Axelrod sobre o papel dos governos acerca da *internet*:

> [Esses governos] despertaram para um fato interessante: cada nó de rede, cada roteador, cada desvio está dentro de fronteiras soberanas de uma nação-estado, e, portanto, sujeitos as suas leis ou transmissões por um cabo submarino ou conexão de satélite de posse de uma companhia que está incorporada a um Estado-nação e sujeita às suas leis. Em outras palavras, não há parte não soberana no "livre" do espaço. (*apud* SINGER; FRIEDMAN, 2017 [2014], p. 208)

É dessa forma que podemos concluir que no espaço cibernético, considerado em si, vem ocorrendo uma *territorialização*, uma vez que a disputa pelo controle de informações e da possibilidade de seu fluxo vem sendo objeto do poder. Ao mesmo tempo, também inferimos que há uma *(re)territorialização* ocorrendo nos demais domínios espaciais, fruto das possibilidades advindas desse recurso. Assim, como exemplos localizados no domínio terrestre, as usinas hidrelétricas e as centrais de distribuição de energia, as estações de tratamento de água e o setor financeiro considerados essenciais para o Estado, e para o seu sistema, são selecionados a fim de uma atenção maior no que tange à segurança e à Defesa.

Mais uma vez, portanto, a delimitação dessa fronteira, de forma clara e precisa, torna-se crucial para a manutenção da harmonia, da segurança, da paz. Com as pressões exercidas nessa nova dimensão e a busca pelo seu empoderamento, há a transformação do conceito *espaço* para o de *território*, vez que, intrinsecamente, circula e se confronta poder.

Como mais um aspecto, a informação, em si, não tem valor caso não tenhamos capacidade de processá-la ou de torná-la inteligível, em certo tempo, para determinados fins. Assim, o conhecimento mais detalhado das características dessa fronteira torna-se primordial nessa nova forma de recurso de poder, pois proporciona condições de defender tanto as informações quanto alguns pontos de uma rede e de um país. O seu uso pode servir, inclusive, para uma *(re)territorialização* dos demais domínios territoriais e para a guerra.

1.4 CIBERNÉTICA COMO MAIS UM RECURSO DE PODER

A *cibernética*, além de um espaço em si, pode ser vista sob outra ótica: a de um recurso de (e do) poder. Nesse aspecto, o poder cibernético apresenta similaridades com o poder advindo das comunicações e da informação; suas possibilidades e seus limites. Joseph Nye afirma que o poder cibernético é o "conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas baseadas em computador – infraestrutura, redes, *software*, habilidades humanas." (NYE, 2012, pp. 162-163). Nessa visada, esse poder é usado tanto para se obter resultado dentro do espaço cibernético – o que coadunaria com a primeira ótica apresentada neste trabalho (o ciberespaço como espaço em si mesmo) e o que J. Nye denominou "intraespaço" –, ou pode se valer dos instrumentos cibernéticos para alcançar resultados nos outros domínios.

Com relação ao conflito interestatal nessa nova dimensão, tomaremos emprestada a definição de guerra cibernética elaborada por Parks e Duggan:

> Guerra Cibernética é um sub-grupo da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existe uma diversidade de espaços cibernéticos, mas o mais relevante para a Guerra Cibernética é a Internet e as redes a ela interligadas. Em termos militares, guerra cibernética deve ser entendida como uma combinação de ataque e defesa a redes de computadores envolvendo operações especiais de informação. (PARKS; DUGGAN, 2001, p. 122, tradução nossa)

Essa definição segue a de Libicki (1995 *apud* FONTENELLE, 2008), quanto à inclusão da *Guerra Cibernética* (espécie) dentro do "grande grupo" *Guerra da Informação* (gênero) (Quadro 1.8), que compreende:

Quadro 1.8: Subgrupos da Guerra da Informação

GUERRA DA INFORMAÇÃO – SUBGRUPOS (ESPÉCIES)	
1	*Command-and-Control Warfare (C2W) ou Guerra de Comando e Controle*
2	*Intelligence-based Warfare (IBW) ou Guerra baseada na Inteligência*
3	*Eletronic Warfare (EW) ou Guerra Eletrônica*
4	*Psychological Operations (PSYOPS) ou Operações Psicológicas*
5	*Hackewar ou Guerra de Hacker*
6	*Economic Information Warfare (EIW) ou Guerra de Informações Econômicas*
7	*Cyberwar (CW) ou Guerra Cibernética*

Fonte: elaborado a partir de Libicki (1995 *apud* Fontenelle, 2008, pp. 15-16).

Ainda, segundo Parks e Dugan (2001), partindo da ideia de que a guerra cibernética é virtual e que a guerra tradicional (chamada pelos autores de cinética) é real, temos a seguinte conclusão:

> Ciberguerra é diferente da guerra convencional, cinética. Tanto ela como sua preceptora, a guerra da informação, dependem das fragilidades dos seres humanos para muitas características. Uma das diferenças fundamentais entre ciberguerra e guerra cinética é a natureza de seus ambientes. Guerra cinética ocorre no mundo físico, regido pelas leis da física que conhecemos e entendemos. Ciberguerra ocorre em um mundo artificial, caótico, com imperfeições. Ciberguerra pode usar alguns dos princípios da guerra cinética, mas existem outros princípios que tem pouco ou nenhum significado no ciberespaço. Por estas razões, os princípios da ciberguerra são, em última análise, diferentes dos de guerra cinética. (PARKS; DUGGAN, 2001, p. 125, tradução nossa)

No tocante à definição de *guerra cibernética*, no Brasil, o Ministério da Defesa (MD) parece ter acompanhado e se adaptado às mudanças no entendimento acerca da cibernética e da guerra nessa dimensão. O Glossário das Forças Armadas, confeccionado pelo MD no ano de 2007, indicava ser um

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

A definição anterior não era muito profícua, por ser muito abrangente, quando não vincula necessariamente a informação ao seu respectivo processamento em computador. Acreditamos que ao nos referirmos à *cibernética*, e ao conflito nesse espaço, inevitavelmente deveremos nos restringir à *informação processada por computador, transitando ou não em uma rede*. Essa é a característica mais marcante e que a difere da Guerra de Informação, *lato sensu*. Esse ponto é importante, quando formos verificar a constituição de um sistema de Segurança e Defesa Cibernética no Brasil, com relação, por exemplo, aos recursos humanos que atuarão nesse ambiente. De imediato, cabe-nos afirmar que, inegavelmente, passarão por formação, capacitação ou especialização na área da ciência computacional, da informática e afins, pois o foco é a informação processada por um sistema computacional: a informação digitalizada.

De 2010, a Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do MD, define *defesa* e *guerra cibernética*, como:

> Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacionais, tais ações caracterizam a Guerra Cibernética. (CARVALHO, 2011, p. 18)

Da comparação entre a definição do MD, de 2007, e esta imediatamente acima, elaborada três anos após, podemos apreender um maior detalhamento acerca da Guerra - e, por conseguinte, da Defesa – nesse domínio. Somos, por exemplo, capazes de inferir, entre outras informações, as seguintes:

1) Tipos de Ações – defensivas, exploratórias e ofensivas.
2) Local: no espaço cibernético.
3) Finalidades – proteção dos sistemas de informação; obtenção de dados para inteligência e danificação dos sistemas de informação do oponente. A obtenção de vantagens pode ser tanto na área militar quanto na civil (infraestruturas ou estruturas estratégicas, por exemplo, quando estamos tratando dos níveis acima do operacional, isto é, do estratégico e do político).

A definição acima, apesar de ser mais precisa e pontual do que a de 2007, também não delimita bem, em si, o *locus* do conflito cibernético, pois ao mencionar “espaço cibernético”, deixa aberto ou pressupõe certo entendimento, logo ficando dependente da interpretação do que seja esse espaço. Contudo, podemos considerá-la melhor do que a definição anterior, a do Glossário do MD (2007), se entendermos que a menção ao espaço cibernético, como vimos, já

pressupõe o uso de computador para o processamento de informações. Essa é a principal característica do ambiente cibernético.

Certamente essa discussão e as dúvidas suscitadas fizeram o Ministério da Defesa atualizar e pormenorizar seu entendimento. Para esse órgão, agora,

> GUERRA CIBERNÉTICA – Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as **ferramentas de Tecnologia da Informação e Comunicações (TIC)** para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2015, **grifo nosso**)

É assim que para a Academia Nacional de Ciências (Washington D.C), ataque cibernético "refere-se à deliberação de ações para alterar, interromper, enganar, degradar ou destruir sistemas de computador ou redes ou programas de informação instalados ou em trânsito nesses sistemas ou redes." (OWENS; DAM; LIN, 2009, p. 1, tradução nossa), o que, em muitos pontos, como vimos, converge para a definição de *operaciones cibernéticas* de Sergio Eissa *et. al* (2012). Mais uma vez verificamos, portanto, a necessidade das ideias *informação* e *computador* ligadas às *TIC* para melhor delimitação no trabalho, acerca da *cibernética*, seu espaço e sua utilização como recurso, e as formas de conflito nesse ambiente.

Ainda nessa temática, torna-se interessante diferenciar segurança da informação de guerra cibernética: do ponto de vista das ferramentas, técnicas e conhecimentos utilizados não há praticamente diferenças "é seguro afirmar que grande parte das pesquisas desenvolvidas, voltadas para a Segurança da Informação, possui aplicações em Guerra Cibernética" (DUTRA, 2011). Isso também é o que pode ser inferido na declaração do general Santos Guerra, ex-comandante do Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx):

> Os ataques que registramos até agora são parecidos com os que acontecem em qualquer empresa. Tentativas de roubos de senhas, negações de serviço, etc. Mas o modo como se obtém uma senha de banco é o mesmo que se pode usar para obter dados confidenciais do Exército. E já tivemos sites do governo derrubados. (GUERRA, 2012)

A principal diferença, assim, reside na origem e na intenção do autor: enquanto a primeira sugere conflitos no campo privado, a segunda envolve necessariamente relações de poder entre Estados. Ações oriundas de um indivíduo com motivações pessoais não podem ser

consideradas como sendo guerra cibernética. Para que esta ocorra, portanto, faz-se necessária a "existência de patrocínio estatal" (DUTRA, 2011). Nesse raciocínio também segue Paulo Zuccaro, antigo subchefe de Comando e Controle do Estado-Maior de Defesa, ao propor uma taxonomia que diferenciasse *Guerra* de *Crime* no ambiente cibernético:

> Guerra Cibernética – É focada em conflito interestatal [...], o que estará por trás das ações, de forma velada, ou não, será a agressão de um Estado a outro na busca da redução de poder nacional, [...].
>
> Crime Cibernético – [...] geralmente as motivações serão de indivíduos ou de pequenos grupos, com fins privados e egoísticos. Na maioria dos casos são ilícitos como objetivos de ganhos econômicos [...]. (ZUCCARO, 2011, p. 61)

A aparência entre essas definições também é tratada, e questionada, pelos pesquisadores da *Universidad de Buenos Aires*, com o fito de diferenciar ações no ambiente cibernético que demandem Segurança das que demandem Defesa: "Que tipo de operações cibernéticas requer a participação do sistema de Defesa Nacional?" (EISSA *et al*., 2012, p. 8, tradução nossa). Em suma, como resposta, chegaram à conclusão tais autores que, para ser considerado ataque cibernético objeto de emprego da *Defensa Nacional*, as ações (*ciberoperaciones*) devem ser conduzidas por atores estatais em um cenário de guerra, orientadas a causar danos às capacidades militares de outro Estado (EISSA *et al*., 2012, p. 9). Desta feita, fica caracterizada, *a priori*, como cena do emprego da *Defesa*, as ações que envolvam *Guerra*, o que termina por acompanhar o que evidenciaram Dutra (2011) e a Minuta de Nota de Coordenação Doutrinária apresentadas acima: *ações* (ataque, defesa e exploração), no *nível operacional*, *entre Estados*.

Corroborando também esse entendimento sobre Guerra Cibernética, Oliveira afirma: "frequentemente utilizado como referência ao 'conflito cibernético' (Ataque X Defesa), entretanto, seu significado mais adequado refere-se à utilização de todo o espectro de recursos cibernéticos, no ambiente de preparo e emprego operacional de frações militares [...]" (OLIVEIRA, 2011, p. 116). A ameaça é tida dentro do ponto de vista da guerra clássica, apenas se tratando de mais uma ferramenta e uma dimensão espacial, isto é, meios à disposição da política para sua continuidade.

O fato é que a guerra cibernética, como mais um recurso de (e do) poder, impõe uma nova realidade para os teatros de operações militares, na medida em que o espaço cibernético se constitui como outro tipo de território, um espaço já submetido ao jogo do poder. Atualmente, a maioria dos sistemas de informação, necessários para o funcionamento da sociedade moderna, encontra-se interligado por meio de redes de computadores. Nesse contexto,

> Os alvos não são mais somente pessoal e instalações militares. Agora, bancos, usinas elétricas, empresas de telefonia e de telecomunicações, sistemas de transporte e logística, serviços de emergência e segurança pública, entre outros são alvos em potencial, uma vez que a indisponibilidade continuada de quaisquer destes serviços certamente levaria uma nação ao colapso. (DUTRA, 2011)

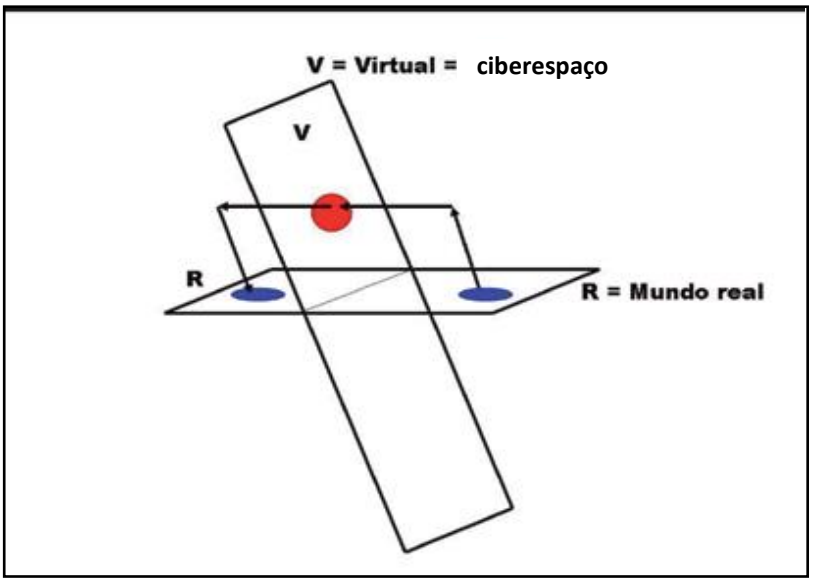
Essa é uma das preocupações de Clark e Knake (2010) quando abordam a *cibernética* e o seu emprego para fim militar. Os autores alegam que os ataques feitos por "guerreiros", ou diríamos soldados, altamente especializados no ambiente cibernético, podem causar danos ou ocasionar a perda sobre o controle de uma rede. Não só as infraestruturas críticas de um país se encontram sob essa vulnerabilidade, como também o sistema de defesa: roubo de informações, derramamento de petróleo, explosão de geradores, descarrilamento de trens, colisão de aviões, envio de um pelotão para uma emboscada e envio de um míssil para um alvo errado são alguns dos exemplos. Ainda quanto ao emprego militar, o Almirante Mike McConnell observou que esses ataques podem ser feitos por controle remoto, além das fronteiras do Estado alvo e que, nesse caso, nenhuma flotilha, míssil intercontinental ou exército permanente poderá defender-se contra tais ataques, por se encontrarem no "éter digital do ciberespaço" (CLARKE; KNAKE, 2010).

É assim que podemos entender que as ações no mundo virtual são possíveis de causar danos no mundo real (PARKS; DUGGAN, 2001). Nesse aspecto também concorda Fontenelle (2008), militar que serviu no Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx) e Daniel Ventre que, utilizando-se da Figura 1.5, afirma: "Um ataque cibernético é um ato agressivo que a partir da dimensão **R** (os atores do ato estão no mundo real) e através da dimensão **V** alcança um objetivo situado em **R**. O ciberataque ocupa o espaço **V**, porém sempre se esforça por produzir um efeito na dimensão **R**." (VENTRE, 2012, p. 35, tradução nossa).

E corrobora o grupo de pesquisadores de Buenos Aires:

> […] embora as ações de guerra cibernética tenham sua origem em um ambiente virtual – a de redes de comunicação e sistemas informáticos – seus efeitos impactam sobre o mundo físico e podem afetar o tráfego aéreo e terrestre, o controle de infraestruturas críticas, o abastecimento energético, de água, entre outros. (EISSA, *et al.*, 2012, p. 9)

Figura 1.5: Relação Espaço Virtual–Real



Fonte: VENTRE (2012, p, 35).

Esses enfoques são importantes, uma vez que reiteram a ideia de transversalidade do espaço cibernético face às demais dimensões espaciais.

Clarke e Knake (2010), ao analisarem alguns incidentes cibernéticos deste século, afirmam que o ataque cibernético já é uma realidade dos conflitos envolvendo Estados-nação. Como evidências, esses autores apontam na direção de cinco aspectos:

1) a guerra cibernética é real;

2) a guerra cibernética acontece na velocidade da luz;

3) a guerra cibernética é global;

4) a guerra cibernética ignora o campo de batalha (os sistemas que dependem de pessoas, como bancos e radares de defesa aérea, são acessíveis a partir do ciberespaço e podem ser rapidamente controlados e "nocauteados" antes mesmo de se derrotar a defesa tradicional de um país);

5) a guerra cibernética já começou.

A guerra cibernética também traz uma questão paradoxal: quanto mais desenvolvida tecnologicamente uma sociedade, maior será sua vulnerabilidade aos ataques cibernéticos; ou seja, quanto mais dependemos de redes de computadores, maior é o receio de que oponentes ataquem essas redes, face ao grau de conectividade. O cálculo de poder e seu derivado equilíbrio parecem ter sido apresentados a uma variável um tanto quanto rebelde à quantificação, para além das inconstâncias inerentes às variáveis tradicionais, tais como: o nível industrial e

tecnológico; a estrutura e o sistema militar; o grau de coesão do corpo social; a participação política e a democracia etc.

Na tentativa de mensuração do poder cibernético de alguns países (EUA, Rússia, China, Irã e Coreia do Norte), Clarke e Knake (2010) criaram critérios de avaliação, que foram transcritos por nós conforme Quadro 1.9. Esses autores consideraram três variáveis: *cyber offensive*; *cyber dependence* e *cyber defense*, na qual: *ofensiva* refere-se à capacidade de atacar outra nação; *defesa* diz respeito à capacidade de um país tomar medidas para bloquear ou mitigar um ataque cibernético *e dependência* significa medida que a nação é interligada por redes e sistemas que podem ser vulneráveis a um ataque cibernético no caso de guerra.

Para Clarke e Knake (2010), os Estados Unidos seguidos de perto pela Rússia são os países com maior capacidade de realizar ações ofensivas no ambiente cibernético. Em seguida, formando uma espécie de segundo time, vem a Rússia e a China. Além desses, cerca de 20 países, entre esses o Irã e a Coreia do Norte, formam outro bloco. A nota atribuída por cada variável era de 0 (zero) a 10 (dez), esta correspondendo à avaliação mais positiva possível para cada tópico.

Quadro 1.9: Capacidade Geral de Guerra Cibernética

ESTADO	CAPACIDADE OFENSIVA	CAPACIDADE DEFENSIVA	GRAU DE DEPENDÊNCIA	SCORE TOTAL
ESTADOS UNIDOS	8	1	2	11
RÚSSIA	7	4	5	16
CHINA	5	6	4	15
IRÃ	4	3	5	12
COREIA DO NORTE	2	7	9	18

Fonte: elaborado e adaptado a partir de Clarke e Knake (2010).

Não obstante a subjetividade dos dados e a não divulgação por completo da metodologia de sua confecção, temos ainda outra possível interpretação, talvez a mais importante a ser extraída e apreendida pelos tomadores de decisão e diversos agentes públicos: uma grande capacidade ofensiva, por si só, não corresponde, no ambiente cibernético, à imunidade contra ataques externos, nem à grande vantagem quando do uso desse tipo de força. Também não corresponde, por conseguinte, à certeza de vitória durante uma guerra nesse domínio. Pelo contrário, conforme a metodologia empregada por Clarke e Knake, o fator preponderante nesse caso passa a ser o nível de interligação, por sistemas de rede, das infraestruturas críticas do país (energia elétrica, transportes, água, suprimentos etc.), isto é, o seu grau de dependência, que

vem a ser “até que ponto as infraestruturas críticas são dependentes dos sistemas de rede e não possuem capacidade real de resiliência[29].” (CLARKE; KNAKE, 2010, tradução nossa).

Assim, o jogo estratégico nesse ambiente parece estar suscetível de apresentar, no momento, muito mais imponderáveis do que os campos de batalha tradicionais. O equilíbrio de forças nesse domínio fica condicionado à avaliação de variáveis além das convencionais. Países com grande capacidade ofensiva nesse espaço podem, ao mesmo tempo, ser extremamente vulneráveis, face, justamente, ao grau de tecnologia e de interligação dos sistemas.

Acompanhando esse entendimento, as variáveis *monitoramento*, *controle* e *armazenamento* das informações (GIDDENS, 2001), que é um recurso crucial de poder, recebem uma nova roupagem, bem mais complexa, devido às características inerentes a esse domínio, sobretudo pelo uso de computadores e de processadores que permitem a multiplicação e a aceleração do fluxo informacional. Para J. Nye (2012), como causas desse fenômeno, além da velocidade proporcionada pelo poder cibernético, a diminuição dos custos de transmissão da informação, ou a redução dos custos no setor da eletrônica (DIAS, 2003), é que proporcionam uma facilidade de acesso a esse recurso, caracterizando uma forma de difusão de poder.

As possibilidades advindas do uso eficiente e eficaz do recurso cibernético transformam-no em uma fonte de poder, aliás, aprimoram ainda mais o controle e o armazenamento das informações, que, no nível político e no estratégico, permite ao Estado, por exemplo, o monitoramento de seu território e de *pontos* de seu interesse, entre esses a própria informação em seus “pacotes”, ainda que fora de seu domínio (extraterritorialidade). Daí, ao mesmo tempo em que se busca o controle e a segurança da informação em si no ciberespaço, encontramos projetos como os sistemas de Proteção da Amazônia e o Sistema de Vigilância da Amazônia (Sipam/Sivam) e o de Defesa Aeroespacial Brasileiro (Sisdabra), e os atuais Sistema Integrado de Monitoramento de Fronteiras (Sisfron) e de Gerenciamento da Amazônia Azul (SisGAAz) e os programas Amazônia Conectada e do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC). É com esse poder, que advém de relações e de exercícios constantes, calcados em um novo nível e aparato tecnológico, que parecem estar preocupados os Estados.

[29] Por *resiliência* entendemos a capacidade de restabelecimento do funcionamento de um sistema após uma interrupção, geralmente inesperada, brusca.

CAPÍTULO 2

PODER CIBERNÉTICO E CIBERESPAÇO: TEORIAS, ESTRATÉGIAS E REALIDADE NO SISTEMA INTERNACIONAL

Após trazermos no capítulo anterior a cibernética sob uma ótica geopolítica, tratando-a do ponto de vista da relação entre Estados e de suas estratégias e estruturas de poder, dentre elas a de Defesa, voltadas para a natureza de um sistema internacional anárquico, portanto dentro de uma concepção realista ou do realismo de poder, buscamos verificar a conformidade do ciberespaço e do poder advindo da cibernética com outras linhas de discursos e de pontos de vista, que acreditam ser esse recurso uma fonte que permite maior liberdade, igualdade e até mesmo fraternidade. A cibernética, sob esta ótica, seria um instrumento que ampliaria as oportunidades de participação democrática, de transparência, de *accountability* e de justiça social, por exemplo, no nível entre indivíduos, entre estes e grupos sociais, entre estes e seu respectivo Estado, e na própria relação entre Estados. Mais que isso, o ciberespaço e suas ferramentas permitiriam o constrangimento de um Estado a partir de ações de indivíduos, da imprensa e de ONG's, configurando, assim, uma difusão do poder. Para elucidarmos essas inquietações acerca das capacidades advindas do ciberespaço, coube a nós buscarmos opções teóricas que respondessem a esse fenômeno dentro desta perspectiva, pois, realmente, esses discursos e pontos de vista também constam da agenda política e de uma série de documentos, da literatura, de reportagens e de nosso dia-a-dia.

Nesse sentido, este capítulo visa trazer à discussão, por um lado, as formas como internacionalistas, acadêmicos, empresas e burocracias de alguns Estados abordam – ou podem vir a abordar – a cibernética dentro de um escopo teórico das relações internacionais (RI) e, por outro – e como base –, inferir dos principais documentos de referência desta pesquisa – a Estratégia Nacional de Defesa (END) e a Política Nacional de Defesa (PND) – a direção apontada pelo planejamento estratégico do Estado brasileiro, considerando, ao mesmo tempo,

esse arcabouço teórico, documental e empírico apresentado e as características do sistema os quais procuram responder. Assim, além de abordar a cibernética sob as lentes das consideradas principais ou fundantes teorias das RI – a realista e a liberal, e suas variações no tempo –, empreendemos um esforço a fim de se pensar esse objeto pela perspectiva da Economia Política Internacional (EPI), nesta inserida a teoria do Poder Global e, ainda, sobre suas implicações para o desenvolvimento de "Estados-economias nacionais" (FIORI, 2004), uma vez que acreditamos que essa forma de explicar a realidade vem coincidindo bastante com os documentos e ações oficiais do Brasil e de outros atores para esse setor.

A questão essencial que este capítulo pretende responder é: qual matriz teórica do campo das relações internacionais tem a melhor capacidade de explicar a realidade, no que diz respeito às possibilidades advindas do poder cibernético e do ciberespaço? Incluem-se aqui, portanto, como realidade, tanto estratégia de preparação para o conflito, como visto no capítulo anterior, quanto a de ganhos relacionados à esfera econômica, e a interação entre essas duas estratégias.

Esforço similar quanto às possibilidades cibernéticas sob a luz de teorias de RI foi feito, por exemplo, pelos pesquisadores brasileiros Leonardo Valente[30] (2007), Bernardo Wahl Jorge (2012), Igor Acácio e Gills Souza (2012), Eduardo Souza e Nival Almeida (2016), Selma Gonzales e Lucas Portela (2018), Lucas Portela (2018) e Jacqueline Marinzeck (2018)[31], além de estrangeiros como Richard Clarke e Robert Knake (2010), Joseph Nye (2012), Dereck Reveron (2012), Ron Deibert (2012), Robert Blackwill e Jennifer Harris (2016), e John Troxell (2018).

Uma das questões de pesquisa de Acácio e Souza foi descobrir "como as teorias de RI buscam explicar os profundos desafios engendrados pelo ciberespaço" (ACÁCIO; SOUZA, 2012, p. 1). Para a análise, Acácio e Souza (2012) selecionaram quatro correntes teóricas das RI: o Realismo, a Escola Inglesa, o Neoliberalismo e a Escola de Copenhague. O pano de fundo foram os estudos de segurança. Dentro deste mesmo contexto, B. Jorge pretendeu demonstrar "como as Relações Internacionais, enquanto área do conhecimento, podem auxiliar na

[30] Embora não utilizasse o termo "cibernética", esse autor, em parte do Capítulo 1 da obra em referência, realizou exercício de reflexão parecido e com o mesmo objeto agora em questão: a informação na sua forma digital. Ver: "*Cap. 1 – A Era da Informação e as Mudanças do Jogo pelo Poder nas Relações Internacionais*", sobretudo entre as páginas 19-41. Nessa mesma parte, pode também ser inferida a ideia de Valente (2007) sobre a relação informação e cibernética, quando esse autor utiliza citação de David Rothkopf (1998) sobre o poder na Era da Informação: "A *realpolitik* de amanhã é a *cyberpolitik*." (pp. 19 e 38).

[31] Ainda no estudo sobre a cibernética e o ciberespaço, embora não preocupados com teorias de RI especificamente, mas considerando possibilidades, conflitos e formas de controle, ver também os trabalhos dos pesquisadores brasileiros Everton Lucero (2011), Luisa Lobato e Michael Kai Kenkel (2015) e Carolina Batista Israel (2015 e 2019). Quanto à existência de uma nova subárea nas Relações Internacionais, as "Relações Internacionais Cibernéticas", ver proposta de Marcos Aurélio Oliveira, Ricardo Gama Neto e Gills Lopes (2015) e Gills Lopes (2016).

compreensão do fenômeno das ‘guerras cibernéticas’.” (JORGE, 2012, p. 1). Este autor trouxe as perspectivas do realismo, do liberalismo e do construtivismo nas RI.

Também seguindo a linha construtivista, embora com um tom de realismo e de política de poder inserido nos respectivos textos, os autores nacionais Souza e Almeida (2016) e Marinzeck (2018) colaboram com a reflexão deste tema sob a luz do construtivismo de Wendt (1992), e da Escola de Copenhague (BUZAN *et al*., 1998), e sua análise sobre o processo de securitização, a partir de uma construção social da realidade e de seus reflexos nas políticas públicas. Para esses autores, a cibernética passou a ser um dos setores securitizados pelos atores estatais, na medida em que sua capacidade de afetar a segurança nacional se tornou uma realidade, considerando também as interações sociais e os reflexos para outros atores das RI, além do próprio Estado, como no caso de organizações terroristas, ONG’s e empresas. Essa ideia é bem interessante, na medida em que se assemelha muito ao estudo das políticas públicas – seu processo e ciclo –, sobretudo quando do momento de decisão do que o governo faz, ou não faz, da participação de outros atores interessados, da transformação do problema em uma “questão política” (*issue*) e do surgimento – e aproveitamento – de “janelas de oportunidade” (RODRIGUES, 2010). Foi exatamente nesse sentido que ocorreu a movimentação política no Brasil para a consecução e implementação de projetos e programas voltados para a segurança e defesa cibernética no recorte temporal desta pesquisa, tendo um ápice em 2013, com o caso Snowden e com a proximidade de grandes eventos internacionais como a Copa das Confederações e do Mundo de Futebol, em 2013 e 2014, respectivamente, e as Olimpíadas, em 2016.

Com relação a autores estrangeiros que se debruçaram sobre o tema, Nye (2012) elaborou um capítulo específico no livro “*O Futuro do Poder*” para trazer reflexões acerca das possibilidades advindas da cibernética, incluindo nessas a de difusão do poder para atores além dos Estados, como organismos internacionais governamentais e não-governamentais, imprensa e outras mídias, da mesma forma que para grupos criminosos e terroristas “desterritorializados”, pois passam a ampliar sua capacidade de articulação via células, em um ambiente reticular. Deibert (2012), além da preocupação com a cibersegurança, abre reflexão acerca da forma de condução dos Estados com relação a essa temática, tendo em vista o modelo político adotado pelo país, sobretudo em questões que envolvem, de um lado, o valor liberdade e, de outro, o valor segurança. Para este autor, as democracias liberais têm uma tendência de maior abertura do ciberespaço, enquanto Estados totalitários, ou com essas características, exercem um controle e monitoramento maior da rede, às vezes se utilizando de censura ou de bloqueios de termos de acesso.

Blackwill e Harris (2016), ao que seguiu Troxell (2018), preocuparam-se com o uso de instrumentos econômicos para fins geopolíticos, definindo, assim, geoeconomia como: “O uso de instrumentos econômicos para promover e defender interesses nacionais e produzir resultados geopolíticos benéficos; e os efeitos das ações econômicas das demais nações sobre os objetivos geopolíticos de um país” (BLACKWILL; HARRIS, 2016, p. 20) no que também acompanhou Troxell (2018). Para esses autores, a cibernética é um desses instrumentos: “Entre os domínios que afetam a competição geopolítica, os que mais se destacam são os da informação, ciberespaço e economia.” (TROXELL, 2018, p. 24). Isso se daria, segundo ainda esses autores, tendo em vista as possibilidades advindas deste recurso, que permite, por exemplo, confrontar ou prejudicar os Estados Unidos e sua respectiva primazia militar sem precisar declarar uma guerra.

Constatamos que a forma como está sendo conduzido o setor estratégico da cibernética no Brasil desafia algumas dessas teorias e confirma, ainda que parcialmente, outras. A Política Nacional de Defesa (2012), por exemplo, logo em seu segundo capítulo, ratifica preceitos do realismo de poder, que enxerga a segurança em sua forma tradicional, o que condiz com o realismo conservador de Huntington (1996 [1957]), pautada no vínculo Estado-território de Westfália, no poder de coerção, legal e legítimo, de formulação *weberiana*, e na diferença de atuação e de amplitude deste poder no ambiente interno e externo, segundo a concepção *hobbesiana*. Como pano de fundo de tudo isso, há a possibilidade da guerra interestatal como continuação da política (CLAUSEWITZ, 1976 [1832]):

> 2. O ESTADO, A SEGURANÇA E A DEFESA
>
> 2.1. O Estado tem como pressupostos básicos território, povo, leis e governo próprios e independência nas relações externas. Ele detém o monopólio legítimo dos meios de coerção para fazer valer a lei e a ordem, estabelecidas democraticamente, provendo, também, a segurança. A defesa externa é a destinação precípua das Forças Armadas.
>
> 2.2. A segurança é tradicionalmente vista somente do ângulo da confrontação entre nações, ou seja, a proteção contra ameaças de outras comunidades políticas ou, mais simplesmente, a defesa externa. (BRASIL, 2012, p. 13)

Todavia, essa mesma Política também considera as perspectivas abordadas pela teoria Liberal das RI e pelos Estudos de Segurança[32], como o conceito de interdependência complexa

[32] E pela Escola Inglesa, consoante Hedley Bull (2002 [1977]), quando tenta conciliar as características do sistema internacional (SI) com os acontecimentos históricos, indicando a existência simultânea de uma “Sociedade Anárquica”, que possui, ao mesmo tempo, valores e objetivos em comum, como liberdade, paz, desejo de

(KEOHANE; NYE, 2001 [1977]) e o reconhecimento da ampliação do conceito de segurança (BUZAN *et al*., 1998), incluindo novos setores, além da agenda político-militar, e outros atores, e não apenas o Estado. Ainda, corroborando esse entendimento, contempla a necessidade de medidas estratégicas, a fim de prevenção ou de defesa para essas novas demandas:

> 2.2 [...] À medida que as sociedades se desenvolveram e que se **aprofundou a interdependência** entre os Estados, **novas exigências foram agregadas**.
>
> **Preservar a segurança requer medidas de largo espectro, envolvendo, além da defesa externa**: a defesa civil, a segurança pública e as políticas econômica, social, educacional, científico-tecnológica, ambiental, de saúde, industrial. Enfim, várias ações, muitas das quais não implicam qualquer envolvimento das Forças Armadas.
>
> Cabe considerar que **a segurança pode ser enfocada a partir do indivíduo, da sociedade e do Estado**, do que resultam definições com diferentes perspectivas. (BRASIL, 2012, p. 13, **grifo nosso**)

Ainda com relação aos documentos de Defesa brasileiros, nesses fica clara a preocupação constante do Estado em fomentar ações que relacionem Defesa com o Desenvolvimento, portanto que vão além das críticas que as correntes não realistas fazem a esta, no tocante à divisão da agenda estatal entre alta e baixa política, por enquadrarem no *status* desta última as questões de natureza econômica. Nesse aspecto, a PND e a END parecem ir além:

> A Política Nacional de Defesa (PND) é o documento condicionante de mais alto nível do planejamento de ações destinadas à defesa nacional coordenadas pelo Ministério da Defesa. [...] **Esta Política pressupõe que a defesa do País é inseparável do seu desenvolvimento**, fornecendo-lhe o indispensável escudo. A intensificação da projeção do Brasil no concerto das nações e sua maior inserção em processos decisórios internacionais associam-se ao modelo de defesa proposto nos termos expostos a seguir. (BRASIL, 2012a, p. 11, **grifo nosso**)
>
> **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, 2012b, p. 43, **grifo nosso**)

Esse ponto é importante, uma vez que, no plano global e histórico, considerando ações relacionadas ao ciberespaço e ao poder advindo de seu uso, percebemos que a separação

---

prosperidade e de cooperação, mas que funciona sob a ausência de uma autoridade, legal e legítima, capaz de impor direção única a todo o sistema internacional (SI), o que justifica a preocupação com a segurança.

Estado/capital não parece tão enfática, no que diz respeito ao desenvolvimento de tecnologias que fomentam a implementação desse recurso de poder, inclusive na origem da sua própria estrutura. Assim, quanto à cibernética, desde esforços norte-americanos, datados ainda da II GM e de durante a Guerra Fria, aos empreendimentos brasileiros atuais – estes pelo menos em tentativa –, a relação Estado-capital se apresentou bastante necessária e sob uma sistemática que passa pelo envolvimento, ou pela busca do envolvimento, da indústria, da burocracia e da academia, o que se denominou complexo industrial-militar-acadêmico (MEDEIROS, 2004; MORAES, 2004; BRUSTOLIN, 2014)[33] ou, mais atualmente, o que é enquadrado na concepção de "sistema da tríplice hélice" (ETZKOWITZ; DZISAH, 2008; MENDONÇA; LIMA; SOUZA, 2008; ÁLVARES, 2016) [34]. A busca, ao que tudo indica, está mais propensa na direção de se conquistar, ou de se ampliar, a capacidade de coerção e o acúmulo de riqueza, porém respeitando capacidades e vulnerabilidades consequentes tanto da política interna quanto do posicionamento dos atores no SI. As políticas públicas de Defesa do país, no recorte temporal desta pesquisa, indicam ir nessa direção, pelo menos em suas intenções.

Junto a esse debate relacionado a teorias de RI e à política de Defesa brasileira, chamou nossa atenção, também, a condicionante geográfica inferida dos documentos e das práticas. A END (2008), por exemplo, trouxe em diversas passagens a preocupação com a manutenção da integridade territorial, com destaque à região amazônica e à faixa de fronteira, pelo distanciamento dos principais centros político-administrativos e econômicos do país, e pelo enorme potencial que apresenta esse espaço, e ao que se denominou Amazônia Azul, porção do Oceano Atlântico adjacente ao litoral brasileiro, que inclui o mar territorial, a zona contígua, a Zona Econômica Exclusiva (ZEE) e sua versão estendida, conforme apresentamos no capítulo anterior. Com relação a todas essas considerações, há movimentos da burocracia nacional no sentido de aumento de capacidade de coerção e, por sua vez, de garantia de recursos estratégicos, a partir da ampliação de monitoramento e controle, como veremos especificamente nos capítulos seguintes. Isso demonstra que, seja na condução da política ou da economia, ou em ambas, em conjunto e mutuamente integradas, estratégias estatais levam em conta seu

[33] Apesar de não utilizar do termo "complexo industrial-militar-acadêmico", podemos inferir em Mazzucato esse mesmo modelo, praticado pelos Estados Unidos a partir da II GM (MAZZUCATO, 2014).

[34] Além desses autores, as políticas públicas de Defesa no Brasil que possuem relação com o desenvolvimento tecnológico tratam explicitamente esse sistema com esta denominação. Ver: Sisdia – Sistema de Defesa, Indústria e Academia de Inovação. Sistema criado em 21 dez. 2016, pela Portaria 1.701, do Comandante do Exército. Idêntica denominação é dada pelo Escritório de Projetos do Exército (Epex), órgão que foi implantado em 10 set. 2012, a partir da estrutura da Assessoria Especial de Gestão e Projetos (AEGP), criada em 7 abr. 2010. No capítulo seguinte tratamos mais especificamente desses órgãos, respectivas funções e estratégias. Desde já, adiantamos que estão sendo cruciais na tentativa de condução do setor cibernético dentro da concepção de geração de *spin offs* ou *spillovers* (externalidades).

componente geográfico da localização, absoluta e relativa, da extensão da superfície e das demais características naturais, e procuram, via tecnologia, tanto aumentar a capacidade de controle sobre seu território, quanto captar riqueza, a partir dos recursos territoriais, ou da tecnologia criada para a coerção. Nesse sentido é a definição atribuída por Medeiros Filho (2010) à geopolítica:

> Entendemos geopolítica como campo do saber voltado para a produção de políticas territoriais a partir da análise de fatores geográficos. Na sua linguagem clássica, sob uma perspectiva realista e *hobbesiana*, a geopolítica é entendida como um instrumento de poder dos Estados. Sob essa linguagem, os aspectos naturais (posição, recursos minerais, clima etc.) e demográficos (densidade, distribuição etc.) recebem grande destaque. Mais recentemente a geopolítica tem sido desenvolvida a partir de uma abordagem multidimensional de poder, que procura considerar novos atores nas relações entre unidades políticas. (MEDEIROS FILHO, 2010, p. 13)

Ao que nos parece, esse pensamento vai muito ao encontro das formulações de William Petty, em meados do século XVII, quando preocupado com a Inglaterra e sua geografia em face do SI. Porém, essa abordagem de teor mais empírico, consta nos capítulos seguintes. Partimos agora para definição sobre o que entendemos por teoria.

2.1 O QUE ENTENDEMOS POR TEORIA: LANÇANDO REDES SOBRE A REALIDADE

Antes de iniciarmos com as considerações acerca de algumas teorias de RI em face do poder cibernético e do ciberespaço, como anunciamos no título do capítulo, pretendemos definir o que entendemos por teoria.

Segundo Van Evera (1997), teoria é uma construção geral que descreve e explana as causas e efeitos de classes de fenômenos. Por sua vez, J. C. Köche indica que: "A busca da compreensão e de explicações universais cada vez mais abrangentes a respeito da realidade, conduzida por um processo de investigação científica, pode conduzir à formulação de leis e teorias." (KÖCHE, 1997, p. 89). Para Karl Popper, "teorias científicas são enunciados universais [...]. As teorias são redes lançadas para capturar aquilo que denominamos 'o mundo': para racionalizá-lo, explicá-lo, dominá-lo. Nossos esforços são no sentido de tornar as malhas da rede cada vez mais estreitas." (POPPER, 2016 [1975], pp. 53)[35].

[35] Essa mesma citação de Karl Popper também pode ser encontrada em José Carlos Köche (1997, p. 92) e em José D'Assumpção Barros (2011, p. 62).

De acordo com Stephen Hawking, uma boa teoria deve satisfazer a dois requisitos: precisa descrever com precisão um número razoável de observações, com base em um modelo que contenha poucos elementos arbitrários; e deve prever com boa margem de definição resultados de observações futuras (HAWKING, 1994 [1988]). Para Samuel Huntington, compreensão exige teorização. Teoria exige abstração, que, por sua vez, exige simplificação e ordenamento da realidade (HUNTINGTON, 1996). Nesse sentido, aponta Van Evera (1997) que uma teoria precisa de pelo menos sete atributos essenciais: amplo poder explanatório; ser simplificada; satisfazer a curiosidade; ter estrutura clara; ser testável; explicar um fenômeno importante, e ter riqueza prescritiva.

Assim sendo, inseridos em todas essas exposições, acerca do entendimento do que é uma teoria, de variadas fontes e campos do saber, podemos inferir conclusões nas seguintes direções: 1) nenhuma teoria consegue explicar totalmente os fenômenos, sobretudo os de natureza humana/social. Pelo contrário, diz Köche: "teorias nunca atingem a totalidade dos aspectos dos fenômenos da realidade" (KÖCHE, 1997, p. 92); 2) a teoria busca a explicação de um fenômeno por meio de sistematização, seja de dados quantitativos ou qualitativos, ou de ambos; 3) a partir da capacidade explicativa torna-se possível prever fenômenos, que, por exemplo, podem ser controlados. Esse ponto, para os atores do sistema interestatal, é importantíssimo, daí a necessidade de "jogar redes cada vez mais estreitas" sobre os fenômenos estudados. Portanto, admitimos tentar ir além do behaviorismo ou positivismo, e da abordagem clássica, histórica, reconhecendo as possíveis imperfeições de um estudo científico na área das relações internacionais, mas buscando criar padrões de comportamento dos atores no SI e respectivos condicionantes[36], sobretudo os de ordem estruturais. Tudo isso para permitir uma melhor compreensão de nosso objeto de estudo.

Por fim, no que diz respeito às teorias de RI especificamente, cabe frisar que nem sempre o enquadramento feito pelos acadêmicos e internacionalistas acerca da visão dos autores corresponde, explicitamente, à visão assumida por estes. O que percebemos é que o enquadramento ou a classificação feita significa, *a priori*, uma tentativa de sistematizar as obras e pensamentos da literatura desse ramo científico e, em não poucas ocasiões, de outros além da RI, fruto até mesmo de posições ideológicas, assumidas ou não. Nesse sentido, notamos claramente a necessidade de uma ótica interdisciplinar e holística para este campo do saber

[36] Aqui tivemos o cuidado de não colocar o termo "determinantes", pois apesar de reconhecermos algumas estruturas do sistema como reais influenciadoras das relações humanas, como é o caso da geografia (KAPLAN, 2013; MARSHALL, 2018), acreditamos que a tecnologia tem o poder de superá-las, mas não sem as levar em conta, e uma dessas tecnologias é, justamente, a cibernética, que traz a informação, um elemento capaz de superar estruturas antes mesmo de ser convertida à forma digital.

(BARROS, 2011), além da tentativa de afastamento de posições pré-formuladas, pois, apesar das dificuldades e da complexidade advindas desse esforço, derivadas da própria condição humana, uma visão unifocal pode conduzir a formulações míopes da realidade e, portanto, inócuas.

Partimos agora para o resultado da leitura, interpretação e análise de teorias de RI e sua relação com o objeto desta tese. Decidimos iniciar pela Teoria Liberal em obediência: 1) à cronologia da sistematização da própria RI como campo científico, que se deu logo após a I Guerra Mundial; 2) como contraponto à exposição feita no capítulo anterior, sob a ótica geopolítica, impregnada, portanto, do viés realista. Na sequência há: a) um complemento, com o objetivo de sistematização, do Realismo ou Realismo de Poder, que surgiu como paradigma para contrapor às formulações da Liberal, e que persiste até hoje; b) a Economia Política Internacional. Por fim, abordamos algumas implicações dessas reflexões para o campo de estudo acerca do desenvolvimento dos Estados.

2.2 SOBRE A TEORIA LIBERAL E SUA NOVA ROUPAGEM

2.2.1 Origem da teoria e principais expoentes

Na teoria liberal, em sua fase idealista ou utópica, a recém-criada disciplina de Relações Internacionais foi buscar seus primeiros embasamentos. A primeira cátedra, criada em 1919, na Universidade de Wales, tinha como objetivo maior compreender as causas dos conflitos, sobretudo os de natureza bélica, e evitá-los. Isso se deu tendo em vista a I Guerra Mundial e suas consequências para o continente europeu. O sentimento era de que os resultados da guerra não tinham sido bons para nenhuma das partes contendoras daquele continente.

A literatura especializada nas RI foi buscar no pensamento político de John Locke, de Montesquieu, de J. Bentham, de J. Stuart Mill e de I. Kant, e no econômico de Adam Smith e D. Ricardo, por exemplo, respostas para a pergunta inicial sobre as causas dos conflitos e os possíveis meios de prevenção. Na história, o ponto de partida referenciado foram as Revoluções Liberais (Gloriosa – 1688/1689; Americana – 1776; Francesa – 1789) e as consequências daí derivadas, incluindo a ascensão da classe burguesa, a difusão das ideias iluministas e a descentralização do poder absolutista, via democracia e autodeterminação dos povos. Este ponto, por sinal, é importante, pois tornou-se uma constante nos pensadores que seguem esta escola, ao considerarem a pluralidade de atores e os conflitos internos dos Estados na

consecução de suas políticas interna e externa, e na consequente formulação de um “interesse nacional”.

2.2.2 Conceitos, premissas e características

Inicialmente, o foco principal para se compreender a guerra foi dado à natureza humana. Na visão liberal, em geral, o homem é bom, necessitando apenas de boas leis para coibir possíveis desvios. Por isso foi atribuída muita importância às instituições, formais e informais.

Da esquerda para a direita, a lógica inserida na Figura 2.1 busca representar, de forma sintética, as principais premissas do pensamento liberal, em suas várias denominações ou classificações, como trouxe Pecequilo (2004), Sarfati (2005), Silva e Gonçalves (2005), Carvalho (2007), Jackson e Sorensen (2007; 2018), por exemplo, que por sua vez utilizaram como suporte as ideias contidas no pensamento de I. Kant e sua “À Paz Perpétua” (2008 [1795]), de W. Wilson e seus “Quatorze Pontos” (1918), de J. Nye e R. Keohane e seu “Poder e Interdependência” (2001 [1977]), de M. Doyle (1983) e respectiva visão sobre o relacionamento entre as democracias liberais no SI, e de R. Rosecrance e sua tese a respeito dos Estados comerciantes (1986).

Figura 2.1: Lógica do pensamento liberal (síntese)

NATUREZA HUMANA BOA	RAZÃO/ RACIONALIDADE/ LIVRE ARBÍTRIO	COOPERAÇÃO	COMÉRCIO	INSTITUIÇÕES (DIREITO, REGRAS, REGIMES E ORGANISMOS INTERNACIONAIS)	- SEGURANÇA COLETIVA - LIBERDADE - PROGRESSO - PAZ

Fonte: o autor.

Em todas as classificações de proposição liberal encontramos, em maior ou menor grau, essas variáveis elencadas na Figura 2.1. O que vai diferenciá-las é a precedência de uma em relação às demais. Isso significa, no campo metodológico, que a discussão ocorre na definição e (ou) constatação da variável independente e, a partir desta, das intervenientes e das

dependentes. Contudo, o destaque para a natureza humana deve ser observado, em que pese não constar de forma explícita nos textos de liberais do pós-II GM. Isso ocorreu, até de certa forma justificada, tendo em vista o fracasso da denominada vertente idealista, utópica, ou do idealismo *wilsoniano*, de explicar, e de propor, soluções para se evitar o conflito, conforme diagnosticado por E. Carr (2001 [1939]).

É sob a ótica de uma natureza humana boa e racional, que se alcança uma consequente cooperação voltada para o desenvolvimento, via comércio, preferencialmente sem barreiras, eis que estas, frequentemente, levam a conflitos. Dessa forma, questões relativas à segurança e, portanto, à defesa, não precisariam ocupar um ponto mais alto da agenda (*high politics*). Pelo contrário, são as regras, os regimes e as instituições em comum, fruto de um maior relacionamento entre os atores do SI, que permitirão o maior desenvolvimento do comércio e, por conseguinte, o alcance do progresso, o que conduz, logicamente, à paz, segundo os liberais. A segurança, nesse caso, deixa de ser pensada de maneira unilateral para ser coletiva, uma vez que há valores, até mesmo interesses comuns, regras, e uma opinião pública que fomentam e passam a exigir transparência e permitir o aumento da confiança nas relações entre os Estados.

Por falar em Estados, os mais atentos notaram que este ator não consta da Figura 2.1. Isso ocorreu, tendo em vista ser o Estado, para essa escola de pensamento – pelo menos por meio do discurso e de alguns elementos textuais – apenas um meio para permitir o funcionamento daquelas premissas, portanto sendo mais uma instituição garantidora, e não um possível obstáculo. É no indivíduo e em suas representações político-sociais, que visam ao progresso, o foco. Nesse sentido, para Moravcsik, na visão liberal o Estado, no mundo contemporâneo, funciona como representante dos interesses políticos domésticos, e não como ator fundamental (MORAVCSIK, 1997 *apud* SARFATI, 2005, p. 105). [37]

Embora englobando as variáveis acima listadas e a respectiva lógica explicativa, também devemos chamar atenção para a observação feita por Pecequilo (2004), no tocante, em uma direção, ao grau de utopia, ou, de outra, ao pragmatismo inferido a partir da leitura de autores e de conceitos tido como liberais. Em uma escala de gradação quanto ao pragmatismo, entendido este como uma tentativa de trazer "mais rigor às vertentes liberais, de forma que possam se converter em uma alternativa factível ao realismo" (PECEQUILO, 2004, p. 149), o liberalismo institucional ou neoliberalismo ou, ainda, o paradigma da interdependência, acatou,

[37] Temos ciência do risco de simplificação ou reducionismo que esse esforço de entendimento pode nos conduzir, uma vez que cada autor tinha um contexto e, por conseguinte, problemas, cenários e instrumentos distintos de investigação. Contudo pensamos ser interessante essa sistematização, na medida em que encontramos traços e ideias comuns nas teses liberais, da mesma forma que nas outas teorias abordadas adiante neste trabalho.

parcialmente, as premissas realistas de: 1) o Estado ser o ator principal do sistema, que, por sua vez, 2) é anárquico. Essa vertente retira o foco das discussões acerca da natureza humana, da ética e do "natural" espírito de cooperação, como abordados pelo idealismo, para a necessidade das instituições e do aprofundamento desses mecanismos no sistema, a fim de manutenção de uma certa ordem. Sob essa ótica, e com essa finalidade, parte da escola liberal, representada, por exemplo, por J. Nye e R. Keohane, procura no conceito de *interdependência complexa* cunhar uma solução para os impasses explicativos até então entre a teoria e a realidade. Sobre esse conceito, podemos entendê-lo como

> o resultado da multiplicação das interconexões globais e da aceleração de fluxos financeiros, demográficos, de bens, de serviços e de informações, com operadores extremamente variados: organizações intergovernamentais, multinacionais, organizações não-governamentais, sociedade civil, dentre outros, os quais passam a ganhar mais espaço nas decisões e discussões internacionais, e o Estado deixa de ter o único papel relevante nas relações internacionais, embora ainda proeminente. (GONÇALVES, 2008, p. 71)

Cabe ainda destacar que apesar de muito utilizado na tentativa de explicar os acontecimentos derivados do processo de globalização em sua nova fase pós-Guerra Fria, o conceito de interdependência pode ser remontado aos escritos de Norman Angell, em "A Grande Ilusão" (1910). Para José Paradiso, no Prefácio da referida obra:

> Ao lado das circunstâncias políticas, mas não de forma independente, produzia-se uma transformação no cenário econômico mundial, de facetas variadas e com múltiplas consequências. O que importava não eram as manifestações conjunturais – retração entre 1875 e 1895 e expansão de 1895 até as vésperas da Primeira Grande Guerra – ou o desempenho de novas potências industriais que reduziam as vantagens obtidas pela Inglaterra, mas sim o fenômeno que havia na sua base: uma nova fase do desenvolvimento capitalista materializada na aceleração do impulso integrador do mercado mundial, associado a impressionante progresso tecnológico. Qualquer que fosse o lugar ocupado pelo observador nesse processo, e a sua interpretação do mesmo, ninguém deixava de perceber a presença cada vez maior do poder financeiro e da grande empresa, e menos ainda a "diminuição do mundo" e a fenomenal **interdependência** dos seus componentes, produzida pelos avanços assombrosos nos transportes e nas comunicações. Como lembra Marc Ferro, no transcurso de poucas décadas "as distâncias diminuem, o mundo encolhe, os intercâmbios se multiplicam e a unidade dos hemisférios é afirmada.". (PARADISO, 2002, p. X)

Podemos inferir essa concepção nas palavras do próprio Angell:

> A **dependência recíproca das nações** foi invocada como argumento, pela primeira vez com uma certa seriedade, por Hume, em 1752, e trinta anos depois por Adam Smith, em uma obra de alcance muito maior. No entanto, no fim do século XVIII, seus argumentos evidentemente ainda não tinham

> influenciado a política geral – é o que transparece do tom dos debates políticos na Inglaterra, na época da revolução americana, e no continente, durante as guerras napoleônicas. Na realidade, a dependência vital dos Estados entre si era praticamente muito limitada, como se pode ver pelos resultados do sistema continental de Napoleão. (ANGELL, 2002 [1910], p. 120, **grifo nosso**)

Outro que se debruçou sobre o pensamento liberal e suas proposições acerca do sistema internacional foi Richard Rosecrance, que defendeu uma mudança no que diz respeito à necessidade do uso da força em face do uso do comércio para a manutenção da paz. Disse Rosecrance (1986) que o uso da força é menos vantajoso para os Estados e que o comércio é cada vez mais importante, sendo a principal razão para a mudança desse paradigma no pós-II GM a

> transformação da base econômica, associada à modernização. Em uma era anterior, a posse do território e amplos recursos naturais eram fundamentais para a grandiosidade. Atualmente, não é mais o caso e os ingredientes essenciais são uma força de trabalho altamente qualificada, o acesso à informação e o capital financeiro. (1986 *apud* JACKSON; SORENSEN, 2007, p. 160).

Contudo, mais uma vez, nesse aspecto, também verificamos ideia bastante similar contida na obra de Angell:

> Devo agora pedir que se recapitulem por um momento as proposições fundamentais da minha exposição, a saber: **as relações mútuas entre os Estados** se modificam rapidamente em resposta à rápida mudança das circunstâncias que as condicionam a uma mais ativa divisão do trabalho, que resulta da maior rapidez das comunicações; essa divisão do trabalho, cada vez mais acentuada, faz com que seja inevitável uma relação de **dependência recíproca** entre os que colaboram no empreendimento comum; **essa dependência recíproca implica, por sua vez, o declínio da força como fator ou recurso empregado nesse relacionamento; o referido declínio do uso da força debilita o significado do predomínio político e, em virtude da própria complexidade da divisão do trabalho, tende à cooperação universal, agrupando as diferentes unidades em uma ordem independente de toda divisão, de modo que as fronteiras políticas deixaram de demarcar fronteiras econômicas ou de coincidir com elas.** Por último, devido ao efeito cumulativo de todos esses fatores e como consequência direta dos mecanismos inerentes à sua coordenação, ocorre o que poderíamos chamar de "**reação telegráfica das finanças**" – a sensibilidade que permite ao organismo perceber rapidamente qualquer lesão de um dos seus componentes. (ANGELL, 2002 [1910], p. 130, **grifo nosso**)

No que confirma Paradiso, também no Prefácio da tradução brasileira desta obra:

> No passado, a conquista de um território trazia vantagens para o conquistador, mas as condições que tornavam isso possível eram agora obsoletas. Onde se localizava o essencial dessa mudança? Na crescente **interdependência das nações**, impulsionada pela divisão do trabalho e a **facilidade das**

> **comunicações**. A mútua subordinação vigente e perceptível através das fronteiras geográficas surgiu principalmente nos últimos quarenta anos, e o seu desenvolvimento e crescimento nesse período foi suficiente para engendrar uma tal relação de **dependência recíproca** entre as capitais do mundo que qualquer perturbação em Nova York repercute sob a forma de transtorno no comércio e nas finanças de Londres, e se essa perturbação é considerável, obriga os homens de negócios de Londres a cooperar com os de Nova York para resolver a crise, e não por razões de altruísmo. **Em suma, o telégrafo e o banco tornam o uso da força militar economicamente estéril**. (PARADISO, 2002, p. XXV, **grifo nosso**)

Chamamos atenção para uma passagem também na obra de Angell, tendo em vista considerarmos a sobreposição de ideias contidas em teses publicadas em tempo mais recente e utilizadas por pensadores que seguem a corrente liberal, como é o caso da crença na racionalidade humana e, a partir desta, o progresso, a interdependência, a necessidade de fomentar as trocas comerciais entre Estados (Estados comerciantes), e a diminuição da influência do poder militar, tudo em direção à paz e à estabilidade, e, principalmente, para os fins mais específicos desta pesquisa, o papel das comunicações nessa relação de causa e efeito, embora aí inserido como simples dado [38]. Assim disse Angell:

> Por isso as trocas precisam ser feitas, contando como coisa certa que uns e outros recebam oportunamente os frutos do seu trabalho; caso contrário, haverá para todos um risco iminente de fome. Essa troca e a confiança na retribuição do trabalho são, em sua forma mais simples, a expressão do **comércio** e do crédito; e a **dependência recíproca chegou a tal complexidade, graças ao desenvolvimento das comunicações em suas numerosas modalidades**, que qualquer perturbação em uma das operações afetará não só as entidades diretamente comprometidas, mas muitas outras, aparentemente isentas de qualquer relação com as primeiras. [...] A mútua subordinação vital aqui indicada, vigente e perceptível através das fronteiras geográficas, surgiu principalmente no curso dos últimos quarenta anos; e o seu desenvolvimento e crescimento nesse período têm sido suficientes para promover uma tal relação de **dependência recíproca** entre as capitais do mundo que qualquer perturbação em Nova York repercute como um transtorno no comércio e nas finanças de Londres; e se a perturbação é importante, obriga os homens de negócios de Londres a **cooperarem** com os de Nova York para debelar a crise não por altruísmo, mas como medida de proteção ao seu próprio **comércio**. **A complexidade das finanças modernas cria a dependência mútua** de Nova York e Londres, de Londres e Paris, e de Paris e Berlim em um grau sem precedentes na história. Essa dependência resulta do uso constante daqueles mecanismos da civilização, nascidos apenas ontem – **o correio rápido, a difusão instantânea das notícias comerciais e**

[38] Aqui expomos apenas alguns trechos da obra de Angell que trata da informação e das comunicações e seu respectivo poder. Há muito mais. Contudo, ressaltamos que esse recurso consta como um mero dado, algo "pré-existente", sem entrar nos detalhes de quem possuía os sistemas telegráficos e quem tinha capacidade de operá-los, assim como as respectivas externalidades daí derivadas. No capítulo 4 retomamos essa discussão, trazendo-a para a contemporaneidade e o domínio sobre os "novos telégrafos internacionais": os cabos submarinos de fibra ótica.

> **financeiras pelo telégrafo, e de modo geral o incrível progresso havido no campo das comunicações** – que colocou em contato íntimo as seis ou sete grandes capitais da Cristandade, ligando-as do ponto de vista financeiro muito mais estreitamente do que jamais estiveram associadas as principais cidades da Grã-Bretanha, no século passado e por muito tempo depois. [...] Uma autoridade financeira que já citei observa que essa **dependência** mútua e **complexa** do mundo moderno se produziu a despeito de nós mesmos [...]. (ANGELL, 2002 [1910], pp. 40-41, **grifo nosso**)
>
> Qual o verdadeiro prêmio da boa conduta entre os Estados? Não é senão **a complexa dependência recíproca**, em virtude da qual toda agressão injustificável por parte de um Estado contra outro recai sobre o agressor. (ANGELL, 2002 [1910], p. 241) [39]

Sob a roupagem e o contexto em que foi desenvolvido o conceito de interdependência complexa por Nye e Keohane (2001 [1977]), visando a uma resposta crível ao realismo, portanto realizando algumas adaptações a partir de Angell (2002 [1910]), podem ser extraídas quatro proposições básicas: 1) atores não-estatais são importantes na política internacional; 2) o Estado não é um ator unitário; 3) o Estado não é um ator racional; 4) a agenda da política é extensa. Essas proposições irão se confundir com o conceito de interdependência complexa desses autores, que traz três características principais: a) existência de múltiplos canais de comunicação e negociação; b) agenda múltipla; c) utilidade decrescente do uso da força.

Quanto aos múltiplos canais, além do uso de inúmeras mídias e de sistemas de comunicação de alcance global e com grande capilaridade, tem-se os diversos fóruns de discussão conduzidos em instituições formais, ou não, mas que interferem sobremaneira, segundo essa corrente, na decisão dos atores do sistema, diminuindo os efeitos da ausência de um governo central.

Com relação à agenda, esta se torna múltipla pelo surgimento de "novas" demandas por segurança, como a energética, a alimentar, a hídrica e a societal, que se relacionam com a segurança econômica. Para essas "inseguranças", nem sempre a separação da agenda em *high politics* e *low politics* torna possível a melhor solução.

Já no tocante à utilidade decrescente do uso da força, este se relaciona com a característica anterior, pois vem a ser uma das consequências: para essas novas demandas, nem sempre a força militar é a melhor opção de solução, ou nem mesmo é capaz de resolver.

Todavia, do visto até aqui, temos que concordar com Figueiredo acerca do liberalismo e sua nova roupagem:

---

[39] Sabemos que essa citação foi longa, no entanto acreditamos ser importante trazê-la na íntegra para mostrarmos literalmente, de forma fidedigna, o pensamento de seu autor e a permanência de seu uso em tempos mais recentes, embora sob nova roupagem.

> As teses neoliberais são, no fundamental, teses do liberalismo clássico. Elas têm sua especificidade e atualidade e refletem, portanto, as novas condições organizadoras do capital nos tempos contemporâneos. Mas mantêm, no que diz respeito aos princípios básicos que as sustentam, entrelaçados elos com o passado. (FIGUEIREDO, 2003, pp. 5-6)

Por fim, de tudo isso apresentado até aqui, podemos chegar a algumas conclusões, a fim de passarmos para a fase da relação entre a proposição teórica e o poder advindo da cibernética e de seu respectivo espaço.

2.2.3 Relação do pensamento (Neo)Liberal com o poder cibernético e com o ciberespaço

Das teorias estudadas ao longo da pesquisa, a liberal é a que traz de forma mais literal a preocupação com as mudanças do sistema a partir do uso das comunicações. Do ponto de vista do liberalismo isso não é uma surpresa, a partir do momento que sendo a cooperação, via instituições, uma das formas de se manter a estabilidade do sistema de Estados, as informações permitem, por exemplo, uma maior transparência das ações dos atores, diminuindo, assim, o dilema de segurança, a corrida armamentista e outras consequências da anarquia. Ocorre que, apesar de não mencionado explicitamente antes, a informação e a comunicação entre os atores do SI estão no núcleo do conceito de interdependência complexa. É a partir do conhecimento sobre as ações dos atores e a ampliação da cooperação que se torna possível o aprofundamento da interdependência e a manutenção da estabilidade do sistema, uma vez que, embora não importando o quanto se ganha, o jogo continuaria a ser positivo para os agentes envolvidos.

Para a corrente liberal, agora voltada para suas considerações acerca da pluralidade de atores no ambiente interno e externo ao Estado, o debate acerca do poder cibernético esbarra em conflitos tradicionais, como o da liberdade *versus* segurança. Para Deibert (2012), por exemplo, a forma de condução das políticas de segurança cibernética depende do tipo de governo do país. Canadá e Estados Unidos, para esse autor, conduzem o setor respeitando a liberdade em detrimento da segurança. Já para Estados totalitários, segundo Deibert (2012), a condução se dá por meio de censura, que no caso do ambiente cibernético ocorre por meio de criação de *firewalls* e de instrumentos lógicos que funcionam como barreiras de acesso a determinadas informações. [40]

[40] Ver casos do Paquistão e a tentativa de censura de vídeos do YouTube, em 2008 (SINGER; FRIEDMAN, 2017 [2014]); a discussão da China x *Google*, em 2010, e o encerramento do serviço de busca devido à censura chinesa (O Globo. 22 out. 2010 Disponível em: http://g1.globo.com/tecnologia/noticia/2010/10/china-revela-versao-propria-do-google-earth.html. Acesso em: 24 mai. 2019), e a exigência chinesa para que as empresas de Internet removessem as referências aos protestos de 1989, na Praça da paz Celestial (SINGER; FRIEDMAN, 2017 [2014]). Contudo, o conflito em torno de censura não é exclusividade de países tidos como autoritários. Um exemplo foi o

Também é importante refletir sobre um ponto que passa bem ao largo da discussão proposta pela corrente liberal e que foi justamente a pergunta do livro de Tim Wu (2006): "Quem controla a internet?". Embora o objeto da pergunta de Wu seja algo "novo" ou na escala do tempo presente, da conjuntura, dos acontecimentos, de Braudel (1965), o núcleo desse objeto continua sendo a informação e respectiva circulação. Quando Angell abordou a possibilidade que os meios de comunicação davam às finanças e, consequentemente, aos atores que a utilizavam, ele não mencionou acerca do controle dessa estrutura. Pelo contrário, isso aparece como mais um dado, algo considerado com certa naturalidade. Porém, como bem sabemos, isso não o é. Sigamos em frente.

2.3 SOB A TEORIA REALISTA OU O REALISMO DE PODER

No que diz respeito ao realismo de poder, muito já expomos, ainda que incidentalmente, sobre esta corrente das RI no capítulo anterior deste trabalho, sob a ótica da geopolítica e, por conseguinte, inserido na relação entre Estados preocupados com segurança. Contudo, como não sistematizamos esse pensamento naquele momento, pois a preocupação era demonstrar a panorâmica acerca do ciberespaço e de suas possibilidades para os atores do sistema, e as estratégias e ações/reações de alguns atores sobre esse tema, acreditamos por bem fazê-lo nessa parte, até para servir de contraponto à visão apresentada anteriormente e para auxiliar na elaboração da parte seguinte, que trata do tema sob a visão da Economia Política Internacional, sobretudo de natureza nacionalista.

2.3.1 Origem da teoria e principais expoentes

Praticamente concomitante ao surgimento da perspectiva liberal das RI, e em resposta a esta, a teoria realista serviu – e serve – como contraponto principal àquelas formulações. Os realistas denominados clássicos, como foi o caso de Edward Carr, buscaram em Tucídides,

caso entre a França e o Yahoo!, em 2000, que envolvia a proibição de leilões virtuais de objetos alusivos ao nazismo. Assim mencionou, à época, Ronaldo Soares, da Folha de São Paulo: "Uma batalha judicial entre entidades francesas de luta anti-racismo e o portal Yahoo! pode estabelecer um novo marco na história da Internet e fazer da França o primeiro país a delimitar "fronteiras" no ciberespaço." (Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft2008200012.htm. Acesso em: 24 mai. 2019.). Ver, ainda, Israel e a sua Cúpula de Ferro Digital (*Digital Iron Dome*), como bem expôs Alice Fortes (2018).

Maquiavel e Hobbes, dentre outros, suas reflexões e argumentos acerca da natureza do sistema internacional. Isso ocorreu tendo em vista os acontecimentos na Europa e em outras partes do sistema-mundo, que, para muitos observadores, iam na contramão dos postulados da corrente liberal, condensados, como vimos, no escrito de Angell (2002 [1910]) e nas ações do então presidente dos Estados Unidos, Woodrow Wilson. A questão fundante que pairava era, sobretudo, de ordem filosófica: a diferença entre o ser e o dever ser, entre o mundo de Aristóteles e o de Platão, entre a realidade e a utopia, como denominou Carr (2001 [1939]). Assim, os teóricos classificados como realistas constroem suas premissas, seus conceitos e sua visão de mundo de um ponto de partida diferente dos liberais, o que os leva, logicamente, a proposições distintas.

2.3.2 Conceitos, premissas e características

Da mesma forma que a corrente liberal, os realistas foram buscar suas fundamentações teóricas iniciais para os acontecimentos então vividos – e para toda a história – na natureza humana, considerando-a em sua essência má. Nesse sentido, "O homem é o lobo do homem" ou o estado de "guerra de todos contra todos", de Hobbes (1983 [1651]), é capaz de sintetizar esse pensamento. A partir daí, com o derivado medo e para controlar suas paixões, o homem precisa estar preparado, contando, em última análise, com suas próprias forças, com seus próprios recursos, para garantir sua sobrevivência.

No plano interno, a existência de uma instituição – o Estado – que contenha a capacidade de coerção e de coação dos indivíduos, via uma espécie de "contrato social", ainda que abstrato, favorece a ordem e a paz. Contudo, no plano externo, com a ausência de um ator universal com coerção legítima, a ordem e a consequente paz só podem ser mantidas, em última instância, por meio do seu próprio poder, o que caracteriza a autoajuda. Dessa forma, entre 1) a natureza humana perversa, 2) as possibilidades dos Estados e 3) a condição anárquica do sistema, os realistas tecem suas proposições, que orbitam por essas ideias, variando apenas a ênfase dada a cada uma.

Da esquerda para direita, na Fig. 2.2, a corrente realista traz a percepção negativa do ser humano, que o conduz ao medo das ações dos outros homens, isto é, à insegurança e a um possível conflito permanente como pano de fundo.

Visando a essas possibilidades, há necessidade de se buscar poder constantemente. Mais que isso, essa busca deve ser preferencialmente de forma relativa, considerando os demais atores, tendo em vista a ausência de poder central no SI. Derivado também dessa perspectiva,

o realismo de poder traz que, em última instância, o Estado deve contar com suas próprias capacidades, e não em alianças ou cooperação. Tudo isso é proposto tendo por fim a garantia da sobrevivência do Estado. Dessa forma, como inferimos da Figura 2.2, as liberdades individuais, as conquistas sociais, como o desenvolvimento e a paz, só são alcançados caso mobilizado todo esse circuito. Nesse instante, apreendemos que a necessidade de preparação para a guerra é uma constante no pensamento realista. E uma estratégia para esse cenário só pode ser planejada e conduzida por um ator que possua poder legal e legítimo para o uso da força, atribuído a ele e reconhecido pelo próprio SI, a partir de princípios, normas e regimes internacionais. E esse ator é o Estado. Nesse sentido, é desta instituição, e não do indivíduo como elaboram os liberais, que partem os fundamentos para conquistas, estatais, sociais e individuais.

Figura 2.2: Lógica do pensamento realista (síntese)

NATUREZA HUMANA MÁ	MEDO	(IN)SEGURANÇA	CONFLITO	- BUSCA DE PODER - AUTO-AJUDA	SOBREVIVÊNCIA DO ESTADO	- LIBERDADES - PROGRESSO - PAZ

Fonte: o autor.

2.3.3 Relação do pensamento realista com o poder cibernético e o ciberespaço

Como vimos no Capítulo 1, a reação dos Estados frente às possibilidades do ciberespaço resulta em empreendimentos que têm, como pano de fundo, uma visão realista das RI. As burocracias estatais, sobretudo as de natureza militar, têm como finalidade a função de se prepararem para a guerra. Por conseguinte, tratar a cibernética sob o viés de segurança e de defesa nacional é algo intrínseco desses corpos.

Por causa disso, inúmeros órgãos especializados em cibersegurança (e ciberguerra) foram criados, sejam em países tidos como liberais democráticos, sejam em totalitários ou de condução planificada. Para além de países, os organismos internacionais também se preparam

dessa forma, demonstrando que as possibilidades do instrumento cibernético no SI são bem reais.

Contudo, acreditamos que, *per si*, embora com alto grau de interação e coincidência entre teoria e mundo real, a vertente realista das RI não consegue responder plenamente à realidade ao confrontarmos seus postulados e as estratégias adotadas para o ciberespaço. Seguimos em frente em nossa investigação, procurando cercar de maneira mais completa possível nosso objeto e respectivas relações.

2.4 SOB A PERSPECTIVA DA EPI: ESTREITANDO AS MALHAS DA REDE

Se as teorias são "redes lançadas para capturar aquilo que denominamos 'o mundo'" (POPPER, 2016 [1975], p. 53), nosso esforço foi de tornar as malhas da rede cada vez mais estreitas. Para isso, deparamo-nos com preceitos e forma de enxergar e explicar o mundo por meio da Economia Política Internacional (EPI). Embora não vista como matriz teórica, tal qual o realismo e o liberalismo, o campo do conhecimento da EPI traz a possibilidade de abordagem de questões a partir da conjugação das relações de poder e da administração da riqueza em nível global.

2.4.1 Origem da teoria e principais expoentes

A EPI, como uma área do conhecimento, começou a ganhar espaço nos anos 1970 (FIORI, 2005; JACKSON, SORENSEN, 2007; COHEN, 2008), ao questionar as tradicionais visões do SI feitas pelas teorias realista e liberal, e suas respectivas tentativas de atualizações. A principal variável adicionada à análise do SI foi de ordem econômica, procurando detectar na sua estrutura e funcionamento explicações para as causas do subdesenvolvimento de algumas nações, do imperialismo de outras e da estabilidade/instabilidade sistêmica, que conduzia a conflitos. Em um artigo seminal, Susan Strange (1988) condenou a ausência de interação entre a economia e a política nas considerações e análises feitas a respeito da natureza do sistema internacional, o que ela denominou como exemplo de negligência mútua (STRANGE, 1988). Nesse sentido, podemos dizer que a EPI surgiu do casamento entre dois campos disciplinares, como apontou Barros: "Pode ocorrer ainda que dois campos de saber separados se agrupem para formar um só, fortalecendo-se mutuamente a partir de uma unidade." (BARROS, 2011, p. 26).

Enquanto o foco das RI eram as questões da guerra e da paz, considerando o fator político-militar preponderante, a EPI não teve espaço. Contudo, após a década de 1960, e não de forma teórica isolada, a discussão sobre a agenda das políticas externas estatais passou a pleitear maior *status* para assuntos econômicos e, a partir desses, uma maior probabilidade de manutenção da estabilidade do sistema. O conceito de interdependência complexa de Nye e Keohane (2001 [1977]), com suas características, considera a ampliação da agenda para além da divisão entre *high* e *low politics*. Todavia, esses autores mantiveram as premissas liberais e a crença no progresso de toda a humanidade, e a visão de que o papel do Estado na economia deveria ser o mínimo possível, algo já difundido desde Adam Smith (2003 [1776]), o que continuou sem ter respostas satisfatórias para a realidade.

Nesse contexto, o neomarxismo tomou a dianteira dessa área, buscando nas ferramentas conceituais e metodológicas propostas por Marx uma resposta àquelas inquietações. Dessa forma, a EPI de viés neomarxista transplantou a luta de classes do nível de análise do Estado para uma relação dessas unidades dentro do SI. A conclusão dessa lógica, em suma, é que o capitalismo necessita de um sistema configurado por países ricos e outros pobres, a partir do jogo das trocas desiguais, da apropriação do excedente econômico por poucos às custas de muitos, derivados da posição de cada país na Divisão Internacional do Trabalho (DIT). Para Jackson e Sorensen (2018), a EPI surgiu, assim, como o 3º grande debate das RI, tendo como questão principal "quem ganha o quê" na economia internacional e no sistema político. A economia mundial seria, nesse caso, um produto do imperialismo capitalista, e o vínculo de cooperação, ou de (inter)dependência, entre os Estados mais ricos levaria ao aprofundamento das vulnerabilidades dos menos desenvolvidos e à ampliação da assimetria.

Inseridas e acompanhando esse debate, podemos afirmar que há paralelamente uma EPI de viés liberal e outra realista (GILPIN, 2002 [1987]; GONÇALVES, 2005). A primeira, enfatizando o poder que a economia internacional tem na condução do SI, procura afastar a ideia da EPI marxista sobre a relação entre os países e o respectivo desenvolvimento-subdesenvolvimento. Para a corrente da EPI liberal, a especialização, a partir das vantagens comparativas de cada país, e as trocas comerciais não seriam instrumentos de imperialismo ou de hegemonia, mas sim de oportunidades de progresso, independentemente da posição que o país ocupa na DIT. Essa corrente teórica, assim, em muito se aproxima do neoliberalismo, ao considerar a natureza do sistema, com unidades político-econômicas desiguais, em termos de capacidade, mas de soberania formal, o que permitiria, pela estratégia de cada unidade, uma mobilidade vertical dentro do SI. Os exemplos de sucesso pinçados da história por essa corrente

indicam os casos da Alemanha e do Japão no pós-II GM e, mais recentemente, da Coreia do Sul, Cingapura e Taiwan.

No que diz respeito à EPI realista, ou mercantilista, ou nacionalista, conforme Gilpin (2002 [1987])[41], esta é a que mais se aproxima da intenção da estratégia de defesa brasileira, tanto no que diz respeito à forma como se aponta para a interrelação entre política e economia – defesa e desenvolvimento –, quanto na forma como enxerga o SI, e procura responder a este, tendo ciência de certa hierarquia entre as nações (países centrais, semiperiféricos e periféricos, ou desenvolvidos, em desenvolvimento e subdesenvolvidos) e das dificuldades daí derivadas, não obstante a soberania de natureza formal reconhecida.

Ao longo de nossa pesquisa, pelo que encontramos na bibliografia e nos casos históricos, detectamos realmente essa ausência de interação entre essas visões ou campos científicos, quando da análise das RI sobre o SI. Para os realistas, embora não assumam explicitamente em algumas ocasiões, o foco principal continua sendo na capacidade de poder, não só a partir da política, mas abrangendo também uma ênfase no fator militar (MEARSHIMER, 2007). Para os liberais, e neoliberais, estes já considerando o Estado como o ator mais importante das RI e o sistema anárquico (KEOHANE; NYE, 2001 [1977]), continuam a enfatizar a eficiência do comércio e os seus respectivos benefícios para todos os participantes do SI, desde que não dificultem a livre troca. Para uma parte dos teóricos marxistas, respeitando as proposições dos escritos de Karl Marx, o fator econômico continua a ser o preponderante no sistema, isto é, a variável independente e o Estado, em última instância, é mero instrumento de uma elite capitalista dominante. Contudo, nenhuma dessas correntes conseguiu abarcar a influência no sistema tendo em vista o relacionamento mútuo dos campos econômico e político. Em nossa investigação acerca do ciberespaço, ainda que de forma exploratória, encontramos muitas pistas que nos conduziu a uma realidade que abrange perfeitamente a interação entre esses dois campos do poder: a partir dos esforços em tecnologia, induzidos, conduzidos e mantidos pelo Estado, mas com participação de empresas privadas e da academia, tudo isso em resposta às demandas do SI, que dependem, por sua vez, de sua posição no mapa mundial.

[41] Na esteira dessa forma de pensamento e modo de ver o SI, ainda que sob outros rótulos ou denominações, podemos ainda citar: Paul Kennedy (1989), ao abordar a relação entre o campo militar e o econômico e suas implicações na ascensão e na queda das nações; Ho-Joon Chang (2004) e Pierre Deyon (2009), ao analisarem como alguns países europeus, com forte intervenção estatal na economia, tornaram-se potência, entre os séculos XVII e XIX, apesar do discurso diferente; Jomo K. S. e Erick Reinert (2016), investigando o desenvolvimento econômico, confrontaram teorias e realidade acerca desse processo e confirmaram a profunda relação histórica entre poder político e econômico, entre coerção e riqueza. Também, mais remoto, acreditamos na contribuição de William Petty (1996 [1690]) e sua Aritmética Política aplicada para a Inglaterra.

2.4.2 EPI, poder cibernético e ciberespaço

A configuração e o funcionamento do ciberespaço, em escala global, em muito se assemelha ao cenário proposto por Braudel (1987) para a esfera econômica, ratificado por Cecílio (2008): há, além da vida material, um nível formado pelo "jogo das trocas", em que as relações são comuns, visíveis, como a ponta de um *iceberg*, e que obedecem, ou pelo menos são submetidas, às leis do mercado, à ética e ao direito, e que os ganhos são normais. É nesse nível que tratamos em nosso cotidiano, assim como grande parte das empresas, das instituições e dos indivíduos, enfim, boa parte dos atores que compõem e operam no SI, como no caso do *e-commerce*.

No nível do "jogo das trocas" do ciberespaço há, inclusive, uma espécie de governança, que no caso do ciberespaço, por contemplar discussões acerca das categorias geográficas espaço e território, diz respeito às questões ligadas à soberania, à geopolítica, à regulação e ao controle jurídico da autoridade política estabelecida ou em exercício, referentes ao "poder para" e ao "poder sobre" (SILVA, 2008, p. 8), com participação de inúmeros atores, públicos e privados, civis e militares. Há regras, há coerção, há tipificação de crime nesse nível – o denominado cibercrime. Como exemplo, no Brasil, em 2014, foi aprovado o Marco Civil da *Internet*, que trouxe definições e comportamentos esperados dos usuários do ciberespaço, e punições para aqueles que não se sensibilizarem com os valores pré-definidos para o funcionamento desse ambiente. Antes mesmo, com a Lei n. 12.737, de 2012 (BRASIL, 2012c), conhecida como Lei Carolina Dieckman, que tratou dos delitos informáticos e a respectiva inclusão no Código Penal (Artigos 154-A e 154-B), registramos esforço nesse sentido.

Inicialmente no âmbito europeu, ainda no tocante a esse nível do ciberespaço, em 2001 foi adotada a Convenção de Budapeste, pelo Conselho Europeu, que também trouxe previsões de regulamentação do ciberespaço e os respectivos instrumentos de coerção para garantir seu funcionamento, voltados para crimes tais como violação de direitos autorais, confidencialidade, integridade e disponibilidade de sistemas informáticos, pornografia infantil e segurança de rede. A intenção dessa Convenção é ter alcance global, funcionando como tratado internacional.[42]

Porém, tudo isso corresponde à camada das "trocas", dos usuários normais, que perfazem, na verdade, a maioria no ciberespaço. Para esse nível, também é importante se

[42] De acordo com o Conselho Europeu, hoje são 63 países signatários que assinaram e ratificaram esse tratado, e mais 3 que assinaram, porém ainda não ratificaram. (Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Acesso em: 5 jun. 2019). O Brasil não aderiu por ter divergência principalmente à questão da propriedade intelectual e à possibilidade de acesso transfronteiriço, sem necessidade de autorização do país.

preparar em termos de segurança, vez que uma ação delituosa aí pode causar danos em várias escalas, desde o furto de senhas e desvios de valores em contas bancárias, e outros crimes digitais, à sabotagem em estruturas estratégicas de um país, de uma região ou de uma cidade. Nesse nível estão conectados, por exemplo, o funcionamento de usinas de eletricidade das várias matrizes energéticas, estão também as redes de telecomunicações, a de distribuição de água, a do controle do tráfego aéreo etc. Para prevenção dessas ações e respectivos danos, embora no "jogo das trocas", há realmente, hoje, uma espécie de governança, envolvendo a participação de vários segmentos da sociedade, nacional e internacional, democrático, equitativo e equilibrado, um modelo de "*multistakeholders*", como frisou Silva (2008), ou multilateral (LUCERO, 2011), ainda que aparentemente.

Sobre esse movimento na direção de uma governança, em 2005, a ONU, via UIT, promoveu discussão, na Cúpula Mundial sobre a Sociedade da Informação e Fórum Global da Internet, que se repetiu em 2015, uma 2ª fase, em Túnis, e que demonstra ter participação crescente em termos de quantidade de países membros, isto é, que aderiram às normas firmadas nesse encontro: de 52 países em 2015, para 71 em 2017. Ainda na ONU pode ser encontrada a Resolução n. 65/230 (2010), tratando de cibercrimes e a tentativa de uma universalização desse modelo. Essa discussão teve início, na ONU, desde a Resolução n. 56/183, de 2001, e na Cúpula Mundial sobre a Sociedade da Informação (CMSI) e Internet Fórum Global, em 2003.

Todavia, como em um cenário *braudeliano*, há no ciberespaço uma espécie de "profundeza", de forças dirigentes, em última instância, de toda a estrutura. Para Braudel, essa camada foi denominada como sendo a do verdadeiro capitalismo, na qual a luta por monopólios é constante e desobedece a qualquer mecanismo de mercado. Há uma porção do ciberespaço, que é, ainda hoje, verdadeiramente assim.

Apesar das inúmeras tentativas de maior abertura e de desconcentração do poder dos Estados Unidos no ciberespaço, este ator continua a deter a "chave geral" de todo o funcionamento da estrutura. Este poder está de posse da Corporação da Internet para Atribuição de Nomes e Números (Icann), que, por sua vez, encontra-se vinculada ao Departamento de Comércio dos Estados Unidos (DoC). A concentração geográfica dos servidores-raiz da Internet também demonstra a assimetria do ciberespaço: dos treze servidores-raiz existentes no mundo, dez se encontram nos Estados Unidos, um na Holanda, na Suécia e no Japão (SILVA, 2008, p. 91; SINGER; FRIEDMAN, 2017 [2014], p. 161; BRASIL, 2014, p. 36) (Ver Quadro 2.1 e Figura 2.3).

Não estamos, com isso, querendo contestar ou criticar negativamente esse fato, e sim, apenas, estamos expondo a realidade, uma constatação, para nos tornarmos aptos a compreender as ações e reações no ciberespaço.

Se, por um lado, esse monopólio ou excessivo poder de controle é visto como ruim para as pretensões de uma sociedade internacional, universal, pautada nos pilares da democracia liberal, por outro termina por funcionar como elemento garantidor do sistema, uma incumbência por sinal vinculada à própria natureza de um Estado *hegemon*, ou candidato a, responsável pelo fornecimento de bens públicos do SI (GILPIN, 2002 [1987]), dentre esses a segurança do fluxo informacional. Ainda nessa esteira, e buscando compreender os motivos que levam à continuidade de centralização do controle no ciberespaço, é fato também que os esforços políticos, econômicos e tecnológicos, por exemplo, foram dos Estados Unidos, inicialmente, o que lhe concede, não só pela história e pela força, mas também pelo direito, esse domínio. A questão, portanto, é, a partir dessa constatação, formular estratégias para essa realidade. Dessa forma, afastamos as pretensões liberais ou neoliberais das RI sobre uma possível governança modelo *multistakeholder* do ciberespaço ou sobre o que Michéle Silva denominou "infraestrutura lógica da Internet" (SILVA, 2008, p. 87).

Quadro 2.1: Lista de Servidores-raiz da Internet, Endereços de IP e Gerentes

NOME DO HOST (HOSTNAME)	ENDEREÇOS DE IP (IP ADDRESSES)	GERENTE (MANAGER)
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC (Holanda)
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN (Suécia)
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project (Japão)

Fonte: adaptado de IANNA[43].

[43] Disponível em: https://www.iana.org/domains/root/servers. Acesso em: 27 mar. 2019.

Figura 2.3: Servidores-raiz (*root servers*) da Internet[44]

Fonte: Silva (2008, p. 92).

A discussão conduzida até aqui tem, além do enfoque *braudeliano*, muita relação com o alerta que fez Friederich List a Alexander Hamilton sobre o funcionamento do SI:

> Prezado Senhor,
> Assim que os três componentes da economia política se revelam [a economia individual, a nacional e a da humanidade ou cosmopolítica], a ciência vem à luz e os erros da antiga teoria ficam claros.
> O objeto da economia individual é meramente obter as necessidades e confortos da vida. O objeto da economia da humanidade, ou, para expressar mais adequadamente, da *economia cosmopolítica*, é assegurar a toda raça humana a maior quantidade de necessidades e confortos da vida.
> A economia dos indivíduos e a economia da humanidade, como tratadas por Adam Smith, ensinam de que maneira um indivíduo cria, aumenta e consome riqueza em sociedade com outros indivíduos e como a indústria e a riqueza da humanidade influenciam a indústria e a riqueza dos indivíduos. A *Economia Nacional* ensina por que meios uma determinada nação, em sua situação particular, pode dirigir e regular a economia dos indivíduos e restringir a economia da humanidade, seja para impedir restrições estrangeiras e poder estrangeiro, ou para aumentar os poderes produtivos em seu próprio interior – ou, em outras palavras: como criar, na falta de um estado de direito, em todo o globo terrestre, um mundo em si mesmo, para crescer em poder e riqueza, para ser uma das mais poderosas, ricas e perfeitas nações da terra, sem restringir a economia dos indivíduos e a economia da humanidade mais do que o bem-estar dos povos permite. (PADULA, 2007, p. 174) [45]

[44] Cada letra corresponde à inicial (em negrito) do "Nome do Horst", conforme Quadro 2.1.
[45] Esta publicação na Revista Oikos, em 2007, contou com uma de *Nota Introdutória* de Raphael Padula, a título de contextualização da obra, do autor e da respectiva repercussão, e com transcrições, na íntegra, de cartas escritas

Assim, no "jogo das trocas" de Braudel ou na "economia individual e na cosmopolítica" de List, os valores e, portanto, as regras são bem diferentes das do nível do verdadeiro capitalismo ou do da "economia nacional", no qual, em última instância, a força prepondera. Sob esse alerta, podemos até concordar com os postulados de uma interdependência complexa promotora de progresso e estabilizadora do sistema, mas isso em um nível ou camada diferente de análise, e já contando a segurança do SI como um dado. Nisso também acompanhamos o que diagnosticou List:

> A. Smith trata da economia individual e da economia da humanidade. Ele ensina como um indivíduo cria, aumenta e consome riqueza em sociedade com outros indivíduos, e como a indústria e a riqueza da humanidade influenciam a indústria e a riqueza do indivíduo. Ele esqueceu completamente do que o título de seu livro "A Riqueza das Nações" prometeu tratar.
>
> Apesar disso, não sou de opinião, senhor, que o sistema de Adam Smith, do ponto de vista científico, seja desprovido de seus méritos. Ao contrário, creio que os princípios fundamentais da ciência só poderiam ser descobertos por seus pesquisadores da economia dos indivíduos e da humanidade. Seu erro consiste em não acrescentar a estes princípios gerais as modificações causadas pelo fracionamento da raça humana em corpos nacionais e em não adicionar exceções às regras ou membros médios às extremidades.
>
> Isto, senhor, é a teoria de Adam Smith e de seu discípulo, Dr. Cooper. Apenas em relação às duas extremidades da ciência, eles estão certos. Mas sua teoria não supre a paz nem a guerra; nem países particulares nem povos particulares; eles não reconhecem de nenhuma forma o fracionamento da raça humana em nações. (PADULA, 2007, pp. 171; 173; 175)

Dessa forma, a camada do ciberespaço relativa ao jogo das trocas ou da economia individual e da cosmopolítica, admite governança e ganhos diversos, entretanto, na camada do ciberespaço ligada às economias nacionais, ou melhor, aos Estados-economias nacionais, o modelo adere ao jogo da paz e da guerra e ao fracionamento geográfico territorial do sistema internacional.

Sobre isso, desde Angell (2002 [1910]), os teóricos que se utilizam das premissas liberais para tentar explicar o SI não comentam; passam bem ao largo. Nesse nível, e por isso, é que uma das conclusões liberais acerca das características do SI é o decréscimo da importância do uso da força. Isso é lógico, para esta forma de raciocinar e considerando apenas esses elementos: se um ator no SI possui pleno domínio sobre o fornecimento de um bem, de forma unilateral, não há necessidade, nem utilidade, do uso da força, pois essa capacidade de fornecer

---

por List a Hamilton, em 1827. Na Carta 1, List tratou do "equívoco fundamental na Teoria do Livre Comércio", formulada por Adam Smith.

bem público pode ser conduzida de forma branda, *soft*, ou inteligente, *smart*, porém funcionando como elemento de barganha para a garantia da ordem e de *status*. E nem se houver possível oponente com capacidade de sabotar o fornecimento desse bem, eis que ele também será afetado pelo dano, como bem alertou Angell (2002 [1910]) sobre a interligação entre New York, Londres e Paris, por exemplo, não obstante a aplicação de sanções uni ou multilaterais. É nesse nível ou camada que se localiza o discurso de Angell, de Smith e, como intitulou List, de seus discípulos.

No tocante às comunicações, no cenário vislumbrado por Angell, embora tendo como principal e inovadora infovia à época o telégrafo, e não o ciberespaço atual, que é digital, essas seriam verdadeiras ferramentas fomentadoras do comércio, da cooperação, do progresso e, por fim, da paz. O telégrafo permitiu, à época de Norman Angell, a manutenção de *status quo* dominante às potências, este não mais vinculado exclusiva ou prioritariamente à posse da terra ou colônias, e sim aos "territórios econômicos" (HILFERDING, 1985 [1910]) e a superação, ainda que parcial, do elemento geográfico "distância", porque diminuiu o tempo entre transmissão e recepção de mensagem. Como observou Sarfati, ao analisar o processo de globalização e os instrumentos que a impulsionam: "Veja que o telégrafo é muito mais revolucionário que a Internet, uma vez que seu advento cortava o lapso de comunicação transatlântico de vários meses para algumas horas, e a Internet corta esse lapso de horas para segundos." (SARFATI, 2005, p. 319).

Outro aspecto que chamou nossa atenção na pesquisa é que o controle do ciberespaço não ocorre diretamente por órgãos da burocracia dos Estados Unidos. Esta é acionada em última instância, para dirimir conflitos de nível "*hard*", como nos casos de designação de nomes e números de domínio globais (gTLDs) e nos domínios de 1º nível (ccTDLs) ou domínios de topo (*top level domain* – TLD's). Contudo, o que transparece na camada mais externa do *iceberg* é que tudo acontece via governança, mas não o é:

> [...] a arquitetura da rede revela uma geopolítica unilateral de governança da Internet, que não admite a representação soberana dos Estados nacionais. É como se houvesse uma recorrência de imperialismo americano no território das redes. (SILVA, 2008, p. 104)

Nesse aspecto, Hinderburgo Pires, professor do Instituto de Geografia da UERJ, manifestou-se perante o Senado Federal do Brasil:

> O ciberespaço continua sendo, na atualidade, um terreno estratégico de interesses econômicos e militares dos EUA e também um campo virtual de guerra, sobre o qual esses interesses devem manter um sistema militar

> permanente de segurança, de vigilância e de proteção de suas redes. (BRASIL, 2014, p. 36)

Embora tenha ocorrido a criação de uma entidade sem fins lucrativos, em 1998, a Corporação de Internet para Nomes Atribuídos (Icann), esta é vinculada – e supervisionada – pelo Departamento de Comércio (DoC) dos Estados Unidos. Essa mudança, que se deu pela pressão crescente por uma Internet comercial (LUCERO, 2011; SINGER; FRIEDMAN, 2017 [2014]), não foi súbita, nem muito menos desorganizada. A abertura para fins de exploração comercial, feita pela Casa Branca, por meio dos chamados "*White Papers*", poderia trazer mais ganhos para a própria manutenção do controle do SI, tanto por razões ligadas ao retorno econômico imediato, quanto via padronização de sistemas, protocolos e máquinas, o que também, por fim, acarreta maior retorno econômico e dependência tecnológica dos usuários em relação às empresas que lideram essa corrida. É aqui que entra a importância da VeriSign, Inc.; é aqui que verificamos uma forte relação entre Estado e empresa no aprofundamento da relação capitalista no SI ou pelo menos na manutenção desta. Interessante o registro de Singer e Friedman:

> E a despeito de esforços para globalizar a governança da Internet, muitos ainda veem a ICANN como um interesse cativo dos EUA. O controle de designar nomes e números ainda pertence, ostensivamente, ao Departamento de Comércio dos Estados Unidos, o qual delega à ICANN, por contrato renovável. Ou seja, os Estados Unidos retêm o controle geral, enquanto a função de gerenciamento é mantida por uma organização liderada pela indústria da área. Ambos têm manifesto interesse em manter o *status quo*. (SINGER; FRIEDMAN, 2017 [2014], p. 41)

A supervisão referida foi formulada via Memorando de Entendimento (MoU) do governo com a Icann, em contrato com a Autoridade de Números Atribuídos pela Internet (Iana) e um acordo de cooperação dos Estados Unidos com a empresa Verisign, Inc. E são esses documentos que revelam a autoridade política dos EUA sobre a raiz do DNS: "[...] os que afirmam que os EUA têm uma política de *laissez-faire* em relação à Internet provavelmente nunca leram o MoU." (SILVA, 2008, p. 78)[46].

Por esses documentos podemos inferir tanto quem possui o controle do arquivo de "zona raiz do DNS", quanto a forte relação entre o poder político e a esfera econômica. Em 2001, por exemplo, a VeriSign foi autorizada a ficar com o domínio ".com", que correspondia, à época, a cerca de 75% de todos os endereços da Internet (SILVA, 2008). O acordo do DoC com a

[46] Ver por exemplo a Emenda 3 ao MoU da Icann-DoC, de 25 de maio de 2001, alterando o MoU de 25 Nov 1998, atribuindo mais poder decisório ao governo norte-americano.

VeriSign também permite ao governo dos EUA a manutenção do controle do sistema, nisso implicando a capacidade de monitoramento, mesmo sendo via empresa privada.

Em 2013, um fato se tornou marcante para os que acompanhavam o debate acerca das possibilidades do ciberespaço e os atores inseridos nesse "jogo". Tratou-se do caso Snowden. Contratado da *Dell*, em 2012, e, posteriormente, no início de 2013, da *Booz Allen Hamilton*, empresas do ramo de informática, computação e comunicações, Snowden prestava serviço à Agência de Segurança Nacional (NSA) norte-americana, nesse período, no Centro Regional de Criptologia da NSA, em Oahu, perto de Honolulu, Hawaí (HARDING, 2014). A essa altura, Snowden já tinha informações e documentos suficientes que provariam a violação, por parte da NSA, da Constituição dos Estados Unidos, no que diz respeito à espionagem de seus próprios cidadãos em solo pátrio, e à Lei de Vigilância de Inteligência Estrangeira (FISA), de 1978. Tendo acesso às redes da intranet da NSA (NSANet) e da do *Government Communications Heardquarters* (GCHQ), a GCWiki, o parceiro britânico nessa empreitada, o analista da NSA constatou não só os acordos entre esses órgãos estatais, como também entre esses e um gigante da Internet, a Verizon, por meio do programa denominado PRISM. Por este programa, a NSA poderia ter acesso direto aos sistemas do Google, Facebook, Apple, Microsoft, Yahoo, dentre outros. Assim trouxe Harding, com base no material entregue por Snowden ao *The Guardian* e, posteriormente, ao *Washington Post*:

> Outro programa secreto tinha um logotipo que remetia ao clássico álbum dos anos 1970, Dark Side of the Moon, do Pink Floyd. Um triângulo branco dividia um feixe de luz em um espectro colorido. O nome do programa era PRISM. Snowden vazou uma apresentação em PowerPoint de 41 slides explicando a função do PRISM.
> Um slide enfatizava as datas em que as empresas de tecnologia do Vale do Silício haviam assumido o compromisso de se tornar parceiras corporativas da agência de espionagem. A primeira a fornecer o material foi a Microsoft. A data era 11 de setembro de 2007. Exatos seis anos após o 11 de setembro [...]. (HARDING, 2014, p. 163)

No Quadro 2.2 procuramos ilustrar empresas e datas de aceite em participar do programa PRISM:

Quadro 2.2 – Datas de Ingresso de Empresas no Programa PRISM

DATA	EMPRESA
Set 2007	Microsoft
Mar 2008	Yahoo
Jan 2009	Google
Jun 2009	Facebook
Dez 2009	PalTalk
Set 2010	YouTube
Fev 2011	Skype
Mar 2011	AOL
Out 2012	Apple

Fonte: elaborado pelo autor com base em Harding (2014, pp. 163-164).

Nas palavras de Edward Snowden, quando em entrevista a Glenn Greenwald, então colunista do jornal inglês *The Guardian*:

> O governo dos EUA coopta o poder corporativo norte-americano para seus próprios fins. Empresas como Google, Facebook, Apple e Microsoft estão fechadas com a NSA. [Elas] proporcionam à agência acesso direto aos *backends* de todos os sistemas que você usa para se comunicar, armazenar dados, guardar coisas na "nuvem", e até mesmo para simplesmente enviar uma mensagem de aniversário ou manter o registro de sua vida. Elas dão à NSA acesso direto, de modo que eles não precisam fazer triagem alguma, e assim não podem ser responsabilizados por nada. (HARDING, 2014, p. 164)[47]

Essa fala de Snowden pode ser ratificada pela solicitação que o general Keith Alexsander, diretor da NSA, fez ao Congresso Nacional, no sentido de colaboração das empresas civis e de isenção e inimputabilidade para essas, nos casos de algum vazamento de informação acerca do monitoramento ilícito (THE GUARDIAN, 2013; HARDING, 2014).

Os relatos de Snowden trouxeram mais possibilidades do domínio do ciberespaço: tratou-se da operação de codinome Upstream, também da NSA, mas com forte participação do GCHQ inglês. Aqui o ponto é a interceptação de cabos submarinos de fibra ótica. "Ele dá à NSA acesso direto aos cabos de fibra ótica que transportam dados da internet e telefone para, a partir de, e por todo os EUA" (HARDING, 2014, p. 165). Pelos slides expostos por Snowden

[47] Interessante que inferimos desta passagem ideia similar ao questionamento de Braudel, ao discorrer sobre o verdadeiro capitalismo: "Será necessário dizer que esses capitalistas, tanto no Islã quanto na cristandade, são os amigos do príncipe, aliados ou exploradores do Estado?" (BRAUDEL, 1987, p. 23).

acerca dessa operação, cabos interligados à América do Sul, à África Oriental e ao Oceano Índico eram exemplos de infovias que continham pontos de escuta da NSA.

O programa Prism e a operação Upstream eram utilizados de forma complementar. Segundo Snowden, por esses instrumentos,

> a NSA não se limita a coletar inteligência estrangeira. Recolhe todas as comunicações que transitam pelos EUA. Literalmente, não há nenhum ponto de entrada ou saída em qualquer lugar dos EUA continental por onde as comunicações possam circular sem ser monitoradas, coletadas e analisadas. (HARDING, 2013, pp. 166-167)

Em relatório oficial de 2009, emitido pelo inspetor geral da NSA e vazado por Snowden, é também atestado, por um lado, a capacidade norte-americana de espionagem ao redor do mundo e, por outro, a parceria existente entre o governo e entidades comerciais. Esse mesmo relatório indica o fato de os Estados Unidos funcionarem como o "*hub*" principal para todas as telecomunicações mundiais e de possuírem relações com mais de cem empresas nacionais norte-americanas, a partir da experiência da Segunda Guerra Mundial. Corrobora essas informações o Senado Federal brasileiro (BRASIL, 2014).

Algumas empresas envolvidas nesse caso se pronunciaram afirmando que não davam acesso direto a ninguém. A maioria disse que isso só acontecia quando recebiam ordem judicial, nesses casos específicos de um tribunal "secreto" formado, em 2006, estranhamente no âmbito da FISA, lei que serviria para proibir espionagem em solo norte-americano. No entanto, de um jeito ou de outro, isto é, voluntária, cooptada ou coercitivamente, o certo é que há parceria, ou possibilidade de, entre Estado e empresas privadas. Nesse aspecto, Dreifuss chamava atenção, no final do século XX:

> Espacialmente, a planetarização destaca a atualidade dos estados nacionais e a abrangência de sua atuação como pivôs político-estratégicos. De fato, as tendências de mundialização e de globalização são reforçadas, paradoxalmente, pela concomitante ação dos estados nacionais em apoio às suas corporações estratégicas, tanto no preparo, consolidação e expansão do próprio "sistema-espaço" nacional (sociedade e mercado), quanto no condicionamento – em perspectiva globalizante e mundializante – de outros países. Neste sentido, **as corporações estratégicas têm bandeira**. (DREIFUSS, 1997, p. 172, **grifo nosso**)

As iniciativas da NSA interceptaram escutas de vários líderes estrangeiros, dentre esses Angela Merkel, então chanceler alemã, Dilma Rousseff, presidente do Brasil[48], e Enrique Peña Nieto, presidente mexicano. Entre os alvos também constavam empresas privadas, como foi o caso da brasileira Petrobras, justamente no período de divulgação da descoberta de petróleo na camada de "Pré-Sal" e das possibilidades de riqueza daí advindas.

A relação entre Washington e empresas privadas não ocorre apenas na área de infraestrutura lógica e de rede da Internet. Na área dos sistemas, dos *softwares* e das máquinas, isso também se dá. O Estado norte-americano, conforme Paulo Cesar Brein, especialista brasileiro em segurança de TIC,

> possui um controle "branco" nas comunicações e em muitos softwares. Há informações que o governo americano possuiria senha de acesso a roteadores que estão espalhados no mundo. […] ninguém pode garantir que o governo americano não tenha uma senha que permita que ele acesse esse roteador, e a partir daí "sniffar"[49] tudo o que passa por ele. Há também informações que sistemas operacionais como Windows, por exemplo, quando vendidos para países inimigos, são fornecidos com algumas funcionalidades adicionais, que permitem o controle remoto de servidores. (BREIN, 2012 *apud* FERREIRA NETO, 2013, p. 121)

Quanto a essa declaração, José Almeida também alertou, em 2005, quando participou pelo Brasil do grupo de trabalho da ONU sobre segurança global dos sistemas de informações e de telecomunicações, que os representantes russos estavam bastante preocupados, pois:

> Em quase todos os computadores vendidos ao redor do mundo, o sistema operacional já instalado pela fábrica é o Windows. Somente a NSA, nem mesmo a Microsoft, possui o algoritmo de *backdoor*[50] do Windows. Segundo os russos, isso permite que a NSA acesse qualquer computador ligado à internet, direta ou indiretamente, o que traz grande segurança às forças dos EUA, no caso de uma ação cibernética. (ALMEIDA, 2011, p. 86-87)

Com o intuito de comprovarmos tais relatos, deparamo-nos com o *Communications Assistance for Law Enforcement Act* (Calea), baixado ainda em 1994, em vigor desde janeiro de 1995, e que traz como viés o monitoramento das operações de telecomunicações que

---

[48] O nome do programa que espionou a presidente Dilma Roussef e a Petrobras era *Blackpearl*. Já para Angela Merkel foi o *Boundless Informant* (HARDING, 2014).

[49] *"Sniffar"*, ou "farejar", no sentido empregado em redes de computadores é um procedimento que ocorre a partir do uso de uma ferramenta denominada *sniffer*, que permite a interceptação e o registro de tráfego de dados. A partir disso, há possibilidades como a captura de pacote, a decodificação e a análise do conteúdo, inclusive em tempo real.

[50] *Backdoor* – ou "porta dos fundos", considerada uma abertura na segurança que pode existir em um programa de computador ou no seu sistema operacional. A partir dela pode haver invasão do sistema para obtenção do controle da máquina ou para instalar vírus ou outros artefatos maliciosos, denominados *malware*.

envolvam uso de recursos digitais, como a *internet* banda larga. Somamos a isso, a exposição de Jonh Douglas Ruwell, do Centro Brasileiro de Perícia na área de segurança da informação, durante o II Seminário sobre Guerra Cibernética, na Academia Militar das Agulhas Negras, no dia 27 de abril de 2013, que confirmou a existência de tal ato legal e explicou seu funcionamento, que resulta na obrigatoriedade de instalação nas máquinas de uma "*backdoor*" para fins de possível vigilância (FERREIRA NETO, 2013).

Quanto a este fato, resolvemos fazer um teste em abril de 2018 para confirmar essa possibilidade. Adquirimos um pacote *Office*, fornecido pela empresa Microsoft. Tentamos instalar este pacote em um *notebook* de uso diário, para fins de trabalho e de estudo. Essa tentativa ocorreu de dentro da Academia Militar das Agulhas Negras (Aman), utilizando-nos de uma rede de acesso à Internet que passava pelo servidor gerenciado pela Divisão de Tecnologia e Segurança da Informação e Comunicações (DTSIC) dessa instituição de ensino.

Após três tentativas, sem êxito, contatamos a *Microsoft*, pelo número de telefone disponibilizado na embalagem do produto. Um funcionário daquela empresa, da área técnica, orientou-nos para nova tentativa, agora passo-a-passo, sob seu comando. A partir deste ponto, precisamos aceitar os termos que permitiu esse funcionário fazer o acesso remoto de nossa máquina. Todavia, por fim, também não conseguimos êxito de dentro da Aman.

Esse técnico, depois de certo tempo de análise, perguntou-nos se estávamos usando uma rede pública. Informamos onde estávamos e a origem de acesso à rede, que era disponibilizado pelo setor de SIC da Aman. Nesse momento ele pareceu concluir sobre o motivo que não permitiu a instalação do produto, nem mesmo na tentativa feita por ele: existia um bloqueio, um limite, uma "fronteira" ou, na linguagem de profissionais de TIC, um *firewall* entre a Internet e a rede interna da Aman. O funcionário da Microsoft nos pediu que fizéssemos uma nova tentativa a partir de outro local, que desse acesso por outra rede, que não a da Aman.

Chegamos em casa, no mesmo dia, e contatamos novamente o número fornecido pela empresa na embalagem do produto. Outro técnico nos atendeu e nos passou orientações quanto aos procedimentos. Também nos foi pedido autorização para acesso remoto de nossa máquina, agora utilizando-nos de nossa rede de acesso doméstica, fornecida por uma empresa privada do setor de telefonia, a Tim. De repente, nossa máquina começou a funcionar "sozinha", o cursor se movimentava, janelas que indicavam instalação eram abertas e fechadas "automaticamente", ou melhor, por controle remoto, de uma pessoa que não conhecíamos, mas que tinha capacidade de acessar todo conteúdo digital armazenado em nosso *notebook*.

As questões suscitadas a partir desse episódio nos levaram a uma série de possibilidades, e dúvidas: é possível acessar máquinas, via rede conectada à *Internet*, remotamente? Em todos

esses casos de acesso, é realmente necessário o pedido de autorização para acesso e manipulação da máquina e de seu conteúdo? É possível criar uma barreira, um *firewall* – no nível indivíduo ou no relacionamento indivíduo-empresas – ou uma "fronteira" do ciberespaço – no nível interestatal?

Especialistas de TIC e SIC da Aman nos informaram que o acesso remoto é possível, dependendo do nível de segurança e da respectiva credencial do agente. No caso da tentativa do técnico da *Microsoft* de acessar nosso computador pessoal via rede interna da Aman, este não conseguiu devido ao bloqueio "lógico" feito pela instituição, por questões de segurança e privacidade. Contudo, caso um agente seja credenciado em níveis mais elevados, a intrusão é possível, ainda que configure ilegalidade. Já em redes domésticas, em sua maioria com níveis de segurança menor, o acesso é possível com maior facilidade. Portanto, há possibilidade de se criar barreiras virtuais, limites, "fronteiras", no ciberespaço. Contudo, caso um agente tenha ferramentas de acesso, como as *backdoors*, ou outros instrumentos fornecidos pelas empresas de *hard* ou de *software*, ou mesmo pelo conhecimento em TIC e SIC (casos de *hacker* ou *cracker*, por exemplo), o acesso pode acontecer. A questão envolvendo a segurança nas infovias é um jogo constante.

Essas respostas nos levaram à compreensão do funcionamento de rede em um ambiente local e regional, mas também nos indicaram possibilidades na escala global, que convergem com nossa hipótese acerca da existência de um território-rede, em que há sim controle, incluindo aí a possibilidade de monitoramento, no ciberespaço, envolvendo desde o nível das relações individuais, como é o caso de *e-mails* e de acesso a redes sociais, como nas camadas dos negócios, nacionais ou internacionais, alcançando a possibilidade de uso na relação entre Estados, incluindo a guerra, nas mais variadas formas[51].

Também concluímos sobre a profunda relação entre Estado e capital e os fins estratégicos buscados na camada do verdadeiro capitalismo *braudeliano* ou da economia nacional de List, ainda que exista um nível de relacionamento que obedeça a valores, à ética e ao direito, a "camada" da economia de mercado ou da economia do indivíduo.

Assim, conseguimos compreender o funcionamento desse circuito, ao contrário do início da pesquisa, em que, ao fazermos a superposição de teorias que buscavam explicar o SI com a realidade, aquelas se encaixavam nesta, com argumentos persuasivos, aparentemente

[51] Um exemplo é a guerra denominada "híbrida", em que inúmeros e variados instrumentos são utilizados no conflito, podendo envolver desde ações convencionais nos espaços terrestre, marítimo e aéreo, quanto – e sobretudo – no espaço das informações, neste inserido o ciberespaço (rede sociais, *e-mails*, *fake news* etc.). Pode haver também uso de mercenários ou de forças subnacionais. Tudo isso em conjunto com operações psicológicas.

consistentes e convincentes, mas com falhas também desse mesmo porte e que não suportavam todos os fatos. Ocorre que esse circuito, ou melhor, podemos falar de dois circuitos, simultâneos, mútuos e interligados, acompanham as regras das camadas *braudelianas* ou da visão de List: na economia de mercado, ou na individual e cosmopolítica, os postulados e premissas liberais são válidas – há respeito ao direito, aos regimes, às instituições, como é o caso da UTI, da OMC, da ONU, dos comitês de governança etc., e há ganhos a partir do comércio, na qual os "Estados comerciantes" podem se valer do livre comércio de Smith e das vantagens comparativas de Ricardo, em relação a outros atores. Aqui também é onde "gira o *software*" do lado "Sociedade", do título da obra clássica de Hedley Bull (1992), no qual os valores são compartilhados, incluindo a aversão à guerra; aqui também serve a utilização do poder na forma branda ou inteligente de Nye (2012).

Todavia, há o circuito do verdadeiro capitalismo ou da economia nacional, em que as "regras" são diferentes e que às vezes o próprio *hegemon*, ou candidato a *hegemon*, as altera, a fim de sua manutenção de *status* de diretor do SI. É nessa aqui que o "jogo das guerras", e não o "das trocas", comanda. Aqui não há possibilidade de uso decrescente da força, pois os rivais nessa camada – aqueles com real capacidade – também possuem capacidade e possibilidade de utilização. Nesse circuito, o funcionamento é *hobbesiano*, é de soma zero, e é "anárquico", como o complemento do título da obra de Bull (1992). Mais uma vez recorremos a List:

> O objeto da economia deste corpo [economia da nação] é não somente a riqueza como na economia individual e cosmopolítica, mas o poder e a riqueza, porque a riqueza nacional é aumentada e assegurada pelo poder nacional, como o poder nacional é aumentado e garantido pela riqueza nacional. Seus princípios norteadores são, pois, não somente econômicos mas também políticos. Os indivíduos podem ser muito ricos; mas se a nação não possuir poder para protegê-los, ela e eles podem perder em um dia a riqueza que acumularam por eras, e seus direitos, liberdade e independência também. (PADULA, 2007, p. 176)[52]

É aqui, portanto, que se encaixam as ferramentas de análise proporcionadas pela EPI, considerando, mutuamente, poder e riqueza. Essa também é a direção apontada pela PND e pela END, conforme mostramos anteriormente.

[52] Aliás, essa passagem em List parece ter inspirado as políticas públicas de Defesa do País a partir de 2008. De se ver, como já exposto anteriormente, a Introdução da Estratégica Nacional de Defesa (2008) e da Política Nacional de Defesa (2012), quando menciona a relação Defesa-Desenvolvimento.

2.4.3 Poder, riqueza e desenvolvimento a partir do ciberespaço

No ciberespaço, a relação entre poder e riqueza pode ser inferida por um olhar mais atento no tocante à forma de criação e de difusão deste objeto. De origem no núcleo de defesa dos EUA e como projeto para responder às demandas do SI no pós-II GM, o principal ou o mais amplo ciberespaço, a Internet, foi concebida pela Arpa, agora Darpa, Agência de Projetos de Pesquisas Avançadas, vinculada ao Pentágono, criada em 1958, com a finalidade de evitar "surpresas tecnológicas, saltando à frente na pesquisa." (SINGER; FRIEDMAN, 2017 [2014], p. 27). Uma, ou a, surpresa a que se referia fora o lançamento da *Sputnik*, em 1957. Esse papel e essa relação entre governo, inovação tecnológica e setor privado também fora diagnosticado por Moraes (2004) e Medeiros (2004), a primeira pesquisa tratando especificamente do desenvolvimento do setor de telecomunicações nos Estados Unidos, sob o impulso estatal, e a segunda abordando o complexo militar-industrial-acadêmico. E essa relação é bem mais ampla, no sentido de envolver várias inovações. Como disse Mazzucato:

> O papel do engajamento militar para o desenvolvimento e o crescimento econômico não diferencia a história dos Estados Unidos da dos outros países modernos. Mas nos Estados Unidos a experiência do desenvolvimento tecnológico necessário para vencer guerras proporcionou grandes lições para aqueles que estão procurando melhorar as políticas de inovação. (MAZZUCATO, 2014, p. 110)

Assim continua essa autora, agora especificamente quanto ao papel da Darpa:

> O papel do Estado na Agência de Projetos de Pesquisa Avançada de Defesa (DARPA) vai muito além de mero financiamento em ciência básica. Trata-se de direcionar recursos para áreas e orientações específicas; trata-se de abrir novas janelas de oportunidades; intermediar as interações entre agentes públicos e privados envolvidos no desenvolvimento tecnológico, [...]. (MAZZUCATO, 2014, pp. 110-111)

Nesse sentido, aproveitando-se da *expertise* e da oportunidade apreendida da II GM, a Nasa também participou desse ambiente de colaboração, que obteve resultados muito positivos como computadores, jatos, energia nuclear civil, *lasers* e biotecnologia [53].

[53] Para Vernon Ruttan (2006), seis tecnologias merecem destaque dentro da relação entre guerra e crescimento econômico: a indústria de aviões, de energia nuclear, de computadores, de semicondutores, a aeroespacial e a *Internet*. Em outra vertente, abordando o papel do capitalismo monopolista, Paul Baran e Paul Sweezy (1966) chegam a conclusões bem similares, não com relação a essas tecnologias, mas no tocante à relação entre preparação para a guerra, desenvolvimento de tecnologias disruptivas, transbordamentos econômicos e existência de monopólios. Esses autores citaram como "invenções que marcaram época": a máquina a vapor, a estrada de ferro e o automóvel. Compreendendo o risco de anacronismo de nossa análise, certamente esses autores incluiriam as

O ponto a ser destacado aqui é o papel do Estado, que pode ser remontado a 1945, a partir do relatório de Vannevar Bush. Passava a ser incumbência do governo entender quais tecnologias ofereciam mais aplicações para fins militares e também comerciais (MAZZUCATO, 2014). Não foi à toa que a criação da Darpa em resposta à Sputnik possibilitou uma inflexão na direção de pesquisas para longo prazo, de preferência de tecnologias de uso dual, com possibilidades de uso para coerção e para lucros. Isso também gerou um ambiente propício para o surgimento de uma cultura de *spin-off*, como foi o caso da *Fairchild* Semicondutor e outras *start ups*, que aumentaram a concorrência por recursos do Estado para pesquisas (MAZZUCATO, 2014).

Assim, o que se aprendeu de Schumpeter (1997 [1911]) acerca do papel das inovações disruptivas e as consequentes ondas de crescimento econômico, é praticado nos Estados Unidos a partir das necessidades com fins de coerção no sistema, em ferramentas para a guerra.

A ideia da possibilidade de transbordamentos para além da política de defesa de um país surgiu ao nos depararmos em várias ocasiões e em fontes bibliográficas com a interligação Departamento de Defesa Norte-Americano (DoD) e *Massachusetts Institute of Technology* (M.I.T.). Nomes como Norbert Wiener, especificamente quanto à cibernética, e Vannevar Bush, de uma forma mais ampla, abrangendo todo o "complexo militar-industrial-acadêmico" dos Estados Unidos, tornaram-se comuns ao longo da investigação científica anterior, sobretudo a partir da eclosão da II Guerra Mundial (NOBLE, 1979; MEDEIROS, 2004; MORAES, 2004).

Antes mesmo, como caso histórico, Trebat (2011) também apontara para esse fato, ao apresentar a experiência que tiveram os Estados Unidos a partir de seu Departamento de Guerra, entre a Guerra da Independência (1776–1783) e a da Secessão (1861–1865). Naquele caso, a expansão territorial e a evolução tecnológica do setor manufatureiro e da indústria ferroviária viabilizaram três pré-condições essenciais ao processo de industrialização daquele país no século XIX: 1) a expansão territorial-agrícola, 2) a evolução de máquinas-ferramentas no setor manufatureiro, e 3) a construção e gerenciamento da malha ferroviária.

Como apontou Trebat (2011), aquele contexto também desencadeou casos clássicos de *spin-off*, ainda que involuntários, por meio do emprego de engenheiros militares nas ferrovias e o investimento na produção de armas de fogo para a economia como um todo. Utilizando-se, naquele período histórico, dos argumentos ligados à segurança nacional e à ideologia (a do Destino Manifesto), o governo estadunidense desencadeou, internamente, a "convergência tecnológica" das fábricas armamentistas para as de metal-mecânica e a "convergência

tecnologias ligadas ao ciberespaço. Contudo, em se tratando de inovação disruptiva, foi Schumpeter que originalmente fez essa ponte entre inovação – monopólios – expansão do capital – crescimento econômico.

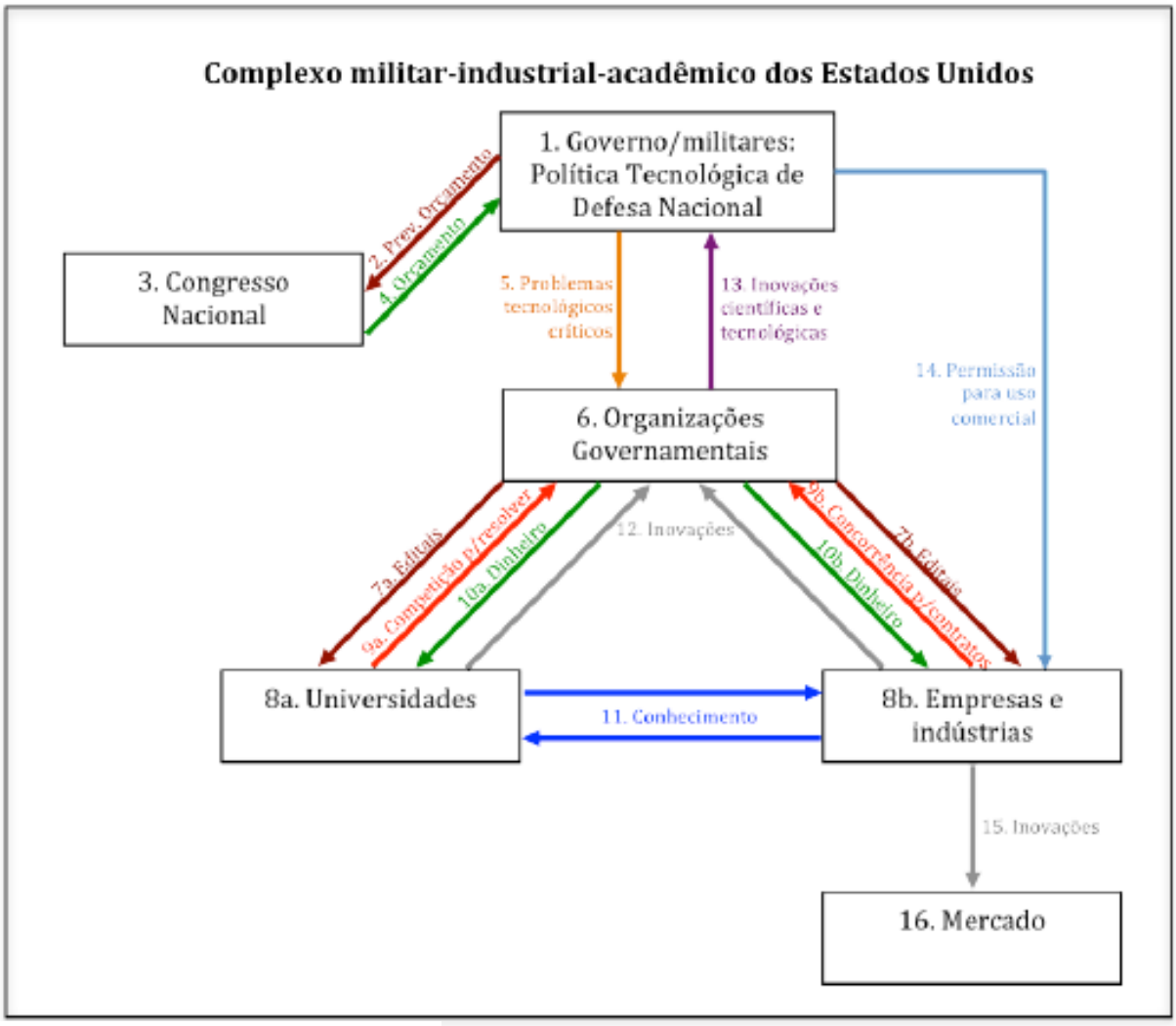
administrativa", com o esforço do Departamento de Guerra em gerenciar ferrovias, como se setor privado fosse (TREBAT, 2011).

Já mais recentemente, o computador pessoal e a Internet estão relacionados ao papel fundamental da Darpa, órgão vinculado à defesa. Contudo, como disse Mazzucato, tudo isso "depois foi esquecido por aqueles que alegam que o Vale do Silício é um exemplo de capitalismo de livre mercado." (MAZZUCATO, 2014, p. 115). Nessa esteira podem ser apontados o Iphone, o Ipod Touch e o IPad, e mais as parcerias público-privadas na Darpa, no AT&T Bells Labs, na Xerox Parc, inseridos na "Corrida do Ouro da Internet" (MAZZUCATO, 2014, p. 136).

A constituição do modelo estadunidense do pós-II GM se mostra bem interessante, ao fomentar a pesquisa e a inovação, via Defesa, com integração dos setores públicos e privados, e entre academia e indústria. Buscou-se constantemente a dianteira tecnológica e a autossuficiência orçamentária do mecanismo de inovação. Brustolin (2014) demonstrou o desenvolvimento desse enredo em sua pesquisa de tese defendida junto à UFRJ (Figura 2.4).

Em suma, chamamos atenção para o funcionamento a partir da fase Nr 6, com a condução das organizações governamentais na indução de pesquisas e de produtos com as universidades (fases Nr 7a; 8a; 9a; 10a) e empresas/indústrias (fases Nr 7b; 8b; 9b; 10b), instigando, via mecanismos públicos (editais) a concorrência/competição, que derivavam em maior eficiência e produtividade. Após isso, ocorre a inovação (em pesquisa, serviço, processo e produto) e a transferência para as agências governamentais responsáveis pela encomenda (Departamento de Defesa, no caso) e, dependendo de questões estratégicas, abre-se essa inovação, parcial ou completa, ao mercado (fase 14), o que garantirá retroalimentação financeira do sistema. Em todo esse mecanismo também pode ser notado o transbordamento do processo de inovação (fases Nr 11, 12, 15 e 16) e os derivados ganhos em eficiência e produtividade, pública ou privada.

Figura 2.4: Fluxograma do Complexo Militar-Industrial-Acadêmico dos Estados Unidos



Fonte: Brustolin (2014, p. 24).

Foi esse mecanismo de interação e em um ambiente de concorrência, capitaneado pelo Estado, embora aparentemente paradoxal a luz de algumas teorias, que contribuiu para o êxito desse sistema, ao contrário do que assistimos no caso da União das Repúblicas Socialistas Soviéticas (URSS), como nos mostrou Antonio Segrillo (1997), com relação ao fardo das despesas militares na economia soviética e sua influência no desencadeamento da *Perestroika*, o que também pode ser reforçado, considerando um recorte histórico mais amplo, de longa duração, com os registros feitos por Paul Kennedy (1989) acerca da ascensão e queda das

grandes potências, e sua ligação com o (des)equilíbrio entre Defesa e Desenvolvimento ou, para a época, entre a força militar e as finanças e uma base econômica produtiva.[54]

Até aqui, no que diz respeito à relação entre poder, riqueza e desenvolvimento, no tocante ao ciberespaço, e também a outras inovações consideradas disruptivas, vimos que há um circuito em que operam Estado-indústria-academia. Todavia, há ainda outro movimento, de natureza não excludente.

2.4.3.1 Dos Circuitos em Camadas de uma EPI e sua Relação com o Desenvolvimento

No Capítulo 1 mostramos o processo de territorialização, desterritorialização e (re)territorialização de Raffestin, o T-D-R, que ocorre sobretudo sob a direção política, tendo como o objeto de tensão o espaço geográfico e a sua transformação e manutenção em território. Contudo, detectamos ao longo deste processo investigatório que há outro processo, concomitante e não excludente, reforçando-o, e que é de ordem econômica.

Se no âmbito interno, no caso dos Estados Unidos, à título de exemplo, há o circuito envolvendo a indução pelo Estado e o desenvolvimento de pesquisas e produtos pela indústria e pela academia, que acarreta inovações e respectivas patentes e direitos derivados, com certa exclusividade temporária, há também, interligando a produção interna com o mercado externo, outro circuito acontecendo como apontou Vernon (1966), ao se debruçar sobre o ciclo de vida dos produtos e sua relação com o comércio internacional. [55] Para esse autor, o ponto-chave é a inovação tecnológica, não a comum, mas sim a disruptiva *schumpeteriana*, capaz de alterar o sistema e de criar – ou manter – monopólios, e esta tem mais possibilidade de ocorrer na camada do verdadeiro capitalismo do que na de mercado. Nessa está contida a preocupação com o surgimento de um produto industrializado (uma inovação), passando pela sua maturidade e, por fim, pela sua padronização na escala global. [56]

---

[54] No capítulo 3 – "*As Finanças, a Geografia e a Vitória nas Guerras: 1660-1815*" –, Paul Kennedy retrata bem a necessidade de sinergia entre força militar e recursos econômicos para a manutenção ou expansão de poder na Europa daquele período.

[55] Destacamos e concordamos com a observação dos autores Eneuton Pessoa e Marcilene Martins: "Ademais, se é verdade que a teoria do ciclo do produto não explica o fluxo de investimentos diretos estrangeiros no atual contexto de integração mundial dos mercados, é também verdade que ela continua bastante aderente à realidade, quando, por exemplo, ajuda a entender por que as empresas multinacionais, em geral sediadas nos países desenvolvidos, em sua estratégia de internacionalização produtiva tendem a se dirigir para países intensivos em recursos naturais e/ou mão-de-obra barata – são estas as vantagens de localização tipicamente oferecidas por esses países –, ao mesmo tempo em que tendem a concentrar naqueles primeiros países a maior parte dos seus investimentos inovativos, assim como as atividades de produção tecnologicamente mais complexas." (PESSOA; MARTINS, 2007, p. 326).

[56] A questão dos monopólios também é abordada por David F. Noble: "Em todas essas indústrias a introdução sistemática da ciência como meio de produção foi pressuposto, e por sua vez reforçado, por monopólio industrial.

Para a teoria elaborada por Vernon (1966), na fase de lançamento do produto, cuja tecnologia passou por um processo de inovação (que depende de quantidade de mão de obra altamente especializada), o produto ganharia o mercado interno, geralmente de países onde a renda da população é maior. Assim, a probabilidade de ocorrer isso é nos atuais países desenvolvidos ou avançados, que conseguem juntar essas variáveis requeridas para a inovação – abundância de capital e capacidade de PD&I. É nesse momento que, para a empresa inovadora e para o Estado onde o produto foi lançado, há um monopólio temporário do produto, portanto permitindo uma sobrevalorização do bem.

Na segunda fase de sua teoria, Vernon afirma que a empresa buscaria uma massificação da produção e, como consequência, a exportação. Nesse período, o poder do monopólio sobre a inovação do produto tenderia a se dissipar, pois os concorrentes estrangeiros entrariam no circuito produtivo. A margem de lucro, assim, seria reduzida.

Na fase da padronização do produto (3ª), o mercado interno do país inovador já estaria saturado e à procura de novas facilidades tecnológicas, isto é, uma demanda surgiria por mais inovações e com a disposição – e capacidade – de pagar mais por isso. Enquanto isso, o mercado internacional já teria conhecimento dos meios de produção e da tecnologia empregada no produto anterior, o que diminuiria a necessidade de uma mão de obra muito especializada e facilitaria, portanto, a replicação do produto em outros países. Nesse aspecto, S. Cavusgil dá o seguinte exemplo:

> Esse tipo de ciclo ficou evidente na evolução dos aparelhos de televisão. A tecnologia de base para televisores foi inventada nos Estados Unidos, e as empresas norte-americanas começaram a fabricá-los na década de 1940. As vendas no país cresceram em ritmo acelerado por muitos anos. Após a TV se tornar um produto padronizado, sua fabricação foi transferida para a China, México e outros países com custo inferiores de produção. (CAVUSGIL *et. al.*, 2010, p. 74)

Nessa fase também, afirma Coutinho *et. al.* (2005), o país inovador, inclusive, prefere importar a sua "inovação" dos outros países (em desenvolvimento ou subdesenvolvido), pois o custo da produção será menor. O foco dos países de ponta em PD&I está, nesta fase, na

---

Esse monopólio significava o controle não apenas dos mercados como da planta produtiva e de equipamentos, mas também da própria ciência. Inicialmente, o monopólio sobre a ciência tomou a forma de controle de patentes. Tornou-se então o controle sobre próprio processo de produção científica, por meio de pesquisa industrial organizada e regulamentada. Finalmente, chegou a incluir o comando sobre os pré-requisitos sociais desse processo: o desenvolvimento das instituições necessárias para a produção de conhecimento, tanto da ciência e de recursos humanos capacitados, quanto a integração dessas instituições dentro do sistema corporativo da indústria de base científica." (NOBLE, 1979, p. 6).

descoberta de uma nova tecnologia, isto é, de outra inovação, a fim de dar continuidade ao ciclo e à obtenção de vantagens, tanto do monopólio transitório sobre a inovação e o seu preço, quanto da capacidade de exportação, na fase da maturidade, quanto, ainda, na fase da padronização, pois apesar da produção se deslocar para outros países "secundários", questões de direito relacionadas à patente e à marca continuam trazendo para o país divisas, saldo favorável no balanço de pagamentos, com reflexos para o orçamento.

E isso não ocorre apenas na esfera privada. O jogo econômico-financeiro e o político-diplomático terminam por confundir capital e Estado. O que foi apontado por Vernon no tocante à inovação nas empresas privadas foi – e é – praticado, também, pelo setor público, na relação entre os Estados, diretamente ou não, o que ocasiona, em não poucas vezes, o cerceamento tecnológico, este entendido como "práticas no sentido de restringir ou negar o acesso ou a posse de tecnologia por parte de terceiros" (MOREIRA, 2017, p. 12), isto é, uma espécie, também, de coerção. Por conseguinte, há necessidade em desenvolver pesquisa para inovação, sobretudo de um setor tão sensível para o ente estatal e sua sociedade: a Defesa.

Mais que isso, aqui a ideia de se fomentar um sistema *nacional* de inovação torna-se uma resposta a essas demandas, uma vez que carrega em si, desde o inferido por List ainda na Alemanha do Século XIX e início do XX (PADULA, 2007), e, mais recentemente, e no Brasil, constando em trabalhos de Becker (2012 [1988]), de Cassiolato e Lastres (2007), e de Ibañez (2011), o elemento *nacional* é realmente visto em sua posição central face à natureza do sistema internacional, composto por recortes espaciais delimitados pelo poder – logo por territórios –, o que nos conduz a enxergar a inovação tecnológica como um dos componentes da geopolítica, consoante apontamos no capítulo anterior, no qual concordamos, mesmo com objeto de estudo diferente, com o que já afirmou Ibañez: "[...] a inovação é, cada vez mais, elemento central da Geopolítica mundial" (IBAÑEZ, 2011, p. 80).

Assim, é por meio da concepção da ideia de um sistema verdadeiramente *nacional* de inovação que podemos fazer uma ponte, um elo, entre a importância do investimento em Ciência, Tecnologia e Inovação (C,T&I), o processo de territorialização e o desenvolvimento econômico, seja para o movimento de manutenção da posse sobre o território, seja no de projeção de poder: "[...] há um novo significado da geopolítica, que não mais atua na conquista de territórios, mas sim na apropriação da decisão sobre seu uso." (BECKER, 2005, p. 21). É porque isso tudo, como registrou Ibañez (2011), proporciona capacidade de exercício da soberania.

2.5 Poder cibernético e ciberespaço sob a ótica de teorias de RI: conclusões parciais e implicações para estratégia brasileira

Como inferimos da bibliografia estudada, dos documentos consultados e dos fatos históricos que envolvem a complexidade do SI, sobretudo no que diz respeito à guerra, à paz e ao desenvolvimento, as teorias de RI conseguem explicar, parcialmente, a natureza do sistema e seu funcionamento. Em se tratando do poder cibernético e das capacidades advindas do ciberespaço, isso não é diferente. Todavia, o que pode diferenciar essas teorias é a capacidade de explicação sistematizada do mundo real, ou a capacidade de "jogar redes cada vez mais estreitas", a fim de apreensão mais próxima que envolve toda a realidade.

Se as ferramentas construídas pelo realismo são capazes de explicar o porquê das estratégias dos países acerca de sua segurança e defesa cibernética, atribuindo às forças armadas um papel crucial nessa condução – alguns países inclusive criando uma nova força, além do Exército, da Marinha e da Aeronáutica, como é o caso da China, da Coreia do Norte e dos Estados Unidos –, também é verdade que o ciberespaço permite uma maior aproximação entre os países, o que acarreta aumento do fluxo comercial e financeiro, amplia a agenda e dá mais transparência às ações governamentais. Nesse aspecto, as infovias, mesmo antes de serem do mundo digital, permitiram e permitem, inclusive, uma maior pressão dos atores internos ao Estado no que diz respeito à definição de políticas públicas.

Também é realidade que dentre as possibilidades advindas do poder cibernético estão a difusão de valores, de comportamentos, de protocolos, normatização e regimes, o que gera maior chance de cooperação.

Abordar o poder cibernético a partir do sistema político do país também parece não servir muito para uma conclusão sólida. Vimos que, embora se utilize do discurso acerca de uma maior liberdade e de garantia de direitos individuais, os Estados Unidos e a Inglaterra, por exemplo, realizaram espionagem de seus próprios cidadãos, por meio de órgãos de suas respectivas burocracias estatais relacionadas à segurança, mesmo com outros setores e poderes do Estado tendo ciência ou não desse fato. Isso, indubitavelmente, vai de encontro aos postulados democráticos.

Atribuir aos instrumentos econômicos uma posição de segundo plano na agenda não parece ter sido a ação da potência global atual. Os esforços foram no sentido de conjugar ganhos políticos e econômicos, em uma relação de retroalimentação recíproca, da forma como List (PADULA, 2007) mostrou e que a própria Estratégia Nacional de Defesa do Brasil (BRASIL, 2012) indicou como um dos pressupostos da relação Defesa-Desenvolvimento no País. Tudo

indica que é a partir de uma estratégia estatal, formulada após a consideração de uma série de fatores, dentre esses o político, o econômico, o psicossocial e o científico-tecnológico. No tocante a este último, sobretudo após a II GM, com o relatório de Vannevar Bush, parece-nos que os EUA aprenderam a inserir na pauta econômica o desenvolvimento de capacidades de CT&I, mas não só para fins de ganhos econômicos. O principal motivo era a resposta à situação do SI à época, que dependia, e muito, de um protagonismo em vários setores para se garantir a segurança, sendo um desses o tecnológico.

Contudo, podemos extrair lições que vão além do debate realista e liberal, mas que perpassam esses dois, ao compreendermos o verdadeiro funcionamento do SI, no que diz respeito à cibernética, visto em camadas. Na camada da economia de mercado de Braudel (1987) ou nas da economia individual e cosmopolita de List (PADULA, 2007), realmente as infovias e os equipamentos conectados ao ciberespaço permitem uma maior participação individual e social, uma maior liberdade e transparência, que favorecem aos aspectos ligados à concorrência, daí o ganho também para o indivíduo consumidor, por possibilitar a ele uma escolha em termos de preço, de qualidade e de outras variáveis, quando da decisão final da aquisição.

No entanto, há outra camada da cibernética ou do ciberespaço, o que Michéle Silva (2008) denominou "infraestrutura lógica", a sua estrutura e normatização mais profunda, na qual persiste o funcionamento do verdadeiro capitalismo narrado por Braudel (1987) ou da economia nacional de List (PADULA, 2007), ao se utilizar de monopólios, tanto no sentido de coerção, como nas decisões finais acerca da distribuição dos números e nomes de domínios (DNS) de primeiro nível ou de topo, quanto com respeito a tecnologias relacionadas às TIC, pelo abismo construído em termos de diferença de qualidade dos equipamentos. Além disso, o uso do ciberespaço pelos atores que o dominam, em última instância, traz possibilidades de melhor utilização de ferramentas de *marketing* empresarial, dentro dessas as relacionadas à publicidade e à elaboração do perfil do mercado, o que traz vantagens à sua capacidade de concorrência.

Ainda se tratando de monopólio, este pode ser observado também na sua forma aprofundada, isto é, verticalizada, via cadeia produtiva e consumidora. Se a conquista e ocupação de territórios terrestres, além-fronteira, não é mais tão importante, o domínio desses mercados o é. Raymond Vernon (1966), embora escrevendo sobre o comércio internacional, tratou de explicar com muita precisão o ciclo de vida dos produtos e como este entrelaça as camadas da economia de mercado e a do monopólio, trazendo, por um lado, um aumento dos ganhos econômicos de quem detém o monopólio e, por outro, uma maior dificuldade de se

ganhar mercado por parte de novas empresas aspirantes. Isso ocorre tendo em vista o poder de padronização, de normas e de equipamentos, também gerenciados por quem detém o monopólio. E esse ciclo é retroalimentado, portanto virtuoso, com ganhos cada vez maiores, aumentando as assimetrias do sistema e sua entropia. A inovação tecnológica ocorreu – e ocorre – nos locais em que se tem maior fomento à pesquisa, o que Vernon observou como países avançados que possuem abundância de capital e capacidade de P&D. Esse fomento, se não em sua totalidade, em grande parte tem como principal indutor o Estado, como foi o caso do Vale do Silício, mais recentemente, ou dos monopólios antigos da Bell, por exemplo.

Assim sendo, à camada dos grandes lucros, nem todos têm acesso. Esse ponto passa a ser importante, na medida em que procuramos compreender as iniciativas brasileiras para o setor cibernético no período de 2008 a 2018 e as dificuldades encontradas pelos países em desenvolvimento para participarem, equitativamente, do "jogo", nem que seja apenas o das "trocas", uma vez que o abismo para o "das guerras" se trata de algo aparentemente bem distante, exceto se contarmos com o acaso ou o imponderável de Clausewitz, pois, afinal de conta, os "jogos não estão feitos" (FIGUEIREDO, 2003, p. 15).

Ao que tudo indica, a preparação para a guerra – e não a guerra em si – pode trazer dividendos positivos para aqueles que souberem "jogar".

CAPÍTULO 3

A CIBERNÉTICA COMO SETOR ESTRATÉGICO E SEUS REFLEXOS PARA A ESTRUTURA DE DEFESA DO BRASIL

O tratamento dado à cibernética, como vimos nos capítulos anteriores, vai além de mero recurso com emprego na indústria e no comércio. Na verdade, a cibernética – que foi idealizada, em meados do século XX, como o ramo científico que pudesse 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 nos 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 tanto do efeito multiplicador[57] econômico que proporciona o setor cibernético, pelo uso, em sua essência, de equipamentos de TIC e respectivas estruturas, que corresponde ao *core* de um dos ciclos

[57] 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; WELLS, 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*. Ainda nesse sentido, estamos falando de externalidade positiva.

virtuosos de inspiração *schumpteriana*, quanto pelas externalidades positivas geradas a partir de investimentos visando ao fornecimento de um bem público, como é o caso do acesso à *internet*.

Outra lição apreendida no decorrer desta pesquisa foi a 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.

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" e para o "das trocas", 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".

Dos capítulos antecessores, pudemos constatar que os 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*[58], algo do tipo: "uma ação, dois movimentos". Tudo isso tratado no nível mais profundo da economia nacional, de List (PADULA, 2007), – e não na cosmopolítica ou da humanidade, ou na do individual –, e na do verdadeiro capitalismo, de Braudel (1987), no qual os pressupostos da corrente liberal ou neoliberal das relações internacionais não conseguem responder à toda realidade, pelo menos àquela dos que não possuem o controle.

A partir deste capítulo, a pesquisa se restringe às iniciativas brasileiras para o setor estratégico da cibernética, com ações visando ora ao espaço – o ciberespaço –, correspondendo à defesa cibernética propriamente dita, que inclui a criação de um núcleo de defesa para esse espaço, no âmbito do Exército Brasileiro (EB), hoje alçado ao nível do Ministério da Defesa, materializado no Comando de Defesa Cibernética (ComDCiber); ora visto como recurso de poder, relacionado a esforços que vão para além do setor Defesa *stricto sensu*, mas que também

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

influenciam este diretamente e, mais que isso, fomentam o desenvolvimento tecnológico e, por consequência, o econômico-social. Nesse caso, visto como recurso de poder, o setor cibernético é abordado mais enfaticamente no próximo capítulo, no qual se encontram projetos ligados à implementação de novas infovias, físicas e virtuais, tais como a construção do cabo submarino Brasil-Europa, do Projeto Amazônia Conectada e do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), enfim ações, projetos e programas que vão além da Defesa *stricto sensu*, abarcando interesse de toda a sociedade, para uso militar e civil.

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)[59], todos respeitando-se o recorte temporal desta pesquisa. No próximo capítulo, cumprindo o previsto inicialmente, outros documentos oficiais e ações são tratados, a fim de demonstrar o transbordamento deste setor para outros órgãos públicos e para empresas privadas.

Inicialmente, a título de contextualização, são apresentadas as principais partes da END (2008 e 2012), assim como as intenções nela contidas. Dessa forma, buscamos entender a formulação de seus eixos estruturantes, diretrizes e setores estratégicos elencados pela burocracia brasileira, em que, além da cibernética, fazem parte o ramo nuclear e o aeroespacial. Para cada um desses setores foi designada uma Força-líder para condução e gerenciamento das atividades. O setor nuclear ficou sob encargo da Marinha, o aeroespacial de responsabilidade da Força Aérea e, quanto ao objeto desta pesquisa – a cibernética –, o Exército foi designado para sua condução.[60]

Outro ponto que despertou atenção foi a intenção explicitada por esse próprio documento, mas não só nesse, na direção de conjugar Defesa e Desenvolvimento[61], 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. Como mostramos a

[59] Até o momento do término da redação deste capítulo, a Minuta do LBDN 2016 não tinha sido aprovada pelo Congresso, por isso a utilização como base prioritária a publicação de 2012, aprovada no ano seguinte, juntamente com a atualização da END e da PND.

[60] Destacamos que essa designação não constava expressamente na END (2008). A decisão acerca da condução dos setores estratégicos ocorreu por meio da Diretriz Ministerial nº 14/2009 do MD. Como concluímos na pesquisa de mestrado, esse processo decisório não aconteceu sem discussões e debates, eis que envolvia – e envolve – distribuição de recursos orçamentários e *status*.

[61] Por exemplo, consta no Capítulo 3 do Livro Branco de Defesa Nacional (LBDN): "Nos três setores, a prioridade é elevar a capacitação científica e tecnológica do País e preparar os recursos humanos." (BRASIL, 2012, p. 70).

seguir, realmente tem se buscado esse paradigma, apesar de óbices estruturais e conjunturais. A título de início da abordagem desse tema pelo documento em tela, assim mencionou a END no primeiro parágrafo de sua Introdução:

> 1. 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)

No decorrer do texto, quando verificamos a pertinência, inserimos ideias e elementos constantes de outros documentos de Defesa, na expectativa de mostrar de forma mais completa possível o arcabouço montado para o setor cibernético.

Para não redigir de forma enfadonha, literal – uma vez que foi a partir da inferência de documentos oficiais – e na medida em que seu conteúdo permitia comentário, apreciação e emissão de juízo de valor, com ligação a outros pontos já abordados nesta pesquisa, teóricos ou reais, ou que são abordados no próximo capítulo, 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".

3.1 A END E OS SETORES ESTRATÉGICOS DENTRO DA CONCEPÇÃO DO BINÔMIO *DEFESA-DESENVOLVIMENTO*

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

Talvez esse seja o ponto que mais despertou nosso interesse por esta pesquisa. Desde que iniciamos nosso percurso pela seara da Defesa[62], tínhamos algumas inquietações que perpassavam pela busca da conciliação entre Defesa e Desenvolvimento ou, pelo menos, de tentativa em conciliar os interesses e necessidades da Defesa do País com suas possibilidades de Desenvolvimento. Essa questão é crucial, pois da forma como é respondida, a princípio, pode servir de aspecto positivo para o País, para além da própria Defesa, ou de negativo, vindo

[62] Como padronização, conforme anunciamos na Introdução, optamos pela grafia de Defesa com inicial maiúsculo, 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.

a ser tanto mais um não cumpridor do mínimo necessário com relação à área de Defesa, como ser mais um dreno de recursos públicos de um País em desenvolvimento e com todas as características que lhes são peculiares. Aqui retomamos a questão contida no projeto desta pesquisa e repetida outrora: 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?

Precisamos lembrar, para responder a essas inquietações, que Defesa é tida, economicamente tratando, como um bem público, que é caracterizado "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, [...]." (VASCONCELLOS, 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) [63]

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, entre segurança e bem-estar. 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,

[63] 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.

2012d, 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 List (PADULA, 2007) e de 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, 2012b, 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, 2012b, p. 100).

Do geral para o particular, e não de forma taxativa, buscamos os esforços do Exército – Força responsável pelo setor cibernético – para atender à END (2008). No todo, esses são os benefícios divulgados pelo Escritório de Projetos do Exército (Epex), conforme Quadro 3.1, no que diz respeito aos programas e projetos desenvolvidos por esta Força:

Quadro 3.1: 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, Desenvolvimento e 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, incluindo 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, abrigo e recursos.

Seguindo nova metodologia da área gerencial, o EB sistematizou essas ações em portfólio com três dimensões. São essas: 1) Defesa da Sociedade; 2) Geração de Força; 3) Dimensão Humana.

Figura 3.1: Portfólio e Subportfólios Estratégicos do Exército

Fonte: Epex (2019).

Dos acima elencados, interessa diretamente a nossa pesquisa o subportfólio *Defesa da Sociedade* e, especificamente, inserido nesse, os programas *Defesa Cibernética na Defesa Nacional* e o *Estratégico da Defesa Cibernética* por ser mais afeto ao tema proposto. Contudo, identificamos que há áreas de interseção entre este e os outros subportfólios, como a própria figura ilustra e como constatamos na realidade. Antes de conhecer esses programas, porém, é preciso identificar a sua origem, concretizada via um documento oficial intitulado *Estratégia Nacional de Defesa*, publicada em 2008 e em suas versões posteriores.

3.1.2 Estratégia Nacional de Defesa (2008, 2012 e 2016) [64]

A publicação da primeira Estratégia Nacional de Defesa do Brasil ocorreu em 2008, constituindo assim um marco no que diz respeito à Defesa no Brasil. Com isso, não estamos afirmando que anteriormente não existiam documentos de Defesa no Brasil, mas sim pretendemos mostrar 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 aproximar a sociedade dos assuntos de Defesa, ou de convidar a sociedade para os debates acerca da definição dos objetivos da Defesa brasileira.

A elaboração da Estratégia teve início ainda em setembro de 2007, quando foi instituído um Comitê Ministerial para a formulação da Estratégia Nacional de Defesa. À frente da condução dos trabalhos estavam os ministros Nelson Jobim, do MD, e Roberto Mangabeira Unger, da SAE/PR (Secretaria de Assuntos Estratégicos, subordinada à Presidência da República), além dos ministros do Planejamento, Orçamento e Gestão (MPOG), da Fazenda e da Ciência e Tecnologia, e os comandantes das Forças Armadas.

Oliveira (2009) afirmou que a END foi uma resposta do governo a impasses na área militar derivados sobretudo de dois acidentes aéreos gravíssimos, envolvendo aviões comerciais[65] e do movimento dos controladores de voo, no qual houve configuração de greve e

[64] As duas primeiras edições da END são bem parecidas, textualmente tratando. Demos mais ênfase quando detectamos mudança de rumo em alguma diretriz, objetivo ou medida e informamos o ano-referência do documento-fonte.

[65] Um em novembro de 2006, em Mato Grosso, com 154 vítimas fatais, após a colisão de um avião da empresa Gol com um jato executivo da empresa Legacy que seguia para os Estados Unidos. Os passageiros e tripulação do jato saíram ilesos. Os pilotos, norte-americanos, foram condenados pela justiça brasileira; outro com aeronave da empresa TAM, em junho de 2007, vindo de Porto Alegre-RS com destino a Congonhas-SP, quando o avião não conseguiu aterrissar na área-limite deste aeroporto, atravessou uma avenida e colidiu com um prédio, ocasionando uma explosão e incêndio. No total foram 199 vítimas.

motim em um tipo de "operação-padrão". Como motivos mais mediatos, Oliveira (2009) também informou a pouca atenção dada pelo chefe do Executivo às Forças Armadas, apesar de a mensagem ao Congresso Nacional de 2003 indicar o contrário. Contudo, não ocorreu, no período de 2003 a 2007, nem a elaboração e publicação do Livro Branco de Defesa Nacional, nem o fomento do debate de temas militares com civis. Isso também demonstrou certa fragilidade institucional do Ministério da Defesa, criado em 1999.

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 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 tema discutido e apreciado pela sociedade, como um todo. Como ouvimos em seminários no decorrer da pesquisa: "Defesa é algo sério demais para se deixar apenas nas mãos de militares" [66]. Literalmente, assim traz a END no nono parágrafo de sua Exposição de Motivos:

> Nessas condições, Senhor Presidente, a atual iniciativa do governo de Vossa Excelência, de colocar as questões de defesa na agenda nacional e de formular um planejamento de longo prazo para a defesa do País é fato inédito no Estado brasileiro. Marca uma nova etapa no tratamento de tema tão relevante, intrinsecamente associado ao desenvolvimento nacional. Reafirma o compromisso de todos nós, cidadãos brasileiros, civis e militares, com os valores maiores da soberania, da integridade do patrimônio e do território e da unidade nacionais, dentro de um amplo contexto de plenitude democrática e de absoluto respeito aos nossos vizinhos, com os quais mantemos e manteremos uma relação cada vez mais sólida de amizade e cooperação. (BRASIL, 2008, p. 6)

A END (2008) foi instituída pelo Decreto Nr 6.703, oriundo do Estado-Maior Interministerial Nr 00437/MD/SAE-PR. Além da Introdução e da Exposição de Motivos, foi dividida em duas grandes partes: I – Formulação Sistemática e II – Medidas de Implementação.

Da primeira parte, destacamos os seguintes tópicos, além da já mencionada busca por uma virtuosa relação entre Defesa e Desenvolvimento:

[66] Mais tarde descobrimos que a ideia contida nesta frase se reporta a uma afirmativa de George Clemenceau, primeiro-ministro francês no início do século XX e, em 1917, também ministro da guerra: "A guerra é assunto sério demais para ser confiado aos generais".

– anúncio das diretrizes estratégicas, no total de 25 (vinte e cinco);
– definição dos setores estratégicos, no total de 3 (três) (nuclear, espacial e cibernético);
– reorganização da indústria de defesa, versando acerca da Base Industrial de Defesa sob uma concepção ideal de desenvolvimento tecnológico independente, e
– considerações acerca do serviço militar obrigatório.

Essa formulação foi sistematizada em 3 eixos estruturantes (Figura 3.1): a) reorganização das Forças Armadas; b) reestruturação da indústria brasileira de material de defesa e c) política de composição dos efetivos das Forças Armadas.

Figura 3.1: Eixos Estruturantes da END (2008)

Fonte: Câmara dos Deputados (2013).[67]

Das 25 diretrizes e desses eixos citados, destacamos abaixo os pontos mais relacionados ao nosso objeto de pesquisa.

[67] Apresentação do General de Exército César Augusto Nardi de Souza, então Chefe de Assuntos Estratégicos do Ministério da Defesa, em Audiência Pública no Congresso Nacional..Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/audiencias-publicas/2013/abril/24-04-2013-politica-de-defesa-nacional-pdn-a-estrategia-nacional-de-defesa-end-e-o-livro-branco-de-defesa-nacional-lbdn/apresentacoes/pdn-end-general-nardi. Acesso em: 18 nov. 19.

3.1.2.1 Eixos Estruturantes e Diretrizes Estratégicas

Com relação aos eixos estruturantes, a END (2008) e suas sucessoras (2012 e 2016) elencam três, como citado e ilustrado anteriormente. Todos esses, de maneira geral, trazem implicações para a consecução da implantação e condução do setor cibernético, como por exemplo 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, buscamos analisar esse documento e suas intenções mais detalhadamente com base nas 25 diretrizes gerais de Defesa e nos objetivos estratégicos específicos de cada Força[68].

Das diretrizes gerais, as que possuem relação com o objeto dessa pesquisa, de forma direta, quando citam o setor cibernético explicitamente, ou indireta, na medida em que influem ou podem ser influenciadas por este, estão enumeradas 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, destacamos o primeiro conceito, tendo em vista a possibilidade que trará 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.

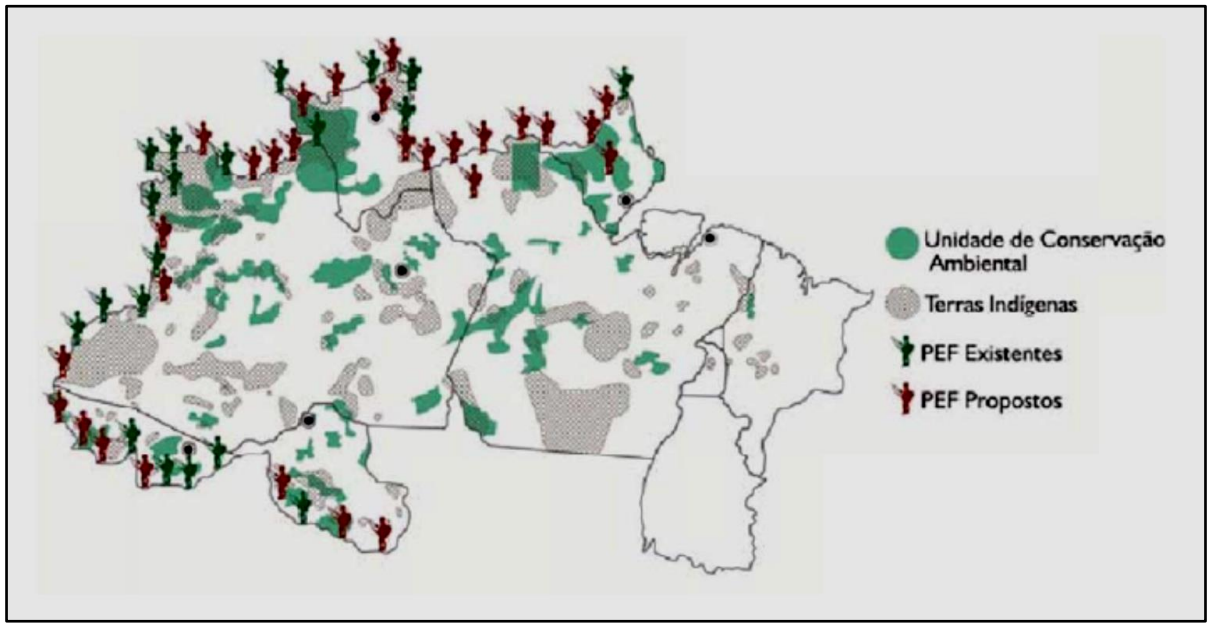
Da mesma forma é a *presença*, que por sua vez depende da *mobilidade*. Assim, logo pela diretriz de nº 2, a Estratégia anunciou a opção pelo uso de recursos tecnológicos, sejam informacionais e de comunicações, sejam ligados à capacidade de transporte, em detrimento da presença permanente de tropa em todo o território nacional, o que seria, neste último caso,

[68] 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.

inviável, tendo em vista sua dimensão de mais de 8.500.000 Km^2, sem contar o espaço abrangido pela Amazônia Azul.[69]

Sobre essa diretriz, testemunhamos, de fato, uma mudança profunda de concepção. Durante as aulas de Geografia na AMAN, nos anos 2006 a 2010, baseadas em apresentações que assistimos de chefes militares de escalões superiores, no Sistema de Planejamento Estratégico (Siplex) de então, de documentos e da literatura especializada[70], anunciávamos aos cadetes – principalmente aos da Arma de Infantaria, por serem os que mais operam nessas localidades – a previsão de implementação/construção de cerca de mais vinte e oito pelotões especiais de fronteiras (PEF), organizações militares localizadas, como o nome indica, em regiões fronteiriças inóspitas e de difícil acesso (Figura 3.2).

Figura 3.2: Pelotões Especiais de Fronteira – previsão do Programa Amazônia Protegida



Fonte: GABRIEL (2015, p. 40).

[69] Essa dificuldade de comando e controle de áreas fronteiriças, que acarreta complexidade de monitoramento, não é exclusividade do Brasil. Os Estados Unidos, por exemplo, com fronteira bem menos extensa ao sul, com o México, e com todo aparato tecnológico, também lidam permanentemente com essa questão.

[70] Segundo Pedro Gabriel, oficial do Exército e pesquisador da área de Defesa: "O Programa Amazônia Protegida tem, como medida a ser desencadeada, a ampliação do número de unidades do Exército na Região Norte, em especial na faixa de fronteira, em que os atuais 21 pelotões especiais de fronteira serão modernizados e 28 novos serão criados na primeira fase estipulada no programa. Esses pelotões, dentro dos projetos contemplados pelo Programa Amazônia Protegida e do SISFRON, receberão equipamentos necessários a ampliar a capacidade de controle e alerta da faixa de fronteira, como radares de vigilância terrestre e aérea e modernos sistemas de comunicação." (GABRIEL, 2015, p. 39).

Com a aprovação da END, essa intenção foi alterada, substituída, em parte, pelos esforços feitos, primeiramente, pelo SisFron e, posteriormente, e ao que tudo indica, pelo Amazônia Conectada[71], isto é, os cerca de 28 Pelotões Especiais de Fronteira não saíram do papel e os investimentos orçamentários e de implementação foram para esses projetos, atendendo, portanto, ao preconizado na Estratégia.

Esse ponto é 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.[72]

> 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 constatamos é uma mudança na concepção estratégica ao considerar não só a questão das distâncias espaciais, geográficas, 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 de 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 o resultado, tanto de uma concorrência comercial quanto de um conflito bélico.

---

[71] 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, 2012b, 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, 2012b, p. 114). Essa foi uma novidade da END 2012 em relação à sua versão de 2008.

[72] Contudo, na Minuta do LBDN de 2016 houve previsão para a implementação de 28 novos PEF. Ao que parece, retornou-se à antiga ideia de presença, de fato, além do monitoramento/controle e da capacidade de mobilidade. Isso pode ser justificado pelo intrínseco teor geopolítico da faixa de fronteira e pelas demandas relacionadas às "novas ameaças" (tráfico de drogas, armas, pessoas etc.).

– 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, que são apresentados e discutidos no próximo capítulo deste relatório de pesquisa.[73]

– Diretriz Estratégica nº 6: tratou do anúncio dos três setores estratégicos – o espacial, o cibernético e o nuclear, e da necessidade de fortalecimento desses. É por meio do fortalecimento desses setores, anunciou a Estratégia, que se contribui para a capacitação dos recursos humanos no conceito de *flexibilidade*[74], 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[75]. O próprio uso de tecnologias que permitam atender aos requisitos do *monitoramento/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/controle)*. (BRASIL, 2008, p. 23, *grifo nosso*)
>
> [...] 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

[73] No Capítulo 4 registramos essa intenção, que foi materializada sobretudo quando da formulação e implantação do Satélite Geoestacionário de Comunicações Estratégicas (SGDC-1).

[74] 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.

[75] Esse cenário também é denominado "guerra em três quarteirões", onde em um único teatro de operações teríamos 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, como apresentamos no capítulo anterior.

> estilo encontra contrapartida na maneira de fazer a guerra, cada vez mais caracterizada por extrema *flexibilidade*. (BRASIL, 2012b, p. 57, *grifo nosso*)

Ainda quanto aos setores estratégicos, a END (BRASIL, 2012b) traz uma seção específica para esses, na parte "Formulação Sistemática". Nessa seção, há um detalhamento do que se deve buscar em cada setor. Para fins desta pesquisa, expomos a seguir os relacionados mais diretamente com a cibernética.

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, concluímos que em mais essa parte do documento é evocada a preocupação com o uso dual. Além disso, a END (BRASIL, 2012b) acenou para a necessidade de se atuar em rede, que, como expomos anteriormente, 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 à variável *espaço*. Mais uma vez, então, enfatizou-se o conceito monitoramento/controle.

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 política (PND) e da estratégia (END) como um todo, vimos que não é só para as Forças Armadas que este setor vem sendo pensado – e executado. Abaixo, no Quadro 3.2, listamos, resumidamente, as prioridades do setor cibernético constantes na END (BRASIL, 2012b)[76] 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)

[76] Grifamos em negrito aquelas prioridades que, em princípio, transbordam a esfera das Forças Armadas.

Quadro 3.2: Prioridades do Setor Cibernético na END – 2012

Idt	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**.[77]
(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: END (2012, pp. 93-95, **grifo nosso**).

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 (vistos na Fig. 3.1). 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

[77] A literatura e os documentos oficiais no recorte temporal desta 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.

(ComDCiber), e ainda previu a ampliação da relação entre este Comando e a segurança de estruturas estratégicas nacionais.

No tocante ao quadro anterior, conforme identificação das prioridades, ainda destacamos o seguinte:

(a) Como mostraremos na seção específica sobre o setor cibernético no Exército, o histórico de criação do Centro de Defesa Cibernética e sua atual estruturação como Comando de Defesa Cibernética das Forças Armadas, aqui cabe registrar que essa previsão se concretizou. O que fora antes um incipiente Núcleo de Defesa Cibernética (NuDCiber), em 2009, 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. Na Figura 3.3, a seguir, podemos visualizar um esboço da estruturação inicial do Sistema Militar de Defesa Cibernética (SMDC), o qual contempla o ComDCiber, para as Três Forças, e o CDCiber, âmbito Exército.

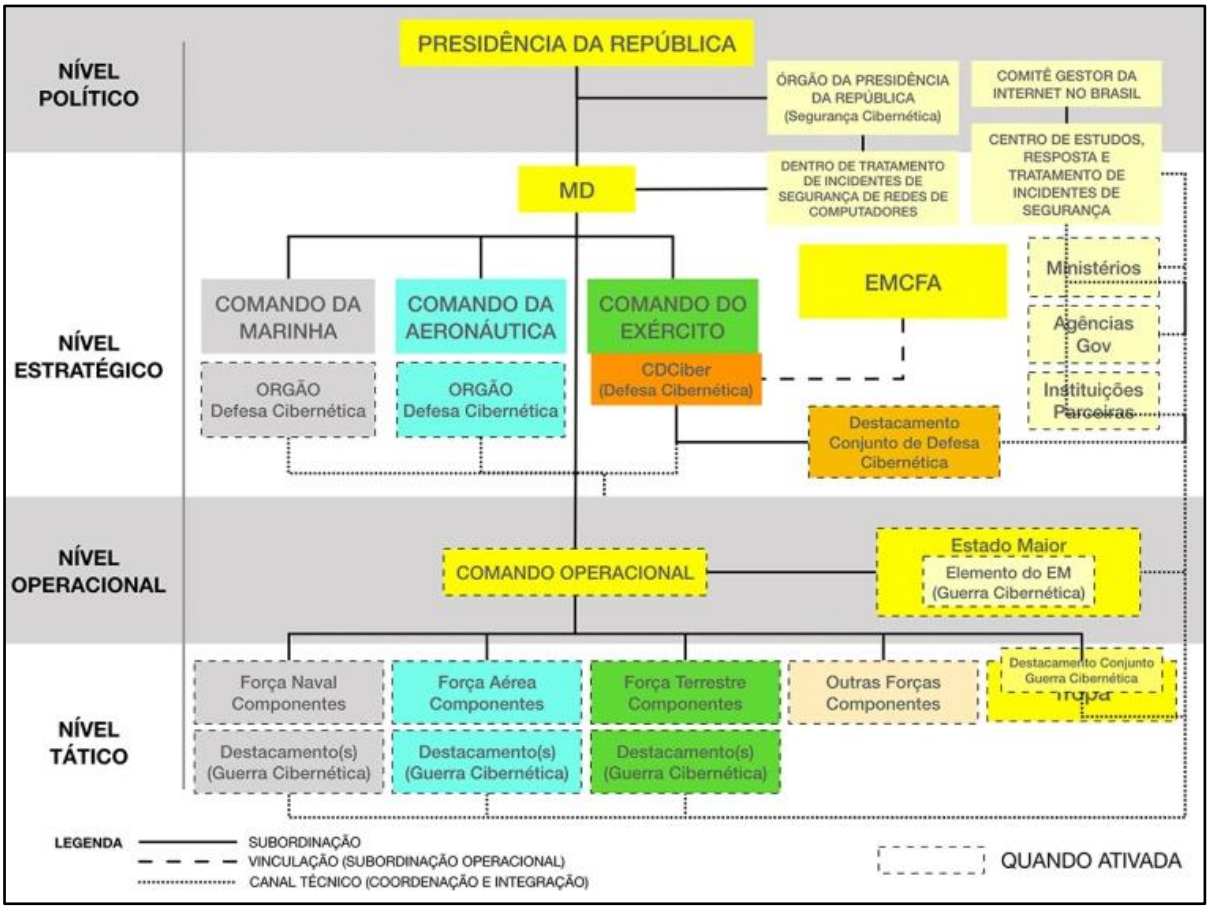
(b) essa prioridade tratou da segurança das informações e das comunicações, baseadas em ferramentas cibernéticas, como por exemplo o uso de certificações digitais, de criptografia e de padronização de normas técnicas não só âmbito Exército, e sim das Três Forças. [78]

(c) Nesse ponto, houve evidências que comprovam os esforços do fomento de pesquisa nesse setor, envolvendo sobretudo a comunidade acadêmica nacional, civil e militar. Há 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 MCTIC, e MD e CAPES, o primeiro com o Programa Amazônia Conectada, este último com os programas de fomento à pesquisa Pró-Defesa e Pró-Estratégia. Devemos salientar, ainda, a criação da Escola Nacional de Defesa Cibernética, em 2015, como uma das prioridades também consideradas e atendidas. Nessa Escola, há participação de militares das três Forças e de civis, agentes públicos federais

[78] A *expertise* nessa área se mostrou importante quando da aproximação institucional entre o Exército, a Itaipu Binacional e o Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro), como consta no Capítulo 4.

e outros convidados, envolvidos diretamente com ações que envolvem defesa ou segurança cibernética. [79]

Figura 3.3: Concepção do Sistema Militar de Defesa Cibernética



Fonte: BRASIL (2014). [80]

(d) (e) (f) Muitas foram as realizações que abrangem essas três prioridades. Talvez a de maior vulto foi o desenvolvimento autóctone de um simulador 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 destacamos 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

[79] Oficialmente inaugurada em 7 de fevereiro de 2019, a ENaDCiber funcionava como núcleo de capacitação desde 2015.
[80] Disponível em: https://www.gov.br/defesa/ptr/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_cibernetica_1a_2014.pdf. Acesso em: 20 out. 2018.

necessários à Defesa Nacional." (BRASIL, 2012, p. 63). Essa diretriz está concretizada por meio do projeto Proteger[81], que visa ampliar a segurança de estruturas estratégicas do País e da condução de grandes eventos. Além de estruturas terrestres, o Proteger se articula 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[82]. 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) listadas no quadro anterior se referem mais à cibernética vista como um espaço, isto é, com preocupações voltadas para máquinas processadoras e respectivas infovias, o ciberespaço, 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, por exemplo:

> 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 nosso**).

Sendo assim, resgatamos a proposta feita por nós no capítulo inicial deste trabalho, em que ilustramos a característica da transversalidade [83], a qual permeia toda natureza e concepção de cibernética. Ademais, a ideia de Becker (2010) no tocante à existência de uma cronopolítica também é evidenciada e, mais que isso, passa a ser buscada como um elemento-chave para o êxito das operações. Tudo isso baseado na informação, no seu uso em rede, na capacidade de

[81] Por ir além da Defesa propriamente dita, logo sob um caráter de transbordamento, este programa é abordado no capítulo seguinte.
[82] Atividade de Inteligência – "Atividade baseada em processo mental, que tem por finalidade produzir e salvaguardar conhecimento de interesse. Desdobra-se em dois grandes segmentos: de Inteligência – objetivamente voltado para a produção de conhecimentos; e de Contra-Inteligência – objetivamente voltado para a salvaguarda de conhecimentos." (BRASIL, 2015, p. 40). Ou, mais especificamente: "Inteligência – A Inteligência é o ramo da Atividade de Inteligência de Defesa (AID) responsável pela produção de conhecimentos relativos a fatos e situações atuais ou potenciais que afetem o processo decisório." (BRASIL, 2015, p. 149).
[83] Conforme Figura 1.4, do Capítulo 1 deste trabalho.

obtenção, tratamento e utilização, e isso passa, impreterivelmente, pela necessidade do uso de ferramentas cibernéticas.

De volta às Diretrizes Estratégicas, após mostrarmos os setores estratégicos anunciados na Diretriz de nº 6, com ênfase na cibernética, assim 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, 2012b, p. 54). A diferença da versão 2008 para a de 2012 da END 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, 2012b, 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/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, 2012b, p. 56).

Nesse ponto a END ratificou, novamente, nosso entendimento apresentado no Capítulo 1, no tocante à transversalidade da cibernética e suas possibilidades, e quanto ao seu uso como recurso para territorializar ou (re)territorializar.

– 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 dentro da região ou à ideia de corrida armamentista 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)/Unasul atuaria como um dos órgãos fomentadores. Houve elaboração de planos de ação sobre a defesa cibernética sul-americana, feitos pelo CDS, contudo permaneceram apenas nos 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, 2012b, p. 60) e para assegurar compras públicas (garantia de demanda); 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 encontramos maior detalhamento, e com maior contundência, 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, 2012b, 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, mais, de uma EPI 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 vislumbramos ser o embrião ou uma tentativa bem próxima do que apontou Brustolin (2014) sobre a interação entre os entes do complexo militar-industrial-acadêmico dos Estados Unidos e sua forma de sinergia. Sobre esse ponto, destacamos o trecho abaixo 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, 2012b, 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, 2012b, p. 105, **grifo nosso**).

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, 2012c, p. 219)

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

a) Criação do Núcleo de Promoção Comercial (NPC-MD): 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, 2012c, 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.[84]

c) Marcos regulatórios para o fortalecimento da indústria de defesa: pautada na Diretriz nº 22 das END (2008; 2012b), 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, concomitantemente com apoio do Itamaraty.

d) Desenvolvimento de Ciência e Tecnologia: por meio da parceria entre MD e o Ministério da Ciência, Tecnologia e Inovação (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, como foi o caso da Federação das

[84] Essa iniciativa que consta no LBDN (2012), como assinalamos, 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).

Indústrias dos Estado de São Paulo (Fiesp), por meio do Comitê da Cadeia Produtiva da Indústria de Defesa (Comdefesa).

– 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 no decorrer da pesquisa nos deparamos 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.

Passamos a seguir, mas ainda sob o arcabouço trazido pela END (2008), a conhecer o setor estratégico da cibernética no Brasil.

3.2 O SETOR ESTRATÉGICO DA CIBERNÉTICA NO BRASIL

Entre 2011 e 2013, fizemos uma pesquisa que resultou em nossa dissertação (FERREIRA NETO, 2013). Naquele relatório de pesquisa, em seu Capítulo III, detalhamos o histórico de implementação desse setor no Brasil. Vimos que 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, como expomos no primeiro capítulo. [85]

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: há 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 inferimos desse curto período

[85] Como apresentamos no Capítulo 1: "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)

textual 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 Gabinete de Segurança Institucional da Presidência da República (GSI/PR), como bem recordou o Coronel Arthur Pereira Sabbat, em audiência pública e interativa. [86]

De maneira geral, podemos visualizar as competências relacionadas ao setor cibernético e respectivas instituições responsáveis conforme o Quadro 3.3:

Quadro 3.3: Setor Cibernético - nível, denominação e coordenação [87]

NÍVEL	DENOMINAÇÃO	INSTITUIÇÃO COORDENADORA
POLÍTICO	SEGURANÇA CIBERNÉTICA	GSI/PR
ESTRATÉGICO	DEFESA CIBERNÉTICA	MD
OPERACIONAL	GUERRA CIBERNÉTICA	FORÇAS ARMADAS
TÁTICO		

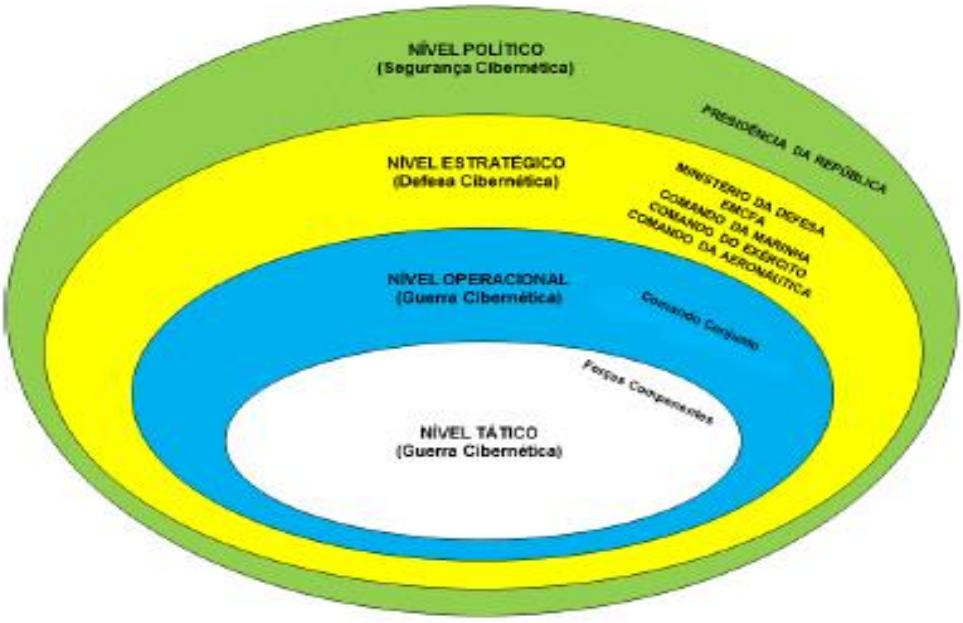
Fonte: Ferreira Neto (2013, p. 161).

[86] 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.

[87] Elaborado a partir da palestra do General José Carlos dos Santos, comandante do CDCiber, na AMAN, em 21 de maio de 2013, conforme Ferreira Neto (2013).

Visto de outra maneira, porém com mesmo significado, assim fica o conteúdo do Quadro anterior, visto agora pela Figura 3.4:

Figura 3.4: Níveis de decisão relativos à Segurança e Defesa Cibernética



Fonte: Cerávolo; Ferreira Neto (2015, p. 81).

E, da superposição do nível de atuação e a descrição das respectivas atribuições/competências, temos o Quadro 3.4:

Quadro 3.4: Atribuições no ambiente cibernético, por nível de atuação

Quadro 10: 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 Ministério da Defesa, interagindo com a 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 político, portanto no nível mais elevado de competência, 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 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)

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 as 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 encontramos 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 de 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, tivemos 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. Partimos agora para conhecer as ações estratégicas, projetos e programas relacionados ao setor estratégico cibernético, com ênfase, neste momento do trabalho, à estrutura da Defesa.

3.2.1 Ações Estratégicas, Projetos e Programas Inseridos no Setor Cibernético

Para compreendermos os esforços do MD, via EB, no tocante ao setor cibernético, também é importante entendermos o contexto em que a Força Terrestre se propôs no período de nosso estudo. Tratou-se, pois, 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 vimos 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.[88]

A partir da definição, por parte do Ministério da Defesa, sobre a responsabilidade pela condução dos setores estratégicos no País[89], 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 Defesa Cibernética (CDCiber)[90], 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 assumidos pelo Brasil perante o público internacional, como foi o caso da Rio+20, da Copa das Confederações (2013), do Mundo Fifa de Futebol (2014) e das Olimpíadas no Rio (2016).[91] Tudo isso previsto no Projeto Estratégico de Defesa Cibernética.

Além da criação de um núcleo, que se transformou logo em um centro de defesa para esse ambiente, o EB delineou – visando atender a cinco áreas de interesse ou vetores

---

[88] 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.

[89] A definição da Força-líder para cada setor não ocorreu no texto originário da END (2008), mas sim posteriormente. Pelo que investigamos, 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 conseguimos 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.

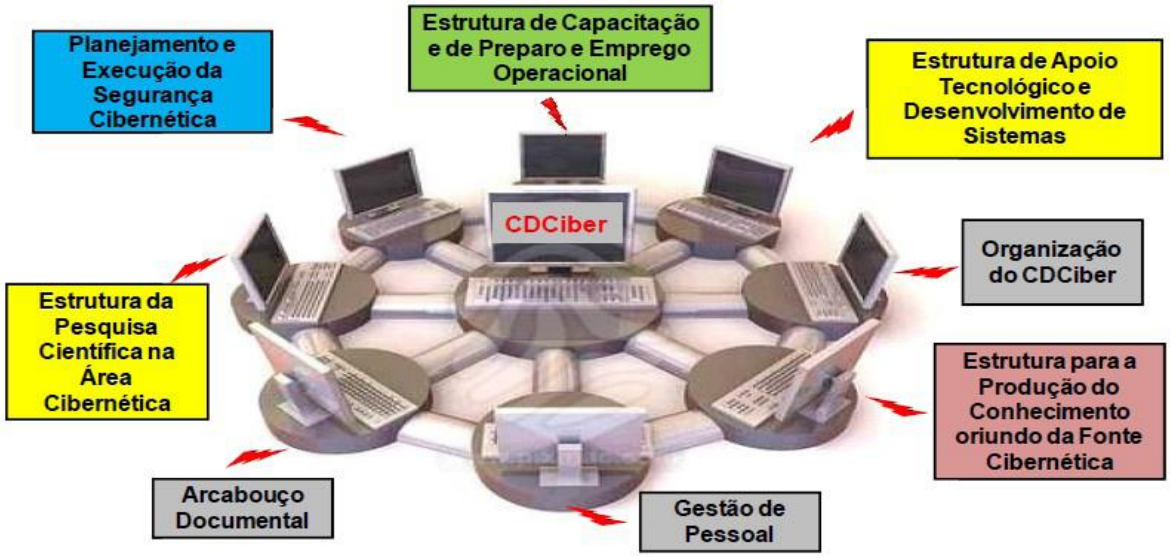
[90] Por meio das Portarias nº 666 e 667, de 4/8/2010, do Comandante do Exército Brasileiro.

[91] 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 nossa percepção enquanto acompanhávamos esse processo inicial de planejamento e de implementação pelo EB.

fundamentais [92]: 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 (Figura 3.5).

Figura 3.5: Projetos Estruturantes do Setor Cibernético



Fonte: Núcleo do Centro de Defesa Cibernética (FERREIRA NETO, 2013).

Fruto também de nossa pesquisa ainda na dissertação, resgatamos a seguir o Quadro 3.5. Nesse, associamos cada projeto acima destacado com o devido órgão responsável por sua condução no âmbito do EB e respectivos objetivos.

[92] 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.

Quadro_3.5: Setor Cibernético - projetos estruturantes, órgãos responsáveis e objetivos

NR	PROJETO	ÓRGÃO RESPONSÁVEL	OBJETIVOS
1	**Capacitação, Preparo e Emprego Operacional**	CCOMGEX	- adequação dos cursos existentes e criação de novos cursos de extensão e especialização para oficiais e sargentos; - aquisição de simuladores para o ensino de Guerra Cibernética no CIGE; - instalação do laboratório para o treinamento de Defesa Cibernética; - instalação de laboratório para o ensino de redes na EsCom; - instalação de laboratórios para o ensino das tecnologias das informações e comunicações (TIC) para outras escolas da linha de ensino militar bélico; - execução de exercício de simulação de combate de Guerra Cibernética; - implantação de um Núcleo de Experimentação Operacional de Guerra Cibernética no CIGE; - implantação de um Destacamento de Guerra Cibernética na 1ª Cia GE.
2	**Segurança Cibernética**	CITEX	- implantação da estrutura física e lógica para o tratamento de incidentes de segurança computacional; - implantação da estrutura física e lógica, no Centro de Telemática de Área (CTA) e nos Centros de Telemática (CT), para prover serviço de acesso corporativo à internet para todas as OM do Exército; - implantação da estrutura física e lógica para a realização de perícia forense nas OM do Sistema de Telemática do Exército; - aperfeiçoamento da Infraestrutura de Chave Pública do EB; - implantação de infraestrutura e processo para certificação de soluções de TIC.
3	**Apoio Tecnológico e Desenvolvimento de Sistemas**		- implantação da Divisão de Segurança da Informação e Comunicações no CDS, constituída das seguintes instalações: Laboratório de Teste de Artefatos Maliciosos; Laboratório de Análise de Técnicas de Invasão de Redes; Seção de Desenvolvimento em Segurança da Informação e Comunicações (SIC); Seção de Validação de Código; Seção de Normatização; Seção de Segurança em Software Livre; - criação no CDCiber das seguintes atividades de apoio tecnológico: Biblioteca Virtual Técnica; Rede Virtual de Laboratórios; Portal de Informação Técnica.
4	**Pesquisa Científica na Área Cibernética**	IME	- elaboração de plano para contratação temporária de pesquisadores e de técnicos em laboratório; - criação de cursos de extensão universitária via ensino à distância, presenciais e mistos, vinculados ao IME; - criação de um campus avançado do IME em Brasília para realização de cursos de extensão; - elaboração de plano de condução de convênios na área científico-tecnológica entre o IME e outras instituições de ensino; - proposição de temas de interesse do St Ciber para a realização de teses de doutorado, dissertações de mestrado e monografias de cursos de extensão.
5	**Centro de Defesa Cibernética**	CDCiber	- construção do prédio do CDCiber; - proposição de Regulamento e de Regimento Interno experimental; - proposição de Quadro de Cargos (QC) e de Quadro de Cargos Previstos (QCP) da OM de caráter experimental; - proposição de Quadro de Dotação de Material (QDM) experimental; - proposição de Sistemas de Informação do Setor Cibernético.

6	**Inteligência Cibernética**	CDCiber	- modernização das atuais estruturas de Inteligência; - elaboração de proposta de capacitação de recursos humanos, no Curso de Guerra Cibernética, realizada mediante cooperação entre a EsIMEx e o CIGE; - criação de estruturas de Inteligência voltadas para o Setor Cibernético; - elaboração de proposta da estrutura organizacional da Divisão de Inteligência do CDCiber.	
7	**Gestão de Pessoal, Arcabouço Documental e RENASIC**		Pessoal	- criação de Relatório de Análise Ocupacional; - criação de Catálogo de Cargos e Atribuições; - criação de um Plano de Admissão de Pessoal Civil; - mapeamento vocacional de militares; - desenvolvimento de Sistema Informatizado para gerir o Plano de Movimentação para o Setor Cibernético; - elaboração de Planos de Capacitação (no meio civil, no meio militar e continuada).
			Documental	- elaboração e publicação da Norma de Referência do Setor Cibernético do Exército; - elaboração e publicação do conjunto de novos documentos normativos necessários para regular as atividades de Segurança da Informação e Cibernética do Exército; - elaboração e publicação das Instruções Provisórias relativas à Doutrina de Guerra Cibernética; - revisão, elaboração e publicação de Instruções Gerais e Reguladoras sobre Segurança das Informações e Comunicações.
			RENASCIC	- promoção do avanço científico-tecnológico da segurança da informação no país, em geral, e da criptografia e defesa cibernética em particular; - fortalecimento e integração das pesquisas em Segurança da Informação e Criptografia no Brasil; - estabelecimento de Laboratórios Virtuais que visem fomentar a pesquisa entre os membros da RENASIC.
8	**Rádio Definido por *Software***	CTEX	- projeto de ciência e tecnologia (C&T) criado com vista ao apoio FINEP, com o termo de referência aprovado pelo Ministério da Defesa (MD). Passou a incorporar o St Ciber pela sua importância estratégica, sendo um projeto do MD sob gestão da Força e colaboração da Marinha e Força Aérea.	

Fonte: elaboração do autor, com base em Ferreira Neto (2013).

Um dos fatos que chamou nossa 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 3.5, ainda que de forma resumida, também passou 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, temos como 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) [93] e a Doutrina Militar de Defesa Cibernética (2014) [94] [95], essas mais estritas às ações e procedimentos em operações militares propriamente ditas.

Além das ações descritas acima, da distribuição de competências e 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, para o qual o Exército foi designado como Força-líder, dirigiu-se a 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

[93] 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.
[94] Aprovada pela Portaria Ministerial nº 3.010/MD, de 18/11/2014.
[95] 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.

(PEDCiber), previsto pela Ação Orçamentária (AO) 147F. [96] Vejamos esses com maior detalhe a partir de agora.

3.2.2 Programa Estratégico da Defesa Cibernética

Do anteriormente denominado Projeto Estratégico Defesa Cibernética, restrito às atribuições âmbito Exército apenas, a partir de 2016 tivemos 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 objetivos:

Quadro 3.6: Objetivos do Programa Estratégico da Defesa Cibernética

OBJETIVOS
a. Disseminar, com as correspondentes medidas de salvaguarda, no âmbito do MD e das Forças Armadas (FA), as atividades do Setor Cibernético do Exército Brasileiro (EB).
b. Gerar capacidades e desenvolver doutrina que possibilitem o ingresso do EB no rol de exércitos que detêm capacidade de atuar no espaço cibernético, com os decorrentes benefícios para a atividade de Comando e Controle nos níveis estratégico, operacional e tático.
c. Ampliar e/ou adequar o arcabouço normativo existente para atender às novas necessidades geradas pela inserção do Setor Cibernético nos níveis estratégico, operacional e tático.
d. Implementar a gestão de recursos humanos para identificar, selecionar, capacitar e manter o pessoal para o Setor Cibernético.
e. Dotar o EB da infraestrutura necessária para desenvolver eficazmente todo o espectro de atividades cibernéticas, particularmente visando a proteger e defender os ativos de informação da Força nas áreas de Segurança Cibernética, Defesa Cibernética e Guerra Cibernética.
f. Proporcionar condições para que o Sistema de Ciência e Tecnologia do EB realize a Pesquisa e Desenvolvimento (P&D), nas áreas de interesse do Setor Cibernético, visando à prospecção tecnológica e à pesquisa científica.
g. Conceber e implantar a estrutura organizacional do Centro de Defesa Cibernética do Exército, aproveitando, preferencialmente, as infraestruturas já existentes.

[96] 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.

h. Desenvolver a cultura de Segurança da Informação e Comunicações (SIC) em todos os escalões do EB.
i. Promover a interação com projetos congêneres ou similares em desenvolvimento nas outras Forças, no MD, em nível governamental e também em instituições civis públicas e privadas, bem como a interação com a comunidade acadêmica nacional e internacional, na área de SIC.
j. Implementar a estrutura de apoio tecnológico para atender às necessidades do Setor Cibernético.
k. Levantar as necessidades de recursos orçamentários para os diversos projetos, estabelecendo um cronograma de desembolso.
l. Produzir os conhecimentos que se fizerem necessários à atividade de Inteligência para o EB.
m. Apoiar as operações da Força Terrestre com as atividades cibernéticas.

Fonte: elaborado pelo autor com base no *site* do Epex (2019).

Isso posto, percebemos 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.

Todavia, também podemos inferir que há previsão de entrelaçamento entre o EB e as outras Forças Armadas e outras instituições, como disposto nos objetivos “i” e “j” listados acima. Isso ocorre tendo em vista a própria natureza da cibernética e de seu componente principal: a informação, que, por si, é fluida.

Muito semelhante aos projetos estruturantes do então Projeto Estratégico da Defesa Cibernética, aprovado em 2010, constam do quadro a seguir os projetos contidos no atual programa estratégico voltado, precipuamente, para as organizações militares componentes do Exército. Aqueles projetos, denominados estruturantes, de 2010, e os atuais, agora contidos em um programa, seguiram as prioridades elencadas para o setor cibernético, conforme vimos na parte inicial deste capítulo. As iniciativas, tanto as previstas como as que realmente se concretizaram, buscaram, simultaneamente, a segurança e a defesa, consideradas em si, e o desenvolvimento, por meio de gestão e capacitação de recursos humanos e de fomento à pesquisa, por exemplo (Quadro 3.7).

Quadro 3.7: Projetos do Programa Estratégico da Defesa Cibernética [97]

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 complementares	**Capacitação**	Esta ação complementar 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 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 conhecimentos, bem como a verificação da aplicação das normas doutrinárias relativas ao setor.

Fonte: elaborado pelo autor com base no *site* do Epex (2019).

[97] Esta é uma nova versão para os projetos estruturantes apresentados no Quadro 3.5, que teve como base pesquisa de dissertação realizada entre 2011 e 2013. Houve alteração em alguns nomes de projetos e adaptações na estrutura, fruto da experiência do setor a partir da atuação nos grandes eventos internacionais e para atender às normas da Administração Pública que tratam de questões orçamentárias, contudo as finalidades continuam as mesmas.

Se o Instituto Militar de Engenharia (IME) foi citado expressamente como instituição de ensino envolvida nos esforços desse setor, também é verdade que outras instituições, civis e militares, também participaram – e participam – desse processo. O Instituto Tecnológico de Aeronáutica (ITA), a Universidade Federal Fluminense (UFF), por meio do Instituto de Estudos Estratégicos (INEST), a Universidade Federal de Pernambuco (UFPE) e o Centro de Estudos e Sistemas Avançados do Recife (Cesar) foram exemplos disso.

O ITA conduziu pesquisas que envolviam o projeto do *Rádio Definido por Software*, da mesma forma que o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD), ambos ligados ao CTEx, que foi a unidade militar gerente do projeto. A UFF, ligada ao incentivo governamental do Pró-Defesa, projeto do MD/Capes fomentador de pesquisas na área de Defesa, da mesma forma que o Pró-Estratégia, capitaneado pela SAE/PR, do qual faziam parte a UFPE, o Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército (ECEME), a Academia Militar das Agulhas Negras (Aman) e o Cesar, em um dos projetos aprovados na área cibernética: o *Vigilância nas Fronteiras e Muros Virtuais: um estudo analítico de políticas públicas e sistemas operacionais de proteção às estruturas estratégicas terrestres*; todos esses também podem ser elencados.

Vários outros casos foram – e são – exemplos de integração militar e civil promovidos pelas iniciativas desse setor estratégico, e de obtenção de produtos e serviços, tangíveis ou não. Listamos alguns a seguir, enquadrando-os nos respectivos anos de consecução (Quadro 3.8):

Quadro 3.8: Principais Entregas do Programa Estratégico da Defesa Cibernética

ANO	PRINCIPAIS ENTREGAS - PROGRAMA DEFESA CIBERNÉTICA
2012	– Aquisição de Equipamento Site Redundância; – Instalação de Sensores de Sistemas de Prevenção de Intrusão (IPS); – Implementação da Redundância do Data Center do CITEx; – Curso de Guerra Cibernética para Oficiais – CIGE e CIE; – Simulador de Guerra Cibernética – CIGE; laboratórios de telemática – AMAN e EsPCEx; – Construção de sala cofre – CIE; – 1° Simpósio de Inteligência Cibernética – CIE; – Aquisição de equipamentos de inteligência forense computacional para o CIE e Companhias de inteligência dos Comandos de Área; – Laboratório de software – 1ª fase (RDS); – Instalações provisórias do CDCiber; – Desenvolvimento do software antivírus Defesa BR; – Aquisição de sistemas de inteligência de Perícia Forense Digital; – Aquisição de computador de alto desempenho.
2013	– Início das Obras da Escola de Comunicações (EsCom); – Montagem de Laboratório de Telemática da Escola de Sargentos de Logística (EsSLog) e da Escola de Sargentos das Armas (ESA); – Aquisição de equipamentos de TI e de *firewall;* de solução forense para redes e contratação de suporte técnico e renovação de licenças; – Desenvolvimento de Simulador de Operações Cibernéticas.
2014	– Criação da Seção de Tratamento de Incidentes de Rede (STIR) do CIE; – Criação de Células Cibernéticas nas Companhias de Inteligência; – Construção parcial das novas instalações físicas do CITEx; – Conclusão da elaboração das Instruções Reguladoras para Gestão da Segurança da Informação e Comunicações do Exército; – Aprovação da Doutrina Militar de Defesa Cibernética; – Implantação do Laboratório de Telemática para a EsCom; – Implantação do Laboratório de Telemática da AMAN e da CIAvEx. – Elaboração do Caderno de Instrução de Segurança da Informação e Comunicações para o SC²FTer. – Adequação do Laboratório de Proteção Cibernética de SC²FTer; – Implantação do Laboratório de Teste de Artefatos Maliciosos, utilizando análise dinâmica de malware; – Execução do Curso de Análise Forense na Escola de Superior de Redes, especializando 15 (quinze) militares das três Forças;

	– Participação de militar no *International Command and Control Research and Technology Symposium* (PVANA X14/634);[98] – Participação de militar na Conferência *Black Hat* em Las Vegas/EUA (Pvana X14/677).
2015	– Instalação do gerador elétrico de emergência; – Manutenção do Sistema de Produção do Conhecimento Oriundo da Fonte Cibernética do CDCiber (HIDRA); – Hierarquização da Estrutura de Tratamento de Incidentes de Rede na EBNet; – Instalação de um Sistema de Prevenção de Intrusões na EBNet; – Instalação de um Sistema de Análise de Vulnerabilidades em Aplicações *Web* no SisTEx; – Implantação de uma Infraestrutura de Chaves Públicas no EB (ICP-EB); – Estabelecimento de Provedores Regionais de Internet; – Virtualização de Servidores; – Capacitação de militares em Engenharia Reversa de Artefatos e teste de invasão em aplicação *Web*; – IV Seminário Internacional de Defesa Cibernética; – Conclusão da 1ª versão do Manual relativo à Doutrina de Guerra Cibernética; – Instalação e operação do SIMOC no Instituto Militar de Engenharia; – Contratação de cursos do Instituto SANS; – Contratação de Pós-Graduação a distância em Tecnologias para Defesa na Universidade de Madrid (Espanha); – Contratação de Mestrado a distância em Ciberdefesa na Universidade de Alcalá (Espanha); – Início das obras de duplicação do pavilhão de ensino do CIGE; – Utilização do supercomputador CRAY na produção de Pesquisa Científica; – Participação de militares no Curso de *Advanced Of Incident Handling* (AIH); – Participação de militar na Conferência *Global Cyberlympic*s; – Participação de militares no Evento *SANS Cyber Defense Initiative;* – Participação de militares na Conferência *Eko Party;* – Entregas de devices SCA implementados e das interfaces da Base *Application* do Núcleo SCA; – Código-Fonte da solução de software integrada L1, L2 e L3 (Ciclo 1).
2016	– Adaptação dos devices SCA para a plataforma comercial utilizada pelo rádio; – Ciclo 1 da Pesquisa e Desenvolvimento de Formas de Onda de HF no padrão militar OTAN STANAG-5066.
2018	– Integração P60, do projeto de Modernização do Radar SABER M60, que trata da integração do radar primário; – Integração S60, do projeto de Modernização do Radar SABER M60, que trata da integração do radar secundário; – Ensaios com Aeronaves, do projeto de Modernização do Radar SABER M60; – Alta Temperatura, do projeto de Modernização do Radar SABER M60, que trata da execução de ensaio de alta temperatura.

Fonte: elaborado pelo autor com base no *site* do Epex (2019).

[98] Pvana – Plano de Visitas e Outras Atividades em Nações Amigas.

3.2.3 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 nosso**)

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, destacamos 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. Na sequência do texto há dois quadros com *objetivos* e *projetos*, respectivamente, que pertencem ao Programa Defesa Cibernética na Defesa Nacional (Quadros 3.9 e 3.10).

Constatamos que o nível de atuação realmente vai 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.

Quadro_3.9: Objetivos do Programa Defesa Cibernética na Defesa Nacional

OBJETIVOS
a. Criar e implantar o Comando de Defesa Cibernética (ComDCiber), na Estrutura Regimental do Comando do Exército, integrado por militares das três Forças Armadas (FA), para atuar nas atividades de ciência, tecnologia e inovação, doutrina, recursos humanos, operações e inteligência de Defesa Cibernética. O ComDCiber deverá contar com o Centro de Defesa Cibernética (CDCiber), como organização militar diretamente subordinada, para executar as duas últimas atividades mencionadas.
b. Promover a capacitação dos recursos humanos do Setor Cibernético, por meio da criação e implantação da Escola Nacional de Defesa Cibernética (ENaDCiber), subordinada ao ComDCiber. A ENaDCiber deverá ser capaz de fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, bem como contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão de Defesa Cibernética e para a melhoria da qualificação da mão de obra nacional para o setor.
c. Dotar o Ministério da Defesa (MD) e as FA de estrutura de defesa necessária para desenvolver eficazmente todo o espectro das ações cibernéticas, de forma interoperável, particularmente visando proteger e defender os ativos de informação do MD e das FA nas atividades de Defesa Cibernética e Guerra Cibernética, por meio do Projeto de Desenvolvimento Conjunto da Defesa Cibernética.
d. Buscar inovações na área de Segurança da Informação e Comunicações, em especial a criptografia, por intermédio da estruturação de uma rede de laboratórios em instituições de pesquisas públicas e privadas nacionais, elevando a competência brasileira nesta área, ao patamar dos países mais desenvolvidos.
e. Implantar sistema de homologação e certificação de produtos de Defesa Cibernética, de emprego dual, civil e militar, viabilizando a obtenção de um ambiente favorável à eliminação ou redução de vulnerabilidades cibernéticas, baseado em estrutura de coordenação e integração de laboratórios especializados em certificação de produtos de Tecnologia da Informação e Comunicações (TIC) e posterior homologação, para emprego nas atividades de Defesa Cibernética, tendo como foco o desenvolvimento das capacitações nacionais.
f. Promover a interação com programas/projetos congêneres ou similares em desenvolvimento nas FA e no MD, em nível governamental, e também em instituições civis, públicas e privadas, bem como a interação com a comunidade acadêmica nacional e internacional, no Setor Cibernético, por meio do Observatório de Defesa Cibernética (estrutura voltada para fomentar interações e proporcionar articulações entre os diversos atores que possuam interesse no desenvolvimento do Setor).

Fonte: elaborado e adaptado pelo autor com base no *site* do Epex (2019). [99]

[99] Disponível em: http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica-na-defesa-nacional/pdcdn-defesa-cibernetica. Aceso em: 5 fev. 2020.

Quadro 3.10: Projetos do Programa da Defesa Cibernética na Defesa Nacional

PROJETOS/ SUBPROGRAMAS	OBJETIVOS
1. Projeto Criação do Comando de Defesa Cibernética (ComDCiber)	Conceber, implantar e consolidar uma estrutura operacional conjunta vocacionada para integrar e coordenar as ações de Defesa Cibernética, no âmbito da Defesa.
2. Projeto Criação da Escola Nacional de Defesa Cibernética (ENaDCiber)	Conceber e implantar uma estrutura de ensino com caráter dual, civil e militar, voltada para: a capacitação no Setor Cibernético; o gerenciamento de recursos humanos e a pesquisa no âmbito do Setor Cibernético.
3. Projeto Implantação e Consolidação da Estrutura de Desenvolvimento Conjunto de Defesa Cibernética	Conceber e implantar uma estrutura que permita a Interoperabilidade de Defesa Cibernética entre as Forças Armadas e entre elas e o MD.
4. Projeto Implantação e Consolidação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDCiber)	Conceber e implantar uma estrutura de laboratórios voltada para a homologação e certificação de produtos de Defesa Cibernética.
5. Projeto Criação do Observatório de Defesa Cibernética	Conceber e implantar um banco de dados de conhecimento especializado e compartilhado para incentivar projetos de P&D&I nacionais no estratégico Setor Cibernético.
6. Projeto Implantação e Consolidação de Sistemas de Informações Seguras	Conceber e implantar uma rede de laboratórios voltados para o aperfeiçoamento de dispositivos e procedimentos de segurança que busquem eliminar vulnerabilidades contra ataques cibernéticos.

Fonte: elaborado pelo autor com base no *site* do Epex (2019).

A ENaDCiber, como os objetivos indicam, contempla discentes civis e militares, componentes das Forças Armadas e de outros órgãos públicos, o que indica a busca de fomento de investimento em "espadas", porém de forma reprodutiva.

Essas foram as entregas desse programa realizadas até o final do recorte temporal desta pesquisa:

Quadro 3.11: Programa Defesa Cibernética na Defesa Nacional – principais 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: elaborado pelo autor com base no *site* do Epex (2019).

Pelo Quadro 3.11 percebemos o alinhamento das entregas aos objetivos propostos pelo programa (Quadro 3.9) e respectivos projetos/subprogramas (Quadro 3.10). 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. Essas últimas entregas são pormenorizadas no capítulo seguinte do trabalho, ao tratarmos do Sistema de Proteção Integrada de Estruturas Estratégicas – o Proteger.

3.3 ESFORÇOS DA DEFESA BRASILEIRA NA DIREÇÃO DE UM COMPLEXO MILITAR-INDUSTRIAL-ACADÊMICO: O PAPEL DO ESCRITÓRIO DE PROJETOS DO EXÉRCITO E DO SISTEMA DEFESA, INDÚSTRIA E ACADEMIA DE INOVAÇÃO

Ainda tratando de iniciativas vinculadas diretamente ao Exército, como condutor do setor estratégico cibernético, um órgão e um sistema foram desenvolvidos, na intenção de abarcar e gerenciar as ações atinentes a esse setor. Com a ampliação das capacidades, do nível de atuação e área de abrangência, logo de demandas, a Força Terrestre precisou criar um escritório de projetos, sobretudo para conciliar as ferramentas e exigências da gestão da coisa pública com as necessidades e os imperativos do setor.[100] Como complemento, e também como elemento norteador, um sistema que buscasse conciliar defesa, indústria, academia e inovação foi delineado, o que contemplou, também, a intenção contida na END e em outras políticas de defesa no período estudado.

Como mostramos ao longo deste texto, muitas intervenientes negativas do setor cibernético foram oriundas da carga burocrática exigida pela legislação em processos de gestão administrativa, mormente os envolvendo a aquisição de produtos e serviços, via licitação. Isso dificultou, ainda, a interação entre os setores público e privado, e entre indústria e academia.

3.3.1 O Escritório de Projetos do Exército

Para atender às diretrizes da END, no âmbito da Força Terrestre, em 10 de setembro de 2012, foi implantado o Escritório de Projetos do Exército (Epex), a partir da Assessoria Especial de Gestão e Projetos (AEGP), criada em 2010.

Como projetos iniciais ligados ao Exército Brasileiro e, portanto, que passavam pela AEGP, ainda em 2010, tinha-se o SisFron, o Defesa Anti-Áérea e o Obtenção da Capacidade Operacional Plena (Ocop). Com a transformação da AEGP em Epex, outros projetos foram englobados, como o Astros 2020, o Proteger e o Defesa Cibernética, além da missão para a qual este Escritório foi criado, conforme Quadro 3.12.

[100] Esse ponto, não no início da pesquisa, como hipótese, mas sim ao final, como constatação, mostrou-se fundamental, uma vez que vários óbices ligados à implementação de políticas públicas deste setor foram relacionados à questão da administração da coisa pública, como normas de licitação.

Quadro 3.12: Missão do Escritório de Projetos do Exército (Epex)

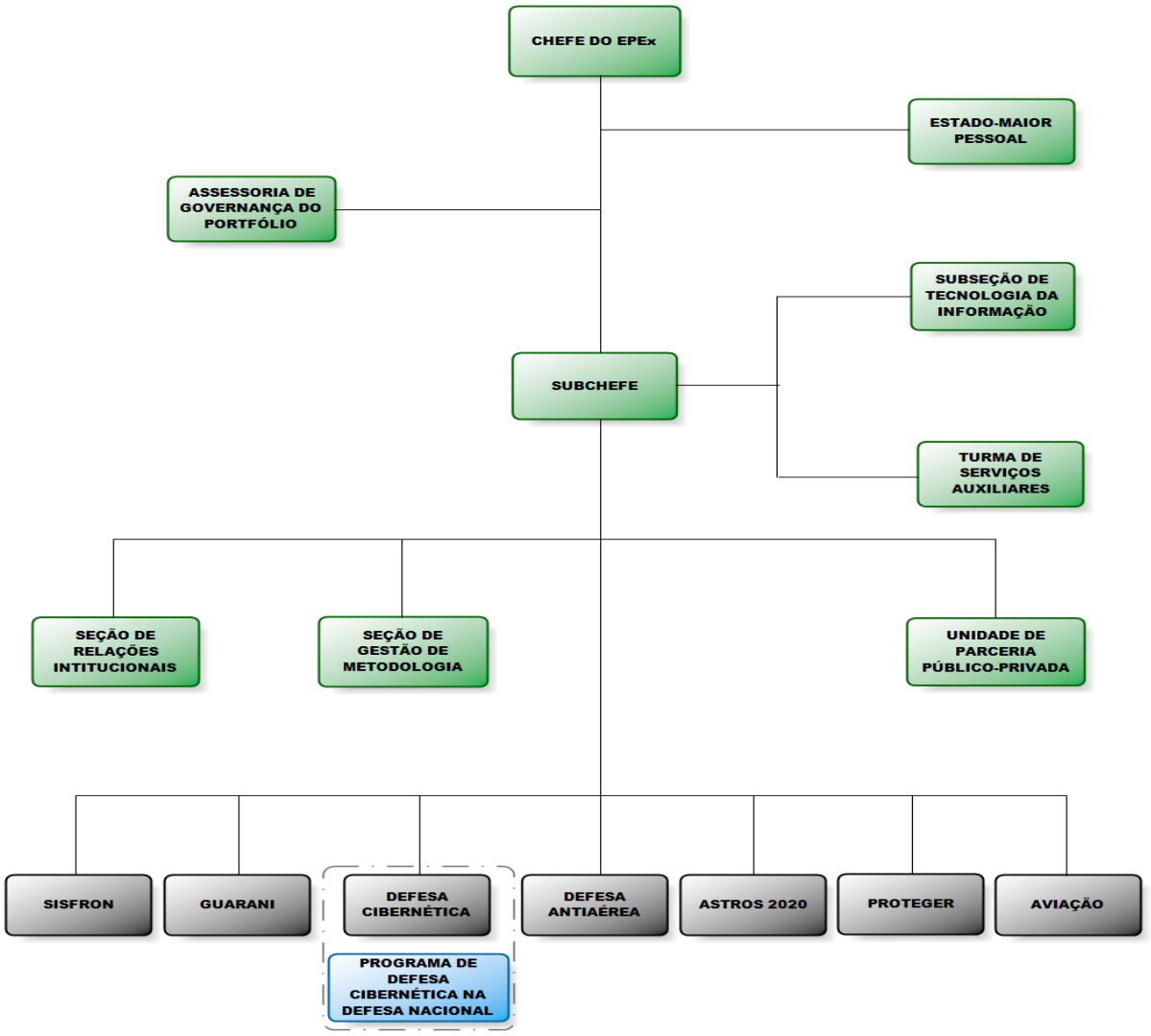
MISSÃO DO EPEX
- Atuar como órgão de coordenação executiva do Estado-Maior do Exército (EME) para fins de governança do Portfólio Estratégico do Exército, constituindo-se no escritório de projetos de mais alto nível da Força.
- Planejar e coordenar as ações de relações institucionais de interesse do Portfólio Estratégico do Exército (Ptf EE), dos Programas Estratégicos do Exército (Prg EE) e dos Projetos Estratégicos do Exército (PEE).
- Propor e manter atualizadas as normas para governança e gestão do Portfólio Estratégico, dos programas e dos projetos estratégicos do Exército Brasileiro.
- Estabelecer ligação com equipes de programas, projetos e com os Escritórios Setoriais de Projetos dos Órgãos de Direção Setorial (ODS), do Órgão de Direção Operacional (ODOp) e dos Comandos Militares de Área (C Mil A) para tratar de assuntos relativos à gerência de programas e projetos estratégicos.
- Atuar como multiplicador do conhecimento em projetos, programas e portfólio.
- Realizar a gestão de projetos de Parceria Público-Privada (PPP).
- Atuar como Secretaria Executiva do Comitê Gestor de PPP do Comando do Exército (CGPCE).

Fonte: elaborado pelo autor com base no *site* do Epex (2019).

Para realizar suas atribuições, o Epex, vinculado ao Estado-Maior do Exército, órgão mais elevado de planejamento da Força, foi mobiliado com uma estrutura para permitir a interface entre as demandas do Exército, por meio de seus projetos, e as oportunidades do mercado, incluindo aí a possibilidade de parcerias público-privadas e a participação do meio acadêmico (Figura 3.6).

Assim, podemos ver a preocupação do Epex para além das questões de metodologia da área gerencial, abarcando também uma seção e uma unidade voltadas para relações institucionais e parcerias, incluindo as de natureza público-privada, no escopo do que se fomentou na relação entre Defesa, indústria e academia.

Figura 3.6: A Defesa Cibernética no Organograma do Escritório de Projetos do Exército



Fonte: Epex (2019).

Como um dos programas, e que mereceu destaque na figura, constou o da Defesa Cibernética na Defesa Nacional, ou seja, aquele que demandou – e demanda – maior coordenação do Exército com outros setores e atores, tendo em vista abarcar espectro de competências e atribuições maior do que o da própria Força, daí a necessidade de uma coordenação.

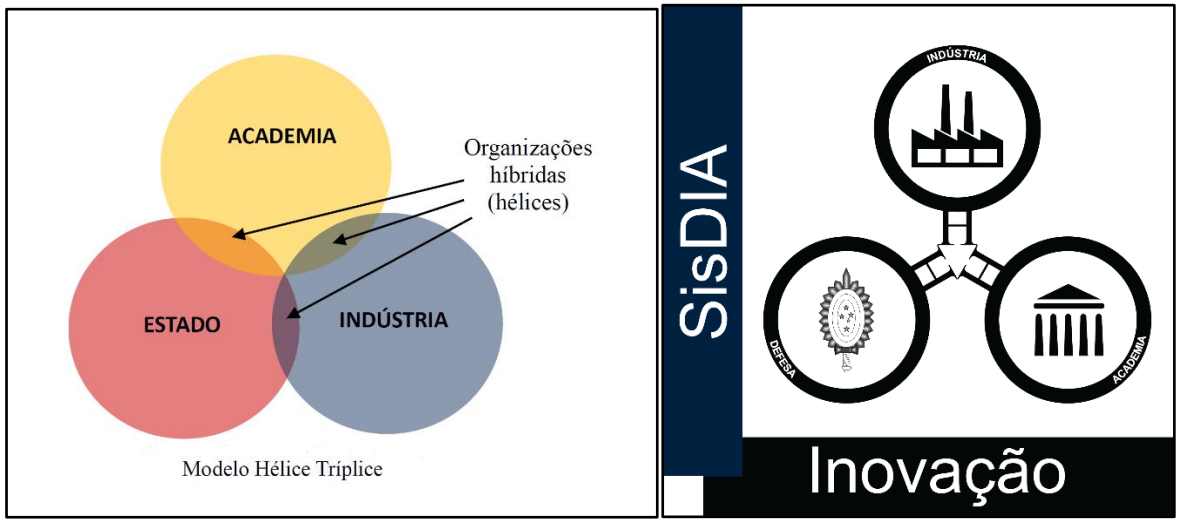
3.3.2 O Sistema Defesa, Indústria e Academia de Inovação (Sisdia de Inovação)

Criado em 2016, pela Portaria nº 1.701, do Comandante do Exército [101], o Sisdia de Inovação tem por finalidade

> potencializar os esforços das áreas governamental, produtiva e acadêmica com vistas a, por meio da inovação tecnológica, contribuir com o desenvolvimento nacional, visando à busca das capacitações produtivas brasileiras de Produtos e de Sistemas de Defesa e duais. (BRASIL, 2019) [102]

O Sisdia de Inovação se baseia expressamente nos preceitos da Tríplice Hélice (ETZKOWITZ, 1994), visando à promoção, portanto, da interação entre Estado, indústria e academia, consoante ilustra a Figura 3.7.

Figura 3.7 – Sistema Defesa, Indústria e Academia de Inovação: concepção



Fonte: Villas Bôas (2016).

Registramos alguns resultados concretos a partir do Sisdia. Foram esses: parceria Exército e Itaipu Binacional; observatório de defesa cibernética; Comitê da Cadeia Produtiva da Indústria de Defesa (Comdefesa), que se traduziu em esforços no sentido de integração da Defesa com as federações das indústrias de Santa Catarina, Rio Grande do Sul e São Paulo, além da Universidade Federal de Santa Catarina, e criação da Agência de Gestão e Inovação Tecnológica (Agitec).

---

[101] Esse sistema foi recriado em 2019, pela Portaria nº 893, que revogou a Portaria 1.701/2016, e instituiu a diretriz de implantação: Sisdia de Inovação - EB10-D-01.001. O teor, finalidade, organização e atribuições permaneceram as mesmas da Portaria anterior.

[102] Disponível em: http://sisdia.dct.eb.mil.br/images/conteudo/Legislacao/Portaria_n%C2%BA_893_19_Jun_19_-_Cmt_Ex.pdf. Acesso em: 23 set. 2019.

O General de Exército Eduardo Villas Bôas expôs os motivos da opção por esse sistema, que ele denominou "novo Sistema de Ciência, Tecnologia e Inovação do Exército" (SCTIEx) (VILLAS BÔAS, 2016, p. 2) [103], da mesma forma que emitiu diretrizes para sua consecução. Disse o então Comandante do Exército que esse sistema deveria

> ter as características de uma organização inovadora, integrada aos ambientes interno e externo ao Exército, voltada para o futuro, com ênfase nos resultados e plenamente alinhada com as necessidades da Força Terrestre. (VILLAS BÔAS, 2016, p. 2)
>
> [...] o Novo SCTIEx trabalhará em estreita sinergia com vários atores, entre eles órgãos do próprio Exército, o Governo, a Academia, as Empresas e Institutos de Pesquisa, as demais Forças e as Agências de Fomento. (VILLAS BÔAS, 2016, p. 17)

O que viabilizaria, pela proposta acima, transbordamentos para projetos/programas da Força, por exemplo o SisFron, o Amazônia Conectada e o Defesa Cibernética, além de possibilitar sinergia de organizações militares do Exército – Ctex, Citex, IME, DCT etc. – com instituições civis.

A seguir, com base em Villas Bôas (2016), listamos (Quadro 3.13) e ilustramos (Figura 3.8) algumas iniciativas que seguem essa linha de pensamento, inseridas no Polo de Ciência e Tecnologia do Exército em Guaratiba-RJ (PCTEG).

Algumas dessas iniciativas foram postas em prática dentro do período desta pesquisa (2008-2018), ainda que não inseridas completamente no Novo SCTIEx, ou até mesmo funcionando antes da implementação de fato desse sistema, mas com o mesmo escopo, uma vez que a intenção de escalões que atuam na área de C&T&I nas Forças Armadas já vinha buscando esse caminho, sobretudo após a END (2008).

Uma experiência do Sisdia de Inovação – embora o resultado tenha sido fora do recorte temporal desta pesquisa – pode ser visto no *workshop* de Pesquisa em Segurança Cibernética na Universidade Federal do Rio Grande do Sul (UFRGS), em que se buscou aproximar o Instituto de Informática daquela instituição acadêmica do Programa Defesa Cibernética na Defesa Nacional.

[103] Publicado no Instituto de Estudos Avançados da Universidade de São Paulo (IEA/USP), em 2016. Disponível em: http://www.iea.usp.br/publicacoes/textos/o-papel-da-ciencia-e-tecnologia-no-processo-de-transformacao-do-exercito-brasileiro. Acesso em: 13 nov. 2019.

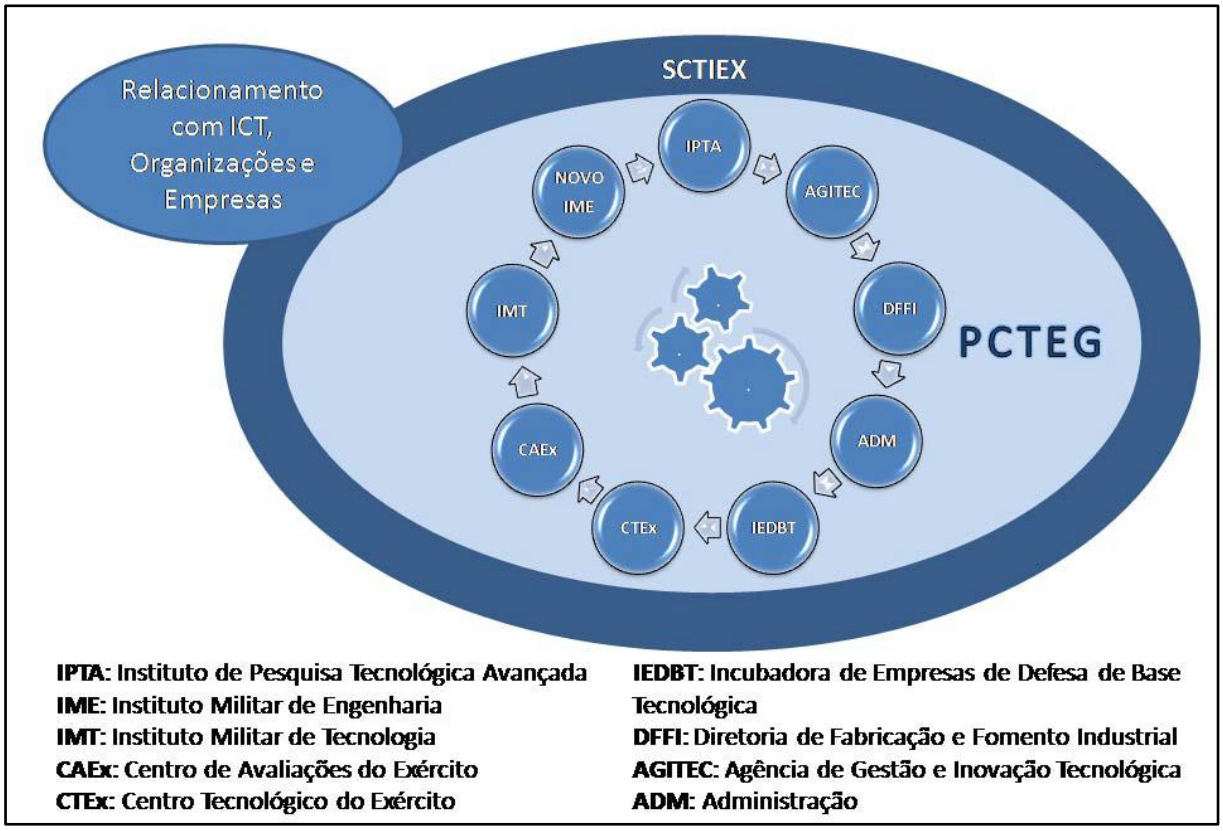
Quadro_3.13: Unidades Componentes do PCTEG e Atribuições Previstas

Unidade	Atribuições
a. Novo Instituto Militar de Engenharia (IME)	- responsável por formar, especializar e aperfeiçoar recursos humanos, pelo ensino superior de Engenharia, e promover a pesquisa científica, para atender às necessidades do Exército Brasileiro e cooperar com o desenvolvimento científico-tecnológico do País.
b. Instituto Militar de Tecnologia (IMT)	- destinado à concepção de projetos de P&D de tecnologia de interesse mútuo do Exército e da Indústria Nacional de Defesa (IND), visando à obtenção de PRODE inovadores e à formação e especialização de tecnólogos militares e civis em áreas de interesse do SCTIEx e da indústria.
c. Centro Tecnológico do Exército (Ctex)	- responsável pela P&D dos projetos de PRODE definidos no Planejamento Estratégico do Exército, em conjunto com a indústria e com a academia.
d. Centro de Avaliações do Exército (Caex)	- responsável pela avaliação dos PRODE desenvolvidos no âmbito do PCTEG e outros materiais produzidos pela BID, de acordo com a normatização internacional, bem como pesquisa na área de metrologia.
e. Diretoria de Fabricação e Fomento Industrial (DFFI)	- encarregada da fabricação, modernização e revitalização de PRODE em complemento à BID, recebimento de licenciamento de tecnologia, o*ffset* e outros meios, transferência de tecnologia por mecanismo de *spin-off* , gestão da Incubadora de Empresas de Defesa do Exército, formação de novas empresas e parcerias por meio de mecanismo de Sociedade de Propósito Específico, gestão do relacionamento com a Indústria de Material Bélico do Brasil (Imbel) e demais empresas da BID e Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (Abimde), dentre outras ações.
f. Agência de Gestão e Inovação Tecnológica (Agitec)	- realiza a gestão da inovação tecnológica, criando um ambiente favorável ao incremento das capacidades científico-tecnológicas e ao desenvolvimento de novos Prode e/ou Sistemas de Defesa para a Força Terrestre. A Agência também é responsável por indicar caminhos da inovação para alavancar os setores industrial e de serviços do País com o uso de tecnologias portadoras de futuro, para que a promoção da Inovação Tecnológica no mercado civil assegure a sustentabilidade da aplicação no setor de Defesa.
g. Instituto de Pesquisa Tecnológica Avançada (IPTA)	- responsável pela Pesquisa e Desenvolvimento de protótipos conceituais inovadores, a partir de estudos da guerra do futuro e da análise de cenários prospectivos realizados pela AGITEC, com a finalidade de antecipar-se às demandas da Força para atuar nesses cenários.
h. Incubadora de Empresas de Defesa (IED)	- encarregada pela incubação de empresas de defesa de base tecnológica, ou seja, empresas novas que se proponham a produzir PRODE inovadores, com elevado conteúdo tecnológico agregado, e, após o período de incubação, ingressar efetivamente na BID.

Fonte: elaborado pelo autor com base em Villas Bôas (2016).

Além da UFRGS e do Exército, participaram desse *workshop* de pesquisa em segurança cibernética representantes da Marinha do Brasil e de empresas de tecnologia do entorno de Porto Alegre, como a CEITEC AS (semicondutores), a DATACOM (equipamentos de comunicações) e a AEL Sistemas (sistemas de defesa). [104]

Figura 3.8: Novo Sistema de Ciência, Tecnologia e Inovação do Exército e o Polo de Ciência e Tecnologia de Guaratiba



Fonte: Villas Bôas (2016).

3.4 POSSIBILIDADES E LIMITES DO SETOR ESTRATÉGICO CIBERNÉTICO

Do visto até aqui, ocorreu entre 2008 e 2018 um processo contínuo de busca de estruturação e de funcionamento do setor cibernético do País, sob a condução, de fato, feita pela instituição Exército Brasileiro. Esse processo incluiu ações tanto voltadas para âmbito do próprio EB, quanto também para as outras Forças e órgãos da Administração Pública Federal,

[104] Informação obtida após consulta deste pesquisador, via e-SIC, ao Comando do Exército, protocolada sob o número 60502002747201991, de 6 de novembro de 2019. Consta dos elementos pós-textuais (Anexo B).

alcançando, não em poucas vezes, o setor privado, como foi o caso do Proteger e das iniciativas relacionadas à BID.

Do Núcleo de Defesa Cibernética do Exército (2009), passando pelo Centro de Defesa Cibernética (2010), também do EB, ao Comando de Defesa Cibernética do Ministério da Defesa, criado em 2016, a partir do planejamento e ações da Força Terrestre, verificamos que esse setor se expandiu no sentido horizontal, abrangendo as outras Forças, e vertical, atingindo o nível político representado nesse caso pelo Ministério da Defesa e pelo GSI/PR.

Essa estruturação não se deu apenas por meio de criação de órgãos ou organizações militares afins (AEGP, Epex, Agitex/DCT etc.). Nesse movimento podem ser fartamente encontradas criações ou aperfeiçoamentos normativos *lato sensu*, diretamente ligados ao MD (Política Cibernética de Defesa, Doutrina Militar de Defesa Cibernética), ou mais abrangentes, interministeriais (Lei nº 12.598/2012, que tratou de condições especiais para compra, contratações e desenvolvimento de produtos e sistemas de defesa; Política Nacional de Segurança da Informação; Programa Nacional de Banda Larga; Estratégia Brasileira para a Transformação Digital – a E-Digital), doutrinários e de ensino (Doutrina Militar de Defesa Cibernética, Escola Nacional de Defesa Cibernética) e de gestão (Projeto Defesa Cibernética, Programa Defesa Cibernética na Defesa Nacional, Sistema Defesa, Indústria e Academia de Inovação).

Ainda como resultado, a BID já pôde ser mapeada e a Seprod/MD, e outros órgãos que participam da concepção do Sisdia de Inovação, como o Epex e o DCT, começaram a colher resultados. Um exemplo foi o credenciamento de uma série de empresas no Regime Especial Tributário para a Indústria de Defesa – o Retid (Lei nº 12.598/2012 e Decreto nº 8.122/2013).

A seguir, no Quadro 3.14, extraímos do *site* do Ministério da Defesa e de dados do governo federal, empresas, categorização (se a empresa é estratégica de defesa ou se é empresa de defesa) e o respectivo produto ou serviço relacionados direta ou indiretamente ao setor cibernético.

Quadro_3.14: Lista de Empresas e Produtos Cadastradas no Ministério da Defesa

EMPRESA/ INSTITUIÇÃO	EED/ED*	PRODUTO
AEL Sistemas	ED	TOP ASSY, LCU (Line of sight Computer Unit)
AGDS	EED	Integração de Sistema/Infraestruturas Críticas - AGDS
ATECH	EED	SPA-GE - Sistema de Planejamento e Análise de Guerra Eletrônica
		SPA-C2 – Sistema de Planejamento e Análise de Comando e Controle
		SERVIÇOS DE PESQUISA E DESENVOLVIMENTO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC) – OPMET
AVIONICS SERVICES	EED	Projeto para Sistemas Embarcados
BLUEPEX	EED	DefesaBR / AVware Software Nacional Antivírus e Antispyware para estações de trabalho e servidores
Cesar	EED	Sistema Aurora-Software para Apoio à Decisão – Cesar
CLAVIS	EED	SADI – Simulador de Ataques Distribuídos de Indisponibilidades – CLAVIS
		Octopus - Software de Segurança da Informação
		Sistema Bart – Baselines, Análises de Riscos e Testes de Segurança
CODE CIPHERS DO BRASIL	ED	CODE CASTLE – Software de Segurança – CODECIPHERS
DATACOM	ED	Comutador Ethernet (Placa de Interface, 24 portas 1000Base-X - SFP e 2 portas 10Gbps – XFP)
DÍGITRO	EED	INVIOLATUS - Sistema que implementa a camada de comunicação segura nas plataformas Dígitro
ENGEVIX	EED	Integração de tecnologia da informação e comunicação (TIC) para soluções
CPqD	EED	DESENVOLVIMENTO DE PROJETOS DE TELECOMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO – FUNDAÇÃO CPqD
KRYPTUS	EED	Módulo de Segurança Criptográfico (HSM - Hardware Security Module) ASI-HSM
Módulo Security Solutions S. A	EED	Software Módulo Risk Manager
NS PREVENTION	EED	Hades – Plataforma de Inteligência Cibernética PIC-NSP
OAS Defesa	EED	Desenvolvimento de Sistemas de Comando, Controle, Comunicações, Vigilância, Inteligência – OAS Defesa
PIQL	EED	Sistema PIQL de Defesa Cibernética
RUSTCOM	EED	Simulador de Operações Cibernéticas – Simoc
SAVIS TECNOLOGIA E SISTEMAS	EED	Desenvolvimento e Integração de Sistemas

* Os requisitos para se tornar uma EED são bem maiores que para uma ED. Dentre esses, destacamos aqueles cuja exigências contêm o teor nacional da empresa, seja pela existência de sede administrativa no País, ou pelo seu respectivo controle. Conforme art. 2º, da Portaria Normativa nº 86/GM-MD, de 2018.

Fonte: BRASIL, 2017. [105]

[105] Disponível em: http://www.dados.gov.br/dataset/produtos-de-defesa. Acesso em: 11 fev. 2020.

Muitas dessas informações dispostas na base de dados governamental condizem com a pesquisa bibliográfica, documental e em sítios da internet, como é o caso da Kriptus, especializada em cibersegurança e criptografia, na qual assistimos à palestra do então Coordenador do Comitê de Cibernética da Associação Brasileira da Indústria de Material de Defesa (Abimde), Roberto Gallo, na *Brazil Cyber Defence Summit & Expo* [106], em Brasília-DF, em 2018; da RUSTCOM [107], da Bluepex [108], da Atech e AEL Sistemas [109], da DATACOM [110], da Dígitro [111], da Fundação CPqD [112], da NS PREVENTION e da OAS Defesa, citadas em várias ocasiões quando se tratava da BID [113] e de seus resultados.

As possibilidades desse setor são inúmeras e, até certo ponto, indefinidas, por se tratar do setor que lida diretamente com a informação em sua forma digitalizada e, por conseguinte, de tecnologias inseridas no contexto da compressão digital, por meio das quais é possível comprimir um sinal para um volume cem vezes inferior ao do sinal de origem, pois são capazes de transmitir a informação, ou informações, em pacotes digitais contendo elementos textuais, sonoros e de imagem compactados (TERRA *et. al*., 2015), o que difere do sistema analógico,

---

[106] Nesse mesmo evento pudemos participar de reunião envolvendo a cúpula do Sisdia de Inovação e assistimos a discussões na busca de parcerias com universidades, indústrias e outras instituições. Também pudemos entender a estrutura do Sisdia, pautada em escritórios regionais que serviriam de fomentadores locais dessa política de inovação. Exemplos de escritórios: Campinas, São Paulo, Recife, Florianópolis e o Núcleo de Estudos Estratégicos do Comando Militar do Sul, em Porto Alegre-RS, este promovendo interação com a UFRGS, como no exemplo do Seminário *Defesa como Estratégia Nacional de Desenvolvimento e de Inserção Internacional do Brasil*. Quanto a esta última informação, disponível em: http://www.ufrgs.br/eventos-estudosestrategicos/evento-1/copy_of_organizacao.

[107] Empresa participante do desenvolvimento do Simulador de Operações de Guerra Cibernética (Simoc), também envolvida com o Sistema de Simulação Construtiva do Comando de Operações Terrestres (Coter).
Um trabalho, de autoria de André Ferreira Alves Machado, oficial do Exército, da Arma de Comunicações, que atua na área de Segurança e Defesa Cibernética, que aborda a utilização do Simoc pode ser consultado em: https://www.gti.uniceub.br/gti/article/viewFile/4322/3635,.

[108] Informe ABIMDE, abril 2017. Disponível em: https://issuu.com/interfacefilmeseartes/docs/abimde_abril_online. Acesso em: 13 fev. 2018.

[109] Informe ABIMDE, abril 2018. Disponível em: https://issuu.com/interfacefilmeseartes/docs/informe_abimde_marco_2018_issuu_. Acesso em: 20 jun. 2018.

[110] Empresa situada em Eldorado do Sul-RS, fabricou produtos intermediários que dão estrutura de telecomunicações, de *backbone* ao acesso de rede, incluindo *design*, monitoramento e gerenciamento.

[111] Ver Portaria 3.439/GM/MD, de 17 de setembro de 2017, que incluiu no rol de produtos de defesa (PRODE), o RAPTUS, que monitora o espectro eletromagnético, e o INVIOLATUS, sistema responsável por garantir comunicação segura na plataforma Dígitro.

[112] Em parceria com o CTEx no desenvolvimento do projeto Rádio Definido por Software (RDS). Detalhamento e resultados dessa parceria, ver: Revista Militar de Ciência e Inovação, edição especial: Gestão da Inovação, 2017, pp. 6-19. Disponível em: http://rmct.ime.eb.br/vol_XXXIV_1sem_2017.html. Acesso em: 10 fev. 2018. Ou em: http://rmct.ime.eb.br/arquivos/revistas/RMCT_1_sem_2017.pdf. Acesso em: 10 fev. 2018. Convém destacar que este projeto se torna muito interessante na medida em que promove interação entre as áreas da guerra eletrônica, que envolve o uso do espectro eletromagnéticos para comunicação via rádio, e a cibernética, pelo uso de *software*. Ver, ainda, artigo: "*Rádio Definido por Software do Ministério da Defesa – visão geral das primeiras contribuições do CPqD"*, publicado no Caderno CPqd Tecnologia – Tecnologia de Defesa, vol. 10, nov. 2014, pp. 9-16.

[113] Relação completa de empresas credenciadas junto à BID como ED ou EED pode ser encontrada em: https://www.defesa.gov.br/arquivos/industria_defesa/cmid/lista_geral_credenciamentos_ed_e_eed.pdf. Relação datada de 19 set. 2017.

que transmite esse conteúdo de forma separada. Esse recurso vai ao encontro da proposta de Transformação do Exército, porque indica a saída do paradigma do meio técnico para o do meio tecnocientífico (SANTOS, 1998) ou informacional (CASTELLS, 2006 [1999]), dos meios e procedimentos da Era Industrial para a do Conhecimento.

Como visto, registramos como um ganho a participação de vários órgãos públicos nessa empreitada. Ao contrário do que imaginávamos *a priori* houve muitas discussões que abarcaram desde a formação de uma agenda *setting* para esse setor, passando pelo planejamento e por sua implantação. Ficamos até certo ponto surpresos com a quantidade de publicações e de arquivos disponibilizados na *internet* em formato de vídeo ou de *slides* de apresentações de órgãos que não estão diretamente inseridos na estrutura da Defesa, e sim de Desenvolvimento, de economia e de finanças, como foi o caso do Ipea, da FGV e do TCU. Em muitos desses textos, as opiniões eram divergentes, o que elevava o nível do debate e proporcionava a correção de rumos, visando à melhor aplicação dos recursos *vis a vis* as demandas.

Em termos ainda de discussões envolvendo a relação recursos-demanda, acompanhamos intensos debates anteriores à escolha da Força que seria a condutora, a Força líder do setor cibernético. A END de 2008 não definiu em seu texto as competências e atribuições. Foi só em 2009 que o MD se manifestou acerca dessas definições, atribuindo o setor nuclear à Marinha do Brasil, o aeroespacial à Força Aérea e o cibernético ao Exército Brasileiro. Quanto aos dois primeiros, seja por razões do histórico de pesquisas, seja pela própria natureza da Força, fica mais fácil de compreendermos essa escolha. Contudo, no tocante ao cibernético, este é objeto de interesse direto de todas as Forças, aliás, do Estado e da Sociedade como um todo, eis que é transversal e contempla o uso das ferramentas tecnológicas disruptivas e as possibilidades daí advindas.

Como limites do setor cibernético, apesar de constar nos documentos de Defesa investigados por nós, em mais de uma vez, a necessidade de subordinação das considerações comerciais em face dos imperativos estratégicos (END, 2008; 2012) e a garantia de uma demanda efetiva e contínua, no sentido de formação e manutenção de um Estado-economia nacional (FIORI, 2004), funcionando, portanto, no nível da economia nacional de List (PADULA, 2007) e ciente do alerta dado por Chang (2004), no tocante à *práxis* de "chutar a escada", o certo é que nosso diagnóstico apontou para alguns percalços de natureza interna ao País.

Os entraves burocráticos foram – e são – muitos, o que corroborou a tese de Agune e Carlos (2017) sobre o que "os governos precisam enxergar". A forma como o governo trabalha, e isso não é exclusividade do Brasil, remonta a conceitos e procedimentos da Era Industrial,

pautado em um modelo em que a *hierarquia*, a *setorialização*, a *especialização* e a *defasagem do arcabouço legal* são características intrínsecas. Sobre essas, assim mencionam Agune e Carlos:

> essas quatro características somadas acabam gerando uma máquina pública pesada, excessivamente burocratizada, autocentrada e inibidora da mudança, incapaz de perceber e acompanhar a profundidade e a velocidade de uma sociedade complexa e plural e uma economia cada vez menos materializada, na qual a inovação passa a ser a rotina. (AGUNE; CARLOS, 2017, p. 147)

Assim, de uma forma geral, o Exército e o Ministério da Defesa, pertencentes à estrutura da APF, logo aos ditames normativos previstos para a coisa e a função pública, apresentam tais características na condução de suas ações, projetos e programas, destarte o movimento na direção de uma transformação.

Por exemplo, a legislação que trata de aquisições de produtos e serviços por parte de órgãos da Administração Pública Federal (APF), como a Lei nº 8.666/1993, tornou bastante complexa a implementação em tempo hábil das ações necessárias para o setor estratégico. Nesse sentido, houve decisões/acórdãos do Tribunal de Contas da União (TCU) que retratam tal dificuldade, como no processo nº 034.424/2013-0 (Acórdão nº 1406/2014), que tratou de

> Possíveis irregularidades ocorridas no Pregão Eletrônico para registro de preços n. 32/2013, promovido pelo Centro Integrado de Telemática do Exército – CITEx, objetivando a contratação de solução composta por hardware e software para análise forense de rede, de tal forma que o tráfego de rede permita realizar: armazenamento, monitoramento, indexação de conteúdo, realização de buscas personalizadas, reconstrução de arquivos e de seções, bem como geração de alertas de segurança e de relatórios personalizáveis que atendam às demandas do órgão licitante. (BRASIL, 2014) [114] [115]

Esse procedimento legal, apesar de ser salutar, a fim de inibir modalidades de corrupção e direcionamento ou privilégio de algum fornecedor, também inibe a aquisição de um produto específico, cuja qualidade ou nível técnico para cumprir determinada missão seja superior. Isso

[114] Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/cibern%25C3%25A9tica/%2520%2520ANOACORDAO%253A%25222014%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/5/%2520?uuid=6272f8b0-4b45-11ea-8b34-4553c756403d. Acesso em: 20 set. 2018.

[115] "O pregão, na forma eletrônica, como modalidade de licitação do tipo menor preço, realizar-se-á quando a disputa pelo fornecimento de bens ou serviços comuns for feita à distância em sessão pública, por meio de sistema que promova a comunicação pela internet." (Fonte: *Site* NormasLegasi.com.br). Lei nº 10.520/2002 (Lei do Pregão Eletrônico), regulamentada pelo Decreto nº 5.450/2005.

sem contar o tempo entre o início e o fim do processo de compra, que no caso em tela se deu por meio de Pregão Eletrônico. [116]

Contudo, parece que o Poder Executivo já sinaliza para atualização do arcabouço normativo que possa impedir ou ser causa de mora na aquisição de equipamentos imprescindíveis a alguma operação de segurança da informação, em sentido amplo [117]. A Política Nacional de Segurança da Informação, aprovada em 26 de dezembro de 2018, prevê dispensa de licitação nos casos que possam comprometer a segurança nacional e cita o caso de "aquisição de equipamentos e contratação de serviços técnicos especializados para as áreas de inteligência, de segurança da informação, de segurança cibernética, de segurança das comunicações e de defesa cibernética." (BRASIL, 2018).

Em se tratando de parte técnica, constatamos ainda dificuldades no sentido de fugir da padronização feita por alguns fornecedores globais – os de *software* proprietário, como indica a nomenclatura da área de informática – seja pela qualidade de seu produto e pelo grau de universalização, seja pelas facilidades oferecidas, como é o caso dos produtos da Microsoft e seu Windows, que terminam exercendo algum grau de coerção ou de instigação para o seu uso. E isso tem relação com a padronização, e tentativa de monopólios, apresentados por nós no capítulo anterior, fruto da constatação de Schumpeter (1997 [1911]) e de Vernon (1966), este via análise do ciclo de vida dos produtos e nos reflexos deste para o comércio internacional, a partir do poder científico-tecnológico. As grandes empresas, e os países que abrigam suas sedes, conseguem ditar a estrutura e o funcionamento do ciberespaço, inseridos aí as camadas do *hardware*, do *software* e do *peopleware*, esta entendida como a camada formada pelos usuários de computadores, de forma geral. Mais que isso, aqui estamos tratando de uma forma de coerção, a partir de recursos econômicos e tecnológicos.

No âmbito do Exército, a fim de tentar escapar dessa instigação/coerção, houve recomendação – e em certos casos determinação – de se utilizar produtos livres (*software* livre – SL) –, isto é, abertos, como é o caso do Linux e da plataforma Ubuntu [118]. Contudo, essa

---

[116] O entrave burocrático para implementação dos projetos não é exclusividade do setor cibernético em sentido estrito. No capítulo seguinte exemplificamos o ocorrido com o Amazônia Conectada, que não atingiu os objetivos propostos, em boa parte, por esses aspectos.

[117] Consoante o Decreto que aprova a Política Nacional de Segurança da Informação, estão contidas no conceito de *segurança da informação*: I - a segurança cibernética; II - a defesa cibernética; III - a segurança física e a proteção de dados organizacionais; e IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. (BRASIL, 2018).

[118] Linux: é um sistema operacional, assim como o Windows, que possibilita a execução de programas em um computador e outros dispositivos. O Linux pode ser livremente modificado e distribuído. É, portanto, um SL. Já Ubuntu é o nome de um sistema operacional construído a partir do núcleo Linux (*Linux Kernel*). É um sistema de código aberto baseado nas normas do *software* livre. Fonte: site Significados – Tecnologia. Disponível em: https://www.significados.com.br/ubuntu/. Acesso em: 10 fev. 2020.

recomendação – ou determinação – em muito é esvaziada, tendo em vista a questão da padronização e consequente (in)compatibilização entre máquinas e programas, das facilidades apresentadas pelas marcas tradicionais, as de *softwares* proprietários, com maior interface e interatividade com o usuário. [119]

Os esforços na direção de não se submeter a essa forma de coerção feita pelas fornecedoras globais proprietárias de *software* não foram pontuais dentre os órgãos da APF, nem tiveram início em 2008; pelo contrário, foram coordenados e em conjunto, oriundos de intenso debate pelos anos 2003/2004. Em 2003, por exemplo, o Governo Federal, por determinação do próprio Presidente da República, instituiu grupo de trabalho para verificar viabilidade de implementação de SL na APF – Decreto Presidencial de 29/10/2003. Apoiaram essa iniciativa, o então presidente do Instituto Nacional de Tecnologia da Informação, Sérgio Amadeu da Silveira, e como instituição especializada, o Serpro. Esse tema, também, foi recorrente nos congressos internacionais sobre *software* livre e governo eletrônico – Consegi.

No âmbito estadual, merecem destaques as iniciativas do Estado do Paraná, pelas leis 14.058, publicada em 28/3/2003, e 15.742, de 18/12/2007, que acompanharam o sentido daquelas iniciativas em favor da implantação de SL na administração, no caso a estadual. O Rio Grande do Sul também foi outro exemplo.

Voltando à área da Defesa, o alto escalão da Força Terrestre [120] é ciente dos riscos que possuem alguns dos produtos universais relacionados à cibernética, como é a existência de *backdoors* instaladas em equipamentos Microsoft/Windows e de programas e serviços do Google, Facebook, Yahoo!, dentre outros, como visto no capítulo anterior, a partir de Harding (2014) e do Senado Federal (BRASIL, 2014), que são capazes de monitoramento e armazenamento constante de informação. Assim está transcrita a participação do Gen. José Carlos em audiência perante CPI do Senado Federal sobre o caso Snowden:

> Dependência tecnológica: a maior parte das redes instaladas no Brasil ou dependem de equipamentos importados ou dependem de operadoras sobre as quais o País possui limitada capacidade de auditagem. Ainda que a criptografia seja de desenvolvimento nacional, se o *hardware* for de fabricação internacional, não se pode garantir que o equipamento não tenha

[119] Em trabalho de conclusão de curso apresentado pelo 1º Tenente Wagner Comin Sonáglio, enquanto aluno da Escola de Administração do Exército (EsAEx), em 2010, publicado em 2011, foram diagnosticadas como as principais dificuldades pelos usuários desse sistema: falta de conhecimento do produto livre (do SL), incompatibilidade entre os sistemas, interface ruim, que não facilita a visualização e o acesso a pastas e arquivos. Ver: *Migração para Software Livre: estudo de caso no ambiente escolar da ESAEX/CMS* (SONÁGLIO; RIBEIRO, 2011).

[120] O General José Carlos dos Santos, um dos pioneiros na consecução do setor estratégico cibernético, mencionou esse risco em audiência pública de Comissão Parlamentar de Inquérito acerca do caso de espionagem dos Estados Unidos relatado por Edward Snowden. (BRASIL, 2014, pp. 198-201).

> uma "porta dos fundos" (*backdoor*) que permita a transmissão de dados sensíveis. Nesse sentido, lembrou que os fabricantes estadunidenses são obrigados, por meio do *Communications Assistance for Law Enforcement Act* (CALEA), a embutir, em seus produtos, *software* que permita às agências de inteligência dos EUA acessar dados que trafegam na rede. (BRASIL, 2014, p. 200)

Essa possibilidade foi levantada também no Capítulo 2 desta tese, a partir da declaração do especialista em segurança da informação [121] e em relato de José Eduardo Portella Almeida, coronel da FAB, em livro publicado pela Secretaria de Assuntos Estratégicos da Presidência da República (BRASIL, 2011) [122], enquanto participante de reuniões sobre segurança e defesa cibernética em grupos de trabalho da ONU, no ano de 2005.

Para contornar essa insegurança, o Exército Brasileiro elaborou e publicou planos de migração para SL, com sua versão inicial em 2004 e alcançando a 3ª edição em 2007 [123]. Nesses documentos, além da finalidade a que se propõe o Plano e a sua relação com a questão do custo/economia, constante no item sobre as "principais razões para a migração" (exemplo de razão citado literalmente no documento: *economia de custos a médio e longo prazo com software fechado*), há expressa em várias ocasiões pontos relativos à segurança (exemplos: maiores segurança, estabilidade e disponibilidade, proporcionadas pelo SL; eliminação de mudanças compulsórias que os modelos fechados impõem, periodicamente, aos seus usuários, em virtude da descontinuidade de suporte a versões; independência tecnológica; possibilidade de auditabilidade dos sistemas e independência de um único fornecedor).

Ainda em 2007, portanto um ano antes do recorte temporal da pesquisa, mas que serviu de elemento norteador para as políticas públicas elaboradas e aprovadas a partir de então, o Exército – e o Governo Federal – pareciam já flertar com o que um ano após, em 2008, apareceria na END. Assim trouxe a 3ª edição do Plano de Migração:

> O momento atual na comunidade e no Governo Brasileiro é marcado por uma nova abordagem na questão do SL, **baseada na visão estratégica e na colaboração entre os atores - empresas, governos, usuários e setor acadêmico**. Desta forma, o DCT deverá atuar como facilitador da colaboração entre o Exército e a Comunidade de Software Livre, inclusive fomentando a

[121] Jonh Douglas Ruwell, do Centro Brasileiro de Perícia na área de segurança da informação, durante o II Seminário sobre Guerra Cibernética, na Academia Militar das Agulhas Negras, no dia 27 de abril de 2013.

[122] Apresentação do resumo do relatório, com apreciação e comentários, em *Desafios Estratégicos para a Segurança e Defesa Cibernética* (BRASIL, 2011, pp. 79-102).

[123] E não só o Exército. A responsabilidade é compartilhada com toda APF. Assim mencionou o Plano de Migração de SL do Exército em relação ao Governo Federal: "O Governo Federal, em seu objetivo de estimular a migração para o SL em Órgãos da Administração Pública Federal, divulgou, e mantém atualizado, o 'Guia Livre' – Referência de Migração para Software Livre do Governo Federal" (www.governoeletronico.gov.br/governoeletronico/index.html). As "Diretrizes de Implementação do Software Livre no Governo Federal" podem ser obtidas por meio do endereço: www.softwarelivre.gov.br/diretrizes. (BRASIL, 2007).

> criação de atividades em linhas de pesquisa, seja no IME ou em outras OM, dadas as suas disponibilidades de pessoal capacitado. **Essas ações devem gerar retorno tanto para o Exército quanto para a Comunidade de SL**, em áreas como Segurança da Informação, Desktop Corporativo, Suítes de Escritório, Servidores Corporativos de Uso Geral, Sistemas Embarcados, Clusters de Alta Disponibilidade, dentre outras. (BRASIL, 2007. pp. 2-3, **grifo nosso**)

Os órgãos da APF também buscaram a migração para SL, seja por razões econômicas, seja pelas de segurança, fomentadas inclusive pelas diretrizes contidas na Política Nacional de Informática, sobretudo em seu artigo 2º, que contempla os princípios dessa Política [124], e que são ratificados pela atual Política Nacional de Segurança da Informação (Decreto nº 9.637/2018) e pela Estratégia Nacional de Segurança Cibernética – E-Digital, aprovada recentemente (em 5 de fevereiro de 2020). Agentes militares, há mais de uma década, também abordam a importância de se atingir esse intento, como apontou a palestra disponibilizada na *internet*, cuja autoria é atribuída ao Coronel Lemos Pita, quando na função de Adjunto da Assessoria 2 do DCT (Figura 3.9): [125]

E o Governo Federal, por meio do Serviço Federal de Processamento de Dados (Serpro)[126] e de Ministérios, como o do Planejamento:

> O secretário de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Rogério Santanna, destacou na abertura do 9° Fórum Internacional de Software Livre (Fisl 9.0), em Porto Alegre, que o software livre é uma opção estratégica do Governo Brasileiro [...] "Quanto mais usarmos software livre, formos independentes de fornecedores de

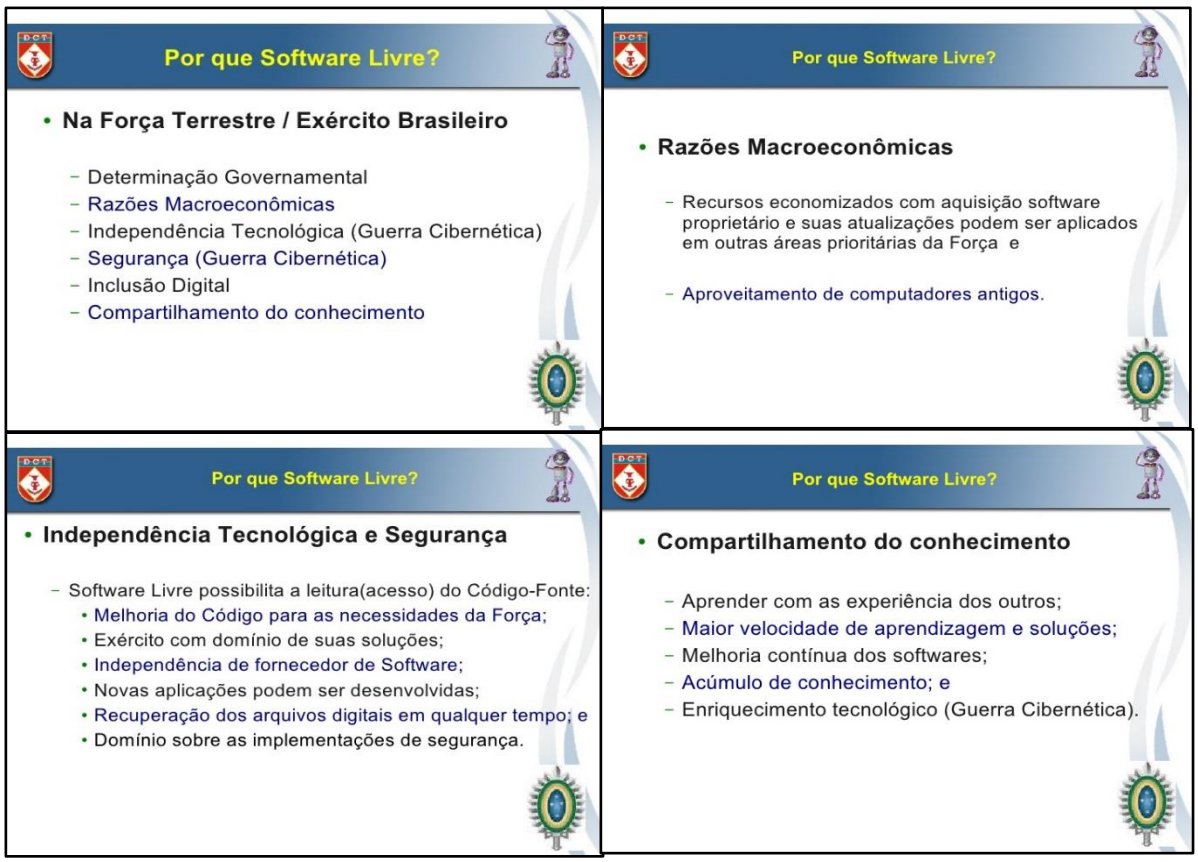
[124] Ver incisos: IV - proibição à criação de situações monopolísticas, de direito ou de fato; V - ajuste continuado do processo de informatização às peculiaridades da sociedade brasileira; VI - orientação de cunho político das atividades de informática, que leve em conta a necessidade de preservar e aprimorar a identidade cultural do País, a natureza estratégica da informática e a influência desta no esforço desenvolvido pela Nação, para alcançar melhores estágios de bem-estar social; VII - direcionamento de todo o esforço nacional no setor, visando ao atendimento dos programas prioritários do desenvolvimento econômico e social e ao fortalecimento do Poder Nacional, em seus diversos campos de expressão; VIII - estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas; [...]. (BRASIL, 1984).

[125] Disponível em: https://pt.slideshare.net/supradados/software-livre-no-exercito. Acesso em: 10 nov. 2019. Para corroborar a autenticidade da autoria, o Serpro indica em seu site, no canal de Comunicação Social, de 7 dez. 2009, a participação desse militar na política do Exército de migração para SL: "Segundo o coronel Lemos Pita, do Departamento de Ciência e Tecnologia (DCT), o uso de tecnologias livres no Exército teve origem há cerca de dez anos, e foi um movimento que começou "de baixo para cima". De acordo com Lemos Pita, a nova versão do Plano de Migração para o modelo livre chegará fortalecida com recente assinatura, pelo Exército, do Protocolo Brasília, que prevê a utilização do padrão aberto para utilização e arquivamento de documentos.". O título da notícia era: "Software Livre é questão de soberania nacional". Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-antigas/software-livre-e-questao-de-soberania-nacional. Acesso em: 10 fev. 2020. Ademais, conhecemos o então Major Lemos Pita quando serviu na AMAN, no início dos anos 2000, na área de tecnologia da informação, o que também corrobora a autenticidade.

[126] Comitê de Implementação do Software Livre no Governo Federal reúne 70 instituições. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-antigas/comite-de-implementacao-do-software-livre-no-governo-federal-reune-70-instituicoes. Acesso em: 20 nov. 2019.

> Tecnologia da Informação e tivermos códigos abertos, melhor será o gerenciamento, a fiscalização e a transparência do governo junto à sociedade". (SOFTWARE LIVRE, 2008) [127]

Figura 3.9: Razões para Utilização de Software Livre



Fonte: DCT (2009).

Ademais, em se tratando de limites ao setor cibernético, os recursos orçamentários previstos para sua implementação e manutenção, embora possuindo continuidade de repasse, tiveram o montante bem inferior, conforme apreendemos na prestação de contas do Ministério da Defesa acerca do Programa vinculado à Ação Orçamentária (AO) 147F, do Programa 2058 – Defesa Nacional, do Plano Plurianual (PPA) 2016-2019, referente à implantação do Sistema de Defesa Cibernética[128], o que comprometeu o cronograma inicial.

A informação acerca deste óbice foi também prestada pelo Departamento de Ciência, Tecnologia e Inovação da Secretaria de Produtos de Defesa, via Serviço de Informações ao

---

[127] Notícia disponível em: http://www.planejamento.gov.br/assuntos/logistica-e-tecnologia-da-informacao/noticias/software-livre-e-opcao-estrategica-de-governo-diz. Acesso em: 10 fev. 2020.

[128] Disponível em: https://www.eb.mil.br/documents/10138/8567855/A%C3%A7%C3%B5es+e+Programas/03d96ae8-91cc-2c54-3440-3670cf13fffb. Acesso em: 13 jan. 2019. Destaque para os documentos das páginas 145-147.

Cidadão do Ministério da Defesa (SIC/MD), a partir da consulta protocolada sob o nº 60502002746201947, de nossa autoria, cujo trecho trazemos em destaque: "[...] o principal óbice reside no baixo orçamento disponível." (BRASIL, 2019).

Esse óbice também pode ser inferido da fala do General José Carlos, quando em audiência na CPI do Senado sobre espionagem dos EUA, em 2014, já mencionada anteriormente:

> Orçamento para segurança cibernética muito inferior ao de outras potências mundiais: no Brasil, o orçamento inicialmente previsto para implantação do setor cibernético dentro do Exército foi de R$400 milhões a ser executado em quatro anos, sendo tal montante reduzido em virtude de cortes orçamentários em toda esfera federal. Sabe-se que as grandes potências mundiais investem montantes na casa dos bilhões de reais. O MD estima que, somente para acelerar a implementação de projetos já em andamento, é preciso dobrar o valor originalmente previsto para o setor. (BRASIL, 2014, p. 200)

Ainda da prestação de contas do MD sobre a AO 147F, são apontados outros fatores intervenientes que prejudicaram o desenvolvimento dessa ação orçamentária, dentre esses: a incerteza da descentralização de créditos, o atraso no desenvolvimento de projetos executivos e a escassez de recursos humanos na área administrativa que possibilitasse fluidez aos processos de licitação. Quanto a esses dois últimos tópicos, enxergamos no Epex – que é vinculado ao Estado-Maior do Exército – uma solução, todavia temos o receio de que na extremidade do circuito de pesquisa, desenvolvimento e produção, isto é, na "ponta da linha", esses entraves administrativos ainda permaneçam por um bom tempo.

Assim, a preocupação demonstrada pelos documentos de Defesa no tocante à garantia de recursos orçamentários contínuos e de maior valor foi, certamente, válida, juntamente com a necessária transformação de consciências apontada por esses. Entretanto, devemos também considerar que os órgãos que compõem o setor de Defesa devem, antes mesmo de planejar e projetar novos produtos ou processos, pensar na possibilidade de transbordamento de suas ações/decisões. Nesse sentido, a pergunta pode ser feita com a seguinte questão embutida: "Como conseguimos atender a essa nova demanda (produto ou processo) de forma a causar um maior transbordamento possível para outros setores e para o desenvolvimento do País?", ou, se preferir: "Como, e quais, universidades, centros de pesquisa, institutos, empresas, poderiam colaborar na consecução de uma demanda da defesa e atingir, além desta própria demanda, dividendos outros para sua permanência ou ampliação de suas capacidades?". Quanto a isso, como apresentamos no capítulo anterior desta tese, os Estados Unidos parecem ter aprendido, e vem praticando, há bastante tempo.

Por fim, aos propósitos que traçamos, e pelo limite de tempo e de espaço desta tese, um ponto mereceu receber atenção, pois apareceu não poucas vezes, quando em conversas para se descobrir entraves para o desenvolvimento de tecnologias de Defesa e para a consolidação da hélice tríplice. Além das já apresentadas questões econômicas, envolvendo a escassez, a sazonalidade ou a burocracia orçamentária, o que gera desconfiança e prejuízo por parte da oferta, isto é, da indústria, foi indicada a barreira ideológica entre Forças Armadas e Universidade, sobretudo a pública, como um aspecto bastante sensível, o que afeta a interação entre duas das hélices do sistema e que torna ainda mais complexo o êxito desse empreendimento.

Aqui, portanto, saímos do campo econômico e adentramos na seara política e histórica da realidade nacional, quiçá, também, de boa parte da América Latina. Lembramos, todavia, que a alteração no nome dos documentos de Defesa não foi por erro ou por displicência gramatical, pelo contrário, tratou de buscar justamente a conversão de esforços da sociedade, como um todo, para um interesse comum, o do desenvolvimento nacional, com independência. Nessa direção, por conseguinte, é necessário pensarmos e apontarmos soluções imediatas, a fim de minimizarmos desconfianças recíprocas, quando e onde existirem. Embora não faça parte desta pesquisa, temos que essa questão é nevrálgica e, até certo modo, persistente na realidade brasileira, o que culmina na criação de obstáculo perene e bastante difícil a ser transposto, entretanto, porém, a história exige, e a cibernética, com suas infovias, pode ser um canal nessa direção.

3.5 CONSIDERAÇÕES PARCIAIS

Neste capítulo vimos a estruturação da Defesa a partir do *status* dado ao setor cibernético como estratégico para o País, em 2008, com a publicação da END pelo Decreto Nr 6.703, oriundo do Estado-Maior Interministerial Nr 00437/MD/SAE-PR.

Esse documento, basilar para as iniciativas do setor de Defesa e de outros afins, como notamos ao longo da investigação, foi dividido em duas grandes partes, uma tratando da formulação sistemática e outra das medidas de implementação. No tocante à primeira, esta anunciou: três eixos estruturantes, que versaram sobre *reorganização das Forças Armadas*, *reestruturação da indústria brasileira de material de defesa* e considerações sobre *composição dos efetivos das Forças Armadas*; 25 diretrizes e três setores estratégicos, dentre os quais o

cibernético, juntamente com o nuclear e o espacial. 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, destacamos a Política Nacional de Defesa e o Livro Branco da Defesa Nacional, ambos de 2012. 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, ou pelo menos minimizar, uma corrida armamentista, por exemplo.

De volta ao binômio Defesa-Desenvolvimento, resgatamos da parte teórica do capítulo anterior a natureza da Defesa para os estudos econômicos. As ações e, logo, os investimentos nesse setor são considerados como uma das falhas de mercado, por serem bem público. Mais que isso, Defesa é um bem público puro, tendo em vista a particularidade concedida aos Estados nacionais pelo princípio da soberania, remontado a Westfália, 1648, e a noção *hobbesiana* de sistema. Por esse princípio, ao Estado cabe o monopólio do uso da força *weberiano*, isto é, dos mecanismos legítimos de coerção e coação, para seu âmbito interno e externo, neste último caso concorrente com os demais atores do sistema internacional de mesmo nível.

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 tratamos de casos de benefício marginal social e do efeito multiplicador que algumas ações estatais podem gerar. Em outras palavras, aqui abordamos a conciliação do conhecido dilema entre investimento "em espadas ou em arados". A alternativa para esse aparente impasse está no próprio binômio instituído pela END ou no que a literatura especializada denominou investimentos militares bivalentes. Contudo, propomos ir além: a Defesa não serve apenas de escudo para o Desenvolvimento, como consta na END (2008) – pelo menos não na experiência norte-americana. Mais que isso: 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 sobre o dilema *escassez de recurso* e *custo de oportunidade*, para resultar em – além do aumento da capacidade de coerção – instrumento potencial de desenvolvimento.

Nesse sentido, a END e a PND previram como necessidade o papel do Estado como garantidor da demanda efetiva *keynesiana* (1936) e de Kalecki (1989 [1954]), só que voltado

para produtos de defesa. Pudemos 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, aprovada a partir de uma medida provisória editada ainda em 2011 (MP nº 544), 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.

Com relação à Seprod e à sua articulação com o setor cibernético, a percepção que tínhamos *a priori* era de pouca ligação ou nenhuma, apesar da intenção anunciada quando da criação da secretaria. Em solicitação feita por meio do sistema de informação ao cidadão (Anexo A), obtivemos como resposta a ratificação daquela percepção inicial, na qual a Seprod afirmou não possuir envolvimento direto quanto ao desenvolvimento do setor cibernético e que acompanhava apenas extraoficialmente a gestão deste setor por parte do Exército. O que notamos, portanto, foi a permanência de grande autonomia das Forças em gerenciar seus programas e projetos e a baixa articulação dessas com a Seprod.

Com relação a entraves, os que envolvem questões administrativas, como processo de licitação, de empenho e de gasto orçamentário, foram algo comum nos projetos e programas do setor. Além disso, a necessidade de recursos humanos especializados nessa área também foi uma constante apontada na literatura e percebida na forma empírica ao longo do período de pesquisa. Quanto a este, acreditamos ser de razão estrutural, isto é, uma necessidade do País, uma vez que a área cibernética envolve assuntos, disciplinas e cursos que demandam conhecimentos de ciências exatas – matemática, física, informática, criptografia, engenharia, por exemplo – nos quais, pelos dados de *rankings* de educação, como o do Programa Internacional de Avaliação de Alunos (Pisa) e do índice de Desenvolvimento da Educação Básica (Ideb), o Brasil apresenta nível bastante baixo.

Outro entrave encrustado na estrutura, só que agora do sistema internacional e de seu comércio, diz respeito à padronização – obtida por algumas empresas, a partir de inovações disruptivas desenvolvidas, que geram monopólios, ainda que temporários – com relação a produtos e serviços em âmbito global, como são os casos da *Microsoft* e da *Aplle*, conforme vistos no capítulo anterior. No tocante à cibernética e ao desenvolvimento de inovações tecnológicas ligadas a essa área, isso passa a ser um problema, tal qual pudemos acompanhar no processo de implementação da plataforma de *software* livre, tanto no Exército quanto em

toda a estrutura da APF no Brasil. Podemos afirmar que o processo de migração para o SL ainda não foi concluído, por apresentar inúmeros óbices, quase todos relacionados à questão da padronização, daí concluímos que se essa capacidade funciona como uma forma de coerção.

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.

Ainda como aspecto negativo, constatamos sazonalidade no tocante à diretriz estratégica de nº 18 (END, 2008), relacionada à integração da América do Sul. Sobre o fomento da cooperação militar regional, este ocorreu parcialmente, com criação de cursos e estágios envolvendo participação de militares dos países sul-americanos, como foi o Curso Avançado de Defesa Sul-americana, que ocorreu na Escola Superior de Guerra (ESG). Contudo, no aspecto ligado à formulação de uma base industrial de defesa regional, embora também constasse nos Planos de Ação do Conselho de Defesa Sul-Americano (CDS) da Unasul, este não foi implementado, sobretudo após 2016.

Em se tratando da formação de um complexo militar-industrial-acadêmico (MEDEIROS, 2004) ou de um complexo militar-universitário industrial, consoante a END (2008 e 2012), pelo lado do Exército verificamos esforços nesse sentido, consubstanciados através da criação de um escritório de projetos, o Epex, para gerenciar projetos e programas e fomentar a articulação com instituições civis, a formulação do SisDIA de Inovação, que trouxe explicitamente, nas palavras do General Villas Bôas, então comandante do Exército, a inspiração da hélice tríplice para dentro da estrutura da Força, a construção de um tecnopolo em Guaratiba e as parcerias entre os estabelecimentos de ensino militar, como do IME e do ITA, e civil, como o CPqD foram realidades.

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 podemos 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.

Visando atender à END e ao contexto internacional contemporâneo, no que diz respeito à natureza da guerra, o Exército Brasileiro – Força Armada responsável por conduzir o setor estratégico cibernético – elaborou o Processo de Transformação (2010), pelo qual propôs ações no sentido de levar a sua capacidade de operação de uma Era Industrial à do Conhecimento. Como consequências desse processo, foram elencados imperativos que serviriam como conceitos norteadores dessas ações. Para os propósitos desta pesquisa, destacamos o imperativo do *monitoramento*, *comando/controle* e *mobilidade*, perfazendo um trinômio. Por esses, o Exército buscou materializar sua transformação adequada às capacidades orçamentárias *vis a vis* as características de seu território (dimensão/superfície, fronteiras, vegetação, relevo, clima). Como consequência, preteriu-se a ocupação física, humana, propriamente dita, por meio dos pelotões especiais de fronteira, ao uso de equipamentos e sistemas que permitissem atuar conforme o trinômio eleito. Assim, como trouxe a END em usa diretriz estratégica nº 9: "[...] os vigias alertam. As reservas respondem e operam [...]" (BRASIL, 2012, p. 53). Dessa forma atendeu-se a questões que envolvem pilares da geopolítica tradicional, por tratar de espaço terrestre e poder, de uma geopolítica contemporânea, a qual inclui a existência de novos espaços e atores no sistema internacional, e o que Bertha Becker denominou cronopolítica, tendo em vista a premissa do tempo nas formulações ligadas à logística da preparação para a guerra e para o desenvolvimento. Aqui se buscou o domínio do espaço e do tempo pelo meio do elemento-chave *informação*, pela capacidade de monitoramento, de comando e controle e de atuação, no local e hora oportunos – mobilidade. Aqui, também, buscou-se capacidade de (re)territorialização.

No capítulo seguinte e final deste relatório de pesquisa, e respectiva reflexão, anunciamos ações, projetos e programas que não estão diretamente inseridos no setor cibernético ora apresentado, capitaneado pelo Exército Brasileiro, porém que são extremamente vinculados a este, seja por servir de estrutura, seja para permitir o funcionamento daquele setor. Nessa parte abordamos a composição de novas infovias, físicas e virtuais; a participação em atividades de segurança cibernética, em operações interagências e a preparação de recursos

humanos, planejadas e implementadas também por outros setores da APF, como foi o caso do MCTIC [129] e do MEC. Passemos a esses então.

[129] De 2008 a 2011, denominado MCT, de 2011 a 2016, MCTI. A partir de então, MCTIC, incorporando as atividades ligadas ao antigo Ministério das Comunicações.

CAPÍTULO 4

A CIBERNÉTICA COMO SETOR ESTRATÉGICO E SEUS REFLEXOS PARA ALÉM DA DEFESA

O setor estratégico da cibernética, consoante o previsto na Política e na Estratégia Nacional de Defesa, e no recorte textual desta pesquisa, teve sua influência percebida para além da estrutura de Defesa propriamente dita.

Inúmeros foram os órgãos da APF inseridos ou que passaram a fazer parte de iniciativas para esse setor, direta ou indiretamente, explícita ou implicitamente. Isso pode ser inferido de estudo de normatizações e estratégias oficiais, e consequentes programas e ações, que envolveram o emprego de tecnologias de informação e comunicações (TICs) por parte do governo federal, tendo como fim a sociedade, tanto em termos de benefícios na área de segurança e defesa, quanto nas áreas econômica, educacional e tecnológica.

Além de documentos estritos de Defesa, como visto no capítulo anterior (Política e Estratégia Nacional de Defesa, Política Cibernética de Defesa, Doutrina Militar de Defesa Cibernética, por exemplo), podemos mencionar o Programa Nacional de Banda Larga (PNBL), a Estratégia Brasileira de Transformação Digital (E-Digital), documentos orçamentários, análises e acórdãos de órgãos federais, como foi o caso do Tribunal de Contas da União (TCU), e relatórios de comissão específica na área de tecnologia e de Comissão Parlamentar de Inquérito (CPI) do Senado. Contudo, focamos nossa análise nas normatizações e ações mais específicas quanto a TICs, que correlacionaram essas ferramentas com a participação de órgãos da estrutura de Defesa e que incluíram ganhos econômico-sociais.

Optamos por esta seleção, também, por razões de coerência metodológica, do ponto de vista dos atores envolvidos na discussão, elaboração e implementação dessas políticas públicas

e a necessidade de ligação desses, ainda que indireta ou ocasionalmente, com algum órgão da Defesa na condução ou na execução de ações.

Também no tocante à metodologia, decidimos dividir o capítulo nos blocos *normatização e estratégias, programas e ações*, e *contribuições de instituições de pesquisa*, seguindo, em cada um desses, a respectiva cronologia.

Algumas das publicações e estratégias pesquisadas e analisadas, da mesma forma que os programas e as ações, como constam adiante, exigiram uma atenção e profundidade maior na análise, tendo em vista a riqueza de detalhes e a intrínseca relação com a temática do transbordamento para além do setor Defesa. Dentre esses, o Programa Nacional de Banda Larga, lançado em 2010, foi decisivo, na medida em que ocorriam concepções de outros projetos e programas relacionados ao setor, pois passou a ser um pilar, no qual se ancorou uma série de ações interministeriais, com integração entre entes de pelo menos dois níveis da federação – o federal e o estadual – e entre os Poderes da República, como foi o caso específico do Programa Amazônia Conectada (2014-2018) [130], e do Programa Proteção Integrada das Estruturas Estratégicas Terrestres (2012), do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (2017) e do cabo submarino Brasil-Europa (2014). [131]

No bloco *contribuições de instituições de pesquisa*, acreditamos por bem registrar e tabular alguns esforços realizados por centros especializados de pesquisa brasileiros, no intuito de, por um lado, valorizarmos o trabalho dessas instituições e, por outro, utilizarmos esses registros, *per se*, como subsídio na fundamentação de nossa tese, no tocante às iniciativas na área de Defesa que geraram, ou que podem vir a gerar, transbordamentos para outros setores.

Começamos, então, pelo bloco *normatizações e estratégias interministeriais*.

---

[130] Em 2019, após acórdão do Tribunal de Contas da União, o MCTIC lançou o Programa Amazônia Integrada e Sustentável (Pais), com previsão de início de implantação em março de 2020. A finalidade é englobar o antigo Amazônia Conectada e ampliar o alcance do fornecimento de banda larga na Região Norte do Brasil e para países vizinhos que estejam na denominada Pan-Amazônia. A implantação e operacionalização da infraestrutura ficará a cargo da Rede Nacional de Ensino e Pesquisa (RNP). Um detalhamento do Pais pode ser encontrado no seguinte link da Câmara dos Deputados: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cindra/arquivos/17-09-2019-1. Acesso em: 21 abr. 2020.

[131] Nossa opção por aprofundar a análise desses projetos/programas ocorreu também por esses serem mencionados em mais de um órgão federal, como foi a referência pelo TCU, quanto à reativação da Telebras pelo PNBL: "Deu-se início ao programa de lançamento do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), com a edição do Decreto nº 7.769/2012. Esta ação, em termos financeiros, é a mais relevante do PNBL e uma importante ferramenta para permitir o acesso à banda larga nas regiões remotas do país. A Telebras iniciou [2015] as tratativas para a construção de um novo cabo submarino conectando o Brasil e a Europa, a fim de ampliar a capacidade de tráfego entre os dois continentes, baratear custos de transmissão e proporcionar mais segurança aos dados transportados." (BRASIL, 2015, p. 29).

4.1 A CIBERNÉTICA COMO SETOR ESTRATÉGICO E SEUS REFLEXOS PARA ALÉM DA DEFESA: NORMATIZAÇÕES E ESTRATÉGIAS INTERMINISTERIAIS

4.1.1 Programa Nacional de Banda Larga (PNBL) – "Brasil Conectado"

O PNBL foi instituído em 12 de maio de 2010, a partir do Decreto Presidencial nº 7.175, fruto de reunião convocada pelo então presidente Luís Inácio Lula da Silva, ainda em setembro de 2009, a fim de coordenação e otimização de atividades com os principais ministérios que estivessem envolvidos com alguma ação voltada para a inclusão digital, tais como o Ministério da Educação, o da Cultura, o das Comunicações e o da Ciência e Tecnologia. [132]

O decreto trouxe como objetivos do programa o fomento e a difusão do uso e fornecimento de bens e serviços de tecnologia de informação e comunicação, com ações voltadas para a ampliação do acesso à *internet* de banda larga [133], a inclusão e capacitação digital, a diminuição de desigualdades social e regional, o desenvolvimento econômico e social, a geração de emprego e renda, o aumento da capacidade dos serviços de Governo Eletrônico (e-Gov), a busca de autonomia tecnológica e o aumento da competitividade brasileira.

Segundo o documento-base do PNBL, divulgado em 30 de novembro de 2010, pela Secretaria-Executiva do Comitê Gestor do Programa de Inclusão Digital (CGPID), este programa se constituiria em elemento central de uma política pública que definisse diretrizes tanto para o mercado quanto para as ações do Estado, tendo como premissa básica a inclusão social via inclusão digital. Assim trouxe o aludido documento: "A inclusão social possui hoje uma nova e importante dimensão: a inclusão digital. A estratificação social e o acúmulo de riqueza cada vez mais se dão em função da capacidade de acessar, produzir e circular o conhecimento" (BRASIL, 2010, p. 6) e ratificou apontando que a questão social não pode ser resultado marginal de uma política de telecomunicações do País. Pelo contrário, essa questão deve ser o primeiro e último objetivo (BRASIL, 2010). Para os idealizadores desta política, a infraestrutura de banda larga serviria como fator de indução do desenvolvimento e de

[132] Texto do decreto disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7175.htm

[133] Banda larga – segundo o documento-base do PNBL, não há consenso quanto ao conceito de banda larga. Na verdade, o governo brasileiro preferiu certa fluidez, uma vez que o mais importante é a disponibilização da infraestrutura que possibilite "o tráfego de informações contínuo, ininterrupto e com capacidade suficiente para as aplicações de dados, voz e vídeo mais comuns ou socialmente relevantes" (BRASIL, 2010, p. 18). Dessa forma, o documento não mencionou a capacidade em termos de linguagem técnica das TICs, mas sim de sua capacidade de aplicação. Em pesquisa complementar, percebemos que não há realmente consenso no tocante à definição de "banda larga" em termos técnicos. De modo geral, é mencionada a capacidade de 10 Mbps (megabits por segundo). Contudo, há referência indicando 15 e até 20 Mbps.

"desconcentração de oportunidades", além de buscar impedir ou pelo menos mitigar o desenvolvimento assimétrico entre as regiões do Brasil.

O PNBL foi inspirado em políticas de expansão de banda larga feita por outros países, alguns em momentos de crise econômica, funcionando, assim, como medida anticíclica, na forma do receituário *keynesiano*. São citados, como exemplos: Alemanha, Austrália, Canadá, Estados Unidos, Coreia do Sul, Japão, Portugal e Singapura. Nesses casos, disse o documento-base do PNBL, a "desconcentração de oportunidades" se caracterizou pelo acréscimo dessa infraestrutura de telecomunicações para a área rural e localidades remotas desses países (BRASIL, 2010).

Ainda como fonte de inspiração do programa, dados do Banco Mundial, quanto ao retorno econômico de investimento nesse setor, diretamente ou por externalidades, são bastante promissores: 1) a cada U$ 5 bilhões investidos em infraestrutura de telecomunicações, são criados de 100 a 250 mil empregos diretos e algo em torno de 2,5 milhões de indiretos; 2) nos países de renda baixa ou média, a cada 10% de aumento de penetração de infraestrutura e serviço de banda larga, há o acréscimo de 1,38% do PIB per capita; 3) a banda larga favorece tanto a economia denominada tradicional (setores tradicionais – agropecuária, extrativismo,...), por tornar possível o aumento de produtividade, pelo uso de TICs, como a economia da informação e do conhecimento propriamente dita (BRASIL, 2010).

Durante avaliação dessa política pública, em relatório emitido em dezembro de 2014, da Comissão de Ciência, Tecnologia, Inovação, Comunicações e Informática do Senado Federal[134], outros pontos foram destacados, sendo, talvez o principal, a possibilidade que o PNBL trazia para o cumprimento da Lei nº 9.472/1997, a Lei Geral de Telecomunicações, a qual prevê o papel do Estado em fornecer acesso a esse recurso, o que resultou na "recriação" da Telebras S. A., que tinha sido privatizada em 1998. Para o relator, esse ponto foi considerado muito positivo como consequência do PNBL.

A partir de então, a Telebras participou diretamente da consecução de satélites, como o SGDC, em parceria com a Empresa Brasileira de Aeronáutica S. A. (Embraer), da implementação da rede nacional de fibra ótica (RNP) e iniciou negociação para construção do cabo submarino Brasil-Europa.

[134] Por meio da Resolução nº 44/2013 do Senado Federal, este órgão do legislativo federal passou a sistematizar as atividades de acompanhamento, fiscalização e controle de políticas públicas realizadas por meio de suas comissões permanentes. A política selecionada para avaliação em 2014 foi o PNBL, conforme Requerimento nº 3 do Presidente da Comissão de Ciência, Tecnologia, Inovação, Comunicações e Informática do Senado Federal.

O Senador Aníbal Diniz, relator do documento em tela, durante o ano de 2014 participou de audiências públicas, *workshops* e reuniões com partes envolvidas no PNBL. Desses eventos, esse senador destacou sua participação no Congresso Latino-Americano de Satélites, em setembro, oportunidade na qual teve de conhecer melhor a proposta do SGDC e a importância das tecnologias de satélites para o País e para o PNBL:

> Vale enfatizar a importância do SGDC para o país. O satélite governamental não somente acolherá os anseios do Ministério da Defesa, em relação à segurança nacional, mas sobretudo possibilitará o atendimento de banda larga nas áreas mais isoladas do nosso território. Em termos financeiros, o SGDC é a ação mais relevante do PNBL [...]. (BRASIL, 2014, p. 7)

Nessa parte do relatório, a autoridade legislativa, ainda que sem essa intenção originariamente, apontou na direção de relação entre aspectos da segurança nacional com o desenvolvimento, este dentro da concepção do PNBL, de inclusão social via inclusão digital.

Continuando a avaliação do PNBL, o Senador Aníbal Diniz participou de reunião com o então presidente da Telebras, Francisco Ziober Filho, e outros funcionários daquela empresa, e de audiências públicas ao longo do mês de novembro de 2014, sendo a última, no dia 18, com representantes do Ministério da Defesa, do Instituto Nacional de Pesquisas Espaciais (Inpe), da Visiona Tecnologia Espacial S. A. – *joint venture* formada em 2013 pela Telebras e Embraer para possibilitar a execução do SGDC –, do Ipea[135] e da Agência Espacial Brasileira (AEB). Por esse esforço, percebemos a intenção no sentido de êxito dessa política, tanto por agentes ligados ao setor aeroespacial e de Defesa, quanto políticos e econômicos, indo muito além de órgãos da APF, envolvendo uma variedade de atores. Contudo, nem tudo foi positivo do PNBL.

No relatório da Comissão de Ciência, Tecnologia, Inovação, Comunicações e Informática do Senado Federal que usamos como referência, e que em muitas partes foi ao encontro de relatórios elaborados pelo TCU, o Brasil Conectado apresentou uma série de problemas, mormente de ordem orçamentária. Como exemplo, dos R$ 2,9 bilhões de investimentos previstos para o PNBL nos anos de 2012-2013, pelo Plano Plurianual (PPA) 2012-2015, apenas R$ 314,7 milhões foram realmente computados e, desses, somente R$ 214,1

[135] A participação do Ipea em assuntos envolvendo Defesa e Desenvolvimento ocorreu, de 2008 a 2018, em muitas ocasiões por nós verificadas e por diversas formas, além da presencial em eventos da natureza aqui relatada. Foram inúmeras publicações, tanto da espécie de textos para discussão, quanto levantamentos minuciosos a respeito da base industrial de defesa, passando por análise estratégica do entorno regional sul-americano e a inserção do Brasil no cenário internacional. Por isso, resolvemos inserir uma seção neste capítulo para registrar de forma sistematizada esses feitos.

milhões, isto é, 7,4% do previsto incialmente, teve sua execução orçamentária concluída (BRASIL, 2014).

Outro aspecto verificado foi a falta de continuidade de planejamento do SGDC, no sentido de lançamento de outros veículos do tipo. Devido à importância constatada pelo senador relator, foi recomendada a elaboração de um novo PNBL, de modo que as políticas públicas do setor de telecomunicações fossem articuladas e com horizonte de longo prazo.

Esse ponto tornou-se importante em nossa pesquisa, pois vimos que é um problema comum, que se repete nos programas e ações governamentais, pelo menos para essa área. Além disso, todavia ainda relacionada ao setor espacial e às suas possibilidades, houve recomendação nesse relatório para ampliar investimentos públicos para lançamento de novos satélites de comunicação, e fomentar parcerias de novos agentes, públicos e privados, e em todos os níveis da federação.

Como ganhos, em linhas gerais, o relatório destacou a (re)criação da Telebras e o desempenho de seu papel no tocante à universalização de acesso à *internet*, buscando cumprir legislação sobre fornecimento de telecomunicações por parte do Estado, consoante Lei Geral de Telecomunicações [136], de 1997, em seus artigos 2º, inciso I, e 79, §1º, por exemplo, e no atual Marco Civil da Internet (Lei nº 12.965/14) [137], mais precisamente em seu artigo 4º, inciso I. [138]

Por fim, ressaltou o documento do Senado Federal que a consecução do PNBL e sua continuidade poderia se tornar um aspecto importante no sentido de o Brasil se tornar liderança regional sul-americana nesse setor, com possibilidade de aglutinar parceiros externos por meio da oferta de banda larga (BRASIL, 2014).

---

[136] Lei nº 9.472: art. 1º - "O Poder Público tem o dever de: I - garantir, a toda a população, o acesso às telecomunicações, a tarifas e preços razoáveis, em condições adequadas; [...].”; art. 79 - "A Agência regulará as obrigações de universalização e de continuidade atribuídas às prestadoras de serviço no regime público. § 1° Obrigações de universalização são as que objetivam possibilitar o acesso de qualquer pessoa ou instituição de interesse público a serviço de telecomunicações, independentemente de sua localização e condição sócio-econômica, bem como as destinadas a permitir a utilização das telecomunicações em serviços essenciais de interesse público." (BRASIL, 1997).

[137] Lei nº 12.964/14: art. 4º - "A disciplina do uso da internet no Brasil tem por objetivo a promoção: I - do direito de acesso à internet a todos; [...].” (BRASIL, 2014).

[138] Em complemento, assim se pronunciou o TCU quanto à reativação dessa estatal pelo PNBL: "Ainda por força desse normativo, houve reativação da Telebras, à qual restou a atribuição de: a) implementar a rede privativa de comunicação da administração pública federal; b) prestar apoio e suporte a políticas públicas de conexão à Internet em banda larga para universidades, centros de pesquisa, escolas, hospitais, postos de atendimento, telecentros comunitários e outros pontos de interesse público; c) prover infraestrutura e redes de suporte a serviços de telecomunicações prestados por empresas privadas, estados, Distrito Federal, municípios e entidades sem fins lucrativos; e d) prestar serviço de conexão à Internet em banda larga para usuários finais, apenas e tão somente em localidades onde inexista oferta adequada daqueles serviços." (BRASIL, 2015, p. 28).

Ainda, no que diz respeito ao PNBL, sua existência viabilizou inúmeras iniciativas governamentais na direção de universalização de acesso à *internet* no Brasil, sobretudo voltadas para regiões do País com maior déficit desse serviço. Dessa forma, não só o SGDC, como foi abordado e ressaltado no relatório da Comissão de Ciência, Tecnologia, Inovação, Comunicações e Informática do Senado, surgiu como resultado anexado a esse programa, mas também o Programa Amazônia Conectada, cujo ator principal na sua condução – o Ministério da Defesa/Exército Brasileiro –, de fato, nem foi designado inicialmente para participar do Comitê Gestor do Programa de Inclusão Digital (CGPID), responsável da condução do PNBL.

Com relação ao CGPID, este sofreu várias críticas pela omissão em suas funções, tanto referentes ao seu próprio funcionamento, quanto às de acompanhamento, como a inexistência de relatórios parciais e anuais de implantação do programa[139]. Contudo, constatamos que houve avanço, tanto no sentido socioeconômico quanto no relacionado à área de Defesa, uma vez que os ministérios dialogaram entre si, ainda que em momento posterior, e buscaram otimizar suas demandas e, assim, maximizar os revezes orçamentários, que não foram poucos.

Em 2011, para substituir essas funções do CGPID, foi criada a Secretaria de Inclusão Digital (SID), pelo Decreto nº 7.462/2011, na estrutura do Ministério das Comunicações (BRASIL, 2015); todavia persistiu, em relação à gestão da política pública, "a dificuldade de coordenação e articulação tanto entre os diversos órgãos do governo federal que, de alguma forma, atuam na política pública de inclusão digital como entre o governo central e os órgãos estaduais e municipais" (BRASIL, 2015, p. 68), pois apesar de sua competência legal, a SID do Ministério das Comunicações "possuía ingerência limitada em relação a diversas ações de inclusão, não tendo, em alguns casos, participação efetiva em seus processos de elaboração, acompanhamento e avaliação" (BRASIL, 2015, p. 68), como ocorreria com o Amazônia Conectada, por exemplo, citado em acórdão do TCU, em 2019, detalhado adiante neste trabalho.

Em 2017, aproveitando-se da experiência e lições acumuladas com o PNBL, e dos respectivos resultados, um grupo de trabalho foi instituído no Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), por meio da Portaria nº 842. Nesse documento, constam algumas alterações em relação ao Brasil Conectado, tais como: a redação literal de princípios ligando Defesa e Desenvolvimento, como consta do artigo 2º dessa Portaria:

---

[139] Segundo o TCU, quanto ao CGPID, "apesar de oficialmente não ter havido sua dissolução, as atividades exercidas pelo citado comitê limitaram-se a duas reuniões, ocorridas em julho de 2010, conforme Ofício 293/SE-C. Civil/PR, [...] não exercendo, assim, suas atribuições relacionadas à articulação da política." (BRASIL, 2015, p. 40).

"VI – o papel central da pesquisa e desenvolvimento em tecnologias da informação e comunicação para a garantia da competitividade e soberania nacional" e a participação de membros do Ministério da Defesa e do das Relações Exteriores no grupo de trabalho ora instituído (BRASIL, 2017). Em 2018, como consequência, foi instituído um novo marco para a inclusão digital no País. Tratou-se da Estratégia Brasileira para Transformação Digital, a E-Digital.[140]

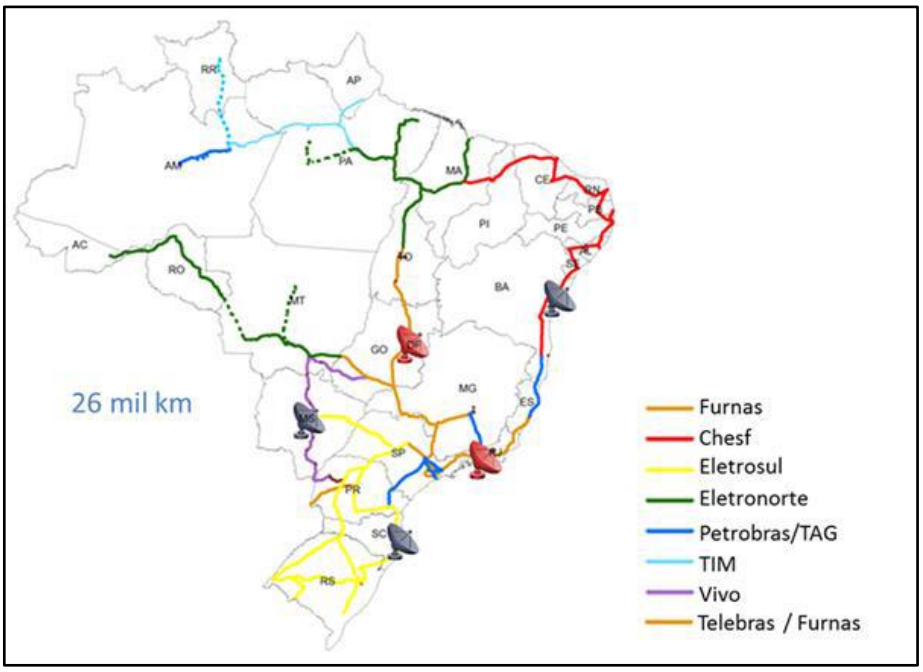
Antes de passarmos para a E-Digital, cabe o registro dos resultados, em termos de infraestrutura de rede, obtidos pelo PNBL e Telebras. Esse esforço, durante o período 2010-2018, ganhou um aporte de força, a partir da publicação do Decreto nº 8.135/2013, que passou a exigir que todas as comunicações da administração pública federal, direta ou indireta, tramitassem por redes de tecnologia da informação e comunicações da própria administração e de subsidiárias. Com isso, a rede nacional de banda larga, ou *backbone* nacional, que era de cerca de 11.000 Km de extensão, em 2011, passou para mais de 25.000 Km, em 2018 (Figura 4.1).

Ou, visto de outra forma, acompanhando a escala temporal, a partir de arranjos e aproveitamento de estruturas da própria administração pública federal, direta, indireta e de subsidiárias destas, por linhas de transmissão de energia elétrica de concessionárias, por gasodutos e rodovias, estaduais e federais (TELEBRAS, 2018), a expansão da rede conduzida pela Telebras pode ser ilustrada pela Figura 4.2.

O fato é que nesse período indicado houve implementação significativa de infovias na direção da Região Norte do País, com a Telebras se aproveitando da infraestrutura de outras concessionárias, como a Eletronorte, a Petrobras/TAG (Transportadora Associada de Gás S. A.) e da empresa de telefonia TIM, além da Região Nordeste, por meio de estruturas da Chesf, muito embora ficasse concentrada no litoral, não cumprindo a diretriz de abranger zonas rurais e remotas.

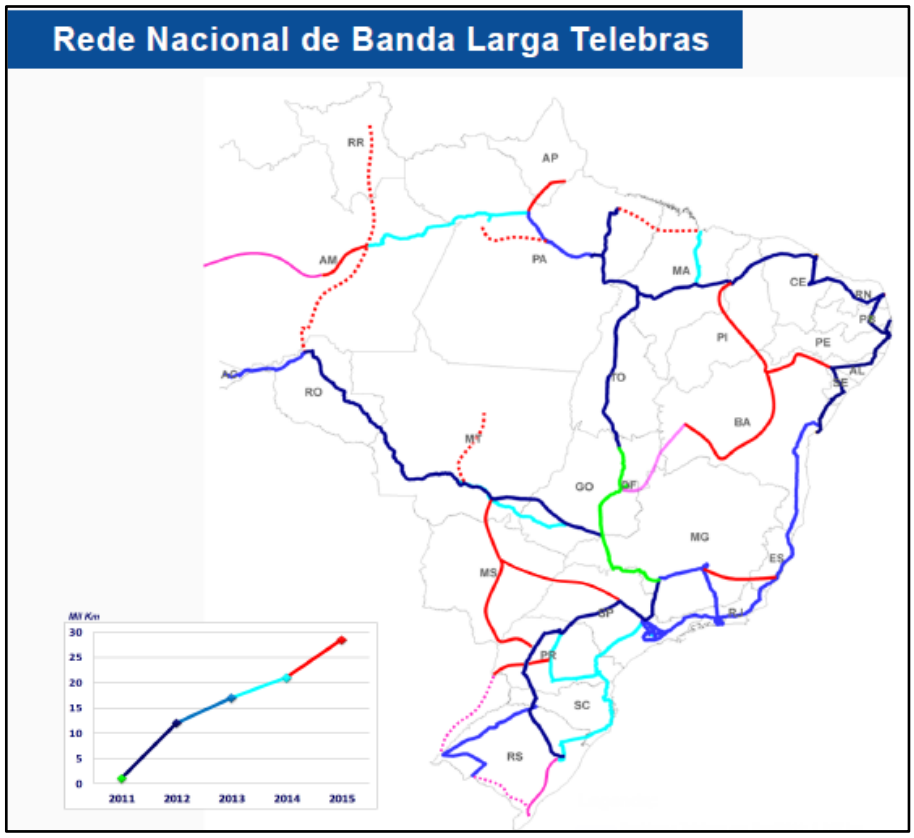
[140] Optamos por inserir a E-Digital na sequência do PNBL na redação final deste trabalho por ser documento de normatização, embora com viés bastante estratégico, e para dar sequência à análise de documentos oficiais que tratam desse tema. Contudo, pela ordem cronológica, houve programas e ações diversos no ínterim entre esses dois marcos normativos. Desses programas e ações, os relacionados aos propósitos desta pesquisa são tratados a seguir.

Figura 4.1: Rede Nacional de Fibra Ótica (2018)



Fonte: Telebras (2018).

Figura 4.2: Rede Nacional de Banda Larga Telebras (2018) [141]



Fonte: Telebras (2018).

[141] Até o dia da conclusão da redação desta tese não conseguimos identificar o que representa as vias na cor rosa. Não encontramos legenda referente, mas acreditamos que sejam projetos não implementados, da mesma forma que as linhas pontilhadas.

4.1.2 Estratégia Brasileira para Transformação Digital - E-Digital

Surpreendemo-nos no final do procedimento de levantamento de dados desta pesquisa, em 2018, no limiar do recorte temporal a que nos propomos investigar, com a publicação do texto da Estratégia Brasileira para a Transformação Digital, conhecida nos meios que a utilizam ou que por essa são abrangidos como E-Digital.

Esse documento é um marco concreto para o País e, também, para fins deste trabalho, uma vez que foi capaz de demonstrar, simultaneamente, a importância das tecnologias da informação e das comunicações e, portanto, da informação digitalizada, não só para o campo político, mas, sobretudo, para o econômico e o social, e traçar diretrizes de gestão norteadoras para políticas públicas que contemplem esse objetivo. Já para este trabalho, a E-Digital contemplou vários pontos anunciados por nós ainda quando da qualificação do projeto de tese, em meados de 2017, no Instituto de Economia da UFRJ, no tocante aos esforços brasileiros para sua realidade interna e internacional, o que, de certo modo, deu-nos novo fôlego e maior certeza do caminho que estávamos trilhando.

Fruto de uma reunião interministerial[142], coordenada pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações, a partir de recomendações do Conselho de Desenvolvimento Econômico e Social (CDES), em sua 46ª Reunião Plenária Ordinária[143], em março de 2017, esta estratégia se propôs ao planejamento de longo prazo para a economia digital no País. Foram mais de trinta órgãos participantes da APF, além de membros da comunidade científica, acadêmica e da sociedade civil. O documento ainda teve como base as respostas dadas a consultas públicas conduzidas pelo MCTIC.

Um dos indicadores citados pelo documento e que serviu de parâmetro foi o Índice de Competitividade Global (*Global Competitiveness Index* – GCI), responsável por medir a competitividade, entendida como "um conjunto de instituições, políticas públicas e outros fatores que determinam o nível de produtividade, procurando refletir o nível de prosperidade que cada país pode atingir" (BRASIL, 2018, p. 7). Pelo GCI, o Brasil, no relatório 2016-2017, constava na 80ª posição de um ranking de 137 países. Segundo a E-Digital, um de seus objetivos, ou talvez o principal, seria "elevar significativamente a posição do Brasil nesse índice ao longo dos próximos cinco anos. O progresso nesse e em outros indicadores estará associado

[142] Grupo de Trabalho Interministerial (GTI) instituído pela Portaria nº 842/2017, do MCTIC.

[143] Conforme consta no site do CDES, as reuniões plenárias desse conselho são o principal canal de diálogo entre os seus membros e a Presidência da República: "As reuniões plenárias são o principal espaço de diálogo entre o colegiado do CDES e o presidente da República.".

ao sucesso da economia brasileira, incluindo a economia digital do País.” (BRASIL, 2018, p. 7).

A E-Digital registrou as possibilidades esperadas a partir do domínio e da democratização da informação digitalizada:

> A digitalização abre novas oportunidades em inúmeras frentes. Hoje já é possível imaginar o acesso aos recursos educacionais de forma igual, não mais afetado pela localização geográfica, renda, raça, gênero e outros fatores. Há cada vez mais vantagens econômicas por meio da automação, da análise de dados e da tomada de melhores decisões baseadas no uso de algoritmos e de dados. Novos temas de proteção de privacidade e de direitos da pessoa humana surgem com a rápida disseminação de dados e com o crescente valor econômico de sua utilização. Uma assistência à saúde mais acessível, mais barata e de maior qualidade para todos é também uma oportunidade promissora das tecnologias digitais. (BRASIL, 2018, p. 8)

Assim sendo, o recurso proporcionado pelo uso adequado de TICs vai além do campo econômico, abrangendo benefícios ligados a direitos sociais, como educação e saúde, e, talvez, o principal, fornecido de forma democrática, conforme preconiza a Constituição Federal. Ainda, pelo uso da informação digital, há possibilidade de superação da própria condicionante geográfica, como ocorre no caso da Região Norte do Brasil, espaço menos favorecido, no que diz respeito a acesso a este recurso, como mostramos mais adiante.

A Estratégia Digital divide o teor de seu texto, para atingir os objetivos de cidadania digital, por um lado, e digitalização da economia, de outro, em cinco temas, conforme Figura 4.3.

Figura 4.3: E-Digital - temas para a transformação da economia e da sociedade

Fonte: BRASIL, 2018, p. 9

Para cada tema desses apresentados, foi constituído um subgrupo, ficando montada a estratégia então dessa forma: i) Infraestrutura; ii) Cidadania e Governo Digital; iii) Pesquisa, Desenvolvimento e Inovação; iv) Segurança e Confiança no Ambiente Digital; e v) Economia Digital.

A estratégia considerou a realidade geográfica e demográfica, nacional e regional, em termos de distribuição de infraestrutura de acesso à informação digital, e previu a participação do Estado como ente garantidor, ou no mínimo fomentador, dessa infraestrutura nos casos de hiato de acesso ou de mercado[144]:

> Nas áreas mais remotas frequentemente são necessárias soluções de rede via satélite, seja no acesso (para conectar a população à Internet), ou no transporte de dados (para conectar estas áreas aos *backbones* nacionais). Neste caso, são especialmente relevantes as políticas públicas que assegurem o provimento de acesso à Internet aos órgãos de presença do Poder Público: instalações administrativas, educacionais, de saúde, segurança pública e também das Forças Armadas. (BRASIL, 2018, p. 13)

Na esteira desse pensamento e constatação, a E-Digital citou esforços feitos pelo Projeto Amazônia Conectada (PAC) e pelo Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), mais voltados para o âmbito interno, e o projeto do cabo submarino Brasil-Europa, que iria "auxiliar na distribuição do tráfego internacional de dados, com melhoria da qualidade da conexão, diminuição de latência, conexão aprimorada com grandes centros de pesquisa europeus e redução dos custos de tráfego." (BRASIL, 2018, p. 21).[145] O TCU, quanto ao cabo submarino internacional, anteriormente já tinha se manifestado quanto à preocupação de que este seja capaz de "proporcionar mais segurança aos dados transportados" (BRASIL, 2015), o que seguiu também outros representantes dos Poderes Executivo e Legislativo federal, sobretudo após o caso de espionagem de 2013, denunciado por Edward Snowden, como demonstramos no capítulo 2.

Com relação ao Amazônia Conectada, a Estratégia Digital citou que o intuito do programa foi atender espaços geográficos não contemplados pela infraestrutura terrestre de banda larga, além de ampliar recursos de comunicação para demandas estratégicas e de Defesa. Já no que diz respeito ao SGDC, este teria o intuito de "atender áreas ainda não contempladas

---

[144] "[...] áreas deficientes em cobertura de infraestrutura ('hiato de acesso'), com alto custo de atendimento e população de baixa renda, ainda que a ampliação do mercado dissemine o acesso em regiões economicamente mais viáveis (reduzindo, assim, o 'hiato de mercado'). (BRASIL, 2018, p. 13)

[145] Essas três iniciativas – PAC, SGDC e cabo Brasil-Europa – são tratadas a seguir neste capítulo. Registramos que na qualificação de nosso projeto de pesquisa o Amazônia Conectada e o cabo submarino Brasil-Europa constavam como objeto de investigação. A E-Digital, neste sentido, corroborou nossa hipótese.

por infraestrutura terrestre de banda larga, além de acrescentar recursos de comunicação para atender necessidades estratégicas e de defesa." (BRASIL, 2018, p. 20). A E-Digital, para essas formulações, baseou-se também na publicação *Política Pública de Inclusão Digita*l (BRASIL, 2015), do TCU, que consistiu em um levantamento das políticas públicas dessa natureza, para fins de parâmetro de monitoramento e controle por parte desse órgão.

O tema *Pesquisa, Desenvolvimento e Inovação*, da Estratégia de Transformação Digital brasileira (Figura 4.1), no qual constou a preocupação com a participação do País nas cadeias globais de valor e com a promoção de empregos e aumento de renda, chamou nossa atenção pelo registro expresso feito quanto a questões ligadas à busca de possíveis transbordamentos para além da pesquisa e da inovação em TICs:

> [...] é imprescindível que sejam priorizadas áreas onde o investimento em Desenvolvimento Experimental e Inovação em TICs poderá trazer ganhos de competitividade ao País, tais como:
> - Segurança e defesa: como o desenvolvimento de plataformas que garantam a interoperabilidade e a coordenação entre os sistemas de comando e controle das três forças de Defesa nacional, utilizando, em particular, ferramentas de rádio comunicação. Além disso, é necessário garantir investimentos no desenvolvimento, por empresas nacionais, de protocolos de rádio comunicação, criptografia e equipamentos de segurança. (BRASIL, 2018, p. 35)

A E-Digital, embora não diretamente relacionada a questões que envolvam segurança e defesa, mas sim a motivações de ordem econômica, de produtividade e de outros ganhos sociais, deixou clara sua relação, e até certo ponto dependência, com o aspecto confiabilidade, tanto no cenário interno do País, quanto no internacional, ao mencionar e usar como parâmetro várias informações que abrangem aspectos da segurança, como é o uso de indicadores da União Internacional de Telecomunicações – o *ITU Global Security Index* –, e dos nacionais do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic) e do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br). Essa ideia se tornou importante na medida em que percebemos a nítida relação buscada pelos elaboradores desse documento no sentido de atrelar ganhos econômicos e segurança/defesa, esses últimos, em muitos pontos no texto, inseridos sob o rótulo "confiabilidade".

Também é verdade que a transformação digital está alinhada com a ideia contida no sistema tríplice hélice, conforme apresentamos nos capítulos anteriores e que é um dos objetivos propostos pelo Sistema de Desenvolvimento, Indústria e Academia (Sisdia) de Inovação do Exército, a partir da END (2008). Expressamente, assim trouxe a E-Digital, ainda em suas ações

estratégicas para o tema *pesquisa, desenvolvimento e inovação* quanto à intenção de integração e coordenação dos entes:

> . Estimular a interação entre universidades, instituições de pesquisa (ICTs) e empresas em ações de PD&I em tecnologias digitais, a partir do uso de mecanismos de fomento (como, por exemplo, as bolsas do Programa de Formação de Recursos Humanos em Áreas Estratégicas – RHAE), bem como por meio de estímulo ao fortalecimento de incubadoras de empresas, parques tecnológicos e demais ambientes inovadores.
>
> . Promover diálogos permanentes entre entidades de representação do governo, da academia e da indústria, de modo a garantir que as políticas e iniciativas de PD&I associadas à transformação digital sejam abrangentes, convergentes e coordenadas." (BRASIL, 2018, p. 36).

Na direção da END (2008), ainda, a E-Digital trouxe expressamente outro papel do Estado nesse empreendimento: "Utilizar o poder de compra público do Estado para estimular o desenvolvimento de soluções inovadoras baseadas em tecnologias digitais." (BRASIL, 2018, p. 35). Essa estratégia, portanto, segue a visão *keynesiana* sobre a demanda agregada ou efetiva contida no PNBL, com relação ao papel do Estado, e avança.

No tocante ao tema *Confiança do Ambiente Digital*, a estratégia de transformação ratifica a divisão apresentada por nós quanto a níveis e tipos de ameaças ou de incidentes nesse ambiente, fracionando-os em duas categorias: 1) a de proteção de direitos e privacidade e 2) a de defesa e segurança no ambiente digital.

Essa divisão se fundamenta tendo em vista a gravidade do dano causado, que pode ser no nível individual, como o acesso indevido à conta bancária, furto de arquivos pessoais, mas também pode afetar uma grande parcela da sociedade, como no caso de sabotagem de infraestruturas críticas ou estruturas estratégicas do País (rede de energia, de telecomunicações, de distribuição de água, controle de tráfego aéreo etc.).

No que diz respeito à proteção de direitos e privacidade, a E-Digital utilizou como referencial o Marco Civil da Internet, lei publicada em 2014[146], e que previu

> princípios, garantias, direitos e deveres, e não esgota o tratamento do assunto, deixando espaço para detalhamento futuro de importantes temas relacionados à rede, tais como proteção de dados pessoais, comércio eletrônico, crimes cibernéticos, direito autoral, governança da Internet, cidadania digital, entre outros.
>
> A primeira e mais fundamental é a dimensão dos direitos humanos. Liberdades de expressão, comunicação, manifestação, associação e direitos de acesso à

[146] Como já anunciada, Lei nº 12.965, de 23 de abril de 2014.

> informação e não discriminação precisam ser incorporados na arquitetura e governança da Internet. Violações dessas liberdades e direitos pelo Estado, empresas e mesmo por usuários precisam ser monitoradas e repelidas com vigor. (BRASIL, 2018, p. 37)

Contudo, essa norma e suas consequências são voltadas para o âmbito interno, isto é, obedecendo ao princípio da territorialidade das leis e, por conseguinte, sendo objeto de coerção legal e legítima concreta.

No que diz respeito à denominada livre movimentação de informações na forma de dados através das fronteiras – *free flow of data* –, esta é de coerção mais complexa, tanto pela natureza do ambiente digital, que é virtual – como abordamos no capítulo 1 – quanto pela diferença de legislação de um país para outro.

Esses aspectos passam a ser relevantes, pois segundo o próprio relatório da Organização para Cooperação e Desenvolvimento Econômico (OCDE), a economia digital será um dos motores do desenvolvimento do Século XXI [147]. Dessa forma, questões envolvendo confiabilidade digital e segurança jurídica nesse ambiente são componentes-chave de sucesso em acordos internacionais de diversas naturezas, o que demanda maior cooperação. Foi por isso que a E-Digital inseriu como uma de suas ações estratégicas para este tema:

> Reforçar instrumentos de cooperação internacional entre autoridades e entre provedores de acesso e conteúdo atuantes em diferentes países, de maneira a garantir a aplicação da lei no ambiente digital, especialmente nos casos em que o caráter transnacional dos crimes e ameaças cibernéticos forçam o envolvimento de mais de uma jurisdição. (BRASIL, 2018, p. 44)

Ainda no tocante às ações estratégicas voltadas para o tema *confiança no ambiente digital*, a Estratégia de Transformação previu a busca de cooperação entre entes governamentais e o setor privado – por exemplo, o setor bancário e de crédito em geral –, visando à adoção de melhores práticas para o setor, o compartilhamento de informações, a adoção de padrões de segurança adequados e uma coordenação quando das respostas a incidentes de rede e de proteção de infraestruturas críticas, além de se preocupar com o treinamento de agentes públicos e recursos humanos do setor privado, para mitigar riscos cibernéticos.

Nesse sentido, em 2018, pudemos assistir a uma reunião que tratou de um exercício, denominado "Guardião Cibernético"[148], em sua primeira versão, e que teve como objetivo a execução das ações estratégicas listadas acima. Participaram, além de integrantes das três forças

[147] Conforme OCDE: http://www.oecd.org/sti/ieconomy/data-driven-innovation.htm. Acesso em: 20 abr. 2020.
[148] Conforme exposto na reunião que assistimos, o *Guardião Cibernético* teve inspiração no exercício de simulação em cibersegurança *Ciber Perseu*, de 2017, realizado em Portugal, sob a coordenação do exército daquele país.

armadas brasileiras, o Banco Central do Brasil, bancos públicos e privados e empresas do setor nuclear. A plataforma utilizada para esse exercício foi o simulador de operações cibernéticas – Simoc – desenvolvido no Brasil, pela parceria entre o Departamento de Ciência e Tecnologia do Exército e a empresa Rustcom[149], conforme explicado no capítulo anterior. Aqui pode ser evidenciado mais um resultado material da sinergia Defesa-Desenvolvimento.

Especificamente em relação ao tema *dimensão internacional* (Figura 4.3), a E-Digital trouxe um capítulo, no qual há registro de constatações sobre as possibilidades advindas das TICs, como o encurtamento de distâncias e de integração regional, com a dinamização de fluxos comerciais e informacionais, daí a necessidade de o Brasil buscar participar desse cenário a partir de uma "perspectiva global, com protagonismo internacional nos fóruns mundiais e multissetoriais, e dedicando atenção especial às questões transfronteiriças de dados, bens e serviços." (BRASIL, 2018, p. 53). Mais uma vez questões de ordem econômica e de segurança surgem na mesma parte do documento.

Continua a Estratégia de Transformação Digital brasileira, no tocante à *dimensão internacional*, abordando aspectos ligados à governança mundial da internet. Sintetizamos o diagnóstico apontado por esse documento e, na sequência, as ações estratégicas, nos Quadros 4.1 e 4.2:

Quadro 4.1: E-Digital - diagnóstico da dimensão internacional

• Complexidade do ecossistema da rede, com diversos atores assumindo papéis distintos;
• Multissetorialidade e definição de papéis e responsabilidades distintos e complementares para cada setor representado - pilares do arcabouço da WSIS na Agenda de Túnis 2005, reafirmados no processo WSIS+10 na Assembleia Geral das Nações Unidas em 2015;
• Persistência do hiato digital;
• Problemas estruturais que contribuem para o hiato digital, como a dificuldade no acesso à tecnologia;
• A assimetria de representatividade entre países nos foros internacionais, dadas as restrições de recursos humanos e financeiros para engajamento em todas as frentes de negociação.

Fonte: elaboração do autor com base na E-Digital (2018).[150]

[149] No site da empresa Decatron também consta sua participação nesse projeto.

[150] WSIS – *World Summit on the Information Society* (Cúpula Mundial sobre a Sociedade da Informação), da União Internacional de Telecomunicações (UIT), da Organização das Nações Unidas (ONU).

Quadro 4.2: E-Digital - Ações estratégicas para a dimensão internacional

• Atuar nos foros internacionais de forma a defender os princípios compatíveis com a Cúpula Mundial da Sociedade da Informação, com a compreensão dos respectivos papéis e responsabilidades dos governos, organizações intergovernamentais e internacionais, assim como a do setor privado e da sociedade civil, tanto de países desenvolvidos como em desenvolvimento; • Impulsionar os temas de governança da Internet em foros, negociações, mecanismos e articulações que tratem desta agenda, usando parcerias em diferentes âmbitos (União Europeia, Mercosul, IBAS, BRICS, G20, ONU, entre outros); • Ampliar espaços multilaterais de negociação de políticas públicas de Internet, especialmente nos temas de jurisdição, proteção de garantias fundamentais, segurança cibernética e tributação; • Atuar pela implantação de novos mecanismos de resolução pacífica de conflitos no ambiente cibernético, tais como a iniciativa do *Group of Governmental Experts* (GGE) das Nações Unidas.

Fonte: elaboração do autor com base na E-Digital (2018).

Como exemplo do que sinalizou a E-Digital sobre a participação nos fóruns internacionais, conforme quadros acima, o Brasil, em 2017, a título de exemplo, participou de discussões sobre esse tema:

- no G20, na 1ª Reunião de Ministros Digitais, em Düsseldorf, Alemanha;
- nos Brics, 3ª Reunião de Ministros das Comunicações dos BRICS;
- no Mercosul, quando liderou, segundo a E-Digital, o processo que resultou no estabelecimento do "Grupo Agenda Digital" (GAD);
- na CEPAL – eLAC, na Reunião Preparatória da 6ª Conferência Ministerial sobre a Sociedade da Informação da América Latina e do Caribe, em Santiago, Chile, e em 2018, na Conferência Ministerial propriamente, que formalizou ações concretas para o processo de integração regional no ambiente digital, estipuladas para o período 2018–2020. Tratou-se da Agenda Digital para a América Latina e o Caribe (eLAC 2020).[151]

[151] A Comissão Econômica para a América Latina (CEPAL) é a responsável pelo apoio técnico ao eLAC, o mecanismo de coordenação das agendas digitais de países da América Latina e Caribe. O ciclo de trabalhos eLAC-2018, apoiado na Declaração Ministerial eLAC-2015, tem foco na integração digital da região. (BRASIL, 2018).

Mesmo com a participação em fóruns que propõem a multilateralidade de governança e a utilização da *internet* como meio para inclusão social e desenvolvimento, interessante ressaltar a recomendação constante da E-Digital em relação a "quem controla a internet". Nessa passagem podemos inferir a síntese do cenário que detectou esta estratégia em relação à *internet*, tida por alguns como ferramenta e bem de uso universal, um *global common*, mas que, em última instância, é ainda administrada unilateralmente, tendo como base pressupostos do realismo de poder, conforme exposto no capítulo 2. Assim trouxe a E-Digital:

> No caso da ICANN (*Internet Corporation on Assigned Names and Numbers*), a autoridade mundial de governança de recursos da rede), a tomada de decisão acerca da gestão de recursos críticos da rede deve ser democrática e transparente. Ademais, é necessário adotar um enfoque realista no tema da governança, cuidando para que nenhum agente tenha sozinho o domínio total dos recursos, e esforçando-se para garantir direitos e assegurar deveres. (BRASIL, 2018, p. 55)

Assim o documento, ainda em 2018, deixou clara a preocupação com a ausência de um multilateralismo, apesar de terem evoluído bastante as discussões nesse sentido, como apresentamos ao longo do trabalho.

Na sequência da redação, apresentamos *projetos*, *programas* e *ações interministeriais* que dizem respeito à cibernética vista como setor estratégico no Brasil para além da Defesa, isto é, inserindo-a, expressamente, na relação Defesa-Desenvolvimento.

4.2 A CIBERNÉTICA COMO SETOR ESTRATÉGICO E SEUS REFLEXOS PARA ALÉM DA DEFESA: PROJETOS, PROGRAMAS E AÇÕES INTERMINISTERIAIS

Como anunciado no início deste capítulo, passamos a tratar agora de *projetos, programas e ações interministeriais* relacionados ao setor cibernético. No decorrer da pesquisa, e da reflexão, e da tradução das conclusões para este texto, ficou evidenciado que as ações, de uma forma geral, poderiam ser divididas quanto a suas finalidades. Por conseguinte, elencamos, primeiramente, as ações que consideraram *a cibernética tanto como espaço quanto recurso de poder*, isto é, ações voltadas para implementação ou ampliação do ciberespaço e de sua utilização como recurso de poder.

Se houve esforços governamentais que mais simbolizaram esta tese e seu recorte temporal, no sentido de espaço e recurso de poder, esses foram os programas Amazônia

Conectada, o SGDC e o projeto de construção do cabo submarino Brasil-Europa, pois partiram de características geográficas do País, logo estruturais, *vis-a-vis* condições políticas e econômicas sistêmicas internacionais, conjunturais e também estruturais, respeitando-se as peculiaridades de cada um.

O primeiro deles ao relacionar características geográficas da região Norte do País – a maior em extensão territorial, equivalendo a cerca de 45% do total, no interior do continente, com uma cobertura vegetal predominantemente de floresta equatorial, de clima quente e superúmido e de difícil acesso – com as necessidades de Defesa e Desenvolvimento, por meio do uso de tecnologias de informação e das comunicações, voltadas primeiramente para minimizar deficiências em infraestruturas diante das peculiaridades do quadro natural, porém não deixando de atender a questões envolvendo preocupação com a fronteira e com a hipótese de pressão internacional sobre os recursos naturais ali existentes.

O segundo, o satélite geoestacionário, um ciberespaço virtual em essência, baseado no espectro eletromagnético, primeiramente, para depois penetrar em cabos e demais estruturas físicas cibernéticas, buscou, como o seu nome sugere, uma maior autonomia para as comunicações estratégicas brasileiras, da mesma forma que a abrangência de todo o território nacional com banda larga de *internet*. Além disso, o SGDC funciona como uma espécie de redundância, isto é, de "dobra de meios", uma alternativa na consecução dos objetivos da RNP e do MCTIC, no que diz respeito à universalização de acesso digital às áreas mais distantes ou de difícil acesso.

O cabo submarino também considera imperativos geográficos, sobretudo a posição relativa do País em relação à Europa, importante centro econômico, financeiro e cultural do sistema internacional. Esse esforço ganhou maior relevância e espaço na agenda política nacional a partir do caso Snowden, um episódio de espionagem cibernética de alcance global, como apresentado no capítulo 2 deste trabalho. Nesse aspecto, apesar de a fluidez da informação através das fronteiras – fenômeno no escopo do "*free flow of datas*" (BRASIL, 2018, p. 38), por ser, aparentemente, capaz de superar a geografia –, as redes e os pontos de respectivas conexões por onde flui essa informação podem possuir bandeiras, isto é, podem responder a um território, a um poder territorializado e, portanto, a um fim, e na tentativa de superar esse direcionamento das redes, além de razões técnicas, pautou-se o projeto da construção de um novo cabo submarino pelo não direcionamento direto para um Estado reconhecidamente espião.

Em um segundo momento, apresentamos a cibernética sob o enfoque de proteção de estruturas estratégicas do País, ou seja, dentro de uma abordagem da cibersegurança, de garantia do funcionamento do próprio ciberespaço.

4.2.1 A Cibernética como Espaço e Recurso de Poder no Brasil: o Programa Amazônia Conectada

4.2.1.1 Realidades Regionais e o Programa Amazônia Conectada

A implantação de uma rede de infovias de fibra ótica subfluviais no leito do Rio Amazonas e de alguns de seus afluentes nos permite evidenciar: 1) a preocupação do Estado com a articulação de seu território, ainda que em porções inóspitas ou de difícil acesso, para, a partir daí, aumentar a possibilidade de comando e controle (político), logo de segurança e de defesa, e de acesso à educação, à saúde e a outros direitos, individuais fundamentais e sociais; 2) a ciência do Estado a respeito das possibilidades advindas com o uso de infovias para se obter ganhos além de políticos, como é o caso do fomento à economia e à ciência e tecnologia; 3) o uso de um instrumento cibernético para além da defesa, possibilitando, ainda, a participação articulada de diversos órgãos públicos, em diferentes níveis de governo, portanto um programa interagências e interministerial.

Não podemos afirmar que a preocupação do Estado com a articulação de seu território, com o objetivo de Defesa e de Desenvolvimento, seja inédita no Brasil (MARQUES, 2007; MEDEIROS, 2010). Na história recente e persistindo nos dias atuais, por exemplo, temos o Programa Calha Norte (PCN), antigo Projeto Calha Norte (1985), e o Programa de Desenvolvimento para Faixa de Fronteira (PDFF)[152], voltados também para essa região do País. Quanto ao primeiro desses, assim explicou Gabriel:

> Talvez o que tenha determinado a longevidade do PCN tenha sido justamente a lógica desenvolvimentista pela qual foi concebido, não se limitando exclusivamente às ações tipicamente militares [...]. O PCN foi concebido abrangendo uma intenção maior, a de desenvolver a Amazônia e integrá-la ao restante do território nacional. Nesse sentido, o programa procurou o desenvolvimento econômico da Amazônia por meio do incentivo à ocupação populacional e à instalação de indústrias, bem como pela da melhoria da rede de comunicações e transportes. (GABRIEL, 2015, p. 35)

[152] A Estratégia Nacional de Defesa de 2008 foi além na busca de aproximação entre Defesa e Desenvolvimento, e na maximização de benefícios sociais: "O Ministério da Defesa e o Ministério da Integração Nacional desenvolverão estudos conjuntos com vistas à compatibilização dos programas Calha Norte e de promoção do desenvolvimento da Faixa de Fronteira (PDFF) e ao levantamento da viabilidade de estruturação de arranjos produtivos Locais (APL), com ações de infraestrutura econômica e social, para atendimento a eventuais necessidades de vivificação e desenvolvimento da fronteira, identificadas nos planejamentos estratégicos decorrentes das Hipóteses de Emprego." (BRASIL, 2008, p. 63).

Também, pelo visto, nas preocupações das políticas públicas de defesa, segurança e desenvolvimento para essa região, há as constantes relacionadas à infraestrutura, que, para o nosso estudo, destacamos a de comunicações, uma vez que é nessa esteira de intenção que surgiu o PAC. [153]

O Programa Amazônia Conectada, a partir de projeto homônimo, cuja origem pode ser remontada ao Memorando de Entendimento nº 14-188-00, de 24 de novembro de 2014 [154], teve como instituições parceiras originárias, no âmbito federal, além do Ministério da Defesa (representado pelo Departamento de Ciência e Tecnologia do Exército – DCT), o Ministério das Comunicações (MC), o da Ciência, Tecnologia e Inovação (MCTI), a Empresa Telebrás S. A. e a Rede Nacional de Ensino e Pesquisa (RNP); no estadual, o Processamento de Dados do Amazonas S. A. (Prodam), a Secretaria de Estado de Ciência, Tecnologia e Inovação do Amazonas (SECTI-AM) e o Instituto de Proteção Ambiental do Amazonas (Ipaam).

Ao longo da execução do programa, outros órgãos também constaram como "novos parceiros estratégicos" (BRASIL, 2015): a Empresa de Tecnologia da Informação e Comunicação do Estado do Pará (Prodepa), as Centrais Elétricas Brasileiras S. A. (Eletrobrás), a Agência Nacional de Águas (ANA), a Agência Nacional de Telecomunicações (Anatel), o Tribunal de Justiça e o Ministério Público do Amazonas, a Defensoria Pública e a Advocacia-Geral da União, o Instituto Brasileiro do Meio Ambiente e Recursos Naturais (Ibama), o Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), a Superintendência da Zona Franca de Manaus (Suframa), as universidades federal e estadual do Amazonas (UFA e UEA) e o Centro Gestor e Operacional do Sistema de Proteção da Amazônia (Censipam).

O objetivo expresso constante na portaria interministerial que instituiu o programa era "expandir a infraestrutura de comunicações e contribuir para as ações do Governo Federal desenvolvidas no âmbito do Programa Nacional de Banda Larga – PNBL na região amazônica." (BRASIL, 2015). Dentre as finalidades, também constantes na mesma portaria (artigo 2º), constam inclusão digital e Defesa Nacional, expandindo suas comunicações militares administrativas e operacionais, a segurança na conectividade para incentivar a pesquisa e a educação, o desenvolvimento tecnológico e a competitividade da indústria local, além de troca de informações sobre o monitoramento ambiental.

---

[153] Seria injusto não citar os feitos do Marechal Rondon, patrono da Arma de Comunicações do Exército Brasileiro, relacionados a comunicações e integração territorial. Aliás, no lançamento oficial do Amazônia Conectada, essa foi a alusão feita pelo então Ministro das Comunicações, Ricardo Berzoini: "O Amazônia Conectada tem tudo a ver com a concepção do Marechal Rondon de tratar as comunicações como questão fundamental. É nossa obrigação conectar essa região amazônica com a tecnologia adequada." (REDE NACIONAL DE ENSINO E PESQUISA, 2015).

[154] Disponível em: http://www.amazoniaconectada.eb.mil.br/pt/index.php. Acesso em: 28 abr. 2019.

Para Roberto Caiafa, jornalista especializado em temas de defesa, aviação e mídia social, dentre os objetivos do PAC, na prática, destacaram-se: "[...] levar serviços de internet de alta velocidade, telemedicina, telesaúde, ensino à distância, entre outros, para população ribeirinhas e indígenas, escolas, organizações militares e órgãos públicos." (REVISTA TECNOLOGIA E DEFESA, 2016, p. 16). A expectativa, disse esse especialista, é que o PAC contribuísse "com as ações do Governo Federal, por meio do Programa Nacional de Banda Larga (PNBL), do Ministério das Comunicações, [...]" (REVISTA TECNOLOGIA E DEFESA, 2016, p. 16), e fosse capaz de apoiar

> as políticas públicas de inclusão digital, de iniciativas às pesquisas, educação, sensoriamento e monitoramento ambiental, e a segurança de dados nacionais [...]. A adoção do programa deverá estabelecer novo marco de desenvolvimento do País, através da informação e do conhecimento." (REVISTA TECNOLOGIA E DEFESA, 2016, p. 16)

A perspectiva do então governador do Estado do Amazonas, José Melo, no ato de lançamento do Programa, corrobora essas ideias quanto aos objetivos pretendidos: "Aqui há petróleo, gás natural, diversidade, luminosidade e um povo. Esse programa vai dar oportunidade à população com serviços nas áreas de saúde, telemedicina, educação e segurança" (REDE NACIONAL DE ENSINO E PESQUISA, 2015). Assim prosseguiu o governador:

> Interconectar a Amazônia vai permitir universalizar o ensino superior e médio, permitir que o povo do interior possa ter oportunidade de acesso ao conhecimento mundo afora, avançar nas pesquisas científicas. Permitirá também, em curto prazo, fortalecer o combate ao tráfico nas fronteiras através da interconectividade das forças armadas. (REDE NACIONAL DE ENSINO E PESQUISA, 2015)

Especialistas na parte técnica de TICs também se manifestaram quanto às expectativas com o PAC diante da geografia da região e suas consequências para o desenvolvimento. Assim, por exemplo, pronunciou-se o presidente da Prodam:

> Por conta da localização geográfica, o nosso Estado sofreu durante muitos anos com a falta de disponibilidade de banda larga. Há, inclusive, algumas cidades que passaram a ter acesso a celular nos últimos cinco anos, enquanto outras apenas recentemente vieram a contar com serviço de internet. [...] Com acesso à comunicação, os produtores poderão desenvolver seus negócios, fechar parcerias e escoar seus produtos até para fora do Estado (PORTAL PRODAM, 2017)

Dessa forma, tanto por especialistas civis, quanto por representantes do poder executivo estadual, além do previsto na portaria interministerial, logo no âmbito federal, que criou o

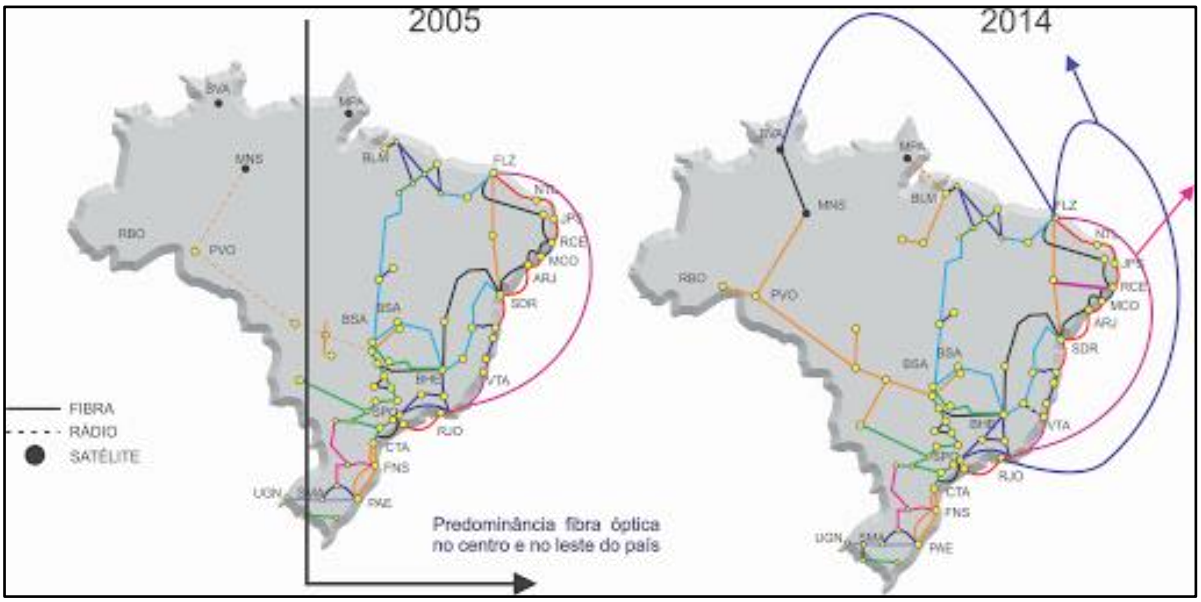
programa, a direção apontada foi no sentido de fortalecimento de redes de pesquisa, de educação, de saúde, enfim, de benefícios ligados a direitos sociais e ao desenvolvimento econômico, e de ampliação da capacidade de medidas de segurança e de defesa, por meio de sensoriamento, monitoramento e controle, a partir do uso do ciberespaço, o que insere este programa no rol de ideias de "uma ação, dois (ou mais) movimentos", caracterizado pelo seu uso intrinsecamente dual. Mais que isso, o PAC também atende a diretrizes expressas constantes de documentos de Defesa, como apresentado no capítulo anterior, no tocante à END, sobretudo as relacionadas às diretrizes 2, 6 e 10, relativas ao trinômio *comando/controle*, *mobilidade* e *presença*, ao uso dual e aos setores estratégicos.

A justificativa da escolha da implantação do PAC na Região Norte do País, mais precisamente no Estado do Amazonas, pode ser sintetizada na existência de um "Tordesilhas Digital" (REVISTA TECNOLOGIA DIGITAL, 2016, p. 16) (Figura 4.4), denominação atribuída ao fato da concentração de grande parte da infraestrutura de cabos ópticos e suas redes nas regiões Sudeste e Sul. Nesse sentido, assim mencionou acórdão do TCU que avaliou o PAC, no que diz respeito aos aspectos de gestão referentes: 1) à sustentabilidade econômica e operacional do projeto; 2) aos pilares essenciais para inclusão de digital de seus beneficiários: "Especificamente com relação ao estado do Amazonas, apenas 37,1% dos municípios possuem *backhaul* de fibra óptica, o segundo menor índice entre os estados do Brasil, perdendo apenas para o Piauí, segundo dados da Anatel." (BRASIL, 2019). [155]

Os dados da Agência Nacional de Telecomunicações a que se referiu o TCU no texto acima datam de 2016. Ainda nesse sentido, "segundo o Plano Estrutural das Redes de Telecomunicações (Pert) da Agência Nacional de Telecomunicações (Anatel), 54% dos municípios sem *backhaul* de fibra óptica estão nas regiões Norte e Nordeste." (BRASIL, 2018).

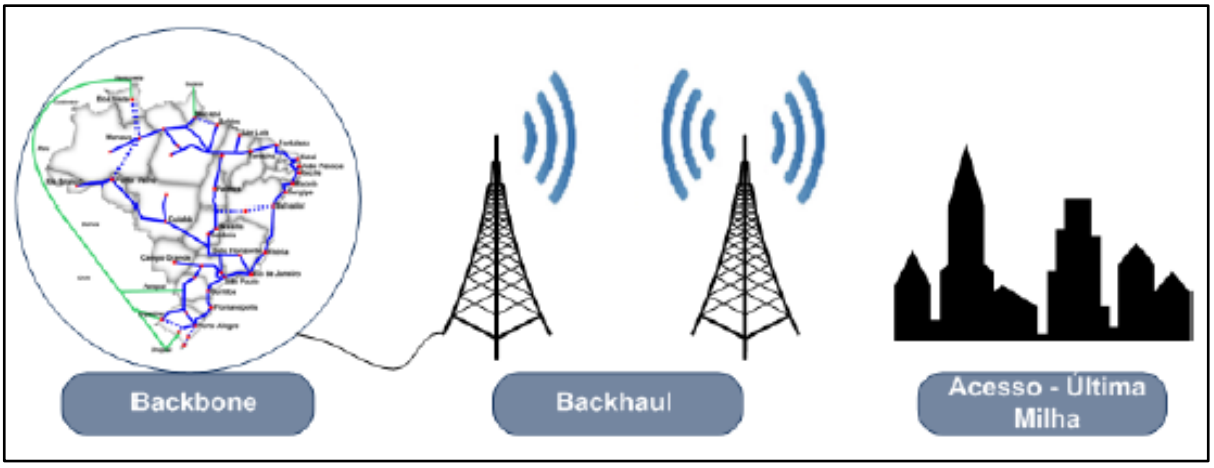
[155] A composição de uma infraestrutura de fibra ótica tal qual a do PAC é formada por: *backbone*, *backhaul* e rede de acesso ou "última milha". Segundo o TCU: "Pode-se definir *backbone* como o núcleo da rede de telecomunicações que interconecta várias partes de outras redes possibilitando a troca de informações. Por *backhaul* considera-se as ramificações das redes de telecomunicações que conectam as redes locais (redes de acesso) ao núcleo da rede (*backbone*). A rede de acesso, também conhecida como última milha, é a infraestrutura da rede que conecta os usuários finais, por exemplo, os fios de cobre, as Estações Rádio Base (ERBs) da telefonia celular ou mesmo redes de acesso de fibra óptica." (BRASIL, 2019). Ver Figura 4.5.

Figura 4.4: Tordesilhas Digital – Brasil (2005 – 2014)



Fonte: BRASIL, 2014.

Figura 4.5: Modelo de Estrutura de Rede



Fonte: BRASIL, 2013.

Outras características diagnosticadas pelo TCU (BRASIL, 2018) [156], que corroboram a necessidade dessa região no tocante ao acesso à internet são que:

a) a Região Norte era, juntamente com a Nordeste, a que apresentava piores condições de acesso à banda larga no Brasil;

b) as regiões Norte e Nordeste eram as que possuíam a maior proporção de municípios que não tinham acesso à internet, bem como apresentavam a menor densidade de acessos de banda larga fixa por domicílio;

[156] Acórdão 2.053/2018-TCU-Plenário.

c) na região Norte, o alto preço do serviço foi listado por 67% dos entrevistados como motivo pela falta de *internet*; essa região era a que apresentava o maior percentual de acesso por banda larga móvel em relação ao acesso por banda larga fixa entre aqueles que tinham acesso à *internet*;
d) apenas 3% dos domicílios com acesso à internet na região Norte apresentavam velocidades de conexão acima dos 10 Megabits por segundo (Mbps);
e) a região Norte apresentava o maior percentual (29%) de alunos de escolas localizadas em áreas urbanas desconectados da internet e, ainda, a maior parte dos estabelecimentos públicos de saúde que não acessavam à internet estava nas regiões Norte e Nordeste.

Em suma, por essas constatações, assim se pronunciou o TCU, quanto à realidade da Região Norte do País e a proposta contida no PAC:

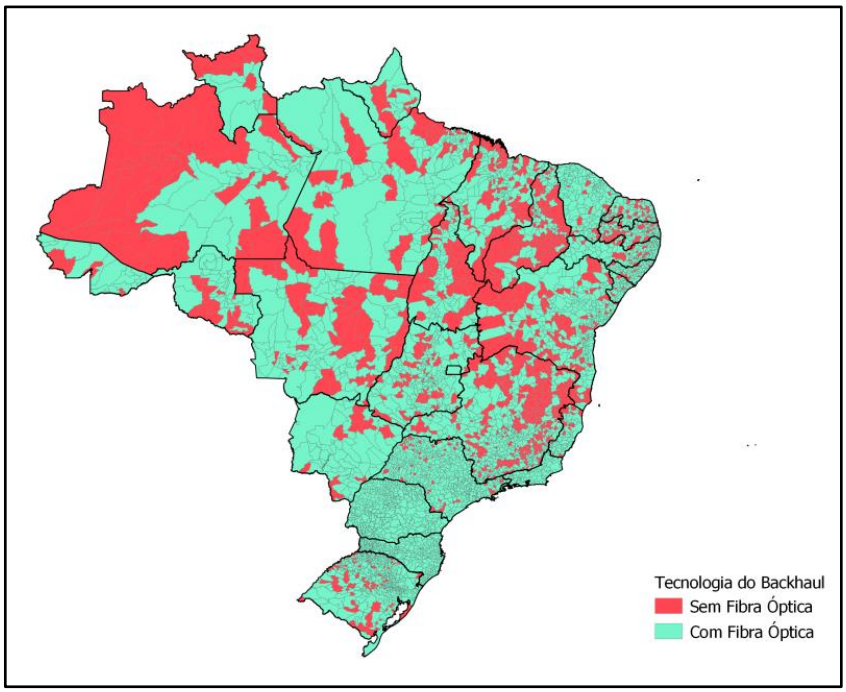
> [...] 6. Todos esses dados apenas confirmam o cenário de oportunidade para a implementação de um projeto dessa natureza com vistas a levar *internet* de alta velocidade a localidades não assistidas na Região Norte, com benefícios para o desenvolvimento da Amazônia e, em última instância, para a integração nacional. (BRASIL, 2019)

Mais que isso, no mesmo acórdão o TCU apontou para outro tipo de aproveitamento obtido a partir da implementação do PAC:

> [...] 7. Mas o PAC teria também função estratégica do ponto de vista da defesa nacional, pois visa promover a expansão da infraestrutura do Sistema Estratégico de Comando e Controle do Exército (SEC2Ex) e do Sistema Militar de Comando e Controle (SISMC2) do Ministério da Defesa. (BRASIL, 2019)

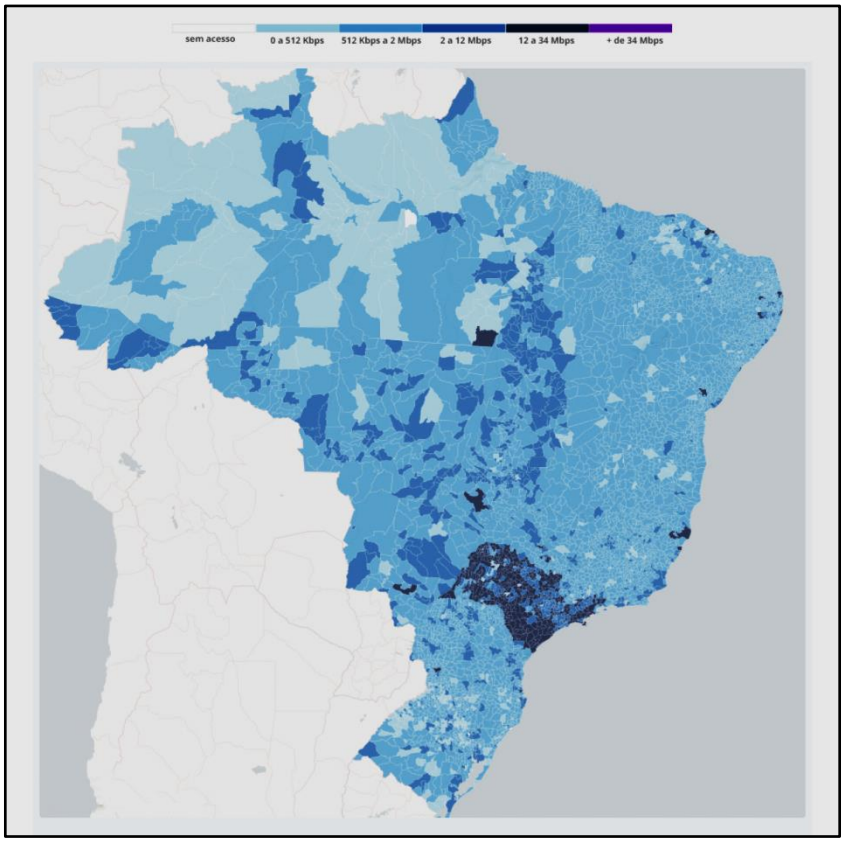
Essas realidades podem ser vistas a partir dos Figuras 4.6 e 4.7, a seguir:

Figura 4.6: Brasil - Tecnologia de Fibra Ótica *Backhaul*



Fonte: Anatel (2019).

Figura 4.7: Banda Larga no Brasil - faixa de velocidade predominante



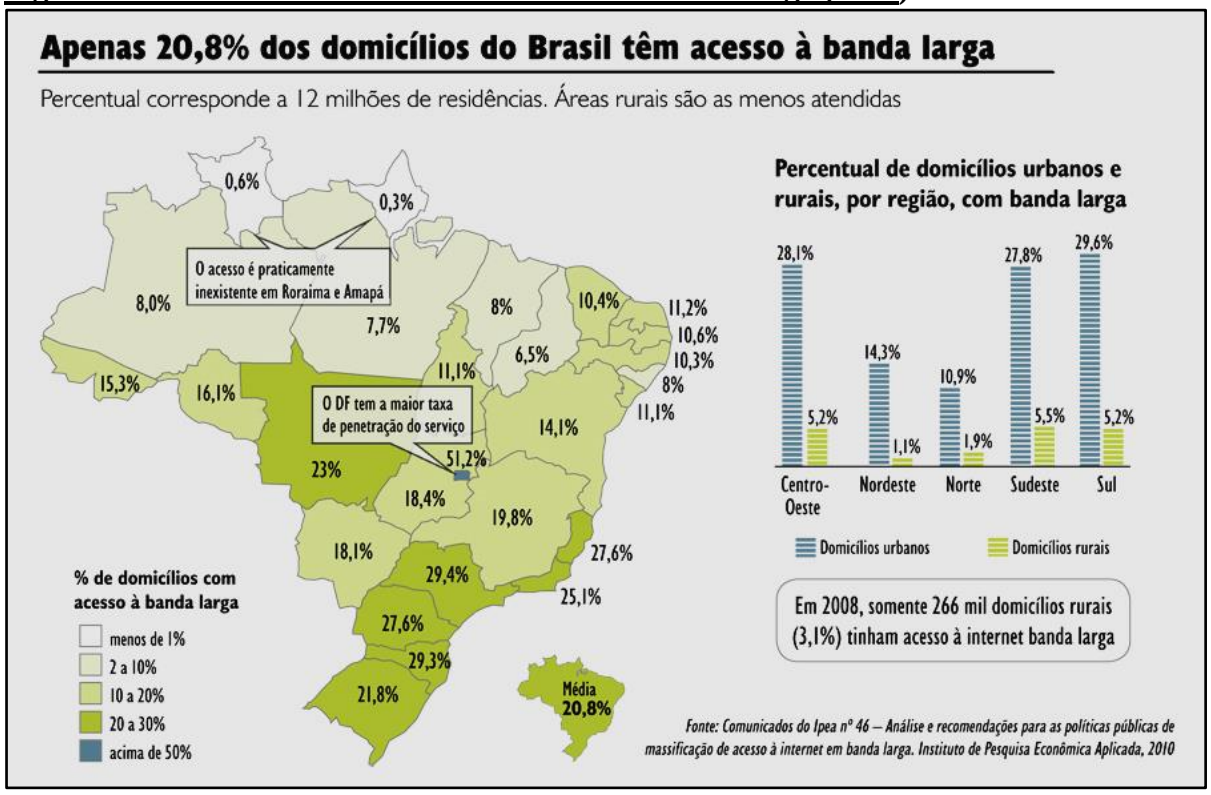
Fonte: G1 (2015).

Dos mapas anteriores, além da ilustração das características já elencadas pelo TCU, podemos perceber que a distribuição de *backhaul* passa a ser importante para se compreender a disponibilidade e a qualidade de *internet* pelos espaços geográficos, pois, ao analisar os mapas, podemos perceber uma relação direta, quando sobrepostos à noção de faixa de velocidade de *internet* banda larga [157] no País.

Ainda no tocante aos mapas, diante do conceito de "Tordesilhas Digital", percebemos um vácuo de uma estrutura de internet digital na Amazônia Ocidental, que em grande parte foi incluída na proposta do PAC.

Também a ilustração abaixo (Figura 4.4) corrobora as perspectivas apresentadas até então acerca do acesso à internet banda larga no País, segundo revista do Senado Federal "Em discussão!" (BRASIL, 2011), tendo como base de dados pesquisa divulgada pelo Ipea, em 2010.

Figura 4.8: Acesso de Domicílios Brasileiros à Banda Larga (2008)



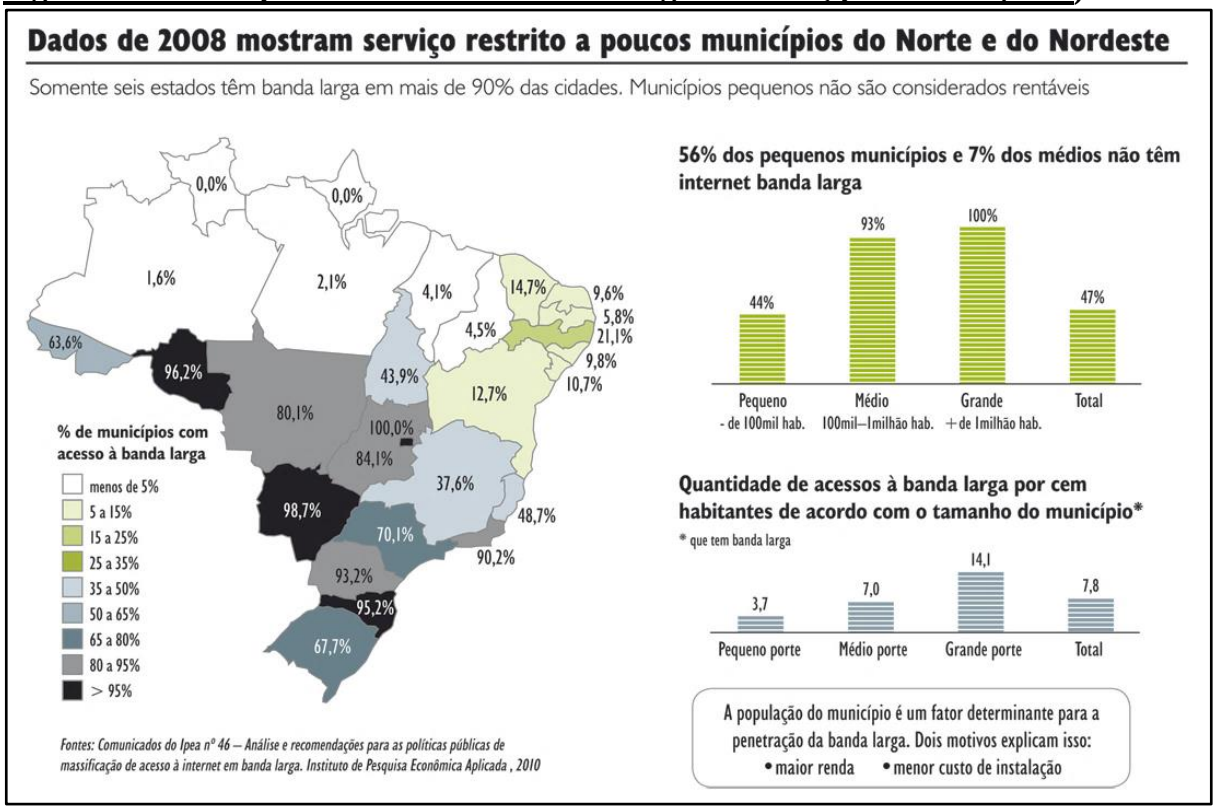
Fonte: Revista Em discussão! (BRASIL, 2011).

[157] Diferentemente da internet via *dial up*, aquela usada nos anos 1990, e que ocorria por meio de sinal telefônico, a banda larga permite uma capacidade maior de transmissão de dados, por meio da compressão digital. A caracterização da *internet* banda larga também varia de acordo com sua velocidade (BRASIL, 2010).

No sentido, por fim, de uma caracterização da importância do PAC para a Região Norte e para o País, os dados da Pesquisa Nacional por Amostra Domiciliar de 2008, realizada pelo IBGE,

> demonstram que no Sul, no Centro-Oeste e no Sudeste a banda larga chega a mais de 27% dos domicílios em zonas urbanas, enquanto no Norte e no Nordeste esse percentual não chega a 15%. Na zona rural, a penetração da banda larga é ínfima: abaixo de 2% no Norte e no Nordeste e de 6% nas demais regiões. (IBGE, 2010)

Figura 4.9: Municípios com Acesso à Banda Larga no Brasil, por Estado (2008)



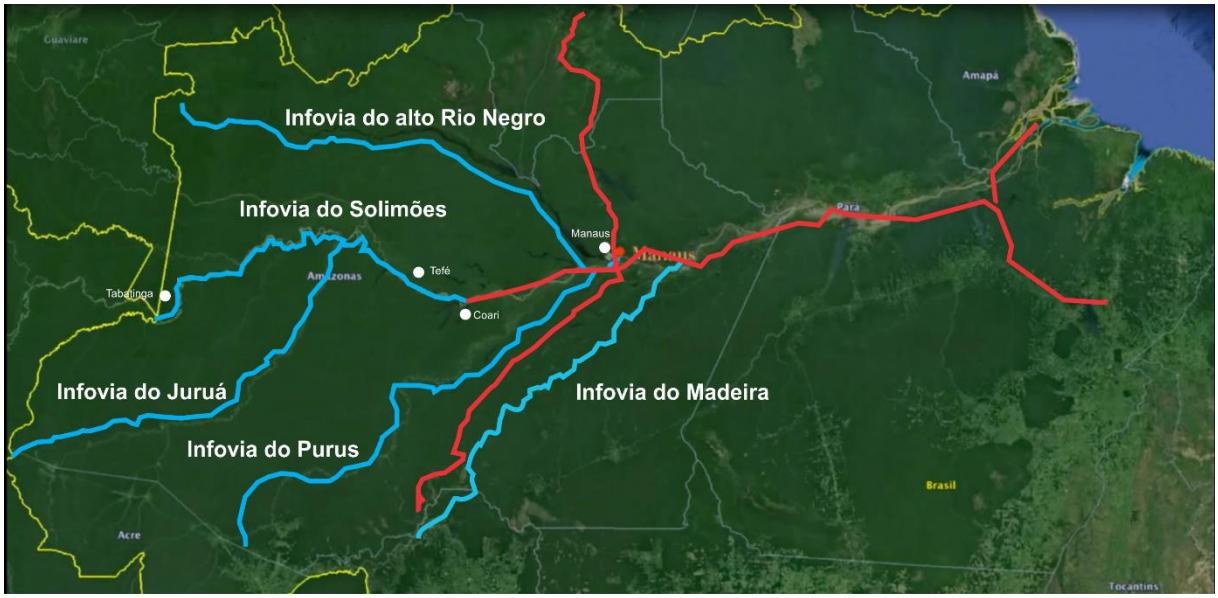
Fonte: Revista Em discussão! (BRASIL, 2011).

Também podemos inferir da Figura 4.9, que a disponibilidade de banda larga era diretamente associada ao tamanho do município, em termos populacionais, isto é, de demanda, de escala. Na realidade, os pequenos ficam expostos ao "hiato digital", nas formas de "hiato de acesso" e "hiato de mercado", conforme diagnóstico feito pelo PNBL e pela E-Digital. Esse, portanto, era o panorama de disponibilidade e acesso à *internet* de banda larga no início do recorte temporal de nossa pesquisa.

4.2.1.2 O Programa

Inicialmente, no projeto, a previsão era a implantação de cerca de 7,8 mil quilômetros de cabo de fibra ótica, distribuídos em cinco rotas, ou infovias, correspondente aos rios Solimões, Negro, Purus, Juruá e Madeira (Figura 4.10). Essa extensão abrangeria 52 municípios do Estado do Amazonas e aproximadamente 3,8 milhões de habitantes (Figura 4.11).

Figura 4.10: Programa Amazônia Conectada – infovias previstas



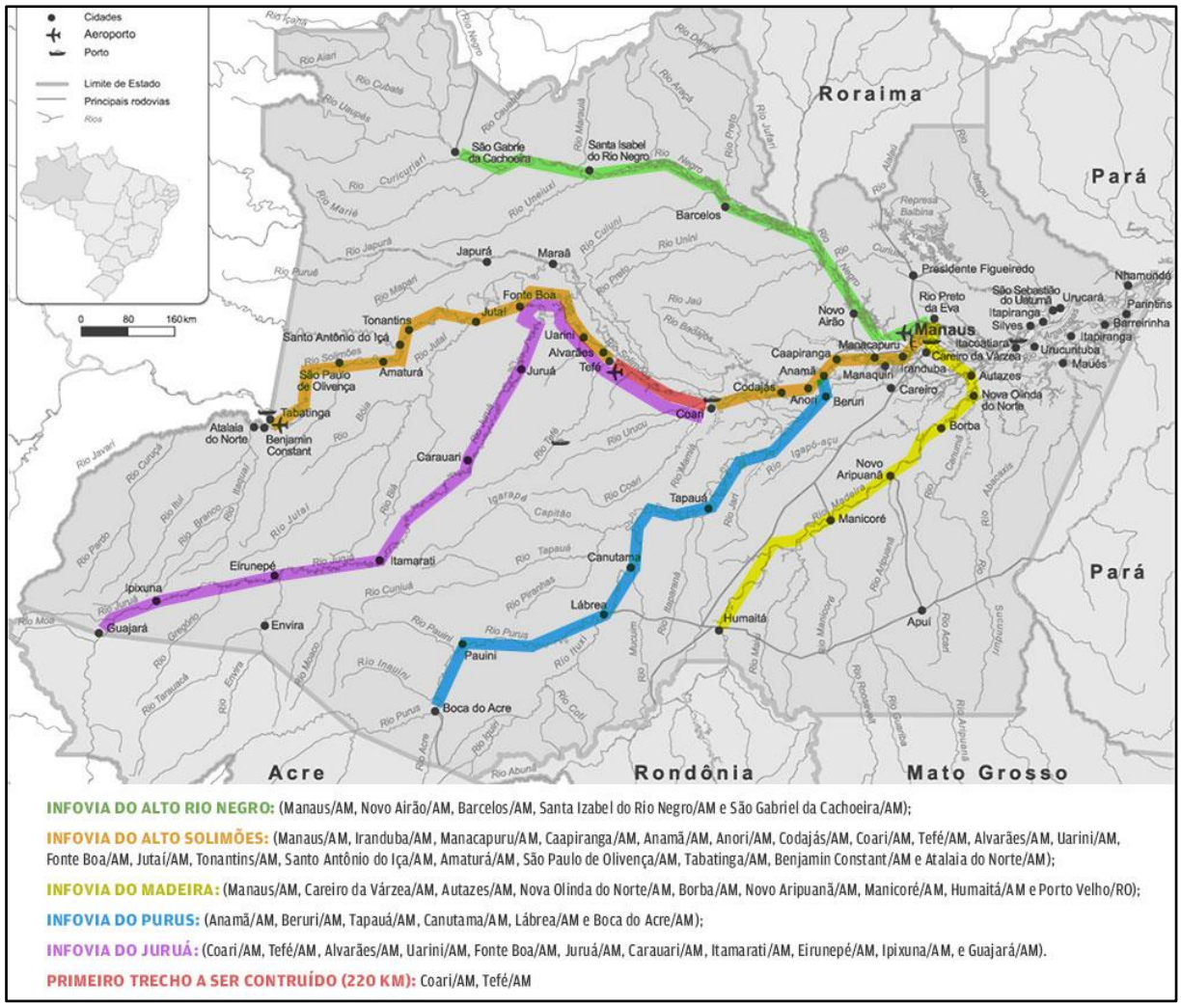
Fonte: Exército Brasileiro. [158]

As cinco infovias mencionadas são as indicadas na cor azul, acompanhando alguns dos principais rios da Bacia Amazônica.

O programa foi dividido em cinco projetos: o Infovias, o Política Pública, o de Gestão dos Serviços de Tecnologia da Informação, o da Cadeia de Valor e o da Estrutura de Manutenção.

[158] Disponível em: http://www.amazoniaconectada.eb.mil.br/pt/downloads/Provedores/#/what

Figura 4.11 – Programa Amazônia Conectada – infovias e municípios previstos



Fonte: Fibracem (2015). [159]

Mais especificamente, no Quadro 4.3 segue a relação de municípios com previsão de serem atendidos pelo PAC, segundo o TCU:

[159] Disponível em: http://fibracem.blogspot.com/2015/08/amazonia-recebera-cerca-de-78-mil.html. Também disponível no site da Editora Convergência Digital: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&tpl=home. Acesso em: 19 abr. 2019.

Quadro 4.3 - Previsão de municípios a serem atendidos pelo PAC

Infovias	Municípios interligados
Infovia do Alto Rio Negro	Manaus/AM, Novo Airão/AM, Barcelos/AM, Santa Izabel do Rio Negro/AM e São Gabriel da Cachoeira/AM.
Infovia do Alto Solimões	Manaus/AM, Iranduba/AM, Manacapuru/AM, Caapiranga/AM, Anamã/AM, Anori/AM, Codajás/AM, Coari/AM, Tefé/AM, Alvarães/AM, Uarini/AM, Fonte Boa/AM, Jutaí/AM, Tonantins/AM, Santo Antônio do Içá/AM, Amaturá/AM, São Paulo de Olivença/AM, Tabatinga/AM, Benjamin Constant/AM e Atalaia do Norte/AM.
Infovia do Madeira	Manaus/AM, Careiro da Várzea/AM, Autazes/AM, Nova Olinda do Norte/AM, Borba/AM, Novo Aripuanã/AM, Manicoré/AM, Humaitá/AM e Porto Velho/RO.
Infovia do Purus	Anamã/AM, Beruri/AM, Tapauá/AM, Canutama/AM, Lábrea/AM e Boca do Acre/AM.
Infovia do Juruá	Coari/AM, Tefé/AM, Alvarães/AM, Uarini/AM, Fonte Boa/AM, Juruá/AM, Carauari/AM, Itamarati/AM, Eirunepé/AM, Ipixuna/AM e Guajará/AM.

Fonte: elaborado pelo autor com base no TCU (BRASIL, 2019).

No tocante ao aporte de recursos para o Amazônia Conectada, este ocorreu em boa parte por meio de parcerias, concretizadas a partir de Termos de Execução Descentralizada (TED) ou por convênios. De acordo com o Quadro 4.4, elaborado a partir de informações disponibilizadas pelo TCU (BRASIL, 2019), a participação das instituições quanto aos recursos foi assim:

Quadro 4.4: Amazônia Conectada – aporte de recursos de parceiros do Programa

TED PARCEIROS	Período	Valor previsto (R$)	Valor transferido (R$)
TJ/AM	julho 2016 a julho 2017	1.500.000,00	1.500.000,00
MEC	setembro 2016 a setembro 2018	10.500.000,00	10.500.000,00
MCTI	outubro 2016 a outubro 2017	3.000.000,00	3.000.000,00
ANA	novembro 2015 a novembro 2016	1.500.000,00	1.500.000,00
TER/AM	novembro 2016 a novembro 2017	1.500.000,00	1.427.876,17
ICMBio	setembro 2016 a setembro 2017	240.000,00	240.000,00
Valor total (parcerias 2015 a 2018)		18.240.000,00	18.167.876,17

Fonte: elaborado pelo autor com base no TCU (BRASIL, 2019).

Além desses instrumentos de parceria, participaram o Ministério da Defesa, o Exército Brasileiro e, ainda, recursos oriundos de emendas parlamentares – Quadro 4.5. Abaixo seguem os valores:

Quadro 4.5: Amazônia Conectada – recursos da Defesa e outros

FONTE DOS RECURSOS	Valor previsto (R$)
MD	15.093.672,69
EB	5.731.268,50
Emendas Parlamentares	321.926,65
Valor total	21.146.867,84

Fonte: elaborado pelo autor com base no TCU (BRASIL, 2019).

O valor total investido pelos órgãos do governo federal brasileiro e pelo legislativo, por meio de emendas parlamentares, foi de R$ 39.314.744,01.

4.2.1.3 Óbices ao PAC

O ineditismo do PAC apresentou alguns óbices que podem servir de lições para futuros projetos e programas desta natureza. Na verdade, no próprio desenrolar da implementação do Amazônia Conectada notamos correções de rumos.

Além da geografia do local no qual foi implementado, em rios sinuosos, com forte correnteza e grande volume de água, e sazonalidade entre período de cheia e de vazante, tendo em vista o regime de alimentação; em face da densa e úmida floresta e do relevo irregular, o PAC expôs alguns problemas de ordem administrativa que influenciaram negativamente no desempenho desta política pública e contrariaram algumas previsões oficiais, como as da E-Digital:

> Um dos aspectos mais notáveis do Projeto Amazônia Conectada é o do modelo de governança e de sustentabilidade, concebido como um trabalho cooperativo. O custo inicial do projeto é compartilhado entre órgãos do poder público, nas esferas Federal e Estadual, demandantes de infraestrutura de banda larga nos municípios. Assim, numa segunda etapa, a partir da disponibilidade dessa infraestrutura, com oferta local de capacidade de transporte de dados, prestadores podem também viabilizar um modelo de negócio sustentável de oferta de serviços de telecomunicações e de acesso à internet à população. (BRASIL, 2018, p. 20)

Utilizamos como base, além do empirismo e de acompanhamento de reportagens, um acórdão do TCU, de 2019, de autoria do Ministro Bruno Dantas, que tratou de, conforme constante no próprio documento, verificar do PAC: 1) se a estratégia de implementação contemplou os pilares essenciais da inclusão digital, que são três: infraestrutura, alfabetização e conteúdo; 2) se a sustentabilidade econômica e operacional foi prevista e articulada.

Além disso, mas ainda relativo à condução e à administração de políticas públicas de Defesa, o resultado de pesquisa de dissertação feita no Ipea por Eduardo Athouguia (SILVA, 2017) nos serviu de fundamentação, uma vez que analisou os arranjos institucionais de dois projetos – o Sisfron e o SGDC – e constatou problemas muito semelhantes ao por nós verificados na análise do PAC e mencionados no supracitado relatório do TCU.

No tocante à sustentabilidade econômica e operacional do PAC, os problemas constatados pelo TCU foram, principalmente, os ligados à governança do programa. Houve, segundo aquele órgão fiscalizador: insuficiência de coordenação e coerência entre os atores envolvidos na política pública; falta de planos e objetivos de médio e longo prazos; escassez de recurso financeiros não só para implementação da infraestrutura, mas também para a operação e a manutenção do funcionamento do sistema. Como conclusão, o TCU apontou que a descontinuidade do planejamento e da estrutura foi um fator complicador.

Ainda no que diz respeito à governança e à distribuição de competências, atribuições e, portanto, responsabilidades, não foi verificada a existência de um plano de gestão de riscos, uma exigência para programas federais dessa magnitude, de acordo com normas do TCU e da Casa Civil da Presidência da República.

Mesmo considerando a existência de um comitê gestor do programa, instituído consoante Portaria Interministerial nº 586/2015 – a mesma que criou o programa –, uma das considerações do TCU foi que "[...] apesar de o MCTIC, Telebrás e EB fazerem parte do Comitê Gestor do Programa, a distribuição de competências entre esses atores não se deu de forma equilibrada com suas respectivas competências e capacidades organizacionais." (BRASIL, 2019)[160]. A falta de coordenação ocorreu, segundo o mesmo acórdão, tanto entre o MD e o EB, quanto entre esses e os outros atores, federais e estaduais.

O Ministro Bruno Alves, nesse sentido, citou o problema envolvendo o MEC e o EB como o mais crônico, a fim de ilustrar a questão da falta de coordenação e de definição de competências e atribuições. De um lado, o MEC disse que os valores repassados para o PAC previam o lançamento tanto do *backbone*, quanto do *backhaul* e da rede de acesso ou da última

[160] Em documento-resposta obtido da Telebras, consta realmente como ator principal da implementação do PAC o Exército e o MD, sem mencionar aquela empresa ou outro ministério na consecução. Ver Anexo "C".

milha, sendo essas duas últimas partes responsáveis por fazer chegar a *internet* até a ponta da linha, isto é, o usuário final, quer órgão público, quer instituição privada ou a população de forma geral. Por outro lado, o EB informou nos autos que o valor repassado foi referente apenas ao projeto de infraestrutura, que previu a instalação e o funcionamento do *backbone*, e não das outras ramificações.

Como consta nos autos do acórdão em que nos baseamos, não tratou o TCU, nesse momento, de verificar a quem cabia a razão, mas sim focar nos óbices que impediram o PAC de atingir sua plenitude, segundo expectativa inicial dessa política pública.

Continuando nos problemas relacionados à deficiência na estrutura de governança, o TCU diagnosticou a falta de prioridade dada ao programa por parte do governo federal, eis que dos 600 milhões de reais previstos inicialmente, apenas 39 milhões foram investidos, de fato, e isso contando com os recursos repassados pelas parcerias, via convênio ou TED (rever Quadros 4.4 e 4.5). Para o TCU, o programa começou sem a devida garantia de recursos recorrentes. Esse órgão fiscalizador concluiu essa parte do relatório assim:

> Ao mesmo tempo que essa capacidade de engajamento e coordenação com diversos atores para o fornecimento de recursos pode ser considerada uma boa prática do programa, ela também demonstra a falta de priorização do programa pelo governo federal, posto que o MCTIC, órgão setorial do governo responsável pelas ações de banda larga e inclusão digital, forneceu menos de 10% do orçamento do programa [...]. (BRASIL, 2019, parágrafo 197)

Em relação ao requisito da *inclusão digital* e dos *três pilares* apontados como chave para a plena consecução do PAC (TCU, 2015), o TCU concluiu que o programa não atingiu plenamente nenhum. A parte referente à *infraestrutura* foi parcialmente entregue, tendo em vista que o PAC foi capaz de oferecer *backbone* e *backhaul* de fibra ótica no interior do Amazonas, conectando organizações militares e órgãos públicos parceiros, contudo, não forneceu rede de acesso para a inclusão digital da população em geral. Esse ponto nos remonta ao já relatado envolvendo o MEC e o EB e a falta de consenso quanto aos objetivos, competências e atribuições no acordo de parceria, e também à baixa participação dos outros atores do comitê gestor, no caso o MCTIC e a Telebrás.

No que diz respeito ao pilar *alfabetização*, este se refere à capacitação do indivíduo para o uso das Tecnologias da Informação e Comunicação (TICs), e, no tocante ao *conteúdo*, este prevê o fornecimento de conteúdo adequado às necessidades do usuário. Segundo o TCU, não houve, entre 2015 e 2018, ações relacionadas a esses dois pilares, fato que comprometeu a efetiva inclusão digital, um dos objetivos do programa. São esses pilares que definem – ou

podem vir a definir – a diferença entre meros usuários da *internet* ou consumidores via *e-commerce* de empreendedores e fomentadores de riqueza original e autóctone. Esses aspectos, portanto, são de extrema importância dentro da concretização verdadeira de poder e riqueza.

Para o Ministro Bruno Dantas, caso fossem contemplados esses pilares, quando da implementação do programa, haveria indicação de avanços significativos em termos de gestão de políticas públicas no Brasil, o que poderia servir de novo marco no desenvolvimento do setor de telecomunicações, sobretudo para as áreas mais deficientes em estrutura deste serviço.

Todavia, o TCU compreendeu, no que concordamos, que a construção de infovias na região amazônica é tarefa que, *per se*, possui alta complexidade e requer, por isso, um aparato de engenharia e logística peculiares, o que esbarrou em outro entrave, qual seja, na indisponibilidade de oferta de serviços dessa natureza na região. Essa constatação também pode ser inferida nos documentos emitidos pelo Exército/MD ao buscarem esclarecer os problemas ocorridos antes, durante e após a implantação, e no que diz respeito à manutenção de seu funcionamento.

4.2.1.4 Histórico de Atividades e Infovias Implantadas

Com relação ao histórico do programa, podemos resumir da seguinte forma:

Quadro 4.6: Histórico das Principais Atividades do PAC

Período/Data	Evento/Atividade
Novembro de 2014	Assinatura do memorando de entendimento
Abril de 2015	Lançamento do projeto piloto finalizado
Julho de 2015	Inauguração do 1° trecho do Projeto Amazônia Conectada
Julho de 2015	Publicação da Portaria Interministerial N° 586
Novembro de 2015	I Workshop Amazônia Conectada
Março de 2016	Lançamento do trecho Coari-Tefé finalizado
Junho de 2016	II Workshop Amazônia Conectada
Maio de 2017	Lançamento dos trechos Manaus-Coari e Manaus-Novo Airão finalizados
Fevereiro de 2018	Publicação da Portaria Normativa N° 5/MD[161]

Fonte: elaborado pelo autor com base no TCU (BRASIL, 2019).

[161] Publicou o Comitê Gestor do PAC no âmbito MD. Até então o comitê era no âmbito do Comando do Exército. Em 2018 já se tinha percepção dos problemas relativos à governança dessa política pública. Essa foi uma medida para tentar minimizar tais fatos. A Portaria nº 586, de julho de 2015, foi a que instituiu o PAC.

Já no tocante às infovias que foram implementadas, em 2018 o total da extensão da rede de fibra ótica subfluvial perfazia aproximadamente 850 Km, o que representava cerca de 10,9% do previsto incialmente.

As cidades interligadas, todas no Estado do Amazonas, foram: Manaus, Manacapuru, Coari, Tefé, Novo Airão e Iranduba, de um total previsto de 52 municípios. Essa rede instalada passou a ser denominada de Vitória Régia (RVR), distribuída da seguinte forma:

– Infovia do Alto Rio Negro ou do Rio Negro: ligação entre duas organizações militares do Exército, inicialmente, com extensão de 10 Km (Cento de Embarcações do Comando Militar da Amazônia – CECMA – e 4ª Divisão de Levantamento[162]). Este foi o primeiro trecho inaugurado do programa. Constou como uma das fases do projeto-piloto. Na sequência foram lançados mais 14Km, interligando a 4ª DL à Comissão de Aeroportos da Região Amazônica (COMARA), também duas unidades militares, sendo a segunda da Força Aérea, todas localizadas no município de Manaus. Após isso, mais 8Km, de Manaus à cidade de Iranduba, e Manaus-Novo Airão, com 127 Km de extensão.

– Infovia do Rio Solimões: onde foi inaugurado o trecho de maior extensão – 232 Km –, ligando o município de Tefé ao de Coari. Ainda no Solimões: Manaus-Manacapuru, com 118 Km; Manacapuru-Coari, com 340 Km, perfazendo nessa infovia o total de 690 Km.

Por fim, com relação à situação do programa, até 2018 os parceiros que participaram com aporte de recurso (Quadro 4.4) não tinham recebido o referido serviço acordado. E, quanto às organizações militares, nem todas tinham acesso ao serviço, devido à falta de manutenção da Rede Vitória Régia ou por causa de atos de vandalismo, como constou no acórdão do TCU (BRASIL, 2019) e em reportagens disponíveis na *internet*.

4.2.2 A Cibernética como Espaço e Recurso de Poder no Brasil: o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC)

Outro esforço brasileiro que registramos no sentido de articular Defesa-Desenvolvimento, passando pela utilização de ferramentas ligadas ao setor cibernético, foi o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), em sua primeira versão (SGDC-1).[163]

---

[162] Hoje denominado 4º Centro de Geoinformação (4º CGEO) do Exército, é uma unidade militar responsável por fazer o levantamento geográfico da região e é vinculada ao Departamento de Serviço Geográfico do Exército.

[163] O lançamento do segundo SGDC, o SGDC-2, está previsto para o ano de 2022, conforme o Programa Nacional de Atividades Espaciais (PNAE) 2012-2021.

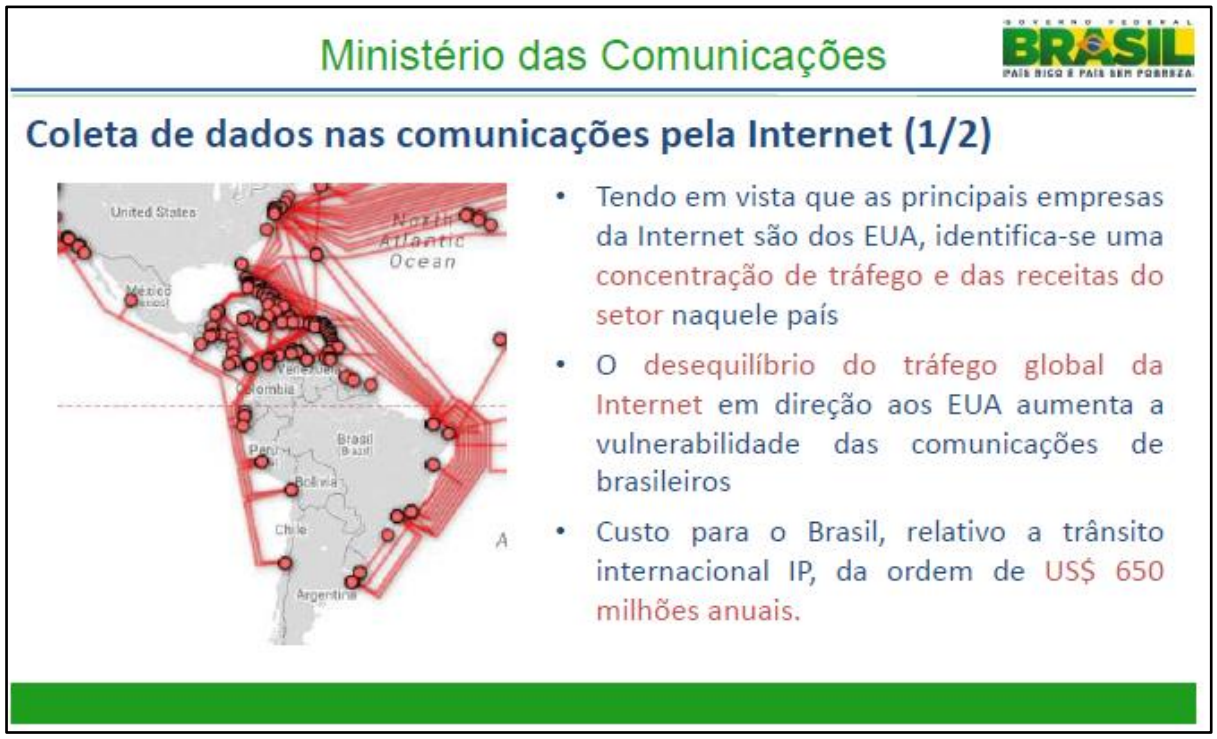
O SGDC fez parte do Programa Espacial Brasileiro (PAE), que tem, pelo menos formalmente, como seu braço executante e atualizadora do programa de uma forma geral, a Agência Espacial Brasileira (AEB), criada em 1994, ano da publicação da Política Nacional de Desenvolvimento das Atividades Espaciais (PNDAE) e, como instrumentos de planejamento e de programação, o Programa Nacional de Atividades Espaciais (PNAE), em suas versões de 1995, 2005 e 2012, e o Programa Estratégico de Sistemas Espaciais (Pese), de 2012, complementar ao PNAE e visando atender à Estratégia Nacional de Defesa (2008).

O PNAE previa a implementação do SGDC mesmo antes do episódio Snowden sobre espionagem dos EUA e inserido em um sistema tal qual o agora denominado hélice tríplice, por meio da interação de Estado-indústria-academia, com ênfase para o fortalecimento da indústria espacial. Todavia, após esse caso de espionagem internacional, o projeto ganhou força, como pode ser constatado por manchete da época:

> O ministro das Comunicações, Paulo Bernardo, citou nesta quinta-feira, 11 [de julho de 2013), os planos para o lançamento de um novo satélite nacional e a construção de novos cabos submarinos ligando o Brasil à Europa e à África como instrumentos para **diminuir a vulnerabilidade do País a interceptações e monitoramentos realizados pelos órgãos de inteligência dos Estados Unidos**. (O ESTADÃO, 2013, **grifo nosso**)

O caso Snowden veio a público no final de junho de 2013. Pouco tempo depois o então Ministro das Comunicações anunciava projetos, a fim de minimizar vulnerabilidades e, ao mesmo tempo, diminuir custo de transmissão de dados em território nacional e intercontinentais. Nesse mesmo período, a Câmara dos Deputados requereu a presença dessa autoridade federal para se pronunciar acerca do fato e expor tais medidas reativas. Nas Figuras 4.12 e 4.13 destacamos *slides* da apresentação do Ministro Paulo Bernardo à Câmara, no tocante ao tema:

Figura 4.12: Aspectos Críticos das Comunicações Globais (2013)



Fonte: Câmara dos Deputados, 2013. [164]

Figura 4.13: Ações Empreendidas pelo Governo Brasileiro pós-Caso Snowden (2013)

Fonte: Câmara dos Deputados, 2013.

[164] Apresentação do Ministro das Comunicações em audiência pública na Câmara dos Deputados, em 14/8/2013. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cctci/audiencias-publicas/2013/eventos-2013/ap-2013.08.14-comunicacoes-eletronicas/min.-paulo-bernardo. Acesso em: 19 abr. 2019.

Constatamos dessa audiência pública do Ministério das Comunicações do Brasil na Câmara dos Deputados o que desenvolvemos no capítulo 2 deste trabalho, acerca do funcionamento da *internet* e de vulnerabilidades em termos de segurança, sobretudo no tocante à unilateralidade, em última instância, dos Estados Unidos no funcionamento do sistema global e em sua capacidade de interferência. Também relembrando o capítulo 2, sobre esse poder e sua influência na interdependência das nações, Norman Angell (1910) não mencionou, no caso, à época, a respeito do poder britânico sobre o telégrafo.

Somamos a isso a questão dos ganhos econômicos advindos com a centralização da parte física da estrutura da *internet* no território estadunidense. Dessa forma, o SGDC passou a ser uma das ações empreendidas pelo Estado brasileiro para fugir ou minimizar essa interferência e esse poder, a partir do fortalecimento de suas capacidades estatais.

Apesar de estar vinculado diretamente ao setor estratégico espacial, logo sob encargo do Comando da Aeronáutica, conforme estipulado pela END (2008) e pela Diretriz Ministerial nº 14/2009, do MD – a mesma que atribuiu o setor cibernético ao Exército e o nuclear à Marinha do Brasil – o SGDC-1 interfere na cibernética vista tanto como espaço, quanto como recurso de poder para o Brasil.

Como espaço – ou ciberespaço – tornou-se uma infovia de espécie diferente daquela do Amazônia Conectada, que é por cabo de fibra ótica subfluvial, e da do cabo submarino Brasil-Europa, por meio de um cabo submarino também de fibra ótica. O SGDC, como recurso, utiliza-se do espectro eletromagnético para atuar nas faixas de frequência denominadas, respectivamente, bandas "X" e "Ka"; a primeira para uso estratégico, militar, controlada pelo MD, a segunda, sob gestão da Telebras, para fins civis, como na inclusão digital via disponibilidade de internet de banda larga buscada pelo PNBL, pela E-Digital e por outras inciativas.

Com relação à banda de uso estritamente militar, a "X", usando equipamentos em uma faixa de 7 a 8 GHz,

> engloba três cenários distintos, que requerem diferentes áreas de cobertura e capacidades: a) uma cobertura regional, abrangendo as Américas do Sul e Central, o Caribe, costa leste norte-americana, costa oriental da África e grande parte do Oceano Atlântico; b) cobertura nacional, sobre todo o território brasileiro e; c) cobertura gerada por um feixe móvel, capaz de gerar uma área de cobertura estreita (40 a 50.000 Km^2), em qualquer ponto do globo terrestre visível pelo satélite em sua posição orbital. (RUSSO, 2013, p. 5)

Já quanto à banda Ka, o satélite geoestacionário possui alcance de todo o território nacional, incluindo a Zona Econômica Exclusiva (ZEE) marítima, de 200 milhas náuticas, permitindo, assim, acesso às localidades mais remotas e sem estrutura de rede, seja por motivos geográficos, sejam econômicos, por questões ligadas à demanda e à escala, e a respectiva relação custo-benefício, quando considera apenas o ganho estritamente financeiro.

O SGDC foi resultado, mas ao mesmo tempo impulsionou, a parceria entre Telebras e Embraer, a partir da formação da empresa Visiona Tecnologia Espacial S. A., uma *joint-venture*[165] constituída para atuar como integradora dos satélites nacionais e, a partir desta *expertise*, ser o braço industrial do Brasil para projetos e desenvolvimento de novas soluções espaciais.[166]

Os ganhos com a implementação do SGDC, consoante a empresa Visiona, relacionam-se à cobertura de 100% de serviços de *internet* a todo território nacional, possibilitando a inclusão digital aos locais que não são atendidos pela estrutura de fibra ótica, e a segurança para as comunicações estratégicas. Além disso, como benefício derivado no tocante à absorção de tecnologia, houve a capacitação em todas as fases do projeto de trinta engenheiros junto à empresa franco-italiana Thales Alenia Space (TAS), responsável pela construção do SGDC-1. O desenvolvimento deste projeto ocorreu na cidade de Cannes, na França.

Para a consecução do SGDC-1 pode ser verificada articulação entre Ministérios, como o da Defesa, o das Comunicações e o da Ciência, Tecnologia e Inovação, e de mais de um Poder, como foi o caso da participação do Legislativo, via Câmara dos Deputados e Senado Federal, tanto em suas comissões especializadas em infraestrutura, ciência e tecnologia, e em audiências públicas, quanto via publicações da Revista Em discussão!, do Senado.

A articulação entre Ministérios pode ser, por exemplo, inferida na Estratégia Nacional de Ciência, Tecnologia e Inovação (ENCTI) (2016-2022), ao abordar especificamente o tema estratégico Aeroespacial e Defesa. Assim consta nessa estratégia, no tocante aos seus objetivos para este tema e respectivas estratégias (Quadro 4.7):

> OBJETIVO - Promover a capacidade do País, para segundo conveniência e critérios próprios, utilizar os recursos e técnicas aeroespaciais na solução de problemas nacionais e em benefício da sociedade brasileira, bem como **fomentar a pesquisa e o desenvolvimento de produtos e sistemas militares**

[165] "Entende-se por ***joint venture*** a associação econômica entre duas empresas, que podem ou não ser do mesmo ramo, durante um período específico e limitado. Essa parceria pode operar de várias maneiras, executando-se para fins logísticos, industriais, comerciais, tecnológicos e outros [...]. Uma *joint venture* também costuma ser chamada de **cooperação econômica** e sua diferença em relação a outras associações é que as empresas envolvidas não perdem suas personalidades jurídicas." (PENA, 2020).

[166] Conforme Caio Bonilla, da Telebras, esta *joint venture* foi constituída com 49% de ações da Telebras e 51% da Embraer.

> **e civis que compatibilizem as prioridades científico-tecnológicas com as necessidades de defesa**. (BRASIL, 2016)

Quadro 4.7: Estratégias da ENCTI (2016-2022) para o Setor Aeroespacial e Defesa

ESTRATÉGIAS ASSOCIADAS
I. Elaboração de "Planos de Ação de Ciência, Tecnologia e Inovação para os setores Aeroespacial e de Defesa" que promovam o compartilhamento de competências em cooperações internacionais observando-se **aspectos de segurança e soberania nacional, bem como os serviços essenciais de comunicação, monitoramento atmosférico e de alterações ambientais no território brasileiro**.
II. Fomentar a pesquisa e desenvolvimento científico, tecnológico e de inovação, visando à criação e fabricação de sistemas espaciais completos de satélites e veículos lançadores e desenvolver tecnologias de guiamento, sobretudo sistemas inerciais e tecnologias de propulsão líquida.
III. Desenvolver aplicações que exploram as tecnologias e os dados espaciais nas áreas de **observação da Terra e de comunicações**.
IV. Promover a **participação contínua e crescente da indústria nacional nos programas e projetos espaciais, aeronáuticos e de defesa**.
V. Implantar e atualizar a **infraestrutura espacial básica** (laboratórios de pesquisa e desenvolvimento, centros de lançamentos e centros de operação e controle de satélites) **e da defesa** (laboratórios de pesquisa e desenvolvimento das Forças Armadas).
VI. Fomentar a pesquisa e o desenvolvimento de sistemas aeronáuticos alinhados com *roadmaps* tecnológicos do avião do futuro.
VII. Contribuir para o **fortalecimento da indústria de defesa** em áreas estratégicas **para o desenvolvimento da capacidade produtiva nacional, com valorização da capacitação do capital humano e a ampliação da persuasão em defesa nacional**.
VIII. Promover a formação e desenvolvimento de novas competências humanas para os setores espacial, aeronáutico e de defesa.

Fonte: BRASIL, 2016, **grifo do autor**.

Podemos apreender disso que tanto Defesa e Desenvolvimento foram – e são – buscados por essa estratégia, como a vinculação entre as tecnologias espaciais com as de comunicações, o que contempla, intrinsicamente, ferramentas cibernéticas.

Tanto é a necessidade dessa integração que em 5 de junho de 2018 houve uma reunião entre representantes do Exército – Força encarregada de coordenar o setor cibernético, como vimos – e da Força Aérea – responsável pelo setor espacial –, esta por meio de sua Comissão de Coordenação e Implantação de Sistemas Espaciais, para alinharem demandas e possibilidades da Força Terrestre para utilização do SGDC no Sisfron e em operações táticas, como são as de garantia da lei e da ordem (GLO) (DEMENICIS, 2018; REVISTA TECNOLOGIA E DEFESA, 2018). Ainda quanto às demandas do Exército, o então comandante do Comando de Defesa Cibernética, general Angelo Kawakami Okamura, assim se referiu em 2018:

> Com o apoio do SGDC, os ataques que utilizam o espectro eletromagnético e o espaço cibernético são monitorados em tempo real, alimentando as atividades de inteligência de sinais e operações em rede [...]. Esse compartilhamento por satélite restrito garante a integridade e reforça a restrição aos ataques cibernéticos de *hackers*, aumentando a segurança dos sistemas em rede e de comunicações nesse cenário cibernético. (REVISTA TECNOLOGIA E DEFESA, 2018)

Essa descrição acerca da reunião entre Exército e Força Aérea e a fala do general Okamura nos levaram ao conceito de guerra centrada em redes (*network-centric warfare*), destacada por nós no Capítulo 1, que é, segundo o Glossário das Forças Armadas brasileiras:

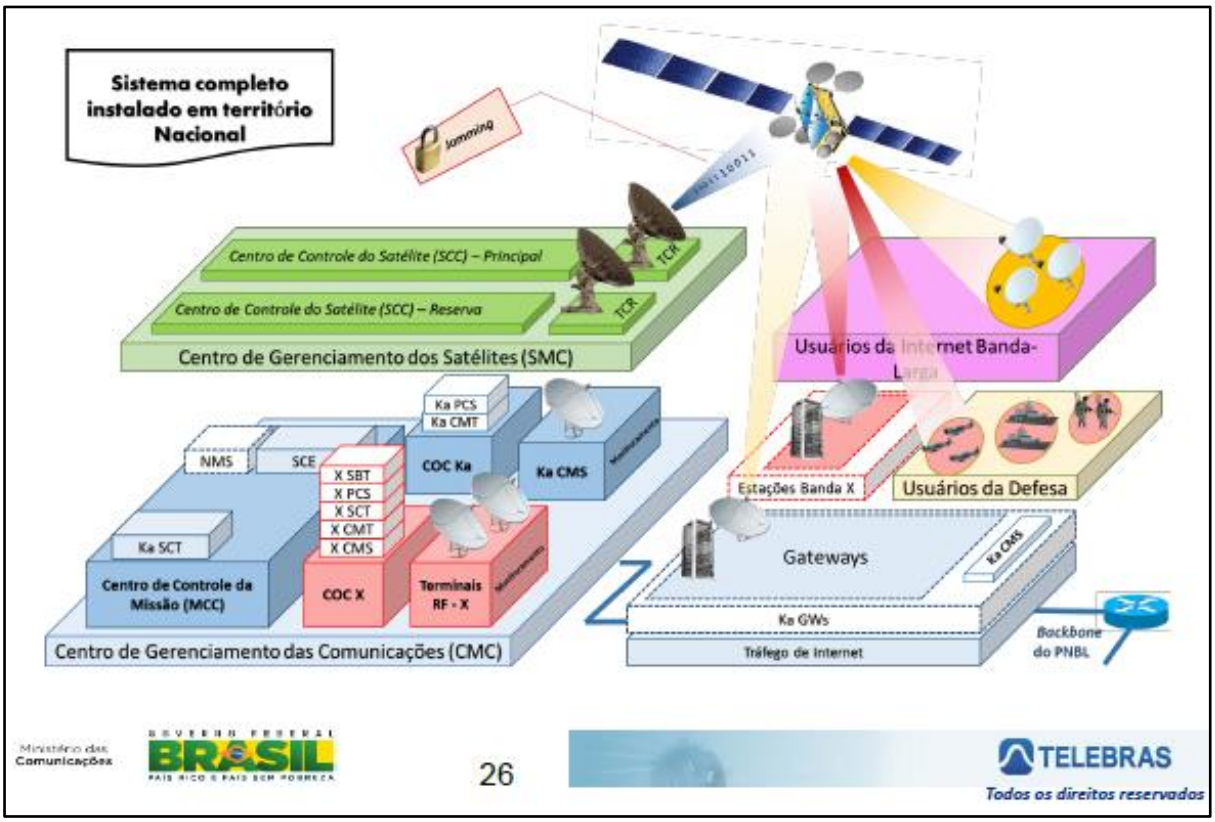
> Guerra que reúne em rede os mais diversos elementos das forças armadas de um país, permitindo-lhe administrar diversas tarefas que vão desde a coleta até a distribuição de informações críticas entre esses muitos elementos. Outorga-lhe maior capacidade de combate ao ligar em rede os elementos de sensoriamento, de combate e de comando. Visa obter melhor sincronismo entre aqueles elementos e os efeitos que podem proporcionar, assim como o incremento na velocidade das operações bélicas e do processo decisório de comando. (BRASIL, 2015, p. 123)

A guerra centrada em redes, por sua vez, contém os conceitos de guerra eletrônica[167], mais voltada para o espectro eletromagnético, e de guerra cibernética, mais relacionada a computadores e à estrutura de recepção, processamento e transmissão das infovias. Tudo isso buscando minimizar as condições impostas pela geografia, seja a morfologia do terreno e sua cobertura vegetal, seja com relação a distâncias, e pela variável *tempo* e o poder advindo da velocidade obtido pela logística, como alertou Bertha Becker (2012 [1988]).

[167] "Conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas." (BRASIL, 2015, p. 125). Esses conceitos também foram apresentados por nós no Capítulo 1 desta tese.

Assim temos o alinhamento das diretrizes da END (2008), quanto ao monitoramento, comando e controle, como um dos paradigmas no processo de transformação das Forças Armadas, e o previsto no Pese (2012), ao explicitar como uma de suas finalidades proporcionar a atuação das forças militares no ambiente da guerra centrada em redes. Daí as funções pretendidas com o uso do SGDC e respectiva estrutura de solo para controle, recepção e processamento dos dados[168]: serviços de observação terrestre, de telecomunicações, de mapeamento de informações, de posicionamento, de monitoramento do espaço e de operações de sistemas espaciais (Figura 4.14).

Figura 4.14: Estrutura e Funcionamento do SGDC



Fonte: adaptado de Senado Federal (2013). [169]

[168] Segundo o Ministério da Defesa (2018), tratou-se do Centro de Operações Principal (COP-P), em Brasília, e Secundário (COP-S), no Rio de Janeiro, que funciona como uma espécie de espelhamento daquele (*back up*), e mais três estações (*gateways*), em Florianópolis, Campo Grande e Salvador, responsáveis por fazer a interconexão entre o satélite e os usuários. Disponível em: https://www.defesa.gov.br/noticias/50849-centro-de-operacoes-do-sgdc-e-inaugurado-em-brasilia.

[169] Apresentação da Telebras à Comissão de Serviços de Infraestrutura do Senado, em 4/11/2013. Disponível em: file:///C:/Users/se%C3%A7%C3%A3oA03/Downloads/DOC_ORADOR_C_8869_K-Comissao-Permanente-CI-20131104EXT053_parte2696_RESULTADO_1383596190255.pdf. Mais uma vez a participação do legislativo federal.

Além disso, há previsão de formação de enlaces do SGDC com outros sistemas, alguns já em operação – como o Sistema de Defesa Aeroespacial Brasileiro (Sisdabra), o Sistema de Comunicações por Enlace de Digitais da Aeronáutica (Siscenda), o Sistema de Comunicações Militares por Satélite (Siscomis) e o Sistema Militar de Comando e Controle (SISMC2) –, outros no futuro – como o Sistema de Gerenciamento da Amazônia Azul e o Sistema de Vigilância das Fronteiras (Sisfron).

O SGDC-1 foi lançado em 4 de maio de 2017 – a previsão inicial era no ano de 2014 – da base de Korou, na Guiana Francesa, devido à sua localização geográfica, próxima à linha do Equador, e porque a base de Alcântara não suportava a capacidade do foguete que lançou o satélite.

O uso da banda "X" começou efetivamente em 30 de junho de 2017, quando a Thales Alenia Space, empresa que detinha a tecnologia e fez parceria com a Visiona, passou o controle total do satélite para técnicos e especialistas brasileiros da Telebras e das Forças Armadas (DEMENICIS, 2018).[170] Em teste operacional ocorrido em junho de 2018, foi verificado que a velocidade de conexão e a capacidade de interligação dos terminais que compõem o sistema atenderam de forma satisfatória aos objetivos pretendidos até então.

Já a banda Ka só começou a ser usufruída pela sociedade no segundo semestre de 2018, devido a litígio na justiça, que chegou ao Supremo Tribunal Federal (STF), envolvendo possível beneficiamento da empresa Viasat, norte-americana, com o acordo feito com a Telebras para ser a exploradora exclusiva desse serviço[171]. Em abril de 2019, segundo a Telebras, já eram mais de 900 mil alunos beneficiados por esse serviço, por meio de 2.800 escolas cadastradas. Desse universo, cerca de 78% nas Regiões Norte e Nordeste (TELE.SÍNTESE, 2019), o que vai ao encontro das expectativas e diretrizes do PNBL e da E-Digital, como vimos.

---

[170] Segundo Demenicis, em *post* publicado no EBlog, após ser lançado pelo foguete Ariane 5 ECA, da empresa Arianespace, o SGDC "foi posicionado, em 11 de junho de 2017, na sua localização definitiva: no meridiano 75° Oeste e a uma altitude de 35.865 km da superfície da Terra." (DEMENICIS, 2018). Disponível em: http://eblog.eb.mil.br/index.php/menu-easyblog/satelite-geoestacionario-de-defesa-e-comunicacoes-estrategicas-1-sgdc-1.html. Acesso em: 29 abr. 2020.

[171] As empresas Via Direta Telecomunicações por Satélite e Internet Ltda. e a Rede de Rádio e Televisão Tiradentes Ltda. questionaram a legalidade do contrato firmado entre a Viasat e a Telebras. Em 22 de maio de 2018 o TCU aprovou os termos do acordo refeito entre Telebras e Viasat, mas apenas em 16 de julho de 2019 o STF autorizou a continuidade do contrato. Sob novos rótulos, agora *Internet para Todos* e *Educação Conectada*, políticas públicas passaram a ser beneficiadas com o serviço, além do *Governo Eletrônico – Serviço de Atendimento ao Cidadão* (GESAC). Convém registrar a participação da Telebras com o SGDC no apoio à tragédia do rompimento da barragem, em Brumadinho-MG, em janeiro de 2019, instalando antenas e prestando suporte de internet para auxílio aos trabalhos de busca. Todavia, vemos fundamentos no questionamento descrito, sobretudo devido à Viasat ser um empresa norte-americana, ainda que a Telebras afirme que a Viasat não passou a possuir controle do satélite, nem da banda "Ka", apenas presta o serviço de distribuição aos usuários.

4.2.2.1 Óbices do Programa

O SGDC apresentou óbices similares ao Amazônia Conectada, no tocante aos recursos orçamentários, que foram inconstantes e de montante bem inferior ao necessário, e em relação à coordenação entre os participantes, isto é, à governança das atividades do setor.

Segundo relatório do Grupo de Trabalho Interministerial para o Setor Espacial – GTI Espacial – criado em 2015 para assessorar os Ministérios da Defesa e da Ciência, Tecnologia e Inovação –, há necessidade de criação de um conselho nacional – o Conselho Nacional do Espaço – a fim de deliberação das atividades do setor. Este Conselho ficaria subordinado à Casa Civil da Presidência da República, o que acarretaria maior ingerência sobre ações interministeriais, com perspectiva de concentrar os esforços no setor, até então dispersos, descentralizados.

Esse mesmo problema foi diagnosticado pelo TCU (BRASIL, 2016) e por Vellasco (2019), aquele identificando, por meio da utilização da matriz de SWOT[172], a governança como uma ameaça à continuidade do Programa Espacial Brasileiro (PEB), esta apontando como causas o esvaziamento da AEB e sua perda de articulação política e capacidade de deliberação, ao ver desfeito o seu vínculo direto com Presidência da República, em 2000, e ser vinculada ao MCTIC. Para Vellasco (2019), haveria necessidade de retorno da vinculação da AEB à Presidência e ao mesmo tempo de se tornar a responsável pelo Comitê Executivo do Espaço, este inserido no Comitê Nacional do Espaço.

O GTI Espacial ainda constatou dificuldade na contratação de pessoal, bens, serviços e obras, fruto das condições impostas pelo marco regulatório constante da Lei nº 8.666/1993, o que foi ratificado no levantamento feito pelo TCU (BRASIL, 2016), que acrescentou, ainda, como consequência dessa dificuldade, o fluxo irregular de contratações e a necessidade de acúmulo de funções de ordem técnica e de gestão administrativa. Somou-se a isso, disse o TCU (BRASIL, 2016), a escassez de concurso público para órgãos do setor espacial, como no caso do Inpe, que acarreta um perfil envelhecido do seu quadro de pessoal.

Por fim, Vellasco (2019), que estudou o desenvolvimento da indústria espacial brasileira, por meio da abordagem institucional, acrescentou que institutos e empresas públicos competem entre si por recursos, como foi o caso do Inpe e da Visiona, por exemplo, e reforçou a fragilidade da AEB, além dos motivos já expostos, pela grande autonomia que possuem o Departamento de Ciência e Tecnologia da Aeronáutica (DCTA), órgão vinculado à FAB e, portanto, ao MD,

[172] Metodologia utilizada na área gerencial para diagnosticar, em linhas gerais, forças (*strengths*), fraquezas (*weaknesses*), oportunidades (*opportunities*) e ameaças (*threats*).

e o Inpe, vinculado ao MCTIC. Daí, para essa pesquisadora, mais um motivo para o desenho de uma nova forma de governança institucional.

4.2.3 A Cibernética como Espaço e Recurso de Poder no Brasil: o cabo submarino Brasil-Europa

A história dos cabos submarinos que permitiram as comunicações entre as nações e continentes, primeiro por sinal de telégrafo, depois por telefone e, mais recentemente, na forma digital, passa por questões que envolvem ciência, tecnologia e, invariavelmente, poder, este entendido como elemento capaz de dar a alguém ou a algum grupo ou instituição a possibilidade de decidir e, por conseguinte, de obter ganhos nos mais diversos campos. Todavia – novamente grifamos – sobre isso nada registrou Norman Angell em sua "Grande Ilusão" (1910) e na sua indicação de ganhos para todos, isto é, nos jogos de soma sempre positivas a partir do fenômeno da interdependência, formada pela transmissão e recepção de dados, que continham, por sua vez, informação para auxiliar o decisor em assuntos de diversas áreas – economia, política, cultura etc. A questão passa a ser: quem detinha (e detém) esse controle? Quem detinha esse poder, no espaço e no tempo oportuno? Este, para nós, é o ponto. E a resposta pode ser inferida da história, com um olhar, segundo Braudel (1965; 1987), não na superfície, nem na conjuntura, mas no conjunto da obra e, se possível, nas partes mais profundas das relações que envolvem poder.

No âmbito global, o primeiro cabo submarino internacional foi responsável por ligar com sinal telegráfico Inglaterra e França, duas potências mundiais, em 1850. Apenas oito anos depois, em 1858, após algumas tentativas e testes, funcionou o intercontinental da *Atlantic Telegraph Company*, com mais de 4.000 Km de extensão, ligando a Europa aos Estados Unidos da América. De ambos os lados estavam entre seus primeiros interlocutores os dois chefes de Estado: a Rainha Vitória, pelo velho continente, e o presidente James Buchanan, pelo lado americano. Essa iniciativa se consolidou apenas em 1866.

No Brasil, o registro do primeiro cabo submarino ocorreu em 1857, junto com a primeira linha telegráfica, com cerca de 50 Km de extensão, dos quais 15 eram submersos, interligando a cidade do Rio de Janeiro (Praia da Saúde) ao município de Petrópolis-RJ, propiciando, além de comunicações para fins diversos, as relacionadas ao exercício do poder central e da corte imperial.

Ainda âmbito Brasil, os primeiros cabos totalmente submarinos foram inaugurados em 1874, por D. Pedro II, e foram responsáveis por interligar Rio de Janeiro, Salvador, Recife e Belém. No ano seguinte, o ponto de Recife foi estendido em direção a João Pessoa e Natal.

1875 também foi marcante para o País, quando o primeiro empreendimento dessa natureza propiciou ligação com a Europa, centro econômico, político e cultural do período. A iniciativa contou com a participação de Irineu Evangelista de Souza, o Visconde de Mauá, que idealizou e financiou, em parte, o projeto, que foi concluído pela *British Eastern Telegraph Company*.

O próximo grande salto no setor de comunicações intercontinental foi em 1956, com a primeira transmissão via cabo coaxial, que propiciava chamada telefônica, mais uma vez ligando a Europa (Escócia) à América do Norte (Canadá), com extensão para Londres, de um lado, e Otawa e New York, do outro do Atlântico. Tratou-se do *Transatlantic* nº 1 (TAT-1). Por trás desse empreendimento estavam, pelo Canadá, a *Canadian Overseas Telecommunications Corporation*; pelo Reino Unido, o *General Post Office Engineering Departament* e, pelos EUA, a *American Telephone and Telegraph* (AT&T) e o *Bell Telephone Laboratories*.

No que diz respeito à fibra ótica, a primeira rede transatlântica entrou em funcionamento em 1988. Era o TAT-8, que, além da *France Telecom* e da *British Telecom*, contava, novamente, com a AT&T e o *Bell Laboratories*.

No Brasil, hoje, há os seguintes cabos submarinos de alcance internacional (Quadro 4.8 e Figuras 4.15 e 4.16):

Quadro 4.8: Cabos submarinos internacionais no Brasil[173]

Cabo	Início de operação	Locais conectados
Americas 1	1994	- Brasil (Fortaleza-CE)–Estados Unidos, passando por Guianas, Trinidad Tobago, Venezuela, Curaçao, Martinica e Porto Rico. Extensão: 8.373 Km.
Unisur	1994	- Argentina (La Plata)–Uruguai (Maldonado)–Brasil (Florianópolis), com 1.995 Km. Mercosul.
Americas 2	2000	- Brasil (Fortaleza-CE)–Estados Unidos, passando por Guianas, Trinidad Tobago, Venezuela, Curaçao, Martinica e Porto Rico (idem Américas 1), com extensão de 8.373 Km. [174]

[173] No site da empresa estadunidense *TeleGeography* (https://www.submarinecablemap.com/#/submarine-cable/), especializada em análise de mercado para os setores de telecomunicações e tecnologia da informação, há um mapa interativo com apresentação dos cabos submarinos globais. Podemos identificar cabo por cabo e respectivas características gerais, como extensão, ano de início de operação, locais abrangidos e empresas controladoras.
[174] Mesmo percurso do Americas 1.

Atlantis 2	2000	- Brasil (Natal-RN)–Europa–África–América do Sul. São cerca de 8.500Km de extensão. [175]
Emergia-SAM	2001	- três Américas, funcionando como anel ótico do continente, através dos Oceanos Pacífico e Atlântico. No Brasil, são abrangidos por este: Santos (SP), Rio de Janeiro (RJ), Salvador (BA) e Fortaleza (CE). São cerca de 25.000 Km de extensão.
Global Crossing – *South American Crossing*	2001	- América do Norte, Central e do Sul, abrangendo Argentina, Brasil, Chile, Peru, Panamá e EUA. Um anel ótico, com aproximadamente 15.000 Km.
Globonet/360 Network	2001	- Estados Unidos–Brasil (Rio e Fortaleza), passando por Venezuela e Bermudas. 23.500 Km de extensão.
America Movil Submarine Cable System-1 (AMX-1)	2014	- América do Sul, Central e do Norte, com 17.800 Km de extensão. Passa por Colômbia, Guatemala, México, além de Brasil e EUA.
Seabras-I	2017	- Brasil–Estados Unidos, com 10.800 Km.
South Atlantic Cable System (SACS)	2018	- Brasil (Fortaleza)–Angola (Sangano), com 6.135 Km de extensão.
South Atlantic Inter Link (SAIL)	2018	- Brasil (Fortaleza)–Camarões (Kribi). Aproximadamente 6.000 Km.
Brusa	2018	- Brasil–Estados Unidos, passando por Porto Rico, com 11.000 Km.
Monet	2018	- Brasil (Santos e Fortaleza)–Estados Unidos (Flórida), com cerca de 10.556 Km.
Tannat	2018	- Brasil (Praia Grande-SP)–Uruguai (Maldonado), com 2.000 Km de extensão, complementar ao Monet.
Junior	2018	- Praia Grande (SP)–Rio de Janeiro (RJ), e dessas se conectando com o Monet, até a Flórida (EUA), também complementar ao Monet. 390 Km.
EllaLink	2020*	- Brasil–Portugal, passando pela Guiana Francesa (Korou) e Ilha de Cabo Verde. 6.200 Km de extensão.
Malbec	2020**	- Brasil (São Paulo-SP e Rio de Janeiro-RJ)–Argentina (Buenos Aires), com 2.500 Km de extensão.

Fonte: adaptado de Teleco e de *TeleGeography/PriMetrica, Inc*.

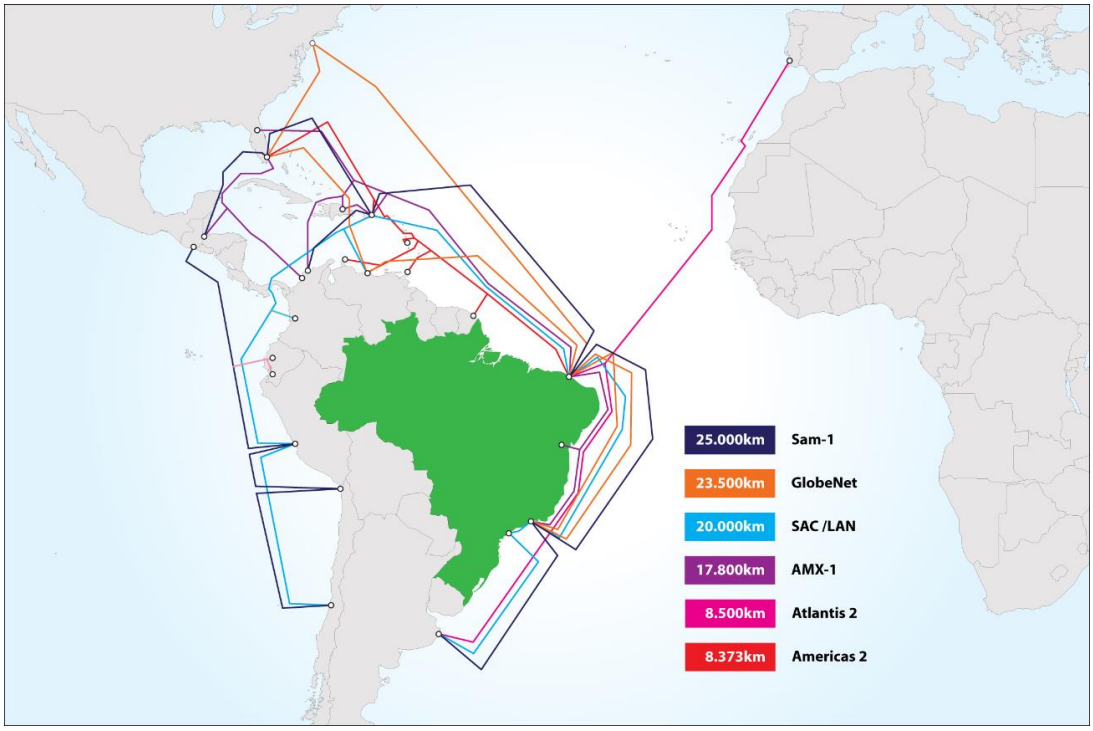
* previsão de funcionamento, segundo *TeleGeography/PriMetrica, Inc* e Consórcio Bella.
** previsão de funcionamento para 2020, consoante empresa GloboNet, responsável pelo projeto.

[175] Essa rede permite ao Brasil acesso aos 5 continentes. É tratada como a rede que representa a infraestrutura global da sociedade da informação.

Figura 4.15: Cabos Submarino no Brasil – escala regional

Fonte: *Site* Teleco.

Figura 4.16: Cabos Submarinos no Brasil – escala intercontinental



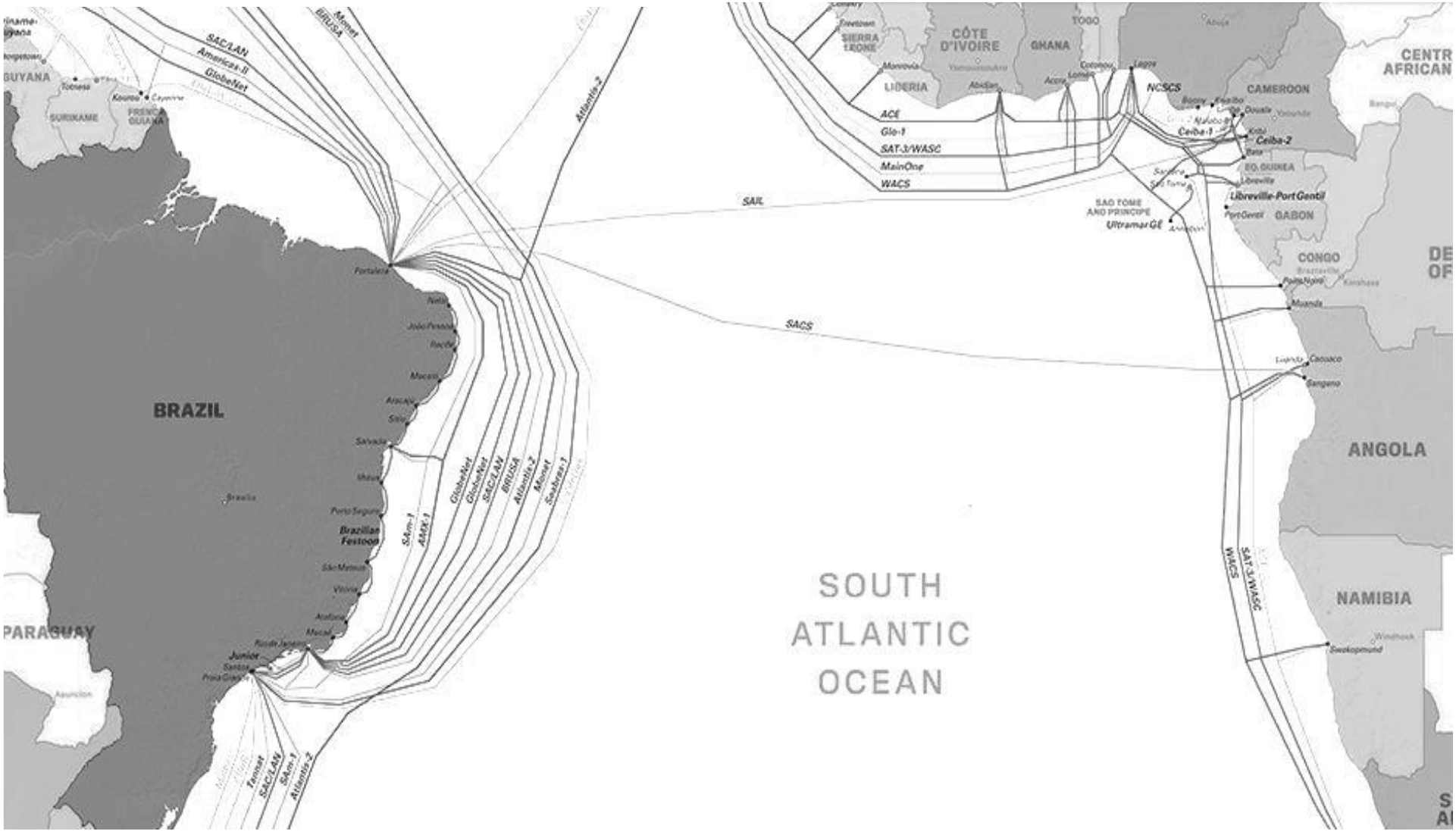
Fonte: Blog Entelco.Telecom.

Na Figura 4.17 há uma consolidação dos cabos submarinos existentes no País, complementando a visão dos mapas anteriores nas escalas local, regional e intercontinental. Desses mapas e do quadro anterior podemos inferir algumas informações.

Primeiro que existe, desde o ano 2000, um cabo submarino ligando Brasil-Europa, o Atlantis 2, contudo sua capacidade não comporta mais a demanda do fluxo de dados. À guisa de parâmetro, o Atlantis 2 possui capacidade de 20 Gbps e transmite quase que exclusivamente dados de voz, enquanto o projeto EllaLink tem a previsão de 40 a 72 Tbps e poderá transmitir no modelo de compressão digital, isto é, texto, som e imagem compactados.

Segundo, de 2008 a 2018, período a que se ateve essa pesquisa, não apenas o cabo da EllaLink foi projetado e/ou implementado. Tivemos o AMX-1, o Seabras-I, o SACS, o SAIL e o Brusa, e, mais recentemente, em 2018, anunciados pela Google, três empreendimentos: o MONET, ligando Santos a Fortaleza e à Flórida (Estados Unidos); o TANNAT, de Praia Grande-SP a Maldonado (Uruguai), e o JUNIOR, de Praia Grande-SP ao Rio e, desta cidade, interligando-se ao MONET. Esses últimos empreendimentos com previsão de início de operação em 2020.

Figura 4.17: Brasil - cabos submarinos internacionais



Fonte: *Site TeleGeography*.

Das infovias implementadas nesse recorte temporal, três ligam o Brasil aos Estados Unidos, dois diretamente ao continente africano e os outros mais no entorno local/regional, porém nenhum diretamente à Europa. Logo, a proposição de 2013, anunciada pelo Ministro de Estado das Comunicações, Paulo Bernardo, e por órgãos do legislativo federal, como mostramos anteriormente (no SDGC-1), no sentido de mitigar a vulnerabilidade do País a interceptações e monitoramento das infovias e respectivo conteúdo por parte dos Estados Unidos (O ESTADÃO, 2013), implementando rotas alternativas, parece não só não ter vingado como ter ido na direção oposta.

De acordo com a Telebras, em consulta feita por nós via ferramenta cibernética Fala.Br (Plataforma Integrada de Ouvidoria e Acesso à Informação) do governo federal, havia também, além do anunciado pelo Ministro das Comunicações, motivações técnicas e econômicas, como a melhoria da qualidade do sinal, pela menor latência ou menor tempo de atraso do sinal, em virtude da menor distância a ser percorrida, uma vez que hoje todos os cabos passam pelos Estados Unidos (um intermediário), e isso levaria à diminuição de custos, devido à ampliação da capacidade de transporte de dados (escala). Atualmente, há o Atlantis-2 em funcionamento, mas este possui uma tecnologia da década de 1990, com baixa taxa de transmissão (BRASIL, 2019b).

Por fim, para nossos propósitos, o EllaLink[176], que seria essa alternativa, não se materializou, de fato, apesar dos diversos pronunciamentos a respeito da celeridade pretendida para a consecução dessa ação:

– em 2013, o Ministério das Comunicações anunciou esse empreendimento, que estava na pauta política desde 2012, prevendo a Telebras como empresa gestora, por parte do Brasil;

– em 2014, a Telebras anunciou a formação de uma *joint venture* com a espanhola IslaLink SL; a presidente Dilma Rousseff, durante a Cúpula Anual Brasil-Europa propôs a intenção da construção do cabo submarino e pediu apoio para a efetivação; a mídia nacional divulgou o pré-acordo firmado entre Telebras e IslaLink;

– em 2015, a Telebras[177] emitiu aos seus acionistas e ao mercado em geral a assinatura do acordo com a empresa IslaLink SL e a formação de sociedade, para fins da construção do cabo

[176] IslaLink, EullaLink e EllaLink são o mesmo empreendimento, correspondendo ao cabo submarino Brasil-Europa, ligando Fortaleza e Santos (Brasil) a Sines (Portugal), com acesso para Madrid. Também, pelo projeto, passará pelas Ilhas da Madeira, Canárias e Cabo Verde. A mudança na denominação ocorreu devido à alteração no comando de acionistas da empresa europeia responsável pelo empreendimento, que hoje é a EllaLink Ireland. A tecnologia do cabo é da empresa *Alcatel Submarine Networks*, uma subsidiária da Nokia.

[177] Da mesma forma que o SGDC, a construção desse cabo submarino estava na agenda política em 2012. Ainda neste ano, em 30 de agosto, a Telebras havia anunciado a assinatura de um memorando de entendimento – uma espécie de pré-acordo – com a IslaLink para este fim. O que ocorreu é que o caso de espionagem denunciado por

Brasil-Europa; anunciou o início da implementação do projeto para 2016, com expectativa para funcionamento em 2017; o Comitê Gestor da Internet no Brasil (CGI.br), em reunião ordinária, abordou a importância do cabo para o Brasil e suas expectativas (BRASIL, 2015); a mídia europeia publicou a participação da União Europeia no financiamento do projeto (LE MONDE DIPLOMATIQUE, 2015);

– em 2016, a Telebras, a EllaLink e o governador de Pernambuco se reuniram para tratarem da possibilidade de inclusão da Ilha de Fernando de Noronha-PE como um dos pontos de acesso ao cabo Brasil-Europa, além das Ilhas de Cabo Verde, Madeira e Canárias, já previstos (ECONOMIA DE SERVIÇOS, 2016);

– em 2017, a imprensa brasileira continuou a divulgação do projeto, porém anunciando alteração no prazo inicial para operação (de 2017 para 2019) (G1, 2017); Reinaldo Camargo, da Telebras, em apresentação ao TCU, ratificou a importância do projeto para o País, associando-o aos esforços do *backbone* nacional, das redes metropolitanas e do SGDC, projetos conduzidos pela Telebras (TELEBRAS, 2017); no *site* da Telebras continuou constando como um de seus negócios prioritários a construção do cabo submarino Brasil-Europa, juntamente com o SGDC na consecução do PNBL (TELEBRAS, 2017);

– em 2018, a Comunidade Europeia, por meio da rede *Building Europe Link Latin American* (Bella), um consórcio de pesquisadores científicos incentivado pela Comissão Europeia, vinculado ao programa "Copérnico", da Agência Espacial Europeia (ESA)[178], anunciou apoio financeiro para a implementação do projeto (BELLA, 2018; MUNDO LUSÍADA, 2018) (Figura 4.18); a Telebras anunciou junto aos seus acionistas e ao Ibovespa o desfazimento do contrato com a EllaLink (TELEBRAS, 2019) e acordou com aquela empresa a compra de parte da capacidade do projeto (direito irrevogável de uso). Isso ocorreu por falta de recursos da parte brasileira. Contudo, registrou a Telebras no mesmo documento, intitulado "Fato Relevante", datado de 2 de janeiro de 2019: "A Telebras reafirma sua missão, garantindo comunicações seguras e estratégicas, oferecendo uma alternativa em internet para o governo brasileiro." (TELEBRAS, 2019).

Edward Snowden em 2013 trouxe a público essa intenção e fez com que se abrisse uma janela de oportunidade para implementação dessa política pública.

[178] Copérnico é um sistema europeu de observação e monitoramento espacial da Terra. Pelo consórcio Bella será disponibilizado ao *Gigabit European Academic Network* (GÉANT) e à RedClara (Rede de Ensino e Pesquisa da América Latina) a utilização dessa infovia por, pelo menos, 25 anos, para fins de troca de informações de investigações científicas em áreas como astronomia, física de partículas e observação da terra (BELLA, 2018).

Figura 4.18: cabo submarino EllaLink Brasil-Europa

Fonte: *Building the Europe Link to American Latin* (Bella).

Em consequência, apesar de a Telebras afirmar em sentido oposto, a proposta de um cabo submarino que trouxesse maior segurança e confiabilidade parece não ter escapado a uma mudança de opção de governo, não atendendo aos objetivos de Estado, o que nos leva, novamente, a concluir acerca de sazonalidades no planejamento e nos investimentos orçamentários.

Não que esse projeto, *per se*, seria o suficiente para proporcionar isso, pelo contrário. Em uma das manchetes, ainda da fase inicial do projeto, assim constava o título: "A Doce Inocência do Cabo da Dilma" (MEIOBIT, 2015). Acrescentamos a isso o fato de entre 2014 e 2018 terem sido construídos pelo menos mais três cabos submarinos em direção aos Estados Unidos.

O procedimento de grampear infovias, como mostramos no capítulo 2 e conforme relatos de E. Snowden (HARDING, 2014) foi – e é – ação que faz parte das relações de poder do sistema, independentemente da emissão de juízo de valor acerca da ética e da moral, e até mesmo das normas de direito.

Mais recentemente tivemos o projeto Bude, que depois foi denominado TEMPORA, a partir da parceria entre britânicos do GCHQ e a NSA, capazes de grampear cabos submarinos, naquele caso os que possuíam ponto de acesso na praia de Bude, Inglaterra (HARDING, 2014). Na história há registros, como o da década de 1970's, no Oceano Pacífico, Mar de Okhotsk, quando um submarino estadunidense – o USS Halibut – implantou escuta, desenvolvida pelo

Laboratories Bell/AT&T, a pedido da NSA, em um cabo submarino soviético. Esse episódio ficou conhecido como Operação Ivy Bells (SONTAG; DREW, 1998).

Em termos de Defesa Nacional do Brasil, explicitamente – muito embora utilizados argumentos no sentido de diminuir a dependência dos Estados Unidos ou de evitar que a informação passe por aquele país, para não ser espionada, ou de diminuir o número de intermediários –, a iniciativa do cabo submarino não mencionou importância ou relação direta, específica, nem também com o setor cibernético, exceto o constante na E-Digital (BRASIL, 2017). Todavia, cremos que para fins estratégicos de comunicações, no nível da Defesa Nacional, esse projeto teria muito a contribuir para o País, se não apenas por questões de garantia de segurança ou confiabilidade, pelo menos nas questões de desenvolvimento, como no caso de investimentos para inovações próprias, tanto as ligadas ao funcionamento da infovia e da distribuição e processamento dos dados, como as de implantação ao longo do oceano. Não encontramos nenhum registro nesse sentido no período que pesquisamos.

4.2.4 O Sistema Integrado de Proteção das Estruturas Estratégicas Terrestres – Proteger

O Proteger foi outra iniciativa criada no bojo do Processo de Transformação do Exército, ainda em 2010, pelo Comando e pelo Estado-Maior da Força Terrestre, e visou à proteção das infraestruturas críticas, ou estruturas estratégicas, do País, além de planejar e prover segurança em grandes eventos – como foi o caso da Copa das Confederações (2013), da Copa do Mundo Fifa (2014) e das Olimpíadas (2016) –, apoio à defesa civil, atendimento em casos de calamidade pública e em medidas de contraterrorismo, por exemplo.

Nesses casos, para além da construção de infovias terrestres, subfluviais, submarinas ou espaciais – estas possibilitadas pelo uso de satélites –, a questão passou a ser a garantia da segurança dos componentes cibernéticos envolvidos na prestação de serviços de natureza essencial para a sociedade como um todo, tanto pela abrangência social, como são os casos da saúde, educação, abastecimento de água e luz residencial, quanto aos setores econômicos em geral – agropecuária, indústria, serviços – e, porque não afirmar, para o funcionamento da própria estrutura governamental e democrática do País, como no caso de emprego em operações de garantia do pleito eleitoral.

Sob o foco do Proteger encontraram-se estruturas relacionadas ao fornecimento de energia elétrica, de telecomunicações, de transporte e de abastecimento de água, consideradas estratégicas justamente pelos reflexos que podem causar para a sociedade no caso de interrupção, tanto pelo acaso ou forças da natureza, quanto por ações intencionais de sabotagem

ou terrorismo, por exemplo. Segundo o general José Fernando Iasbech (Exército), então gerente do projeto Proteger, em entrevista ao Sindicato Nacional das Indústrias de Materiais de Defesa (SIMDE): "o Proteger vai ampliar as capacidades do Exército para a proteção da sociedade. Vamos trabalhar não apenas na crise, mas preventivamente para diminuir a vulnerabilidade das instalações estratégicas do país." (SIMDE, 2013). Afirmou ainda esse mesmo militar que "o Brasil é o único do Brics (grupo formado por Brasil, Rússia, Índia, China e África do Sul) que não tem esse sistema integrado de proteção" (DEFESANET, 2012).

Assim, esse sistema é mais uma das iniciativas propostas pelo Exército visando cumprir as diretrizes constantes na END (BRASIL, 2008) e na PND (BRASIL, 2012) e respectivas atualizações (ver Figura 4.19).

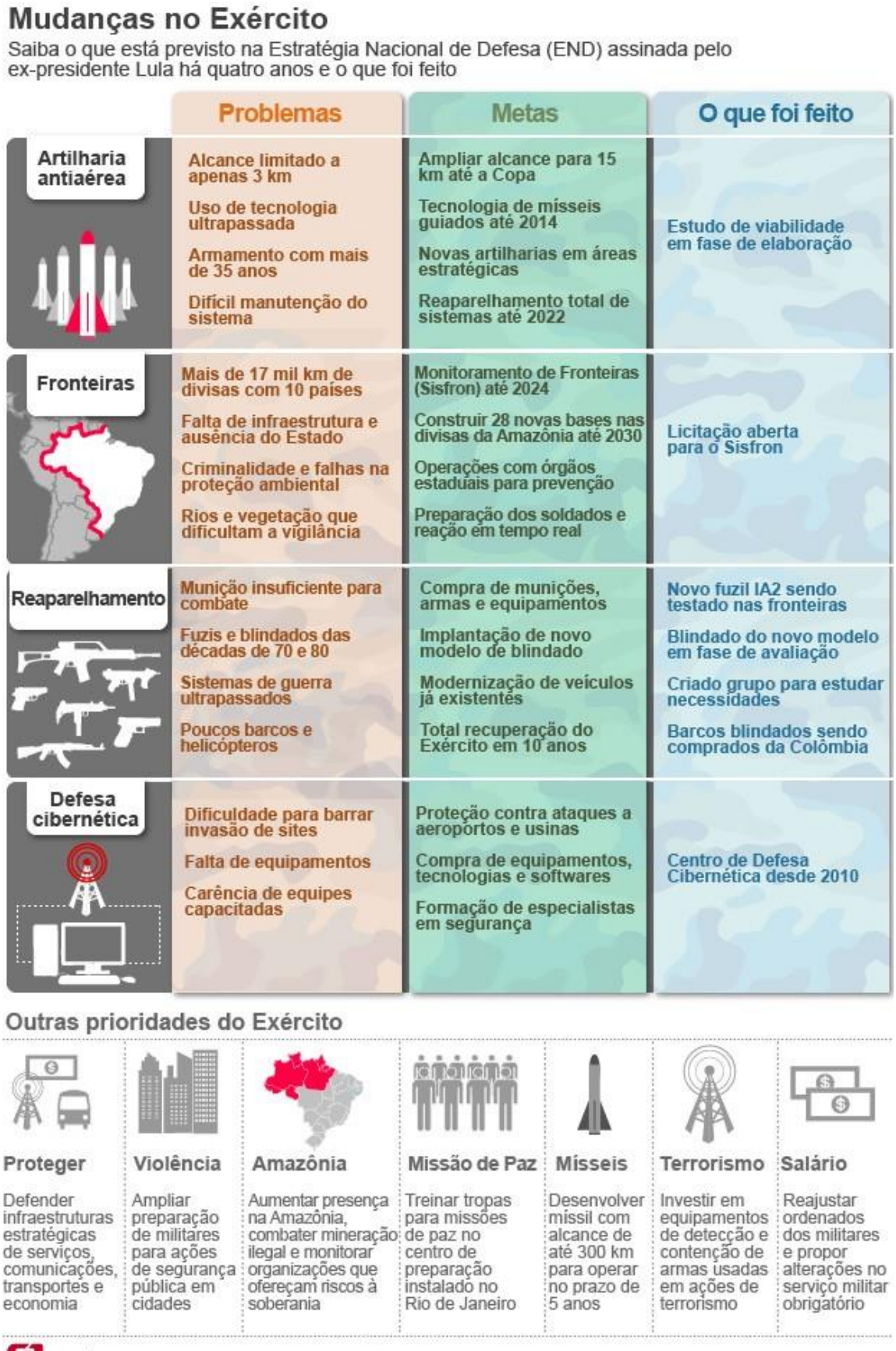
Juntamente com o Proteger, como vimos no capítulo anterior deste trabalho, houve – e há – outros projetos, que depois se transformaram em programas, como foi o caso da defesa cibernética, com duas vertentes, uma voltada para a garantia da segurança cibernética da própria estrutura militar e outra dirigida à sociedade como um todo, que é o Programa Defesa Cibernética na Defesa Nacional. Este último é relacionado diretamente ao Proteger, pois abarcou estruturas fora da de Defesa, estritamente tratando.

No caso da Figura 4.19, o Proteger consta como "Outras prioridades do Exército" (canto inferior esquerdo da figura), mas não devido à importância, e sim porque dependeria de ações coordenadas com outros setores, de dentro e de fora da Administração Pública Federal. Em 2012, para ilustrar, testemunhamos essa preocupação por oficiais do Centro de Comunicações e Guerra Eletrônica do Exército (CComGex) e do Centro de Defesa Cibernética, em Brasília, quando participamos de um estágio de cooperação de instrução com cadetes da Arma de Comunicações da Academia Militar das Agulhas Negras naquelas organizações militares. As questões discutidas eram relacionadas a como planejar, propor e realizar esse tipo de proteção em instalações que envolvem pessoas jurídicas nem sempre públicas? Haveria autorização? Até que ponto não seria vista como uma interferência ou até mesmo intrusão? Quais as possibilidades e os riscos jurídicos para esse empreendimento? Enfim, esses eram alguns dos pontos que mereciam devida atenção.

Em julho de 2013 pareceu que os trabalhos apresentaram continuidade, uma vez que –

> Em conjunto com o Gabinete de Segurança Institucional (GSI), o Exército listou 644 pontos críticos e indispensáveis para a proteção. São instalações de infraestrutura de transportes (227), energia (222), comunicações (80), água (80), nuclear (6) e outras (29), como Itaipu Binacional, subestações e linhas de transmissão de energia, refinarias e as usinas nucleares de Angra dos Reis (RJ). (SIMDE, 2013)

Figura 4.19: Transformação do Exército – áreas e projetos, metas e situação



Fonte: G1 (2012).

Como podemos notar do recorte textual anterior, as questões postas em 2012 começaram a ser resolvidas, e em conjunto com outro órgão, o GSI/PR, permitindo uma abrangência maior das ações, ainda que naquele momento inicialmente sob o caráter de um levantamento. Ao que tudo indicava o modelo adotado seguiria o preconizado para operações interagências.

Também no período 2012/2013, houve a inclusão do Proteger na justificativa da ação orçamentária 14T6, da Lei de Diretrizes Orçamentárias para 2013. A intenção, indicou esse documento, era de que o Proteger capacitasse

> tropas a serem empregadas na proteção das Estruturas Estratégicas Terrestres com prioridade para as situadas no eixo Rio de Janeiro – São Paulo (UHE de Ilha Solteira, Terminal de São Sebastião, Subestação de Bauru e de Ibiúna, Terminal de Cabiúnas, REPLAN, REDUC e Usinas Nucleares de Angra dos Reis), ampliando também capacidades do Exército Brasileiro para atuar na proteção da sociedade nas ações de garantia da lei e da ordem com medidas de apoio à Defesa Civil e ao controle de danos, na garantia de votação e apuração, dentre outras ações subsidiárias, num ambiente de cooperação interagências." (BRASIL, 2012)

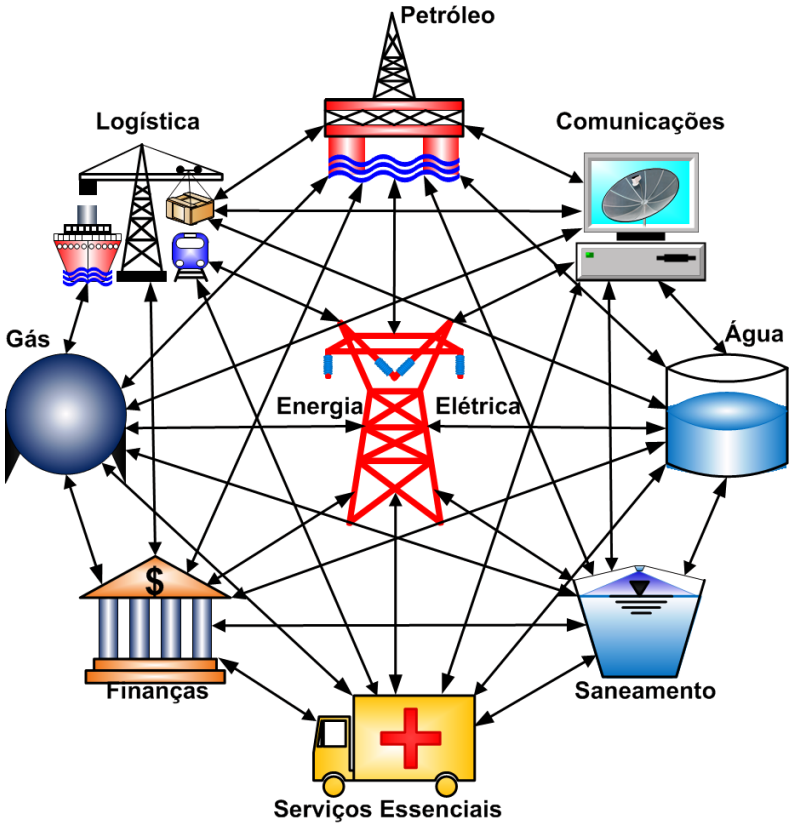
Em 2015, além das participações do Proteger nos eventos internacionais de 2013 e 2014, no Brasil, as questões postas em 2012 continuaram a ser enfrentadas: o Centro de Defesa Cibernética e a Rede Nacional em Segurança da Informação e Criptografia (Renasic), juntamente com a Itaipu Binacional, organizaram o IV Seminário Internacional de Defesa Cibernética, nas instalações de Itaipu, em Foz do Iguaçu-PR. Isso serviu para aproximar mais a defesa cibernética e a principal usina geradora de energia hidrelétrica do País, tanto pela capacidade gerada e distribuída, quanto pela sua área de abrangência, que coincide com o Centro-Sul, região mais industrializada e de maior contingente populacional, logo que demanda – e depende de – maior quantidade de energia.

Não é por acaso a necessidade dessa integração entre a Defesa e uma estrutura econômica. Como registramos no início deste trabalho, energia e informação são elementos interdependentes e que, juntos, podem vim a gerar e manter, em última instância, poder, eis que este é, em sua essência, relacional (RAFFESTIN, 1993). Essa mesma integração de estruturas e Defesa é realidade nos Estados Unidos e faz parte de uma de suas estratégias (CLARKE; KNAKE, 2010).[179] Essa mesma preocupação também é do conhecimento do Exército Brasileiro, uma vez que as ações e a fala dos agentes decisores foram nesse sentido. Sobre isso,

[179] A *Defensive Triad Strategy* enumera explicitamente como prioridades: segurança dos *backbones*, em parceria governo e empresas (AT&T, Verizon, Level 3, Qwest, Sprint); segurança da rede de energia; garantia da própria Defesa (CLARKE; KNAKE, 2010).

o General de Divisão Amin Naves, Comandante da Defesa Cibernética[180], expôs a necessidade de se rever no Brasil a relação entre o público e o privado, no que diz respeito à gestão cibernética das infraestruturas críticas (estruturas estratégicas), citando como exemplo os Estados Unidos, onde essa consta como uma de suas maiores preocupações, sobretudo quanto ao setor elétrico (Figura 4.20).

Figura 4.20: Interação Energia Elétrica com Outras Atividades



Fonte: Parque Tecnológico Itaipu (2018).

[180] Em audiência pública e interativa que fez parte do Plano de Trabalho de Avaliação de Políticas Públicas, conduzida pelo Senador Espiridião Amin, na Comissão de Relações Exteriores do Senado Federal, em 5 set. 2019, a partir do requerimento nº 24/2019. A audiência tratou do Programa de Defesa Cibernética. Embora ocorrida após o recorte temporal da pesquisa, decidimos por inserir essas ideais em nosso relatório, uma vez que trataram de período anterior, desde a implantação do setor cibernético, o que coincidiu exatamente com este trabalho. A própria audiência, em si, retratou o uso de ferramentas cibernéticas como via para atender aos princípios da transparência e da publicidade, exigidos da Administração Pública perante a sociedade. Essa seção está gravada e pode ser acessada por meio do link: https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=16768. Essa audiência foi uma das que ocorreram entre setembro e outubro de 2019 a respeito da Defesa Cibernética no Brasil. Uma dessas audiências, inclusive, foi secreta, com a participação de senadores, de membros das três Forças Armadas, do GSI/PR e do Ministério da Justiça, porque tratou de temas sensíveis quanto a gargalos do País no setor cibernético, incluindo questões ligadas à segurança das infraestruturas críticas.

O que ocorre é que no nosso dia-a-dia não percebemos, muitas das vezes, a ameaça que significa, para nós, empresas, organizações e Estado, a supressão de um desses elementos. Ao que parece, o Exército levou em consideração no seu planejamento as estratégias de outros países, como inferimos da afirmação do general Iasbech a respeito dos Brics e o funcionamento de um sistema de proteção integrada de estruturas estratégicas, e da *Defensive Triad Strategy* estadunidense.

Ainda em 2015, a Itaipu e o Parque Tecnológico Itaipu, em 12 de fevereiro de 2015, criaram o Centro de Estudos Avançados em Proteção de Estruturas Estratégicas (Ceape²), que passou a contar com possibilidades na área de capacitação, conscientização e segurança cibernética, e com um laboratório, o Laboratório de Segurança Eletrônica, de Comunicações e Cibernética (Lasec²), com a finalidade de identificar vulnerabilidades de Sistemas de Informação e em Sistemas de Automação Industrial (ICS/SCADA). [181]

Em termos de laboratório, há ainda em Itaipu o Laboratório de Segurança Cibernética em Ambiente de Tecnologias de Informação e Automação aplicada em Sistemas Elétricos, o LaSC, funcionando como ambiente de simulação e conta com técnicos de Itaipu e de seu Parque Tecnológico, além do Instituto Militar de Engenharia (IME). Esse laboratório visa à prevenção de ataques cibernéticos, por meio de monitoramento do ciberespaço e de seu hardware, podendo identificar sinais anômalos, normais ou implantados.

Na direção, ainda, de mitigar ameaças cibernéticas e de entrelaçar Defesa e estruturas ligadas ao desenvolvimento do País, em 4 de setembro de 2017 foi firmado acordo entre o Exército Brasileiro, a Fundação Parque Tecnológico Itaipu (FPTI) e a Itaipu Binacional. Integrantes dessa parceria expuseram a intenção de irem além, como na fala do diretor-superintendente da Fundação Parque Tecnológico de Itaipu (FPTI), Ramiro Wahrhaftig: "No futuro, poderemos ter uma estrutura de nível internacional [na área de defesa cibernética] e esse é mais um passo que estamos dando neste sentido [...]" (ITAIPU, 2017) e na do superintendente de Engenharia de Itaipu, Jorge Habib Hanna El Khouri: "O que se planeja é somar esforços para estabelecer espaços de pesquisa, de desenvolvimento, de inovação, para que toda a sociedade possa ser beneficiada." (ITAIPU, 2017).

Em meados de 2018 foi a vez do Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro) firmar parceria com o Centro de Defesa Cibernética. A iniciativa focou

[181] Equipamento que funciona com o Sistema de Supervisão e Aquisição de Dados (Scada) que foi alvo, em 2010, na usina nuclear iraniana, de um ataque cibernético, que partiu dos Estados Unidos e de Israel, e ocorreu sorrateiramente, por meio de um *pen drive* infectado por vírus. O dano, no entanto, foi grave. O programa nuclear do Irã pode ter tido um atraso de dez anos.

no desenvolvimento de metodologia nacional e requisitos para certificação de produtos de *hardware* utilizados em sistemas de tecnologia da informação. Consoante o então Presidente do Inmetro, Carlos Augusto Azevedo, apesar da preocupação com defesa cibernética ser própria das Forças Armadas, cabe àquele órgão estabelecer padrões primários de produtos no País, visando à qualidade (BRASIL, 2018). Interessante o final da fala do General de Divisão Amin nesse evento:

> Tão logo esse trabalho termine, estaremos em condições de, por exemplo, certificar laboratórios brasileiros capazes de realmente checar equipamentos de *hardware* em geral para saber se eles fazem exatamente aquilo para que foram criados **e, principalmente, se fazem alguma coisa que não era pra fazer**". (BRASIL, 2018, **grifo nosso**)

Certamente, além de oportunidades econômicas e de desenvolvimento de tecnologias próprias por parte de laboratórios nacionais que queiram se credenciar, o Comandante da Defesa Cibernética se referiu ao caso de espionagem de 2013 e à existência de *backdoors* e outros componentes em *hardwares* de fabricação estrangeira, o que permite acesso externo às máquinas e respectivos sistemas e informações.

Ainda em 2018, como relatamos na abordagem da E-Digital, ocorreu o exercício de simulação denominado "Guardião Cibernético", cujo equipamento utilizado para as tarefas de ataque e defesa cibernética foi desenvolvido no País, o simulador de operações cibernéticas (Simoc), que favoreceu não só os aspectos de confiabilidade de sistemas digitais como o incentivo a empresas e instituições realizarem parceria para inovações tecnológicas genuínas. Esse mesmo evento foi saudado pelo Senador Espiridião Amin, durante audiência pública e interativa naquela Casa do Congresso Nacional, em setembro de 2019. Expôs esse senador o orgulho que tinha do Estado de Santa Catarina por ter participado desse projeto (BRASIL, 2019).

Participaram do Guardião Cibernético, como apontamos anteriormente, além de integrantes da estrutura de Defesa Cibernética, membros do setor financeiro, do nuclear e da administração federal. A previsão era que em 2019 haveria o segundo evento desta natureza, com a intenção de ampliar a quantidade de participantes e setores envolvidos. [182]

[182] Em 2019 de fato veio a ocorrer o Guardião Cibernético II, e contou com cerca de duzentos participantes e 40 instituições, dentre essas as dos setores elétrico, nuclear, telecomunicações e financeiro, além da defesa e da APF.

4.3 O SETOR ESTRATÉGICO DA CIBERNÉTICA ALÉM DA DEFESA: CONTRIBUIÇÕES DE INSTITUIÇÕES DE PESQUISA

Cremos que seja interessante o registro em uma seção dessa pesquisa das contribuições de instituições de pesquisa nacionais com relação ao entrelaçamento Defesa-Desenvolvimento no recorte temporal de nosso estudo. O caso específico que mereceu maior atenção foi o do Instituto de Pesquisa Econômica Aplicada, o Ipea. Não que apenas esse instituto tenha contribuído com o tema. Afirmar isso não teria o menor teor de verdade.

De 2008 a 2018 muitos foram os institutos de pesquisa e de ensino que trataram do tema Defesa e buscaram, em algum momento, entender sua relação com o desenvolvimento econômico, social e tecnológico. Apenas como exemplos, em terras fluminenses: o Instituto de Estudos Estratégicos (Inest), criado a partir de esforços de docentes vinculados ao Programa de Pós-graduação em Estudos Estratégicos (PPGEST), da Universidade Federal Fluminense (UFF). Antes desse, o Programa de Pós-graduação em Ciência Política (PPGCP), também da UFF; o Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia (Coope), da Universidade Federal do Rio de Janeiro (UFRJ), e o Instituto de Economia, também dessa universidade, com os programas de pós-graduação em Políticas Públicas, Estratégia e Desenvolvimento (PPED), e em Economia Política Internacional (Pepi). Em 2010 assistimos à criação da graduação em Defesa e Gestão Estratégica Internacional (DGEI) e, em 2017, do Instituto de Relações Internacionais e Defesa (Irid), ambos da UFRJ.

Em instituições paulistas, encontramos pesquisas na direção de Defesa-Desenvolvimento no programa interinstitucional de Pós-graduação em Relações Internacionais San Tiago Dantas e no Instituto de Relações Internacionais (IRI) da USP; no Planalto Central, a Universidade de Brasília (UnB); no Nordeste, o Programa de Pós-graduação em Ciência Política da Universidade Federal de Pernambuco e o de Ciência Política e Relações Internacionais da Universidade Federal da Paraíba; no Norte, o Programa de Pós-graduação em Estudos de Fronteira, da Universidade Federal do Amapá, e, no Sul, o Programa de Pós-graduação em Relações Internacionais da Universidade Federal de Santa Catarina e o Programa de Pós-graduação em Estudos Estratégicos Internacionais da Universidade Federal do Rio Grande do Sul.

Consideramos com maior detalhamento o Ipea, porque foi um caso de *think thank* não vinculado à instituição de ensino superior, como no caso de universidades e faculdades, uma vez que nesses departamentos, sobretudo os mais voltados a esse tema, é prática comum esse

tipo e tema de pesquisa. Além disso, no percorrer da pesquisa, verificamos o Ipea em inúmeros eventos sobre esse tema e com grande quantidade de publicações a respeito.

Também ao longo da investigação, descobrimos que o papel desempenhado por instituições de pesquisa foi – e é – primordial na consecução de resultados oportunos para um país. Vários livros e artigos relatam essa relação intrínseca entre pesquisa, defesa e desenvolvimento, nos mais diversos matizes. Os de relações internacionais, de estudos estratégicos e de geopolítica são, talvez, os que mais tratam desse assunto. Contudo, os de economia também fazem menção a essa parceria e seus ganhos. Dentre os de economia, os de economia política internacional se destacam. Porém, não só esses.

Resolvemos procurar alusão também a essas parcerias profícuas em fontes das ciências econômicas mais gerais, aquelas indicadas para estudo no início do curso, à título de introdução, e que abordam a divisão da economia dos clássicos à nova economia, passando pela escola marginalista, pelo marxismo, institucionalismo, por exemplo, e nos chamou muita atenção o constante em Pinho e Vasconcellos (2003) ao exporem, literalmente – embora em meia página da obra, passando quase desapercebido –, a associação nos Estados Unidos, no decorrer da II Guerra Mundial, de pesquisadores das áreas da matemática, estatística, economia e administradores para realizarem estudos ligados ao campo militar, como foi o caso do *Office of Strategic Services* (OSS), que chegou a contar com centenas de cientistas, inclusive muitos dos quais conhecemos os trabalhos: Paul Baran, Charles Kindleberger, Walt Rostow, Paul Sweezy, e do *Statistical Research Group*, de Columbia, como Milton Friedman e George Stigler. Foi a partir dessas iniciativas, disseram Pinho e Vasconcellos (2003) que surgiu a famosa RAND *Corporation, Research and Development*. A relação virtuosa entre ciência, tecnologia, capitalismo e poder, nos Estados Unidos e em suas grandes corporações, em um período ainda anterior ao da II GM, também pode ser vista em David Noble (1979).

O registro de parcerias entre pesquisa, Defesa e Desenvolvimento também foram feitos por Medeiros (2004) e Moraes (2004), aquele investigando o desenvolvimento tecnológico dos Estados Unidos no pós-II GM como um empreendimento militar e esta, mais especificamente, porém também dentro da concepção da formação de complexos militar-industrial-acadêmicos, tratando das telecomunicações e de sua influência no poder global que possui os EUA.

Ao que tudo indica, sobretudo após publicação da END (BRASIL, 2008), o Brasil vem demonstrando ações nesse sentido, buscando uma interação maior entre a academia, a indústria e as Forças Armadas do País.

No capítulo anterior, quando vimos o setor estratégico da cibernética e sua repercussão na estrutura de Defesa do Brasil, mencionamos a intenção do Exército, responsável pela

condução da cibernética, de implementar o Sistema de Defesa, Indústria e Academia de Inovação, o SisDIA, que, por sua vez, baseou-se no sistema da hélice tríplice. Todavia, não foi só do setor militar que partiram inciativas nesse sentido.

Do Instituto de Pesquisa Econômica Aplicada (Ipea), destacamos quarenta publicações, de tipos variados, mas que apontaram, no período de 2008 a 2018, uma busca de maior aproximação entre a academia e a defesa, e sua relação com o desenvolvimento. Ainda que nem todos concluam apontando, em definitivo, soluções, o certo é que se debruçaram sobre o tema e o discutiram. Temas como o cenário estratégico regional sul-americano, a inserção do Brasil no cenário internacional e a importância da base industrial de defesa podem ser encontrados. Das quarenta publicações por nós tabuladas no Quadro 4.9, destacamos algumas por abordarem, diretamente, além da defesa, o setor cibernético. Em todas estas foram verificadas as possibilidades advindas do uso da cibernética por parte do Estado e da sociedade. No entanto, um dos trabalhos nos despertou mais interesse e que serviu, inclusive, de uma das questões de nossa tese.

Duarte (2012) verificou a relação entre investimento em tecnologia militar e seu transbordamento econômico. Para esse autor, nem sempre as tecnologias demandadas pelo estamento militar causam efeito positivo no campo econômico.

Concordamos, parcialmente, com Duarte e sugerimos uma nova proposição: talvez a pergunta a ser formulada não devesse ser "se" investimento em tecnologia de defesa causa ganhos econômicos" (na forma de *spin-in* ou de *spill over)*, mas sim de "como". Essa simples mudança, no início de uma política pública, pode trazer resultados bem mais complexos, como a busca de formação de uma cadeia de valor e de um ciclo virtuoso entre defesa e desenvolvimento, tal qual apontada por Brustolin (2014), ao analisar o circuito estadunidense em que funciona esse mecanismo. E essa mesma pergunta, do "como", deveria partir de todos os atores envolvidos, ou seja, de militares, pesquisadores, engenheiros, empresários, burocratas etc.

Além dessas publicações, o Ipea foi responsável pelo levantamento da percepção do povo brasileiro sobre possíveis ameaças, dividindo as respostas regionalmente. Esse estudo, publicado em 2011, serviu de subsídio para políticas públicas de defesa e de segurança. A título de exemplo, para a Região Norte, a percepção de ameaça indicava preocupação quanto ao crime organizado, a desastres naturais e a epidemias maior do que uma possível guerra com potências estrangeiras ou países vizinhos. Contudo, quando a pergunta foi mais específica, enfocando a questão dos recursos naturais e a possibilidade de invasão militar estrangeira para cobiça desses

recursos, a resposta obtida, da Região Norte, foi de mais de 65% acreditando muito ou totalmente nesta hipótese.

Ainda relacionados ao tópico instituições de ensino e pesquisa, a defesa cibernética se tornou curso superior, como constam dos anúncios nos sítios das universidades Estácio de Sá, da UniDomBosco (UniDBSCO), da Uninter, do Centro Universitário Unieuro e da Faculdade de Informática e Administração Paulista (FIAP), além de especializações nessa área, no Centro de Estudos Internacionais sobre Governo, da UFRGS, e na Faculdade Unyleya, esta com sede no Rio de Janeiro, capital, mas com alcance nacional, via EaD. As disciplinas ministradas nesses cursos, em geral, versam sobre segurança cibernética, inteligência artificial, internet das coisas (IoT), perícia forense, *ethical hacking* e criptografia, o que demanda, intrinsecamente, conhecimento aprofundado de matemática, que vem sendo um óbice marcante nos índices publicados acerca dos resultados das avaliações da educação brasileira, como o do Programa Internacional de Avaliação de Alunos (Pisa) e do índice de Desenvolvimento da Educação Básica (Ideb), como mencionamos no capítulo anterior.

Por fim, com sedes em Brasília-DF e Manaus-AM, descobrimos a Softex, uma organização da sociedade civil de interesse público (OSCIP), que desenvolve pesquisas em prol da transformação digital. Em uma das linhas está o Programa de Pesquisa, Desenvolvimento e Inovação em Defesa Cibernética, em parceria com o MCTIC e o MD. No texto do documento referente a esse programa consta a relação entre pesquisa, tecnologia, desenvolvimento e defesa. Dentre os objetivos listados encontramos o de 1) apoio, promoção da inovação e da ampliação da competitividade na indústria brasileira de tecnologia em Defesa Cibernética, e 2) fomento à pesquisa, desenvolvimento e competitividade da indústria brasileira de *software* e serviços de TIC, ou seja, literalmente buscando a relação Defesa-Desenvolvimento. Mais uma vez inferimos, se não em sua plenitude, exemplos que demonstram a concretização do que a END e a PND denominaram cultura de Defesa.

Quadro 4.9: Publicações do IPEA Relativas a Temas de Defesa Nacional (2008-2018), por assunto

Nr	Tipo de publicação	Nr edição	Título	Ano	Assunto específico
1	Periódico	46	Revista Desafios do Desenvolvimento	2008	- reportagem com os Ministros Mangabeira Unger e Jobim sobre a END (2008).
2	Livro	-	Políticas de Incentivo à Inovação Tecnológica no Brasil	2008	- no capítulo 15, cooperação entre Ministério da Defesa e COPPE/UFRJ, no modelo Triplo Hélice.
3	Periódico	47	Revista Desafios do Desenvolvimento	2009	- reportagem sobre esforços políticos acerca da nova END (2008).
4	Texto para Discussão	1715	A Inserção Externa da Indústria Brasileira de Defesa: 1975–2010	2010	- indústria de defesa.
5	Entrevista	69	Diretoria de Estudos e Relações Econômicas e Políticas Internacionais	2011	- entrevista com Marcos Antonio Macedo Cintra acerca da criação da Dinte/IPEA[183].
6	Livro	-	Prospectivas, Estratégias e Cenários Globais	2011	- defesa e desenvolvimento do Brasil e em perspectiva comparada.
7	Texto para Discussão	1670	Militares e Política no Brasil	2011	- relação civil-militar.
8	Boletim	8	Economia e Política Internacional	2011	- impactos de novas tecnologias em políticas de defesa.
9	Periódico	19	Radar: tecnologia, produção e comércio exterior	2012	- dinâmica do setor de Defesa no Brasil.
10	Texto para Discussão	1748	Tecnologia Militar e Desenvolvimento Econômico: uma análise histórica	2012	- tecnologia militar e desenvolvimento.

[183] Um dos eixos temáticos previstos pelo planejamento estratégico do Ipea a ser tratado pela então recém-criada Diretoria de Estudos e Relações Econômicas e Políticas era sobre "política de defesa nacional e segurança internacional, além da reconfiguração da geoeconomia e da geopolítica global." (IPEA, 2011). Disponível em: http://www.ipea.gov.br/desafios/index.php?option=com_content&view=article&id=2653:catid=28&Itemid=23. Acesso em: 19 fev. 2020.

11	Texto para Discussão	1754	Dos "Dividendos da Paz" À Guerra Contra o Terror: Gastos Militares Mundiais Nas Duas Décadas Após o Fim da Guerra Fria -1991-2009	2012	- gastos militares.
12	Texto para Discussão	1758	Base Industrial de Defesa Brasileira	2012	- indústria de defesa.
13	Texto para Discussão	1760	Conduta da Guerra na Era Digital e Suas Implicações Para o Brasil: Uma Análise de Conceitos, Políticas e Práticas de Defesa	2012	- política e estratégia de Defesa.
14	Livro	-	Defesa Nacional para o Século XXI: Política Internacional, Estratégia e Tecnologia Militar	2012	- política e estratégia de defesa e tecnologia militar.
15	Periódico	24	Radar: tecnologia, produção e comércio exterior	2013	- sistemas de inovação, Defesa e TIC
16	Nota Técnica	10	**Base industrial de defesa brasileira: características das firmas e percepção dos empresários do setor**	2013	- indústria de defesa.
17	Texto para Discussão	1850	A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual	2013	- **defesa cibernética** no Brasil e estudo comparado.
18	Texto para Discussão	1877	Processos de Obtenção de Tecnologia Militar	2013	- tecnologia militar.
19	Texto para Discussão	1878	A Dinâmica Recente do Setor de Defesa no Brasil: Análise das Características e do Envolvimento das Firmas Contratadas	2013	- setor de Defesa.
20	Texto para Discussão	1878a	*The Defense Industry in Brazil: Characteristics and Involvement of Supplier Firms*	2013	- setor de Defesa.
21	Periódico	13	Boletim de Economia e Política Internacional	2013	- Defesa nacional e segurança internacional.
22	Nota Técnica	11	Tecnologias e riscos: armas cibernéticas	2013	- tecnologia, **segurança e defesa cibernética**.
23	Livro	-	Estratégias de Defesa Nacional – desafios para o Brasil no novo milênio	2014	- estratégia e defesa nacional.
24	Livro	-	O Brasil e o seu Entorno Estratégico: América do Sul e Atlântico Sul	2014	- defesa e segurança regional.
25	Texto para Discussão	1963	Intermediação Estatal nas Exportações de Equipamentos Militares: As Experiências da Rússia e da França	2014	- comércio internacional de equipamentos militares.

26	*Discussion Paper*	0195	*The Defense Industry in Brazil: Characteristics and Involvement of Supplier Firms*	2015	- setor de Defesa.
27	Periódico	37	Radar: tecnologia, produção e comércio exterior	2015	- sistema de inovação em Defesa.
28	Livro	-	Amazônia e Atlântico Sul: desafios e perspectivas para a defesa no Brasil	2015	- defesa e segurança: temas diversos.
29	Livro	-	Sistemas Setoriais de Inovação e Infraestrutura de Pesquisa no Brasil	2016	- sistema setorial de inovação tecnológica e tecnologia de defesa.
30	Texto para Discussão	2178	Desnacionalização da Indústria de Defesa no Brasil: implicações em aspectos de autonomia científico-tecnológica e soluções a partir da experiência internacional	2016	- indústria de defesa.
31	Texto para Discussão	2182	O Fortalecimento da Indústria de Defesa no Brasil	2016	- indústria de defesa.
32	Periódico	22	Boletim de Economia e Política Internacional	2016	- defesa e segurança.
33	Livro	-	Mapeamento da Base Industrial de Defesa	2016	- indústria de defesa.
34	Livro	-	Brasil 2035: cenários para o desenvolvimento	2017	- desenvolvimento, paz, defesa e segurança internacional.
35	Texto para Discussão	2335	O Futuro da Inserção Internacional do Brasil: questões para o desenvolvimento até 2035	2017	- desenvolvimento, paz, defesa e segurança internacional.
36	Periódico	23	Boletim de Economia e Política Internacional	2017	- exportação a partir da base industrial de defesa do Brasil.
37	Livro	-	Fronteiras do Brasil: uma avaliação de políticas públicas	2018	- defesa, segurança e desenvolvimento.
38	Texto para Discussão	2423	O Centro de Lançamento de Alcântara: abertura para o mercado internacional de satélites e salvaguardas para a soberania nacional	2018	- tecnologia, geopolítica, defesa e segurança.
39	Texto para Discussão	2428	Submarino Nuclear Brasileiro: defesa nacional e externalidades tecnológicas	2018	- tecnologia, defesa, segurança e desenvolvimento.
40	Texto para Discussão	2440	Sistema Integrado de Monitoramento de Fronteiras em Perspectiva	2019 **	- tecnologia, defesa, segurança e desenvolvimento.

** Apesar de ter sido publicado em 2019, inserimos no Quadro acima em virtude do teor da publicação, que corrobora em muito com nossa tese, pela pouca diferença temporal e por ter siso concluído a partir de esforços no período abarcado por nós.

4.4 DIVIDENDOS PARA ALÉM DA GUERRA

Pelo que percorremos durante esta pesquisa, podemos afirmar que houve transbordamento para além do setor de Defesa, quando nos referimos a ações que envolveram o setor cibernético, no período entre 2008 e 2018, conforme constante na END (2008). Se no capítulo anterior esse efeito teve sua origem na estrutura de Defesa stricto sensu do País, neste pudemos verificar que essa empreitada também ocorreu em sentido oposto, isto é, de outros órgãos públicos em direção à Defesa. Isso pode ser encontrado na redação da E-Digital, elaborada em 2017 e publicada em 2018, e em ações dos Ministérios da Ciência, Tecnologia e Inovação, nas parcerias envolvendo o Amazônia Conectada, o SGDC-1 e a parceria para desenvolvimento de rádio por *software* livre entre Ctex, ITA e CPqD.

Essas externalidades tiveram seus reflexos vistos tanto no que diz respeito a questões geopolíticas, que são, por essência, mais relacionadas com Defesa, quanto, também, na seara político-administrativa, econômica e tecnológica do País, com base na análise de normatizações elaboradas e publicadas, de estratégias adotadas, de projetos e programas interministeriais, e pela produção de institutos de pesquisa econômica, no caso mormente do Ipea, *vis-a-vis* a realidade.

Em algumas ocasiões, esses ganhos foram mútuos e interdependentes, como no caso do satélite geoestacionário, pelo qual se originaram externalidades de ordem geopolítica (comunicações estratégicas, por meio da banda de frequência "X"), econômico e social, com o uso da banda "Ka", e científico-tecnológico, com a cooperação internacional feita entre a *joint venture* constituída pela Embraer e Telebras – a Visiona Tecnologia Espacial – e a franco-italiana Thales Alenia Space, e o ganho não só de *expertise* no acompanhamento do projeto e do lançamento, quanto na formação de recursos humanos, incluída aí a transferência de tecnologia.

Outro caso de ganhos em mais de um setor foi o do Proteger, que envolveu aspectos tanto de segurança cibernética propriamente dita, como criou dividendos na área econômica, científica, tecnológica e geopolítica, e demonstrou integração entre Defesa e Desenvolvimento, pois tratou da implementação de proteção integrada em estrutura estratégica do País, na hidrelétrica binacional de Itaipu, responsável por grande parte do fornecimento de energia elétrica do Centro-Sul, o que interfere em indústrias e na população em geral.

Mais que isso, inseridos no Proteger houve a criação de laboratórios de pesquisa e de prevenção contra intrusão cibernética, como a que ocorreu no sistema SCADA utilizado na usina nuclear iraniana, em 2010, fomentado por EUA e Israel. Esse programa também

demonstrou que o Brasil buscou seguir modelos de proteção integrada estrangeiros, como foi a *Defense Triad Strategy* estadunidense e em estratégias de outros integrantes dos Brics, e indicou possibilidades de estender esses benefícios para os países vizinhos, como Paraguai e Argentina.

Por razões didáticas, dividimos os dividendos percebidos da maneira a seguir.

4.4.1 Dividendos geopolíticos

No tocante aos ganhos geopolíticos, o aumento da capacidade de monitoramento, comando e controle territorial foi nítido nas ações propostas e executadas pelos órgãos e empresas envolvidos. Como vimos, o Amazônia Conectada, mais específico para o Estado do Amazonas, e o Satélite Geoestacionário de Defesa, com amplitude de todo o território nacional, incluindo a zona econômica exclusiva e o entorno regional, foram exemplos concretos desses ganhos, apesar dos percalços administrativos, técnicos e orçamentários pelos quais passaram, o que demandou melhorias no processo.

O Amazônia Conectada, geopoliticamente, buscou integrar unidades militares da região amazônica, via cabos subfluviais, pelo uso de internet de banda larga em uma área que tem bastante deficiência estrutural nesse tocante. A intenção foi de construir uma infovia – um ciberespaço – para, a partir deste, obter recursos de poder.

O SGDC, uma infovia baseada no espectro eletromagnético da Terra, também foi desenvolvido para a obtenção de recursos de poder, por meio de uma tecnologia mais avançada e de maior alcance para fins de monitoramento espacial.

Ainda no sentido geopolítico, poderia ser apontada a tentativa de diminuição da dependência de um único país (os Estados Unidos), no que diz respeito às rotas dos cabos submarinos de telecomunicações intercontinentais das quais participa o Brasil. Contudo, como mostramos, essa ação não só deixou de ser implementada, como a Telebras, empresa responsável inicialmente pela condução do projeto, representando o Brasil, afastou-se dos objetivos traçados, deixando a cargo de um consórcio europeu e da empresa EllaLink Ireland o prosseguimento dessas ações. Nesse caso específico, parece-nos que a antiga questão da sazonalidade de governo superou, mais uma vez, as razões de Estado.

Com referência à implantação de cabos submarinos, no intervalo de 2014 a 2018 foram lançados pelo menos mais seis empreendimentos dessa natureza em direção aos Estados Unidos, e nenhum à Europa, o que corroborou a distância entre o discurso e as práticas. Assim, tanto a questão da segurança, como foi inúmeras vezes apontada como fato relevante na consecução do projeto Brasil-Europa, quanto as razões de ordem econômica, com a tentativa

de diminuição de custos de transmissão e de melhoria do sinal, devido à diminuição de latência, parecem ter sido deixadas de lado quando no momento da materialização.

Por fim, quanto aos dividendos mais correspondentes à seara geopolítica, destacamos que em todas essas ações o elemento geográfico foi uma constante, embora em uma leitura, observação e análise superficial pudesse passar despercebido, como algo dado, seja nas normatizações, quando o PNBL e a E-Digital registram as preocupações estatais quanto à existência de um "Tordesilhas Digital", seja nos programas implementados ou não, ao tratarem da construção de infovias para ultrapassarem o espaço. Esses esforços, aliás, são, em sua essência, objetos para superação da própria realidade geográfica. Mais que isso, como afirmou Bertha Becker (2012 [1988]): buscaram ser parte de uma logística para, se não vencer, pelo menos diminuir a questão temporal. A informação, dentro dessa concepção, guiada por ferramentas tecnológicas cada vez mais eficazes, é o elemento possibilitador *lablachiano*, em face de um elemento condicionante ou, em muitas das vezes, tido como determinante.

4.4.2 Dividendos político-administrativos

No tocante a ganhos político-administrativos, para a consecução da normatização e dos projetos, programas e ações, pode ser apontado o entrelaçamento de boa parte da burocracia estatal nesse intento. Identificamos ações do Poder Executivo, por meio do GSI/PR, da SAE/PR, de ministérios (Defesa; Comunicações; Ciência, Tecnologia e Inovação; Educação, por exemplo) e no nível estadual; do Poder Legislativo, com a participação em não poucas ocasiões de comissões especializadas do Senado Federal e da Câmara dos Deputados, uma inclusive à título de inquérito (CPI do Caso Snowden, 2013), no sentido de investigação e monitoramento de políticas públicas que, como mostramos, aproximaram Defesa e Desenvolvimento – aí incluindo a participação do TCU –; por audiências públicas e por publicações, como foram as da revista *Em discussão!*, do Senado.

Uma dessas participações que nos chamou bastante atenção foi relatada pelo Senador Aníbal Diniz, enquanto membro de comissão do Senado Federal que avaliou o PNBL. Dentre os achados da investigação daquela comissão encontramos expressamente a surpresa com que esse parlamentar teve com os reflexos obtidos a partir da implementação do SGDC, que seriam não apenas para o PNBL, mas também para a defesa nacional. Também reiterou esse senador a importância da recriação da Telebras com a função de coordenação e execução das missões do programa de banda larga, na busca de uma garantia legal em vigor desde 1997 – a Lei Geral das Telecomunicações – e reforçada pelo Marco Civil da Internet, que previu a responsabilidade

do Estado em prover acesso universal a esse serviço. Disso, por exemplo, verificamos a expansão de 2011 a 2015 da rede de fibra ótica nacional – o *backbone* nacional – utilizando-se de infraestruturas já parcialmente existentes e sob jurisdição de outras empresas estatais, como as da BR/TAG e da Eletronorte.

Também na esfera de ganhos no campo político-administrativo percebemos uma espécie de fortalecimento da cultura de Defesa, uma vez que com o passar dos anos, entre 2008 e 2018, houve um aumento de participação dos temas relacionados com esse setor em discussões atinentes a outros ministérios. O próprio PAC e o SGDC poderiam ter sido conduzidos pelo MCTIC e o MC, por exemplo. Todavia, ambos tiveram atuação de órgãos militares, que em muitas das vezes não foi de forma secundária, pelo contrário. Nesse sentido, o Ministro das Comunicações à época, Paulo Bernardo, quando em audiência pública no parlamento usou como um de seus argumentos a questão da segurança estratégicas das comunicações. Da mesma forma, funcionários do alto escalão da Telebras e membros do CGI.br usavam essa preocupação como argumento em prol da importância dessas políticas.

4.4.3 Dividendos econômicos

Com relação aos dividendos econômicos, e aqui também incluímos os sociais, embora não atingindo um ideal – considerado aqui como o máximo de execução do projeto ou programa de acordo com o planejado e delineado na fase de elaboração da política pública e o índice de impacto na sociedade –, houve também resultado, no geral, positivo.

O Amazônia Conectada ficou mais restrito ao uso militar, isto é, às comunicações entre organizações militares, uma vez que a infraestrutura complementar que permite o acesso do usuário final não foi implementada (*backhaul* e rede de acesso). Ficaram de fora desse ganho outros parceiros que, muito embora tivessem participado com aportes financeiros, não tiveram o acesso garantido.

Esse gargalo foi apontado pelo TCU, com base em depoimentos de agentes dos órgãos envolvidos, os quais apontaram para problemas como a de governança inoperante, tendo em vista a ausência ou má distribuição de competências e atribuições, a fraca participação de um dos órgãos mais interessados no programa – o MCTI – com a sobrecarga no Exército, que não foi capaz de gerir todas as frentes a que se propôs inicialmente. Esse desequilíbrio de funções e atribuições, conforme mostrou o TCU, servirá de lição para os próximos programas dessa natureza, como é o caso do Pais, que substituiu o Amazônia Conectada, com a ambição de

abranger uma área ainda maior com infraestrutura de cabos subfluviais para oferecer *internet* de banda larga até as redes de acesso dos usuários finais.

Todavia, já no tocante ao SGDC, apesar da morosidade para aprovação do uso da banda "Ka", destinada para fins civis, os dividendos foram muitos: apoio à defesa civil, como no caso de Brumadinho; *internet* nas escolas e em áreas rurais e remotas do País, além do fomento ao desenvolvimento.

Esses empreendimentos buscaram, além da relação Defesa-Desenvolvimento, a "inclusão social, pela inclusão digital", como anunciou o PNBL e, posteriormente, a E-Digital, considerando também a capacidade multiplicadora que possuem os investimentos ligados a este setor e ao fornecimento da banda larga, como apontou o Banco Mundial. A intenção de mitigar as diferenças sociais e regionais, a partir de disponibilidade de acesso à *internet*, foi um dos elementos norteadores dessas políticas que, embora pudessem onerar os cofres públicos em um primeiro momento, transformar-se-iam em acréscimos no PIB, não só em termos absolutos, como também os ligados à produtividade e ao efeito multiplicador, uma vez que o setor de TIC proporciona intrinsecamente ganhos para ele mesmo e para os demais.

Por fim, no tocante aos aspectos econômicos e sociais, destacamos a importância que deve ser dada à previsão feita pelo TCU quanto aos pilares da inclusão digital. A *alfabetização* e da criação e gestão do *conteúdo* que circula nessas infovias fazem a diferença entre usuários comuns, consumidores de produtos exógenos, logo passivos, economicamente tratando, e usuários ativos, com poder de criação e de difusão de inovações próprias, com capacidade de se configurarem em *startups*, por exemplo, como indicou Harvey (2003).

4.4.4 Dividendos tecnológicos: na direção de um complexo militar-industrial-acadêmico?

Sim. Os esforços no período analisado por nós indicam ir na direção de uma tentativa de formação de uma espécie de complexo militar-industrial-acadêmico ou como trouxe a END, complexo militar universitário-empresarial, funcionando sob o sistema da tríplice hélice. A aproximação de instituições militares com universidades e empresas não aconteceu esporadicamente, muito pelo contrário. Nesse período, as tentativas foram constantes no sentido de propiciar interação e sinergia, apesar das dificuldades apontadas.

Essas ações também colaboraram para o aperfeiçoamento estatal no sentido de desenvolvimento de tecnologias próprias do setor cibernético, como o Simulador de Operações de Guerra Cibernética (Simoc) e seu uso no exercício Guardião Cibernético, que envolveu,

além de órgãos estatais, representantes do setor privado, como foi o caso do setor financeiro, preocupados com aspectos de segurança e confiança digital.

Além disso, as parcerias feitas dentre órgãos da estrutura de Defesa e Itaipu e, mais recentemente, o Inmetro, proporcionaram um ambiente para fins de desenvolvimento de medidas e tecnologias ligadas à cibernética e, por conseguinte, à prevenção de incidentes em ferramentas de TIC, sejam em estruturas estratégicas, sejam em componentes indevidos constantes em produtos dessa área, como os *hardwares*, de tecnologia não autóctone, por meio da criação de laboratórios especializados no combate à intrusão ou no aperfeiçoamento da capacidade de resiliência.

CONSIDERAÇÕES FINAIS

Chegamos ao final de nossa pesquisa e relatório de tese, no qual podemos concluir que, no período compreendido entre 2008 e 2018, no Brasil, foi posta em prática uma estratégia nacional formulada para o setor Defesa, mas que atingiu objetivos para além da preparação para a guerra, permitindo, dentre outras externalidades positivas, transbordamento econômico-tecnológico no País.

O problema central que nos conduziu a este intento foi compreender qual e como foi a política de defesa cibernética adotada pelo Brasil, no período 2008-2018, assim como verificar a forma de inserção desta política no panorama internacional e a que procurou responder.

Concomitantemente a esse problema central, buscamos verificar as chances de continuidade desse esforço em um país que, tradicionalmente, não se envolve em conflito interestatal. Além disso, porém intrinsecamente relacionada à anterior, outra inquietação foi responder se haveria, por meio desta política, oportunidade de fornecimento de um bem público puro – Defesa –, ou seja, um bem que consiste em monopólio legal e legítimo do Estado, portanto, economicamente, não excludente e sem rival, com transbordamento econômico-tecnológico positivo, tendo em vista o *core* desta política de defesa – a cibernética – ser baseado em ferramentas de tecnologia da informação e das comunicações, logo uma tecnologia dual.

Inicialmente, a hipótese formulada indicou que pelo atual significado dado ao conceito de cibernética e das políticas que a conduzem, existiriam empreendimentos, estatais e privados, nacionais e internacionais, no sentido de territorialização do "novo" domínio espacial – o ciberespaço – e, também e a partir deste "novo" recurso de poder, uma (re)territorialização dos domínios geográficos tradicionais que porventura estivessem ou viessem sendo submetidos ao processo de globalização.

Somamos a essa hipótese, como uma espécie de arcabouço, de forma secundária, a consideração de que, historicamente: 1) a pressão competitiva pelos espaços geográficos e,

consequentemente, pelo aumento da capacidade de segurança (abrigo) e de oportunidades econômicas (riqueza) seria fenômeno comum, que poderia ser visto tanto aplicado na dimensão terrestre, quanto nas demais dimensões espaciais; 2) os Estados, juntamente com o grande capital privado, seriam atores principais dessa empreitada, buscando conciliar coerção e capital; e, que 3) nem todos os atores seriam capazes de participar desse jogo competitivo, que envolve tanto o "jogo das trocas", quanto o "jogo das guerras".

Dessa forma, no que diz respeito ao Brasil, o setor cibernético contido na END (2008), documento aprovado pelo Decreto Nr 6.703, oriundo do Estado-Maior Interministerial MD/SAE-PR, seria um passo importante na direção da formação de uma espécie de "complexo militar-industrial-acadêmico", que poderia se espraiar para além do espaço nacional, envolvendo, também, países sul-americanos, no sentido de uma base industrial de defesa regional, acompanhando a ideia de uma cooperação regional para uma dissuasão extrarregional capitaneada pelo Brasil. Por fim, inserido ainda dentro do contexto da hipótese, acreditávamos que a própria Estratégia Nacional de Defesa (2008) trouxe essas ideias como inspiração no desejo de fomentar a formação ou consolidação de um Estado-economia nacional (FIORI, 2004; 2008), por meio do binômio Defesa-Desenvolvimento. Essas foram as expectativas iniciais formuladas por nós.

A título de resultados e para fundamentar o que afirmamos no primeiro parágrafo destas considerações finais, no plano teórico e normativo a Estratégia Nacional de Defesa do Brasil, publicada em 2008, foi um marco para o País, no sentido de buscar aglutinar esforços para além da própria Defesa. Os empreendimentos, como pudemos ver no decorrer da pesquisa e desta redação, foram no sentido de buscar a participação da sociedade para reflexão, discussão e planejamento sobre esse tema. Decerto há algumas oportunidades de melhoria, como ultrapassar a fase de questionamento do "*se*" investir em Defesa para a do "*como*" fazê-lo, tendo como objetivo não só este setor, mas sim as possíveis externalidades, sobretudo para um país em desenvolvimento com suas características peculiares, como os quesitos desigualdade de distribuição de renda e baixo indicador de produtividade. Nesse ponto, devemos pensar a Defesa não apenas como um escudo para o Desenvolvimento, como trouxe a END (2008) em sua introdução, e sim para além, enxergando-a como uma verdadeira força-motriz. É dessa forma que conjugamos positivamente o aparente dilema entre investimento em "espadas ou arados" ou entre "canhões e manteiga". Essa ideia e as respectivas ações, projetos e programas devem partir tanto de agentes da própria Defesa, como também dos outros atores envolvidos no sistema, como decisores na esfera pública e na indústria e pesquisadores da academia.

No primeiro capítulo alcançamos a definição de *fronteira-ponto* formulada em nossa dissertação só que agora por outro caminho, o do investimento em capacidades científico-tecnológicas e econômicas inserido em um arcabouço geopolítico não mais tradicional, *hobbesiano* apenas, mas sim de caráter multidimensional e com outros atores, em que para o domínio, o controle e a gestão do território o uso de outros recursos de poder faz-se necessário, além do uso da força estrita. Vista a partir de recursos políticos ou de meios econômicos, a *fronteira-ponto* evidencia não o enfraquecimento do Estado frente ao processo denominado globalização, pelo contrário. Esse novo tipo de fronteira corresponde, embora aparentemente contraditório, à própria universalização do sistema interestatal capitalista. A *fronteira-ponto* é a materialização do acúmulo de poder, via recursos tecnológicos, que também leva à conclusão sobre o aumento do *gap* entre os que possuem ou não esta capacidade. É nesse sentido que ratificamos nossa concordância com Gottman (1975), Becker (2012 [1988]), Medeiros Filho (2010) e Ibañez (2011), por exemplo, no que diz respeito à impossibilidade de negligenciar a geopolítica ou, mais que isso, à necessidade de considerar os elementos geográficos na consecução dos interesses estatais traduzidos em suas políticas. Nesse sentido, qualquer política, ou teoria, que não considera o conceito precípuo da geopolítica, o território, realmente opera no vácuo.

No tocante às teorias, estratégias e realidade no sistema internacional referentes à cibernética e ao ciberespaço, como mostramos no segundo capítulo, a chave de interpretação dos fenômenos sociais e do sistema internacional proposta por Braudel nos permitiu compreender o funcionamento das camadas desse sistema e entender o porquê de teses liberais, ou destas sob uma nova roupagem, parecerem possuir tão boa capacidade explicativa. Isso ocorre tendo em vista essas considerarem como objeto apenas uma das camadas do funcionamento do sistema e seu respectivo circuito – o da economia de mercado. Todavia, aqui cabe o que alertou também Padula (2007), com base em Friederich List, e, em um tempo presente, *braudeliano*, Ha-Joom Chang (2004), no tocante ao teor *nacional* do sistema. Uma estratégia nomeada como *nacional* não responde, ou não deve responder, a questões ligadas à economia de mercado apenas, e sim deve ir além, procurando ver, estudar e responder ao sistema como um todo, considerando suas camadas, sobretudo a que possuir maior poder de influenciar esse todo. As regras nesta camada são bem diferentes das da outra; nesta a competição se utiliza de outros instrumentos, bem além dos utilizados na do mercado; aqui a competição pode funcionar tanto no "jogo das trocas", com garantia de uma demanda agregada, do efeito multiplicador partindo do investimento público e de formação de monopólios, como, e sobretudo, no "das guerras", em que na maioria das vezes regras, sejam gerais, sejam éticas,

morais ou jurídicas, nacionais ou universais, não importam. Além de instrumentos de coerção que se fundamentam no uso da força propriamente, nesta camada há utilização de meios econômicos, científico e tecnológicos, conforme registrado por Blackwill e Harris (2016), a fim de coagir outrem a fazer aquilo que está inserido em objetivos que não os próprios, ainda que não faça parte do escopo inicial dele como previsibilidade de ganho. Isso é possível, acreditamos, por ser a informação, agora na forma digitalizada, elemento que consegue atuar na direção de minimizar tanto as falhas de mercado quanto as incertezas oriundas do "dilema do prisioneiro", diminuindo, pois, a insegurança dos atores envolvidos, pelo menos para os atores que a possuem.

No plano real, empírico, material, verificamos que o País realizou inúmeros esforços no sentido de atender ao previsto na END e nos documentos consequentes referentes ao setor cibernético – Política Nacional de Defesa, Livro Branco de Defesa Nacional e respectivas atualizações no período 2008-2018.

Especificamente no que diz respeito à Defesa, no capítulo três verificamos que uma estrutura foi montada e posta em funcionamento em curto espaço temporal, visando não só cumprir o determinado na Estratégia como responder aos compromissos internacionais assumidos pelo Brasil, sobretudo entre 2013 e 2016, com as Copas das Confederações (2013) e FIFA de Futebol (2014), e as Olimpíadas (2016). Também em 2013, e em resposta ao sistema internacional, especificamente em sua camada mais profunda, uma janela de oportunidade se abriu para a materialização das políticas públicas do setor cibernético e congêneres com a exposição do episódio Snowden e seus reflexos para o sistema. O que tinha sido percebido como importante e estratégico para um país, ainda que compondo um espaço considerado virtual e, portanto, abstrato, tornou-se realidade.

Esse esforço empreendido pela Defesa foi fundamentado também nos conceitos ou imperativos estratégicos constantes da END (2008), como o do monitoramento/controle, da mobilidade e da presença, pelos quais o uso da tecnologia, aqui inseridas tanto a de capacidade de comunicações quanto a de transporte, transformaria o modo de pensar o termo *presença*, entendendo-o não especificamente no sentido físico, de uma onipresença, o que pela geografia do País é algo bem complexo, e sim no uso de recursos capazes de alertarem o efetivo militar em tempo hábil e permitir o deslocamento para o devido recorte espacial objeto de conflito. Isso é resumido pela expressão contida na própria END: "os vigias alertam, as reservas respondem e operam" (BRASIL, 2008, p. 53). Essa mudança e respectivas alterações no planejamento de operações da Força Terrestre também atendeu ao preconizado no Processo de Transformação do Exército, em que, dentre os objetivos preconizados, continha a necessidade

de prover habilidades e competências aos combatentes para saberem operar com atuais recursos tecnológicos dentro de uma doutrina que aceita a flexibilidade como ação.

Inferimos dessa parte do trabalho exatamente a preocupação demonstrada por Bertha Becker a respeito da importância dada à variável *tempo*. Para essa autora, além da escala espacial, ligada à geopolítica, a escala do tempo seria um fator primordial, proporcionado, de acordo com as capacidades, por uma estrutura logística, o que se consubstanciaria uma cronopolítica, por permitir atingir oportuna e pontualmente – além da consciência situacional do planejador, do estrategista ou do decisor – em termos de espaço-tempo, o seu objetivo. Foi realmente nesse sentido, de uma maneira geral, que a Força Terrestre pautou seus planejamentos e ações.

Da estrutura da Defesa partiram ações também na direção de outros órgãos da Administração Pública Federal, do setor econômico e universitário. Dois programas surgiram para contemplar essas ações: o Estratégico da Defesa Cibernética, voltado para âmbito Exército, e o da Defesa Cibernética na Defesa Nacional, refletindo o espraiamento desta política.

Quanto ao primeiro, muito mais ligado à estrutura de Defesa, os projetos nesse inseridos contemplaram, além da implementação de um centro de defesa especializado em cibernética, áreas como segurança e apoio tecnológico, referentes à dotação de infraestrutura necessária para realizar a proteção cibernética dos ativos de informação da própria instituição e para o desenvolvimento de sistemas; inteligência e pesquisa cibernética, e gestão de talentos.

Com relação ao Programa Defesa Cibernética na Defesa Nacional tivemos a criação do Comando de Defesa Cibernética, abrangendo não apenas o Exército, mas também as outras Forças e órgãos da APF, e da Escola Nacional de Defesa Cibernética, que visa promover ensino de natureza dual, civil e militar, no tocante à segurança cibernética e de suas estruturas, formação de recursos humanos e pesquisadores na área.

Para permitir maior relacionamento entre o Exército, as outras Forças Armadas e instituições civis, houve a criação do Escritório de Projetos do Exército, incumbido, além da parte gerencial e técnico-administrativa dos projetos, das relações institucionais, da gestão de metodologia e da busca de parcerias público-privadas.

Além disso, e na busca de fomentar literalmente o previsto na END acerca da relação entre Defesa-Desenvolvimento, ocorreu a formulação do Sistema Defesa, Indústria e Academia de Inovação, o Sisdia de Inovação, inspirado no sistema da hélice tríplice, que, nas palavras do então comandante da Força, general Eduardo Villas Bôas, teria como objetivo potencializar esforços das áreas governamental, produtiva e acadêmica, por meio da inovação tecnológica,

para contribuir com o desenvolvimento nacional, tanto na busca das capacitações de produtos e de sistemas de Defesa como nos de uso dual (VILLAS BÔAS, 2016).

Como resultado dessa forma de pensar e de agir, registramos ao longo da pesquisa a parceria feita entre Exército e Itaipu Binacional, a criação do observatório de defesa cibernética, do Comitê da Cadeia Produtiva da Indústria de Defesa (Comdefesa), que se traduziu em esforços no sentido de integração da Defesa com as federações das indústrias de Santa Catarina, do Rio Grande do Sul e de São Paulo, além da Universidade Federal de Santa Catarina e da Agência de Gestão e Inovação Tecnológica (Agitec). Ainda no sentido de materialidade de ações, aconteceu a criação do Polo de Ciência e Tecnologia de Guaratiba, com o fito, dentre outros, de promover estreita sinergia entre vários atores, dentre os quais órgãos do próprio Exército, do governo, a academia, as empresas e os institutos de pesquisa, e as demais Forças e agências de fomento de C,T&I.

Como dividendos oriundos diretamente da estrutura da Defesa tivemos ainda o levantamento da Base Industrial de Defesa, que contou com apoio do Ipea, e que permitiu o cadastramento de empresas e produtos de defesa passíveis de benefícios fiscais instituídos pela Lei do Prode (Produtos de Defesa), como ficou conhecida a Lei nº 12.598, de 2012, a partir de Medida Provisória nº 544, de 2011, outro ganho para o setor. Apenas no que diz respeito à cibernética, apresentamos lista de aproximadamente vinte empresas e respectivos produtos englobadas por este esforço. Bens relacionados com a segurança cibernética, desenvolvimento de sistemas e com as comunicações estratégicas podem ser encontrados nessa lista, com participação de órgãos da Defesa, da academia e, sobretudo, de empresas nacionais, obedecendo ao previsto na END e acompanhando o delineado pelo Sisdia de Inovação.

Ainda no capítulo 3 identificamos alguns óbices para implementação ideal das ações do setor cibernético. Em suma, um aspecto é relacionado ao que apontamos no capítulo anterior, no plano teórico, no que tange à dependência de tecnologia autóctone, de natureza disruptiva e sistêmica, gerada na camada do verdadeiro capitalismo, capaz de criar padronização de seu uso em âmbito global, como apreendemos dos escritos de Schumpeter (1997 [1911]) e o relacionamos com os de Vernon (1966). Na área cibernética, inclusive no setor Defesa, reconhecido por autoridades militares do mais alto escalão em sede de CPI no Senado, como foi a fala do general José Carlos dos Santos, então Comandante do Centro de Defesa Cibernética do Exército, há elevada dependência de produtos estrangeiros, o que, por um lado, diminui a confiabilidade no ambiente digital, como é o caso da existência de *backdoors*, e, por outro, aumenta os gastos com aquisições de produtos deste setor, interferindo direta e negativamente na balança comercial do País. Mesmo com tentativas em sentido contrário, como a de utilização

de *software* livre, como o *Ubuntu*/*Linux*, promovida pelo governo federal, não houve êxito por completo. É por isso que aqui concluímos, mais uma vez, pelo poder advindo da tecnologia, funcionando como uma espécie de coerção, forçando os usuários dos sistemas, dos mais diversos níveis de atuação, a utilizarem produtos padronizados, como são as plataformas *Windows*/*Microsoft*.

Outro aspecto verificado como entrave à consecução plena das políticas voltadas para o setor cibernético se relaciona com as características da burocracia estatal. Dos argumentos apontados por Agune e Carlos (2017), destacamos principalmente a questão envolvendo a setorialização e a defasagem do arcabouço legal. Este, por exemplo, demonstrado pelas dificuldades trazidas pelo processo licitatório estipulado pela Lei nº 8.666, de 1993, ainda que por meio do pregão eletrônico, como constatou o TCU em processos que tinham por objeto a aquisição de meios cibernéticos. As exigências constantes na lei, que são em essência boas para o Estado como um todo, no sentido de inibir delitos administrativos e de corrupção, dificultaram a aquisição de bens e serviços específicos para este setor estratégico. Entretanto, no limite final do recorte temporal desta pesquisa – exatamente no dia 26 de dezembro de 2018 – foi aprovada a Política Nacional de Segurança da Informação, prevendo a possibilidade de compras mais céleres no tocante a itens que possam comprometer a segurança nacional, como os da área de segurança da informação e defesa cibernética, da inteligência e das comunicações.

Em termos de setorialização, as Forças planejam e atuam, na maior parte das vezes, de forma autônoma, no tocante aos seus projetos estratégicos, ainda que tenham afinidade entre si. A criação de uma secretaria, a Seprod, no âmbito MD, foi em atenção a END (2008), que estabeleceu a criação de um órgão que tivesse como objetivo o aprimoramento de processos ligados à pesquisa e 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. Todavia, há muita dificuldade de ingerência ou mesmo coordenação da Seprod, conforme inferimos, dentre outros, do documento-resposta de uma consulta que fizemos àquele órgão, via *e-Gov*, o que configura uma baixa articulação entre esses atores (Anexo A).

Além disso, como oportunidades de melhoria do setor cibernético, internas ou externas a este, foram constatadas: a) a sazonalidade de recursos foi apontada, tanto em declarações de militares e civis que atuam diretamente, quanto pelo TCU e pela Seprod, no mesmo documento-resposta mencionado anteriormente; b) a dificuldade em termos de recursos humanos para a área cibernética, pois esta exige, em sua grande parte, conhecimentos ligados às ciências exatas e afins, aí inseridas a matemática e a física, e suas derivadas, como a engenharia, a análise de

sistemas, a criptografia, por exemplo; c) a barreira existente entre Forças Armadas e Universidade no Brasil, sobretudo a pública, o que afeta diretamente a interação entre duas das hélices do sistema de inovação e desenvolvimento, o que torna, por conseguinte, ainda mais complexo esse empreendimento. Aqui, portanto, como apontamos no capítulo 3, lembramos que um dos objetivos na alteração dos nomes dos principais documentos acerca da Defesa no País ocorreu para fins de conciliar esforços da sociedade, como um todo, para um interesse comum, na direção do desenvolvimento nacional de forma independente.

No quarto e último capítulo, apresentamos os resultados condizentes com os esforços ligados ao setor estratégico da cibernética oriundos de outras esferas governamentais que não a da Defesa. Vimos que no decurso temporal desta pesquisa a aproximação entre outros ministérios e o da Defesa veio ocorrendo gradativamente e de forma não linear.

O Programa Nacional de Banda Larga, Plano "Brasil Conectado" (2010), inicialmente não atribuiu tanta ênfase a questões de Defesa em seus planejamentos e ações de implementação do acesso à banda larga no País no contexto de uma "inclusão social via inclusão digital", assim vertendo na direção dos campos econômico e social, como política distributiva e de "desconcentração de oportunidades", buscando mitigar, também, o desenvolvimento assimétrico das regiões do País. O mais próximo que o "Brasil Conectado" trouxe de relação com a Defesa, mesmo assim de maneira indireta, foi a referência que fez um de seus objetivos quanto à necessidade de busca de autonomia tecnológica. Contudo, isso foi apenas em um primeiro momento.

Em 2010, como uma das consequências do PNBL, tivemos a reativação da Telebras S. A., a qual recebeu a missão de materializar o constante na Lei nº 9.472/1997, a Lei Geral de Telecomunicações, que prevê o papel do Estado em fornecer acesso a esse recurso, e que foi reforçada e adaptada para os novos meios de comunicações pelo Marco Civil da Internet, Lei nº 12.965, de 2014. O que em 2011 perfazia em torno de 11.000 Km de rede de fibra ótica nacional, em 2018 alcançou 25.000 Km, fruto, além de ações capitaneadas pela Telebras S. A., do aproveitamento de redes pré-existentes utilizadas por concessionárias do setor elétrico e energético, como Furnas, Eletronorte, Eletrosul e Petrobras/TAG, e pela publicação do Decreto 8.135, em 2013, que exigiu que toda a comunicação de órgãos da APF, direta ou indireta, fossem transmitidas por redes de TIC da própria APF.

Em 2014, pudemos constatar, por meio da leitura de relatórios de órgãos do congresso nacional e de ministérios brasileiros, e pela realidade, a inflexão dada ao programa, aproximando-o do setor Defesa. Além do relatório da CPI relativa ao caso Snowden, acessamos as conclusões da Comissão de Ciência, Tecnologia, Inovação, Comunicações e Informática do

Senado Federal, acerca do PNBL, política pública selecionada como objeto de avaliação naquele ano. Por esse documento, inferimos a maior preocupação dada à Defesa por essa política, ao mencionar explicitamente a importância do Satélite Geoestacionário de Defesa e Comunicações Estratégicas e do Programa Amazônia Conectada para o êxito do "Brasil Conectado", em termos de desenvolvimento econômico-social e de capacidade de exercício de soberania.

Em 2017, houve a ratificação, em termos de normatização, do que vínhamos percebendo na esfera empírica: a discussão feita por um grupo de trabalho interministerial, que resultou na Portaria nº 842, do MCTIC, como planejamento para a elaboração de uma estratégia digital para o País. Nesse documento, expressamente constava tanto a importância que deveria ser atribuída ao papel central da pesquisa e desenvolvimento em tecnologias da informação e comunicação para a garantia da competitividade, como também para a soberania nacional. E, diferentemente da formulação do PNBL, para a E-Digital participaram membros do Ministério da Defesa e do das Relações Exteriores.

Em 2018 ocorreu, então, a publicação da E-Digital, confirmando a ideia de que existiam iniciativas de outros ministérios em parceria com o da Defesa para fins de ganhos não só econômicos, tecnológicos e sociais, como já trazia o PNBL, mas também em termos de Defesa, de soberania. E tudo isso, novamente expresso na norma que instituiu a estratégia, via desenvolvimento de tecnologias da informação e comunicação, logo de ferramentas cibernéticas. Em inúmeras passagens dessa estratégia há referência a preocupação com a segurança no ambiente digital, correlacionando este com as áreas de segurança e defesa cibernética, no que percebemos que até em termos de linguagem e de conceitos houve uma sintonia entre os órgãos.

A E-Digital, além de considerar a realidade nacional, fez questão de abordar a dimensão internacional de seu empreendimento e citou, em mais de uma ocasião, como exemplos positivos, o lançamento do SGDC, o Amazônia Conectada e a necessidade de manutenção de esforços no sentido de implementação de cabos submarinos que permitam ao Brasil alternativas de rotas, sobretudo para a Europa. Como sabemos, quanto a este último projeto, além de razões econômicas e técnicas, estas no tocante à melhoria da qualidade e velocidade do sinal, uma motivação – talvez a maior – foi o caso de espionagem dos Estados Unidos, em 2013.

A Estratégia de Transformação Digital considerou aspectos ligados à governança da *internet* e reforçou o descrito e explicado por nós no capítulo dois desta tese, no tocante à questão: "quem controla a *internet*?". Além de diagnosticar o cenário, tal qual o fizemos, demonstrando certa unipolaridade por parte dos Estados Unidos em termos de controle das

estruturas físicas do ciberespaço e de fluxos, devido à sua posição relativa de "nó-maior" da grande rede mundial de computadores, ponto central do ambiente reticular da *internet*, a E-Digital propôs iniciativas e incitou as instâncias nacionais que lidam diretamente com essa discussão no sentido de ampliação da governança, uma democratização no acesso e controle deste espaço e recurso de poder. Esses foram os empreendimentos normativos registrados.

Já no que diz respeito à materialização dos projetos, programas e ações, destacamos o Programa Amazônia Conectada, o Satélite Geoestacionário de Defesa e Comunicações Estratégicas e o Sistema Integrado de Proteção de Estruturas Estratégicas Terrestres, o Proteger.

Quanto ao Amazônia Conectada, ou PAC, este conjugou iniciativas do Ministério da Defesa, do Exército Brasileiro, do Ministério da Ciência, Tecnologia e Inovação, do das Comunicações e da Telebras, no âmbito federal e, no estadual, de diversos outros órgãos do Estado do Amazonas, tanto pertencentes ao poder executivo quanto do judiciário daquela unidade federativa. Esse programa tinha por finalidades, de maneira geral: 1) a inclusão digital e o desenvolvimento local, sobretudo na porção centro-ocidental desse estado, localizada na parte menos favorecida em termos de estrutura de rede de fibra ótica – o "Tordesilhas Digital" –, isto é, sem o devido acesso a *backbone*, *backhaul* e redes de acesso local, denominadas também "última milha", que permitem chegar o sinal de *internet* banda larga, de fato, ao usuário final; 2) o suporte ao monitoramento ambiental, à segurança de dados nacionais e o combate às diversas espécies de tráfico existentes naquela região, articulando segurança pública e Defesa.

Além do lançamento da infraestrutura de rede, o PAC previa ações no sentido de alfabetização dos usuários e de gerenciamento próprio do conteúdo, todas essas previstas nas normas públicas federais brasileiras como ações que permitem, de fato, a consecução da inclusão social via inclusão digital. Aqui o risco é ter apenas acesso à rede, sem, contudo, poder desta se aproveitar para fins de inovação e de ganhos econômicos. Sem a alfabetização adequada e a capacidade de gerir conteúdo, o usuário passa a ser mero consumidor, econômico, social, cultural etc., sem ultrapassar a barreira exigida para ser um empreendedor, capaz de se utilizar de ferramentas do ciberespaço para sua autonomia em sentido amplo.

Apesar de ter sida elogiada pelo TCU, em acórdão bastante elucidativo e completo sobre o Amazônia Conectada, esta iniciativa apresentou oportunidades de melhoria que vão desde o aspecto de governança da política pública, uma vez que, segundo o TCU, houve uma distribuição desproporcional de funções, atribuições e competências na condução do PAC, com sobrecarga para o Exército Brasileiro, que não dispõe de capacidade suficiente para, sozinho, planejar, implementar e monitorar o programa. Em contrapartida, o MCTI, o MC e a Telebras, além do aporte de recursos – e mesmo assim em quantidade ínfima para a magnitude da

empreitada – praticamente não se envolveram na execução. Ademais, ocorreu, fruto também da falta de especificações no processo de governança, desentendimento entre a Defesa e o Ministério da Educação acerca do previsto no contrato de convênio e o que foi entregue. Esse foi um ponto em que políticas desse porte precisam buscar melhorias.

Em números, dos 7,8 mil quilômetros inicialmente previstos, em 2014, o PAC concluiu, em 2018, 850 Km; dos 52 municípios que seriam conectados pela rede, 6 foram beneficiados, constituindo-se, esses, na Rede Vitória Régia, o que perfaz um pouco mais de 10% do objetivo inicial. Todavia, o aporte de recursos também contribuiu para esta baixa efetividade: dos R$ 600 milhões previstos para o programa, cerca de R$ 39 milhões foram, de fato, investidos, isso contando com transferências e convênios feitos de outros órgãos, federais e estaduais, para viabilizar o PAC. Segundo acórdão do TCU, para um programa dessa grandeza e importância, deve haver previsão orçamentária de recursos recorrentes, a fim de se evitar sazonalidades políticas e econômicas.

O Satélite Geoestacionário de Defesa e Comunicações Estratégicas, o SGDC-1, foi outro dos programas que procuraram minimizar, por um lado, a dependência tecnológica brasileira na área das telecomunicações e, por outro, ampliar a capacidade do Estado em monitorar seu território. Essas ações se pautaram, apesar de muitas vezes não ditas explicitamente, em ferramentas cibernéticas e levaram em conta, também, a realidade econômica e social do País, no sentido de prover as áreas mais remotas ou em casos de desastres ambientais com acesso à *internet* banda larga.

Esse programa proporcionou ao Brasil, além da formação de recursos humanos a partir de cooperação com empresa ítalo-francesa com repasse de tecnologia da área, a utilização de uma parte do espectro eletromagnético, da banda "X", para fins militares, e da banda "Ka" para uso civil. Com previsão de entrar em funcionamento em 2014, a banda estratégica militar entrou em operação em 2017, logo após o lançamento do satélite; já a "Ka" demorou um pouco mais, tendo em vista contestações ligadas à concessão dessa banda a empresa estrangeira, o que, em tese, comprometeria a própria função do satélite e, também, não permitiria a especialização da empresa nacional na área. Essa contenda alcançou a esfera do STF e apenas em meados de 2018 foi dada autorização para seu funcionamento, tendo como beneficiária da concessão feita pela Telebras S. A., a empresa Viasat, dos Estados Unidos. Aqui indicamos um bom tema para futuras pesquisas, no sentido de entender o porquê desta inflexão da Telebras e se há risco para a segurança do programa, sobretudo no tocante às comunicações estratégicas, uma vez que o SGDC-1 é calcado em uma conjugação de áreas da informação, proporcionando tanto ações ligadas à guerra cibernética, quanto à eletrônica, alcançando, assim, o conceito da guerra

centrada em redes. Ainda no tocante à Telebras, verificamos que a inflexão entre 2017 e 2018 não foi exclusivamente quanto a esse empreendimento, abarcando, também, iniciativa ligada à implementação de outra infovia baseada em fibra ótica.

Como projeto previsto, mas não executado em sua totalidade temos o da construção do cabo submarino de fibra ótica denominado comumente como cabo Brasil-Europa. A história da construção de cabos submarinos, primeiro os telegráficos, depois os telefônicos e hoje os de fibra ótica, que permitem a compressão e circulação da informação na forma digital, está ligada a projetos de poder, envolvendo a participação do Estado, do grande capital privado e da C,T&I. Foi assim com o primeiro cabo telegráfico internacional, em 1850, ligando França e Inglaterra, na Europa do século XIX; foi assim com o primeiro intercontinental, entre Inglaterra e Estados Unidos da América, em 1858. Em 1956, novamente Estado e grande corporação se aliaram e materializaram outro meio de comunicação, agora via cabo coaxial, que permitiu as chamadas telefônicas, por meio do *Transatlantic* nº 1 (TAT-1). Por trás desse empreendimento, como apontamos no quarto capítulo, estavam a canadense *Canadian Overseas Telecommunications Corporation*, a britânica *General Post Office Engineering Departament* e, pelos EUA, a *American Telephone and Telegraph* (AT&T) e o *Bell Telephone Laboratories*. Esses três últimos atores – Estados Unidos, AT&T e *Bell Laboratories* – voltaram a se encontrar em 1988 na consecução do TAT-8, cabo submarino de fibra ótica, que, contou também com a *France Telecom* e a *British Telecom*.

No Brasil, este projeto e consequência do poder, visto a partir dos cabos de comunicação, seja de qual tipo for, pode ser visto desde a construção do primeiro cabo telegráfico, que ligou a cidade do Rio de Janeiro a de Petrópolis, sede administrativa e residencial da Família Real. Contemporaneamente, o Brasil possui um cabo submarino que permite acesso direto à Europa, desde 2000. Contudo, este é ultrapassado em termos de capacidade e de velocidade de informação, fazendo com que grande parte das infovias direcionem primeiro a mensagem para os Estados Unidos e, depois deste, para a Europa, pois é assim que funciona a grande rede. Novamente foi com o caso Snowden que surgiu a oportunidade para ampliar esta capacidade e buscar aumentar a segurança, embora a construção de um cabo, em si, não seja suficiente para se evitar espionagem. A intenção apresentada pelas autoridades brasileiras, sobretudo ligadas às telecomunicações, era de construção de um novo cabo de fibra ótica. Até a conclusão de nossa pesquisa, esse projeto não apenas não foi concluído como o que se constatou no mundo real foram empreendimentos planejados e implementados que indicam no sentido contrário. Mais três cabos submarinos de grande capacidade foram construídos e postos em funcionamento ligando Brasil aos Estados Unidos.

Aqui, ao que tudo indicou, parece ter sido posto de lado interesses estratégicos em favor dos econômicos.

A experiência que chamou bastante nossa atenção por materializar a aproximação entre Defesa e Desenvolvimento, tanto na teoria quanto na prática, foi a do Sistema Integrado de Proteção das Estruturas Estratégicas Terrestres, o Proteger. O foco desse sistema, que atendeu ao previsto tanto no Programa Defesa Cibernética na Defesa Nacional quanto à E-Digital, é a segurança do funcionamento de infraestruturas críticas do País, ou estruturas estratégicas, como as ligadas à rede de energia elétrica, de transporte, de abastecimento de água, refinarias e usinas nucleares, por exemplo. A inspiração desse sistema foi baseada na *Defensive Triad Strategy* estadunidense (2010), que previa como fundamentais a segurança das informações da própria estrutura da Defesa, da rede de energia e dos *backbones*, estes cuidados pela parceria entre os governos daquele país e empresas, como a AT&T, a Verizon e Level 3. Em 2018, no Brasil, ocorreu um exercício de simulação – o Guardião Cibernético – o qual envolveu, além da Defesa, empresas e instituições de pesquisa. Esse exercício teve ainda como novidade a utilização de um simulador de operações cibernéticas de tecnologia autóctone – o Simoc. As parcerias inseridas no Proteger já contam com a ligação Exército e Itaipu Binacional e Exército e Inmetro, este último cuidando de especificações e certificação de equipamentos da área de TIC e informática, a fim de minimizar riscos quanto a vazamento de informações ou de sabotagem.

Finalizando o registro no tocante ao setor cibernético e seus reflexos para além da Defesa, constatamos uma participação intensa de institutos de pesquisas nacionais, com destaque para o Ipea. Foram mais de quarenta contribuições relativas à pesquisa sobre Defesa e tecnologia e, dessas, pelo menos quatro relacionadas diretamente à cibernética e, por conseguinte, a ferramentas de TIC, buscando articular questões de segurança no ambiente digital com o desenvolvimento. A participação de institutos e de programas de pesquisa nessa área perfaz a outra hélice do Sisdia de Inovação, contemplando Defesa, indústria e academia, na direção do denominado complexo militar-industrial-acadêmico ou, como nominou a END, um complexo militar industrial-acadêmico nacional.

O que sentimos falta de materialidade, apesar da previsão na END e em outras normas, como os planos de ação do Conselho de Defesa Sul-americana, foram iniciativas no que tange à consecução de uma base industrial de defesa regional, sobretudo quando investigamos a área cibernética. Podemos até mencionar o Proteger como um desses esforços, na medida em que este configura parceria entre o Brasil e o Paraguai, a partir da participação da Itaipu Binacional. Também podemos enxergar no SGDC-1 uma oportunidade para o transbordamento regional, tendo em vista a capacidade do satélite em prover imagens de toda a América do Sul, incluindo

seus limites marítimos. No entanto, pelo que previa a END, dentre outros documentos, as ações nesse sentido foram bem modestas.

Como recomendação ou indicação para pesquisas futuras no tocante ao setor cibernético, o estudo específico de uma empresa nacional cadastrada pela BID e pelo MD e sua relação com os órgãos de Defesa e com a academia pode proporcionar uma visão em nível mais específico das relações existentes, dos processos exitosos e dos respectivos entraves para o setor cibernético, da mesma forma que pode funcionar como *expertise* para outros setores estratégicos. O estudo desse mesmo objeto partindo de outro ator, como uma universidade ou instituto de pesquisa, ou da própria Defesa, também apresenta bastante oportunidade para obtenção de lições.

A continuidade de estudo sobre os programas governamentais relacionados, direta ou indiretamente, ao setor cibernético, em período posterior ao recorte temporal desta pesquisa, como ao que tudo indica é o Programa Amazônia Integrada e Sustentável, também pode servir de parâmetro para o aperfeiçoamento de políticas públicas do setor e de ganhos multidimensionais.

No nível macro, do sistema internacional e de inovações disruptivas, causadoras de externalidades positivas em várias áreas e setores, como é a *internet* das coisas (IoT), a investigação sobre a *internet* 5G e suas consequências é outra sugestão de pesquisa que dialoga, e muito, com a matriz teórica e com os achados deste trabalho, e que está, hoje, na agenda *setting* de vários Estados, inclusive do Brasil. Assistimos a uma audiência pública e interativa no Senado, em 2018, sobre o Programa Defesa Cibernética na Defesa Nacional em que um dos temas mais debatidos foi exatamente este e a preocupação das autoridades, civis e militares, públicas e privadas era conhecer a posição brasileira no tocante ao nível de desenvolvimento desta tecnologia.

Ainda como recomendação ou indicação de possíveis trabalhos que envolvam o saber pensar política e economia, vistos de forma mútua e interdependente, e considerando o ambiente internacional, uma dúvida que nos ocorreu no transcurso da pesquisa, principalmente depois de assistir às explanações dos professores Carlos Lessa e Dark Costa, em um dos encontros proporcionados pelo Pepi na sala 102 da UFRJ – Praia Vermelha, e acompanhar, naquele momento, a profundidade de suas reflexões em termos de políticas e estratégias de desenvolvimento nacional, e que, portanto, dizem respeito também à tecnologia, foi a constatação da inexistência de uma indústria automobilística nacional. O País tem um vasto e bem estruturado parque industrial, é verdade, porém em nenhuma de suas partes tem, em sua raiz, o nacional. As mais antigas instaladas no País são de origem estadunidense, inglesa,

francesa, alemã, italiana e, um pouco depois, japonesa. Quanto a este último, foi uma das consequências do crescimento econômico nipônico sob uma política aliada de "desenvolvimento autorizado" ou "à convite" durante a Guerra Fria.

Isso chamou nossa atenção devido à verificação de que países considerados até certo tempo emergentes, como Coreia do Sul e China, utilizaram-se – e ainda buscam se firmar – da indústria automobilística para promoverem ou ampliarem seu crescimento. Talvez, a título de hipótese sugestiva, pela capilaridade que possui esse tipo de indústria, pela escala de seu mercado consumidor, pelo retorno positivo para balança comercial e de pagamentos, pela projeção de poder, vista no sentido bem amplo, incluindo aspectos ligados ao *brand* empresarial e a relação deste com o país, e – talvez aí resida o grande "X" da questão – pela capacidade de proporcionar, devido ao ambiente de elevada concorrência, interna e externa, investimento em C,T&I na fronteira do conhecimento e que possuem alto índice de possibilidade de transbordamento para outros setores, inclusive o da academia e o da Defesa de suas respectivas nacionalidades. Ao que nos parece, tendemos, mais uma vez, a concordar com Dreifuss no sentido de que as corporações estratégicas têm bandeira. Todavia, como afirmamos acima, isso é apenas no nível hipotético, como indicação ou recomendação para futuras pesquisas.

Já que mencionamos o programa que nos permitiu o desenvolvimento desta pesquisa, o Programa de Economia Política Internacional (Pepi) da UFRJ, registramos nossa incompreensão no tocante à desvalorização deste perante à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), uma vez que, como demostramos neste relatório de pesquisa, este programa tem como uma de suas finalidades – se não a principal – pensar a relação entre países *vis-a-vis* a natureza do sistema no qual estão inseridos. Dessa forma, a busca do entendimento acerca da estrutura e do funcionamento deste elemento singular que é o SI, considerando sua geografia, sua história e seus elementos políticos, econômicos e tecnológicos, permite aos formuladores de políticas públicas e decisores das respectivas implementações um olhar crítico e holístico deste objeto, na intenção de construir ferramentas cognitivas que fomentem estratégias e políticas reais e de desenvolvimento, eis que este último, como nos mostrou Celso Furtado, não é linear e nem algo dado. Ao que tudo indica – e nesta parte peço atenção da coordenação do programa e dos membros de seu conselho deliberativo: ou aceitamos os indicadores criados pela Capes, ainda que não concordemos plenamente com esses sob argumentos de os mesmos atribuírem muito valor à quantidade e à forma, porém nem sempre ao conteúdo e à profundidade de reflexão, ou poderemos vir a sofrer consequências mais prejudiciais e, talvez, irreversíveis, o que atingirá não só o programa, seus docentes,

discentes e quadro de funcionários, como, e principalmente, o País. Votamos a favor de decisão que indique ir na direção de sua continuidade.

Enfim, seja na consecução da *fronteira-ponto,* a partir do uso da força bélico-militar, por meio da utilização de armas cibernéticas, ou a partir da capacidade tecnológica, via instrumentos de TIC, que permitem aumentar a capacidade de monitoramento e controle, seja na de saber atuar no circuito das camadas do "jogo das trocas" e no "das guerras", o campo do conhecimento abarcado pela economia política internacional, dentro da ideia de "uma ação, dois (ou mais) movimentos", possui ferramentas cognitivas muito interessantes, elucidativas, no sentido de capacidade de interpretação dos fenômenos do mundo real, a fim de realização de planejamentos, de políticas e de suas respectivas implementações, e tudo isso considerando o teor nacional em um determinado espaço, geográfico, e um tempo, histórico, nos quais os recursos tecnológicos, sobretudo os ligados à informação, permitem, se não extinguir, ao menos mitigar a natureza do imponderável. Afinal de contas, os "jogos não estão feitos"!

REFERÊNCIAS

ACÁCIO, Igor D. P.; SOUZA, Gills L. *Segurança internacional no século XXI*: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço. Anais do 36º Encontro Anual da ANPOCS. 2012.

AGUNE, Roberto; CARLOS, José Antônio. "Radar da Inovação – O que os governos precisam enxergar". *Estudos Avançados*, São Paulo, v. 31, n. 90, p. 143-157, maio, 2017. Disponível em:<http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142017000200143&lng=en&nrm=iso>. Acesso em: 3 fev. 2020.

ALMEIDA, José Eduardo P. "A Tendência Mundial para a Defesa Cibernética". In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011. pp. 79-102.

ÁLVARES, João G. *Os Contratos de Offset como Instrumento da Política Pública no Setor de Defesa*. Dissertação (mestrado). 226f. Centro Universitário de Brasília. Programa de Mestrado em Direito e Políticas Públicas. Brasília, 2016.

AMARANTE, José Carlos A. do. A Batalha Automatizada: Um sonho Exequível? *Cadernos de Estudos Estratégicos*. Centro de Estudos Estratégicos da Escola Superior de Guerra, Rio de Janeiro, n. 9, pp. 3-18, jul. 2010.

AMERICAN SOCIETY FOR CIBERNETICS FOUNDATIONS. *Defining 'Cibernetic'*. 2008. Disponível em: <http://www.asc-cybernetics.org/foundations/definitions.htm>. Acesso em: 20 dez. 2016.

AMORIM, Celso. "Aspectos da Defesa Cibernética". In: SEMINÁRIO DE DEFESA CIBERNÉTICA, 3., 2012, Brasília. *Palavras do Ministro da Defesa*... Brasília: MD, 2012. Disponível em: <https://www.defesa.gov.br/arquivos/2012/Pronunciamentos/Ministro_defesa/discurso_seminario_defesa_cibernetica_out_2012.pdf>. Acesso em: 20 nov. 2012.

ANGELL, Norman. *A Grande Ilusão*. Brasília: Editora Universidade de Brasília, Instituto de Pesquisa de Relações Internacionais; São Paulo: Imprensa Oficial do Estado de São Paulo, 2002 [1910].

BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011.

BAYLIS, John; WIRTZ, James J. "Introduction". In: BAYLIS, John; WIRTZ, James J; GRAY, Colin (Org.). *Strategy in the Contemporary World*: an introduction to strategic studies. 3. ed. New York: Oxford, 2010, pp. 2-15.

BECKER, Bertha. "Geopolítica da Amazônia". In: *Estudos Avançados*, São Paulo, v. 19, n. 53, p. 71-86, abr., 2005. Disponível em:

http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142005000100005&lng=en&nrm=iso>. Acesso em 17 jul. 2016.

_____. *Manual do Candidato*: Geografia. Brasília: Fundação Alexandre de Gusmão, 2009.

_____. "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.

BRAUDEL, Fernand. *A Longa Duração*. Revista de História. Ano XVI. n. 62. abr.-jun., 1965.

_____. *Dinâmica do Capitalismo*. Rio de Janeiro: Rocco, 1987 [1985].

BRASIL. Lei n. 7.232. Dispõe sobre a Política Nacional de Informática, e dá outras providências. 1984.

_____. *Política de Defesa Nacional*. Brasília, 1996.

_____. Lei n. 9.472. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. 1997.

_____. Decreto Presidencial n. 3.505. *Instui a Política de Segurança da Informação*. Brasília, 2000.

_____. Lei n. 10.520. Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências. 2002.

_____. Gabinete de Segurança Institucional da Presidência da República. Lei n. 10.683. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. 2003.

_____. Exército Brasileiro. Departamento de Ciência e Tecnologia. *Plano de Migração para Software Livre no Exército Brasileiro*. 1. ed. 2004. Disponível em: http://www.sgex.eb.mil.br/sistemas/be/boletins.php. Acesso em: 20 ago. 2018.

_____. *Política de Defesa Nacional*. Brasília, 2005.

_____. Decreto 5.450. Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências. 2005.

_____. Exército Brasileiro. Departamento de Ciência e Tecnologia. *Plano de Migração para Software Livre no Exército Brasileiro*. 3. ed. 2007. Disponível em: http://www.softwarelivre.gov.br/casos/Plano_Migracao_Soft_Livre_13FEV07.pdf. Acesso em: 20 ago. 2018.

_____. Ministério da Defesa. *Glossário das Forças Armadas*. 2007.

BRASIL. *Estratégia Nacional de Defesa*. Decreto n.º 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 2008.

_____. Exército Brasileiro. Portaria n. 666, de 4 de agosto de 2010, do Comandante do Exército. *Cria o Centro de Defesa Cibernética do Exército e dá outras providências*. Brasília, 2010.

_____. Exército Brasileiro. Portaria n. 667, de 4 de agosto de 2010, do Comandante do Exército. *Ativa o Núcleo do Centro de Defesa Cibernética do Exército e dá outras providências*. Brasília, 2010.

_____. *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*. v. 01. Brasília: Gabinete de Segurança Institucional da Presidência da República, nov. 2010a. Disponível em: < http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em 8 ago. 2011.

_____. *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.

_____. Decreto n. 7.175. *Institui o Programa Nacional de Banda Larga [...]*. 2010.

_____. Estado-Maior do Exército. *Processo de Transformação do Exército*. 2010.

_____. Decreto n. 7.462, de 19 de abril de 2011. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Ministério das Comunicações, dispõe sobre o remanejamento de cargos em comissão [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Decreto/D7462.htm. Acesso em: 20 mai. 2018.

_____. Senado Federal. *Revista em Discussão!* Brasília, 2011. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/200060. Acesso em: 20 set. 2017.

_____. Presidência da República. Medida Provisória n. 544. *Estabelece normas especiais para as compras, as contratações de produtos, de sistemas de defesa, e de desenvolvimento de produtos e de sistemas de defesa, e dispõe sobre regras de incentivo à área estratégica de defesa e dá outras providências*. Brasília, 2011.

_____. Lei nº 12.598, de 21 de março de 2012. *Estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa; dispõe sobre regras de incentivo à área estratégica de defesa*. Brasília, 2012d.

_____. Mensagem Presidencial n.º 323, de 17 de julho de 2012. Envia ao Congresso Nacional a proposta da *Política Nacional de Defesa* de 2012a. Disponível em: <https://www.defesa.gov.br/arquivos/2012/mes07/pnd.pdf>. Acesso em: 13 abr. 2012.

_____. Mensagem Presidencial n.º 323, de 17 de julho de 2012. Envia ao Congresso Nacional a proposta da Estratégia Nacional de Defesa de 2012b. Brasília, DF: 2012b. Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf. Acesso em: 24 nov. 2012.

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

_____. Decreto n. 7.769. *Dispõe sobre a gestão do planejamento, da construção e do lançamento do Satélite Geoestacionário de Defesa e Comunicações Estratégicas - SGDC*. Brasília, 2012.

_____. Lei n. 12.737. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 2012.

_____. Ministério da Ciência, Tecnologia e Inovação. Programa Nacional de Atividades Espaciais – PNAE: 2012-2021. Agência Espacial Brasileira. Brasília: Ministério da Ciência, Tecnologia e Inovação, Agência Espacial Brasileira, 2012.

_____. Programa Estratégico de Sistemas Espaciais. 2012. Disponível em: https://www2.fab.mil.br/ccise/index.php/o-que-e-o-pese. Acesso em: 20 set. 2019.

_____. Ministério da Defesa. *Política Cibernética de Defesa*. Brasília, 2012.

_____. Exército Brasileiro. Portaria n. 1.253, do Comandante do Exército. *Aprova a Concepção de Transformação do Exército e dá outras providências*. 2013.

_____. Lei de Diretrizes Orçamentárias para 2013. Anexo III: relação das informações complementares ao projeto de lei orçamentária de 2013. Brasília, 2012. Disponível em: https://www.camara.leg.br/internet/comissao/index/mista/orca/orcamento/OR2013/Info_complem/vol1/02_IncisoII.pdf. Acesso em: 20 jul. 2019.

_____. Exército Brasileiro. Portaria do Comandante do Exército n. 1.253. *Aprova a concepção de transformação do Exército e dá outras providências*. 2013.

_____. Casa Civil. Decreto n. 8.135, de 4 de novembro de 2013. Dispõe sobre as Comunicações de Dados da Administração Pública Federal Direta, Autárquica e Fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm. Acesso em: 20 mai. 2019.

_____. Senado Federal. *Revista em Discussão!* Brasília, 2014. Disponível em: http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/index.html#INDICE. Acesso em: 20 set. 2017.

_____. Lei n. 12.965. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Brasília: Câmara dos Deputados, 2014.

_____. 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.

_____. Memorando de Entendimento n. 14-188-00, de 28 de novembro de 2014, sobre a Execução do Programa Amazônia Conectada. Disponível em: http://www.amazoniaconectada.eb.mil.br/pt/downloads/Memorando_de_Entendimento_Amazonia_Conectado.pdf. Acesso em: 30 out. 2017.

_____. Tribunal de Contas da União. *Acórdão n. 1.406*. 2014. Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/1406%25202014/ANOACORDAO%253A%25222014%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/6/%2520?uuid=adf51910-bec4-11ea-a974-27f41eec421b. Acesso em: 20 nov. 2019.

_____. Senado Federal. Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática. *Relatório de Avaliação do Programa Nacional de Banda Larga (PNBL)*. Brasília, 2014.

_____. Ministério da Defesa. *Doutrina Militar de Defesa Cibernética*. 2014. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 18 fev. 2018.

_____. Tribunal de Contas da União. *Políticas Públicas de Inclusão Digital*. Brasília: TCU, 2015. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15005860201501F69C07E6B0A&inline=1. Acesso em: 20 nov. 2019.

_____. Portaria Interministerial n. 586, de 22 de julho de 2015. Institui o Projeto Amazônia Conectada e dá outras providências. Disponível em: http://www.amazoniaconectada.eb.mil.br/pt/downloads/DOU_2015_07_Secao_1_pdf_20150723_25_Portaria_Interministerial_Amazonia_Conectada.pdf. Acesso em: 30 out. 2017.

_____. Ministério da Defesa. *Glossário da Forças Armadas*. 2015.

_____. Exército Brasileiro. *Projeto Amazônia Conectada*. 2015. Disponível em: http://www.amazoniaconectada.eb.mil.br/pt/. Acesso em: 20 jun. 2017.

_____. Tribunal de Contas da União. *Relatório de Levantamento de Auditoria do Programa Aeroespacial Brasileiro*. 2016. Disponível em: https://portal.tcu.gov.br/data/files/5F/81/63/41/6F109510EE89EF851A2818A8/016.582-2016-0%20-%20Programa%20Espacial%20Brasileiro.pdf. Acesso em: 30 set. 2019.

_____. Ministério da Ciência, Tecnologia e Inovação. *Estratégia Nacional de Ciência, Tecnologia e Inovação - 2016-2019*. Brasília, 2016.

_____. Lei n. 13.249, de 13 de janeiro de 2016. *Institui o Plano Plurianual da União para o período 2016 a 2019*. Brasília, 2016.

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

_____. Ministério da Ciência, Tecnologia e Inovação. Portaria n. 842, de 17 de fevereiro de 2017. *Institui Grupo de Trabalho para elaborar proposta de estratégia brasileira de economia digital*, a ser posteriormente submetida à consulta pública e enviada na forma de minuta de Decreto Presidencial à Presidência da República. Brasília, 2017.

_____. 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.

_____. Ministério da Defesa. Portaria Normativa n. 86, de 13 de dezembro de 2018. *Estabelece procedimentos administrativos para o credenciamento, descredenciamento e avaliação de Empresas de Defesa - ED, Empresas Estratégicas de Defesa - EED e para a classificação e desclassificação de Produtos de Defesa - PRODE, e Produtos Estratégicos de Defesa – PED.* 2018.

_____. Exército Brasileiro. *Escritório de Projetos do Exército Brasileiro*. 2019. Disponível em: http://www.epex.eb.mil.br/index.php/component/content/article?id=462#:~:text=Por%20fim%2C%20cabe%20ressaltar%20que,paz%20social%20e%20a%20seguran%C3%A7a.. Acesso em: 20 set. 2019.

_____. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Estratégia Brasileira para Transformação Digital*. Brasília, 2018.

_____. Tribunal de Contas da União. Acórdão n. 2053, de 29 de agosto de 2018. Relatório de Levantamento de Avaliação do Programa Nacional de Banda Larga. Brasília, 2018. Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/2053/ANOACORDAO%253A%25222018%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/4/%2520?uuid=adf51910-bec4-11ea-a974-27f41eec421b. Acesso em: 30 nov. 2019.

_____. Presidência da República. Decreto n. 9.637, de 26 de dezembro de 2018. *Institui a Política Nacional de Segurança da Informação [...]*. Brasília, 2018.

_____. Tribunal de Contas da União. Acórdão n. 2641, de 30 de outubro de 2019. *Relatório de Auditoria Operacional do Programa Amazônia Conectada*. Brasília, 2019. Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/2641/COPIARELATOR%253A%2522BRUNO%2520DANTAS%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/1/%2520?uuid=adf51910-bec4-11ea-a974-27f41eec421b. Acesso em: 30 nov. 2019.

_____. Anatel. *Mapeamento de Redes*. 2019. Disponível em: https://www.anatel.gov.br/dados/mapeamento-de-redes. Acesso em: 13 jun. 2018.

_____. Exército Brasileiro. Portaria n. 893, do Comandante do Exército. *Recria o Sistema Defesa, Indústria e Academia de Inovação (SisDIA de Inovação)*. 2019.

_____. Decreto n. 10.222, de 5 de fevereiro de 2020. *Aprova a Estratégia Nacional de Segurança Cibernética*. Brasília, 2020.

BREIN, Paulo Cesar. *Fronteira Cibernética* [mensagem pessoal]. Mensagem recebida por <wbfneto@bol.com.br> em 3 out. 2012.

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.

BULL, Hedley. *A Sociedade Anárquica*. Brasília: Editora Universidade de Brasília, Instituto de Pesquisa de Relações Internacionais: São Paulo: Imprensa Oficial do Estado de São Paulo, 2002.

BUZAN, Barry; WEAVER Ole; WILDE, Jaap. *Security*: a new framework for analysis. Boulder and London: Lynne Rienner Publishers, 1998.

BUZAN, Barry; HANSEN, Lene. *A Evolução dos Estudos de Segurança Internacional*. São Paulo: Editora Unesp, 2012.

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.

CANONGIA, Claudia; MANDARINO JÚNIOR, Raphael. "Segurança Cibernética: o desafio da nova Sociedade da Informação". *Parcerias Estratégicas* - Revista do Centro de Gestão e Estudos Estratégicos do Ministério da Ciência e da Tecnologia, Brasília, v. 14, n. 29, pp. 21-46, 2009.

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

CARR, Edward H. *Vinte Anos de Crise: 1919-1939*: uma Introdução ao Estudo das Relações Internacionais. 2. ed. São Paulo: Universidade de Brasília, Instituto de Pesquisa de Relações Internacionais, Imprensa Oficial do Estado de São Paulo, 2001 [1939].

CARVALHO, Paulo Sergio Melo de. "O Setor Cibernético nas Forças Armadas Brasileiras". In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011, pp. 13-34.

CASTRO, Iná Elias de. *Geografia e Política*: território, escalas de ação e instituições. 3. ed. Rio de Janeiro: Bertrand Brasil, 2010.

CASTRO, Iná Elias; GOMES, Paulo Cesar; CORRÊA, Roberto Lobato (Org.). *Geografia*: conceitos e temas. 5. ed. Rio de Janeiro: Bertand Brasil, 2003.

CASSIOLATO, José E., LASTRES, Helena M. M. “Inovação e sistemas de inovação: relevância para a área de saúde”. In: *Revista Eletrônica de Comunicação, Informação e Inovação em Saúde.* Rio de Janeiro, v.1, n.1, p.153-162, jan.-jun., 2007.

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

CAVUSGIL, S. T.; KNIGHT, G.; RIESEMBERGER, J. R. *Negócios Internacionais*: estratégia, gestão e novas realidades. São Paulo: Person Prentice Hall, 2010.

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.

CECÍLIO, Marco B. *Fernand Braudel no Mundo Contemporâneo e a Acumulação Acelerada de Riquezas*: economia de mercado e capitalismo como opostos 2008. Dissertação (mestrado) 162f. – Universidade Federal do Rio de Janeiro/Instituto de Economia/Programa de Pós-graduação em Economia Política Internacional. 2012.

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

CLARKE, Richard; KNAKE, Robert. *Cyber War:* The Next Threat to National Security and What to Do About It. New York: CCCO, 2010.

CLAUSEWITZ. Carl von. *On War*. New Jersey: Princeton University Press, 1976 [1832].

COHEN, Benjamin. *International Political Economy*: an intellectual history. Princeton: Princeton University Press., 2008.

COUTINHO, Eduardo S.; LANA-PEIXOTO, Fernando V.; RIBEIRO FILHO, Paulo Z.; AMARAL, Hudosn F. “De Smith a Porter: um ensaio sobre as teorias de comércio exterior”. In: *Revista de Gestão USP*, São Paulo, v. 12, n. 4, pp. 101-113, out/dez, 2005.

DAHL, Robert A. *The Concept of Power*. *Behavorial Science*, v. 2:3, jul., 1957.

DALLARI, Dalmo de Abreu. *Elementos de Teoria Geral do Estado*. 19. ed. atual. São Paulo: Saraiva, 1995.

DEFESANET. Exército faz plano para proteger instalações estratégicas. 18 de julho de 2012. Disponível em: https://www.defesanet.com.br/terrestre/noticia/6820/Exercito-faz-plano-para-proteger-instalacoes-estrategicas. Acesso em: 13 ago. 2019.

DEIBERT, Ron. “Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace”. *Calgary: Canadian Defense & Foreign Affairs Institute*, August, 2012. Disponível em: <http://ebookbrowse.com/distributed-security-as-cyber-strategy-pdf-d380969236>. Acesso em 1 nov. 2015.

DEMENICIS, Luciene da S. *O Satélite Geoestacionário de Defesa e Comunicações estratégicas (SGDC)*: uma análise das contribuições para a Defesa Nacional. Trabalho de Conclusão de Curso (Especialização em Ciências Militares). 90f. Escola de Comando e

Estado-Maior do Exército, Rio de Janeiro, 2018.

DEYON, Pierre. *O Mercantilismo*. 4. ed. São Paulo: Editora Perspectiva, 2009.

DIAS, Leila Christina. Redes: emergência e organização. In: CASTRO, I. E. de; GOMES, P. C. C.; CORRÊA, R. L. (org.). *Geografia:* Conceitos e Temas. 5. ed. Rio de Janeiro: Bertrand Brasil, 2003. pp. 141-162.

DINH, Nguyen Q.; DAILLER, Patrick; PELLET, Alain. *Direito Internacional Público*. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2003.

DOYLE, Michael. "Kant, Liberal Legacies, and Foreign Affairs". In: *Philosophy and Public Affairs*, vol. 12, n. 3, 1983, pp. 205-235. Disponível em: https://web.archive.org/web/20140216082244/http://www.politics.ubc.ca/fileadmin/user_upload/poli_sci/Faculty/price/Debating_the_Democratic_Peace__Doyle.pdf. Acesso em: 14 fev. 2014.

DREIFUSS, Renan. *A Época das Perplexidades*: mundialização, globalização, planetarização. Petrópolis: Vozes. 1997.

DUARTE, Érico E. "Conduta da Guerra na Era Digital e suas Implicações para o Brasil: uma análise de conceitos, políticas e práticas de Defesa". *Texto para Discussão* n. 1760. Instituto de Pesquisa Econômica Aplicada. Brasília, 2012. Disponível em: https://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1760.pdf. Acesso em: 30 jun. 2016.

DUTRA, André Melo Carvalhais. *Introdução à Guerra Cibernética:* a necessidade de um despertar brasileiro para o assunto! 2011. <Disponível em http://161.24.2.250/sige_old/IXSIGE/Artigos/GE_39.pdf>. Acesso em: 8 out. 2013.

EARLE, Edward M. "Adam Smith, Alexander Hamilton, Friederich List: fundamentos econômicos do poder militar". In: PARET, Peter. *Construtores da Estratégia Moderna*: de Maquiavel à era nuclear. v. 1. Rio de Janeiro: Biblioteca do Exército, 2001. pp. 295-349.

ECONOMIA E SERVIÇOS. *Porque o novo cabo submarino Brasi-Europa é importante*. 5 de agosto de 2016. Disponível em: https://economiadeservicos.com/2016/08/05/por-que-o-novo-cabo-submarino-brasil-europa-e-importante/. Acesso em: 5 out. 2019.

EISSA, Sergio G.; GASTALDI, Sol; POCZYNOK, Ivan; TULLIO, Elina Z. "El ciberespacio y sus implicancias em la defensa nacional. Aproximaciones al caso argentino". In: CONGRESSO DE RELACIONES INTERNACIONALES DA UNIVERSIDAD NACIONAL DE LA PLATA, 6., 2012, La Plata. Disponível em: <http://www.iri.edu.ar/VI_congreso/ponencias/EISSA_GASTALDI_POCZYNOK_ZACARIAS_DI%20TULLIO_el%20ciberesoacio%20y%20sus%20implicancias%20en%20la%20defensa%20nacional.pdf>. Acesso em: 27 nov. 2012.

ELIAS, Norbert. *O Processo Civilizador*. 2. ed. Rio de Janeiro: Jorge Zahar, 1994 [1939].

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

ETZKOWITZ, Henry. “Academic-industry relations: a sociological paradigm for economic development”. In: Leydersdorff, L.; Van Den Besslaar, P. *Evolutionary economics and chaos theory*: new directions in technology studies. London: Pinter Publishers, p. 139-151, 1994.

ETZKOWITZ, H.; DZISAH, J. Triple Helix Circulation: the heart of innovation and development. *International Journal of Technology Management & Sustainable Development*, v.7, n.2, p.101-15, 2008.

EVERA, Stephen v. *Guide to Methods for Students of Political Science*. London: Cornell University Press, 1997.

FERREIRA, Kelly de S. *China e a Ásia Central: petróleo, segurança e os Estados Unidos*. Campinas, SP, 2012, 99f. Dissertação (mestrado em Relações Internacionais). Universidade Estadual de Campinas, 2012.

FERREIRA NETO. Walfredo B. *Por uma Geopolítica Cibernética: apontamento da grande estratégia brasileira para a nova dimensão da guerra*. Dissertação (mestrado). 206f. 2013. Instituto de Estudos Estratégicos. Universidade Federal Fluminense. 2013.

FIGUEIREDO, Eurico de L. “Globalização, Neoliberalismo e a Estratégia do Poder: os jogos não estão feitos”. In: Santos, Theotônio (coord.) *Os impasses da globalização*, III, Rio de Janeiro/São Paulo, Editora PUC-Rio/Edições Loyola, 2005.

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

_____. *O Mito do Colapso do Poder Americano*. Rio de Janeiro: Record, 2008.

_____. “Muito Antes de Keynes”. *Valor Econômico*. 24 abr. 2012. Disponível em: http://www.centrocelsofurtado.org.br/arquivos/image/201204251227410.Fiori%20ValorE%2024-04-12.pdf. Acesso em: 28 jun. 2016.

_____. *Economia Política Internacional e Relações Internacionais*. Palestra proferida em 12 set. 2005, na Semana de Economia Política Internacional da Faculdade de Economia e Administração da Universidade de São Paulo. Disponível em: https://chacombolachas.wordpress.com/2008/03/08/economia-politica-internacional-e-teoria-das-relacoes-internacionais/. Acesso em: 13 set. 2015.

FONTENELE, Marcelo Paiva. *Análise e Proposta de Articulação de Esforços no Contexto da Defesa Cibernética da Administração Pública Federal*. 2008. 65 f. Monografia (Especialização em Gestão de Segurança da Informação e Comunicações) - Universidade de Brasília, Brasília.

FORTES, Alice L. da S. *A Cúpula de Ferro Digital*: a estratégia de cibersegurança nacional de Israel. Trabalho de Conclusão de Curso. Centro Universitário Lasalle do Rio de Janeiro. Curso de Relações Internacionais. 2018.

FURTADO, Celso. *Formação Econômica do Brasil*. 32. ed. São Paulo: Companhia Editora Nacional, 2005 [1959]. Disponível em:

https://docente.ifrn.edu.br/eduardojanser/disciplinas/economia-brasileira-comex/livro-formacao-economica-do-brasil-celso-furtado/view. Acesso em: 19 abr. 2017.

G1. *Banda Larga no Brasil*. 2015. Disponível em: http://especiais.g1.globo.com/tecnologia/banda-larga-brasil/2015/. Acesso em: 13 jun. 2017.

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

GIDDENS, Anthony. *O Estado-nação e a Violência*. São Paulo: Edusp, 2001.

GILPIN, Robert. *A Economia Política das Relações Internacionais*. Brasília: Editora Universidade de Brasília, 2002 [1987].

GLEICK, James. *A Informação*: uma história, uma teoria, uma enxurrada. São Paulo: Companhia das Letras, 2013.

GONÇALEZ, Selma L. de M.; PORTELA, Lucas S. "A Geopolítica do Espaço Cibernético Sul-americano: (in)conformação de políticas de segurança e defesa cibernéticas?" In: *Austral*: Revista Brasileira de Estratégia e Relações Internacionais. V. 7, n. 14, jul/dez, p. 217-241, 2018.

GONÇALVES, William. *Relações Internacionais*. Rio de Janeiro: Jorge Zahar, 2008.

GOTTMANN, J. *A Evolução do Conceito de Território*. Boletim Campineiro de Geografia, v. 2, n. 3, Campinas, 2012 (1975).

GUERRA, Santos. Exército Brasileiro prepara sistema de prevenção contra ataques cibernéticos. *British Broadcasting Corporation.* 10 fev. 2012. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2012/02/120208_guerra_cibernetica_cc.shtml. Acesso em: 12 abr. 2012.

HARARI, Yuval N. *Homo Deus*: uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

HARDING, Luke. *Os Arquivos de Snowden*: a história secreta do homem mais procurado do mundo. Rio de Janeiro: LeYa, 2014

HARVEY, David. "A Arte de Lucrar: globalização, monopólio e exploração da cultura". In: MORAES, Denis (org.). *Por uma Nova Comunicação*: mídia, mundialização cultural e poder. Rio de Janeiro: Record, 2003. pp. 139-172.

HASBAERT, Rogério. *Territórios Alternativos*. Niterói: EdUFF; São Paulo: Contexto, 2002.

HAWKING, Stephen. *Uma Breve História do Tempo*: do "Big Bang" aos buracos negros. Lisboa: Gradiva, 1994 [1988].

HILFERDING, Rudolf. *O Capital Financeiro*. São Paulo: Nova Cultural, 1985 [1910].

HOBBES, T. *O Leviatã ou Matéria, Palavra e Poder de um Governo Eclesiástico e Civil*. São Paulo: Civita, 1983 [1651].

HUNTINGTON, Samuel P. *O Soldado e o Estado*: Teoria e Política das Relações entre Civis e Militares. Rio de Janeiro: Biblioteca do Exército, 1996.

IBAÑEZ, Pablo. *Geopolítica e Inovação Tecnológica*: uma análise da subvenção econômica e das políticas de inovação para a saúde. Tese (doutorado). 250f. Universidade de São Paulo. Departamento de Geografia. Programa de Pós-graduação em Geografia Humana. 2011.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *Mapeamento da Base Industrial de Defesa*. Brasília: Agência Brasileira de Desenvolvimento Industrial; Instituto de Pesquisa Econômica Aplicada, 2016.

ISAAC, David M. Vozes do Azul: Teóricos do Poder Aéreo. In: PARET, Peter. *Construtores da Estratégia Moderna*: de Maquiavel à era nuclear. v. 2. Rio de Janeiro: Biblioteca do Exército, 2001. pp. 211-242.

ISRAEL, Carolina B. *Redes Digitais, Espaços de Poder*: sobre conflitos na reconfiguração da Internet e as estratégias de apropriação civil. Tese (doutorado). 378f. Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo. Departamento de Geografia. São Paulo, 2019.

ITAIPU. Exército e Itaipu ampliam investimentos em Defesa Cibernética. 5 de setembor de 2017. Disponível em: https://www.itaipu.gov.br/sala-de-imprensa/noticia/exercito-e-itaipu-ampliam-investimentos-em-defesa-cibernetica. Acesso em: 12 mai. 2018.

JACKSON, Robert H.; SORENSEN, George. Introdução às Relações Internacionais: teorias e abordagens. Rio de Janeiro: Jorge Zahar, 2007.

_____. Introdução às Relações Internacionais: teorias e abordagens. 3. ed. Rio de Janeiro: Jorge Zahar, 2018.

JOMO K. S.; REINERT, Erik S. *As Origens do Desenvolvimento Econômico*: como as escolas do pensamento econômico têm abordado o desenvolvimento. São Paulo: Globus Editora, 2016.

JORGE, Bernardo W. G. de A. “Das Guerras Cibernéticas". In: CICLO DE ESTUDOS ESTRATÉGICOS, 11, 2012, Rio de Janeiro. *Segurança e Defesa Cibernética*. Disponível em:<http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XICEE/paper/view/29/50. Acesso em: 12 ago. 2012.

KANT, Imanuel. *À Paz Perpétua*. São Paulo: L&PM Editores, 2008 [1795].

KAPLAN, Robert D. *A Vingança da Geografia*: a construção do mundo geopolítico a partir da perspectiva geográfica. 1. ed. Rio de Janeiro: Elsevier, 2013

KENNEDY, Paul. *Ascensão e Queda das Grandes Potências*: transformação econômica e conflito militar de 1500 a 2000. Rio de Janeiro: Editora Campus, 1989.

KEOHANE, Robert; NYE, Joseph S. Realismo y Dependencia Compleja. In: _____. *Poder e interdependência*. La política mundial en transición. Buenos Aires, Grupo Editor Latinoamericano, 1977.

KÖCHE, José C. *Fundamentos da Metodologia Científica*: teoria da ciência e iniciação científica. Petrópolis: Editora Vozes, 1997.

KOLOSSOV, Yuri; GONCHAR, Dmitry V. Delimitation of Airspace and Outer Space: A Legal View. *Revista Brasileira de Direito Aeronáutico e Espacial*. Rio de Janeiro, n. 89. 2006. Disponível em: <http://www.sbda.org.br/revista/Anterior/1780.htm>. Acesso em: 20 dez. 2012.

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

LACOSTE, Yves. *A Geografia*: isso serve, em primeiro lugar, para fazer a guerra. 3. ed., Campinas: Papirus, 1989. Disponível em: <http://www.geoideias.com.br/geo/images/livros/a%20geografiaIves%20Lacoste.pdf>. Acesso em: 23 jul. 2012.

LÉVY, Pierre. *Cibercultura.* São Paulo: Editora 34, 1999.

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.

LOBATO, Luisa; KENKEL, Kai M. "A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra". In: *Contexto Internacional*. Rio de Janeiro, vol. 37, no 2, mai/ago, 2015, p. 629-660.

LOPES, Gills V.; GAMA NETO, Ricardo B. "Armas Cibernéticas e Segurança Internacional". In: MEDEIROS FILHO, O.; FERREIRA NETO, W.; GONZALES, Selma L. de M. (org.) *Segurança e Defesa Cibernética*: da fronteira física aos muros virtuais. Recife: Editora UFPE, 2014. pp. 23-46.

LUCERO, Everton. *Governança da Internet*: aspectos da formação de um regime global e oportunidades para a ação diplomática. Brasília: Fundação Alexandre de Gusmão, 2011.

MAGNOLI, Demétrio. *O corpo da pátria*: imaginação geográfica e política externa no Brasil (1808-1912). São Paulo: Editora da Universidade Estadual Paulista: Moderna, 1997.

MAHAN, Alfredo T. *The Influence of Sea Power History, 1660-1783*. Gutemberg Projector e-Book. Disponível em: http://www.gutenberg.org/files/13529/13529-h/13529-h.htm. Acesso em: 21 fev. 2017.

MANDARINO JÚNIOR, Raphael. Reflexões sobre Segurança e Defesa Cibernética. In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011. pp. 105-128.

MARINZECK, Jacqueline B. *Análise sobre a Segurança Cibernética Internacional no Século XXI após os Ciberataques Mundiais de 2017*. Trabalho de Conclusão de Curso. 117f. Centro Universtário Curitiba. Curso de Relações Internacionais de Curitiba. 2018.

MARQUES, Adriana A. *Amazônia*: pensamento e presença militar. Tese (doutorado). 233f. Faculdade de Filosofia, Letras e Ciências Humanas. Departamento de Ciência Política. Universidade de São Paulo. São Paulo, 2007.

MARSHALL, Tim. *Prisioneiros da Geografia*: 10 mapas que explicam tudo o que você precisa saber sobre política global. São Paulo: Zahar Editora, 2018.

MARTIN, André Roberto. *Fronteiras e Nações*. 4. ed. São Paulo: Contexto, 1998.

MATTOS, Carlos de Meira. *Estratégias Militares Dominantes*: sugestões para uma estratégia militar brasileira. Rio de Janeiro: biblioteca do Exército, 1986.

_____. *Geopolítica e Teoria de Fronteiras*: fronteiras do Brasil. Rio de Janeiro: Biblioteca do Exército, 1990.

_____. A Geopolítica e as Projeções de Poder. In: *Geopolítica.* vol I. Rio de Janeiro: Editora FGV, 2011 [1977]. pp. 305-312.

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

MEARSHIMER, John J. *A Tragédia da Política das Grandes Potências*. Lisboa: Gradiva, 2007.

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.

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.

MELLO, Leonel I. A. *Quem tem medo da geopolítica?* São Paulo: Hucitec/Edusp, 1999.

MENDONÇA, M. A. A.; LIMA, D. G.; SOUZA, J. M. de. "Cooperação entre Ministério da Defesa e COPPE/UFRJ: uma abordagem baseada no Modelo Triple Helice III". In: NEGRI, J. A. de; KUBOTA, L. C. (Ed.). *Políticas de incentivos à inovação tecnológica no Brasil*. Brasília: IPEA, 2008. Capítulo 15, p. 581-607.

MONSERRAT FILHO, José. "Relações entre Direito Espacial e Direito do Desenvolvimento". *Revista Brasileira de Direito Aeronáutico e Espacial*. Rio de Janeiro, n. 90, 2007. Disponível em: <http://www.sbda.org.br/revista/Anterior/1795.htm>. Acesso em: 19 dez. 2016.

_____. Introdução ao Direito Espacial. *Revista Brasileira de Direito Aeronáutico e Espacial*, Rio de Janeiro, dez. 1997. Disponível em: <http://www.sbda.org.br/textos/textos.htm>.

Acesso em: 21 dez. 2016.

MORAN, Daniel. Geography and Strategy. In: BAYLIS, J.; WIRTZ, J. J.; GRAY, C. S. *Strategy in the Contemporary World*: an introduction to strategic studies. 3. ed. New York: Oxford University Press, 2010. pp. 124-140.

MOREIRA, Marcílio Marques. Karl Deutsch, a Política e a Cibernética. In: *Deutsch na UNB:* conferência, comentários e debates de um simpósio internacional realizado de 11 a 15 de agosto de 1980. Brasília: Editora da UNB, 1980.

MOREIRA, William de Sousa. Ciência e tecnologia militar: "política por outros meios"?. *Revista da Escola de Guerra Naval,* [S.l.], v. 18, n. 2, p. 71-90, feb. 2017. ISSN e-2359-3075. Disponível em: <https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/314>. Acesso em: 4 jul. 2017.
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.

NOBLE, D. F. *American by Design*: science, technology, and the rise of corporate capitalism. New York: Alfred Knopf, 1979.

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

O ESTADÃO. *Brasil pode ter cabo submarino e satélite*. 11 de julho de 2013. Disponível em: https://link.estadao.com.br/noticias/geral,brasil-pode-ter-cabo-submarino-e-satelite,10000033354. Acesso em: 20 jun. 2019.

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.

OLIVEIRA, João Roberto de. "Sistema de Segurança e Defesa Cibernética Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional". In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011. pp. 105-128.

_____. *Fronteira Cibernética*. [mensagem pessoal]. Mensagem recebida por <wbfneto@bol.com.br> em 02 out. 12.

OLIVEIRA, Marcos A. G.; GAMA NETO, Ricardo B.; LOPES, Gills V. *Relações Internacionais Cibernéticas (CiberRI)*: oportunidades e desafios para os estudos estratégicos e de segurança internacional. Recife: Ed. UFPE, 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. C*onvenção sobre Aviação Civil Internacional*, de 7 de dezembro de 1944. Disponível em: <http://www2.anac.gov.br/biblioteca/decretos/convencaoChicago.pdf>. Acesso em: 12 abr. 2012.

_____. Resolução n.º 1962 (XVIII), de 13 de dezembro de 1963. *Trata sobre Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Cósmico, inclusive*

a Lua e demais Corpos Celestes. 1966. Disponível em: http://legis.senado.gov.br/legislacao/ListaPublicacoes.action?id=118828. Acesso em: 11 ago. 2012.

_____. *Convenção das Nações Unidas sobre o Direito do Mar*, de 10 de dezembro de 1982. Disponível em: <https://www.egn.mar.mil.br/arquivos/cursos/csup/CNUDM.pdf>. Acesso em: 23 out. 2011.

OWENS, William A.; DAM, Kenneth W.; LIN, Herbert S. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington D.C.: The National Academies Press, 2009.

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

PARADISO, José. "Prefácio". In: ANGELL, N. *A Grande Ilusão*. São Paulo: Imprensa Oficial do Estado de São Paulo, 2002.

PARET, Peter. Clausewitz. *Construtores da Estratégia Moderna*: de Maquiavel à era nuclear. v. 1. Rio de Janeiro: Biblioteca do Exército, 2001.

PARKS, Raymon C.; DUGGAN, David P. *Principles of Cyber-warfare*. In: WORKSHOP ON INFORMATION ASSURANCE AND SECURITY, Academia Militar de West Point, jun., 2001. Disponível em: <http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf >. Acesso em 04 de outubro de 2011.

PECCEQUILO, Cristina S. *Introdução às Relações Internacionais*: temas, atores e visões. Petrópolis: Vozes, 2004.

PESSOA, Eneuton; MARTINS. Marcilene. "Revisitando a Teoria do Ciclo do Produto". In: *Revista de Economia Contemporânea*. V. 11, n.2, mai/ago, 2007.

PETTY, W. *Aritmética Política*. São Paulo: Nova Cultura, 1996 [1690].

PINHO, Diva B.; VASCONCELLOS, Marco A. S. (org.). *Manual de Economia*. 4. ed. São Paulo: Saraiva, 2003.

PORTAL PRODAM. Amazônia Conectada traz oportunidades para provedores regionais. 6 de abril de 2017. Disponível em: http://www.prodam.am.gov.br/2017/04/06/amazonia-conectada-traz-oportunidades-para-provedores-regionais/. Aceso em: 20 set. 2018.

PORTELA, Lucas. *Movimentos Centrais e Subjacentes no Espaço Cibernético do Século XXI*. Dissertação (mestrado). 149f. Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército. 2018.

POPPER, Karl R. *A Lógica da Pesquisa Científica*. São Paulo: Cultrix, 2016 [1975]).

POSEN, Barry R. "Command of the Commons: The Military Foundation of U.S. Hegemony". *International Security*, v. 28, n. 1, summer, 2003, pp. 5–46. Disponível em: <http://belfercenter.ksg.harvard.edu/files/posen_summer_2003.pdf>. Acesso em: 20 set. 2012.

RAFFESTIN, Claude. *Por uma Geografia do Poder*. São Paulo: Ática, 1993.

RANGEL, Vicente Marotta. *Direito e Relações Internacionais*. 8. ed. São Paulo: Revista dos Tribunais, 2005.

REDE NACIONAL DE ENSINO E PESQUISA – RNP. *Amazônia Conectada*. 23 de julho de 2015. Disponível em: https://www.rnp.br/noticias/amazonia-conectada#:~:text=%E2%80%9CO%20Amaz%C3%B4nia%20Conectada%20tem%20tudo,as%20comunica%C3%A7%C3%B5es%20como%20quest%C3%A3o%20fundamental.&text=Ele%20garantiu%20ainda%20que%20%E2%80%9Co,e%20a%20integra%C3%A7%C3%A3o%20da%20Amaz%C3%B4nia%E2%80%9D. Acesso em: 20 set. 2017.

REVERON, Derek S. *Cyberspace and National Security*: threats, opportunities and power in a virtual world. Washington D. C.: Georgetown University Press, 2012.
REVISTA TECNOLOGIA E DEFESA. *Amazônia Conectada*: o maior programa de expansão das comunicações na Amazônia Ocidental. Ano 33. n. 145. 2016. Disponível em: https://issuu.com/tecnologia_defesa/docs/ed.145-editada. Acesso em: 12 mai. 2018.

_____. *10 Perguntas para o General Okamura, Comandante da Defesa Cibernética do Exército Brasileiro*. 26 de março de 2018. Disponível em: https://tecnodefesa.com.br/10-perguntas-para-o-general-okamura-comandante-da-defesa-cibernetica-do-exercito-brasileiro/. Acesso em: 30 out. 2018.

REZEK, José Francisco. *Direito Internacional Público*: curso elementar. 10. ed. rev. atual. São Paulo: Saraiva, 2005.

RODRIGUES, Marta M. A. *Políticas Públicas*. São Paulo: PubliFolha, 2010.

RODRIGUES, Alexandre Reis. Portugal e o espaço estratégico de interesse. In: *Jornal de Defesa e Relações Internacionais*. Revista Segurança e Defesa, Loures: Diário de Bordo Editores, 2012. Disponível em: <http://database.jornaldefesa.pt/politicas_de_defesa/portugal/JDRI%20009%20221112%20Portugal%20e%20o%20espa%C3%A7o%20interesse.pdf>. Acesso em: 27 nov. 2016.

ROSECREANCE, Richard. *The Rise of the Trading State*: commerce and conquest in the modern world. New York: Basic Books, 1986.

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

RUSSO, Waldo. "Satélite Brasileiro Geoestacionário de Defesa e Comunicações". *Ciência e Cultura*, São Paulo, v. 65, n. 4, pp. 4-5, 2013. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252013000400002&lng=en&nrm=iso>. Acesso em: 19 fev. 2020.

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

SALES, João Rufino de. *Guerra Cibernética*. Palestra proferida no II Congresso sobre Crimes Virtuais e Formas de Proteção. Federação do Comércio de São Paulo, São Paulo, em 28 set. 2010.Disponível em:<http://www.ebah.com.br/content/ABAAABQZQAG/guerra-

cibernetica-joao-rufino>. Acesso em: 22 jun. 2012.

SANTOS, Milton. *A Natureza do Espaço*: técnica e tempo. Razão e emoção. São Paulo: Hucitec, 1996.

SANTOS, José Carlos dos. *General detalha implantação do Centro de Defesa cibernética, novo órgão brasileiro*. [Brasília]. Folha de São Paulo, 7 mai. 2012. Entrevista concedida a Nelson de Sá. Disponível em: http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml. Acesso em: 8 mai. 2012.

_____. General José Carlos dos Santos: "Podemos recrutar hackers". [Brasília]. *Revista Época*, 15 jul. 2011. Entrevista concedida a Leandro Loyola. Disponível em: http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html. Acesso em: 20 jul. 2011.

SARFATI, Gilberto. *Teorias de Relações Internacionais*. São Paulo: Saraiva, 2005.

SAQUET, Marcos Aurelio. *Abordagens e concepções sobre território*. São Paulo: Expressão Popular, 2007.

SHAKARIAN, Paul. "Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008". *Military Review*, nov./dez., 2011. pp. 67-74.

SCHUMPETER, Joseph A. *Teoria do Desenvolvimento Econômico*: uma investigação sobre lucros, crédito, juro e o ciclo econômico. São Paulo: Nova Cultural, 1997 [1911].

SEGRILLO, Antonio. "A Questão do 'Fardo das Despesas Militares' na Economia Soviética e sua Influência no Desencadeamento da Perestroika: reconsiderações à luz de novos dados". In: *Textos de História*. V. 5, n. 1, 1997. pp. 92-117.

SILVA, Eduardo Q. da. *Políticas públicas e capacidades estatais*: um exame dos Projetos Estratégicos de Defesa sob a ótica dos arranjos institucionais. Dissertação (mestrado). 143f. Instituto de Pesquisa Econômica Aplicada, Programa de Pós-Graduação em Políticas Públicas e Desenvolvimento, área de concentração em Economia, 2018. Brasília: IPEA, 2018.

SILVA, Michéle Tancman Candido da. *A Geopolítica da Rede e Governança Global da Internet a partir da Cúpula Mundial sobre a Sociedade da Informação*. 2008. Tese de doutorado. Faculdade de Filosofia, Letras e Ciências Humanas. Programa de pós-graduação em Geografia Humana, Universidade de São Paulo, São Paulo, 2008.

SILVA, Guilherme A.; GONÇALVES, William. *Dicionário de Relações Internacionais*. São Paulo: Manole, 2005.

SILVEIRA, Fernando Malburg da. "*Cyberwarfare*: a nova dimensão da guerra". In: *Revista do Clube Naval*, ano 119, n. 360, out./nov./dez., 2011.

SIMDE. Sindicato Nacional das Indústrias de Materiais de Defesa. 2013. *Projeto Proteger do Exército*. 19 de julho de 2013. Disponível em:

http://www.fiesp.com.br/simde/noticias/projeto-proteger-do-exercito/. Acesso em: 13 abr. 2018.

SINGER; FRIEDMAN. Segurança e Guerra Cibernéticas: o que todos precisam saber. Rio de Janeiro: Biblioteca do Exército, 2017 [2014].

SMITH, Adam. *Uma Investigação sobre a Natureza e as Causas da Riqueza das Nações*. vol. 2. São Paulo: Martins Fontes, 2003 [1776].

SONÁGLIO, Wagner C.; RIBEIRO, Alexandre J. "Migração para Software Livre: estudo de caso no ambiente escolar da EsAEx/CMS*". Revista Interdisciplinar de Ciências Aplicadas à Atividade Militar*. n. 2, 2. sem. Salvador: EsFCEx/CMS, 2011.

SONTAG, Sherry; DREW, Christopher. *Blind Man's Bluff*: the untold story of american submarine espionage. New York: Public Affairs, 1998.

SOUZA, Marcelo Lopes de. O Território: sobre espaço e poder, autonomia e desenvolvimento. In: CASTRO, I. E. de; GOMES, P. C. C.; CORRÊA, R. L. (Org.). *Geografia:* Conceitos e Temas. 5. ed. Rio de Janeiro: Bertrand Brasil, 2003. pp. 77-116.

SOUZA, Eduardo A. A. de; ALMEIDA, Nival N. de. A Questão da Segurança e Defesa do Espaço Cibernético Brasileiro, e o Esforço Político-administrativo do Estado. *Revista da Escola de Guerra Naval*, [S.l.], v. 22, n. 2, p. 381-410, mar. 2017. ISSN e-2359-3075. Disponível em: <https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/479>2016. Acesso em: 20 jun. 2018.

SOUZA, Gills L. Relações Internacionais Cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos de segurança internacional. Tese (doutorado). 165f. Universidade Federal de Pernambuco, CFCH. Programa de Pós-graduação em Ciência Política, 2016.

SPYKMAN, Nicholas J. *America's Strategy in World Politics: The United States and the Balance of Power*. New York: Harcourt, Brace and Company, 1942. Disponível em: https://academic.oup.com/sf/article-abstract/21/1/112/1992102?redirectedFrom=fulltext. Acesso em: 3 jul. 2020.

STRANGE, S. *State and Markets*: an introduction to international political economy. Londres: Pinter, 1988.

TELE.SÍNTESE. *Cobertura do SGDC abrange 2 milhões de alunos, diz governo*. 13 de agosto de 2019. Disponível em: http://www.telesintese.com.br/cobertura-do-sgdc-abrange-2-milhoes-de-alunos-diz-governo/. Acesso em 20 fev. 2020.

TERRA, L.; ARAÚJO, R.; GUIMARÃES, R. B. *Geografia*: conexões: estudos de geografia geral e do Brasil. 3. ed. São Paulo: Moderna, 2015.

THE ECONOMIST. *Cyberwar*: War in the fifty domain. 01 jul. 2010. Disponível em: <http://www.economist.com/node/16478792>. Acesso em: 20 jun. 2017.

THE GUARDIAN. *NSA director Keith Alexander defends surveillance tactics in speech to hackers*. 31 jul. 2013. Disponível em: https://www.theguardian.com/world/2013/jul/31/nsa-keith-alexander-black-hat-surveillance. Acesso em: 20 ago. 2019.

THEOPHILO, Roque. *A História da Cibernética*. Disponível em: http://fisiologiaeciberneticapaineldopaim.blogspot.com/2012/01/historia-da-cibernetica-roque-theophilo.html . Acesso em: 25 ago. 2012.

TOFFLER, Alvin; TOFFLER, Heidi. *Guerra e Antiguerra*: sobrevivência na aurora do terceiro milênio. Rio de Janeiro: Biblioteca do Exército, 1995.

TOURÉ, Hamadoun. ONU organiza primeira simulação contra ataques cibernéticos. *Organização das nações unidas no Brasil*. 02 dez. 2011. Disponível em: <http://www.onu.org.br/onu-organiza-primeira-simulacao-contra-ataques-ciberneticos/>. Acesso em: 12 mai. 2012.

TREBAT, Nicholas M. *O Departamento de Guerra e o Desenvolvimento Econômico Americano, 1776-1860*. Tese (doutorado). 252f. 2011. Universidade Federal do Rio de Janeiro/Instituto de Economia/Programa de Pós-graduação em Economia Política Internacional. 2011.

TROXELL, John F. "Geoeconomics". In: *Military Review*. Army University Press, jan.-feb. p. 5-22. 2018. Disponível em: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Troxell-Geoeconomics.pdf. Acesso em: 20 mar. 2018.

TUCÍDIDES. *História da Guerra do Peloponeso*. São Paulo: UnB/IPRI, 2001.

VALENTE, Leonardo. *Política Externa na Era da Informação*: o novo jogo do poder, as novas diplomacias e a mídia como instrumentos de Estado nas Relações Internacionais. Rio de Janeiro: Revan, 2007.

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

VELLASCO, Fabiany M. M. e. *O Desenvolvimento da Indústria Espacial Brasileira*: uma abordagem institucional. Dissertação (mestrado). 143f. Programa de Mestrado Profissional em Governança e Desenvolvimento. Escola Nacional de Administração Pública, 2019.

VENTRE, Daniel. "Ciberguerra". In: *Seguridad Global y Potencias Emergentes em un Mundo Multipolar*, XIX Curso Internacional de Defensa, 2011. Zaragoza: Imprenta Ministerio de Defensa, 2012. pp. 32-45.

_____. "O Dilema da Fronteira Virtual: quando os Estados se tornam construtores de ciberfronteiras". In: *Dilemas*: Revista de Estudo de Conflitos e Controle Social. Rio de Janeiro. Ed. especial n. 3. 2019. pp. 75-96.

VERNON, Raymond. *International Investment and International Trade in the Product Cycle*. Quaterly Journal of Economics. 1966

VESENTINI, José William. Apresentação. In: LACOSTE, Y. *A Geografia – isso serve, em primeiro lugar para fazer a guerra*, Campinas, Papirus, 1988, pp. 7-13.

_____. *Novas Geopolíticas*. 2. ed. São Paulo: Contexto, 2003.

VESENTINI, José William. *Novas Geopolíticas*. 2. ed. São Paulo: Contexto, 2003.

VILLAS BÔAS, Eduardo D. da C. "O Papel da Ciência e Tecnologia no Processo de Transformação do Exército Brasileiro". In: *Instituto de Estudos Avançados*. Universidade de São Paulo. 2016. Disponível em: http://www.iea.usp.br/publicacoes/textos/o-papel-da-ciencia-e-tecnologia-no-processo-de-transformacao-do-exercito-brasileiro/view. Acesso em: 5 set. 2018.

WIENER, Norbert. *Cibernética e Sociedade*: o uso humano de sêres humanos. 4. ed. São Paulo: Cultrix, 1973 [1954].

WILSON, Woodrow. *Os Quatorze Pontos*. 1918. Disponível em: https://m.folha.uol.com.br/mundo/2008/11/466290-conheca-o-tratado-de-paz-de-14-pontos-proposto-por-woodrow-wilson.shtml, Acesso em: 3 set. 2016.

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

ZUCCARO, Paulo Martino. "Tendência global em segurança e defesa cibernética – reflexões sobre a proteção dos interesses brasileiros no ciberespaço". In: BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília: Secretaria de Assuntos Estratégicos, 2011. pp. 49-77.

ANEXO A - Resposta do Ministério da Defesa, via e-SIC

Anexo B – Resposta do Comando do Exército, via e-SIC

Anexo C – Consulta à Telebras S. A., via plataforma Fala.BR