UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE ESTUDOS ESTRATÉGICOS
MBA EM ESTUDOS ESTRATÉGICOS E RELAÇÕES INTERNACIONAIS

LUCAS LEAL BOSI

A MANUTENÇÃO DAS FRONTEIRAS BRASILEIRAS NO ESPAÇO CIBERNÉTICO: UMA ABORDAGEM FÍSICA

NITERÓI
2019

LUCAS LEAL BOSI

A MANUTENÇÃO DAS FRONTEIRAS BRASILEIRAS NO ESPAÇO CIBERNÉTICO: UMA ABORDAGEM FÍSICA

Trabalho de Conclusão de Curso apresentado à Coordenação do Programa de MBA em Estudos Estratégicos e Relações Internacionais da UFF (PPGEST - INEST/UFF), como requisito parcial para obtenção do grau de especialista em Estudos Estratégicos e Relações Internacionais

Orientador: Prof. Dr. Fernando Manoel Athayde Reis

NITERÓI - RJ

2019

Ficha de Avaliação de Trabalho de Conclusão de Curso em Relações Internacionais (Monografia)

Título do Trabalho: **A manutenção das fronteiras brasileiras no espaço cibernético:** uma abordagem física

Aluno: Lucas Leal Bosi

Avaliadores:

_____

Prof. Dr. Fernando Manoel Athayde Reis – Orientador (Avaliador 01)
Departamento de Estudos Estratégicos
e Relações Internacionais

_____

Prof. Dr. Bruno Pessoa Villela (Avaliador 02)
Departamento de Estudos Estratégicos
e Relações Internacionais

RESUMO

As alterações sofridas nas relações internacionais a partir do surgimento do domínio cibernético são abordadas, muitas vezes, com uma visão estratégica de alto nível e, por este motivo, podemos deixar de estabelecer relações importantes com a base da questão. Este trabalho foca na maior rede do mundo e analisa a influência da infraestrutura física componente do domínio cibernético traçando paralelos com a soberania e as capacidades de segurança da informação e defesa cibernética nacionais. Desta forma, objetiva investigar, em termos físicos e tangíveis, qual o nível de controle Estatal sobre o *backbone* da Internet no Brasil e se propõe a servir como uma leitura intermediária entre os aspectos técnicos e estratégicos.

ABSTRACT

The changes in international relations since the emergence of cyberspace are often approached with a high-level strategic vision, and for this reason we may fail to establish important relationships with the basis of the issue. This work focuses on the largest network in the world and analyzes the influence of the physical infrastructure component of the cyber domain making parallels with national sovereignty and information security and cyberdefense capabilities. Thus, it aims to investigate, in physical and tangible terms, what's the level of State control over the Internet backbone in Brazil and targets to serve as an intermediate reading between the technical and strategic aspects.

LISTA DE ABREVIATURAS E SIGLAS

Anatel – Agência Nacional de Telecomunicações

DDoS – Ataque Distribuído de Negação de Serviço

DNS – *Domain Name System*

DSL – *Digital Subscriber Lines*

FTP – *File Transfer Protocol*

HTTP – *Hypertext Transfer Protocol*

IETF – *Internet Engineering Task Force*

ISP – *Internet Service Providers*

OSI – *Open System Interconnection*

PLC – *Power Line Communication*

PPP – Protocolo ponto-a-ponto

PPP – Provedores de Pequeno Porte

PTT – Pontos de Troca de Tráfego

RFC – *Request for Comments*

SMP – Serviço Móvel Pessoal

SMTP – *Simple Mail Transfer Protocol*

TCP/IP – *Transmission Control Protocol/Internet Protocol*

TIC – Tecnologia da Informação e Comunicações

UDP – *User Datagram Protocol*

URL – *Uniform Resource Locator*

VoIP – *Voice over IP*

WWW – *World Wide Web*

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Rede de computadores, segundo Tanenbaum, é “um conjunto de computadores autônomos interconectados por uma única tecnologia”. A partir desse conceito básico, Tanenbaum também conceitua a Internet como uma rede de redes e a *World Wide Web* (WWW) como sendo um sistema distribuído – aquele que atua em conjunto com outros, mas que possui transparência ao usuário final de forma a parecer um único sistema coerente – que funciona na Internet (TANEMBAUM, 2003, p. 18). A relevância dessas definições pode ser facilmente explicitada: As informações de países, empresas, e indivíduos estão armazenadas em dispositivos e serviços que permitem acesso a redes de computadores e, na grande maioria dos casos, à Internet. Daí surge a necessidade de proteger a informação e a infraestrutura que armazena, trafega e processa esses dados. Essa atividade de proteção é bastante complexa, principalmente quando estamos conectados à Internet. Por este motivo, vale a pena partirmos do início para entendermos didaticamente a evolução e o estado atual dessa problemática.

Desde o princípio, a Internet foi fundamentada na ideia de que haveria múltiplas redes independentes e de *design* variado conectadas entre si. A ARPANET seria apenas a precursora das redes baseadas em trocas de pacotes que logo se conectaria a enlaces satelitais, rádio, entre outros (LEINER et al., 2009).

No fim da década de 60, a ideia de necessitar de um circuito exclusivo entre dois pontos para que se estabeleça a conexão entre eles era bastante aceitável, tendo em vista a tecnologia ser uma evolução das linhas telefônicas tradicionais – onde eram utilizados comutadores de circuito para realizar esse chaveamento, o que já era uma evolução quando comparado às telefonistas que realizavam essa tarefa manualmente. Como forma de otimizar a utilização dessa infraestrutura, surge a noção de comutação de pacotes, sem que interferisse na concepção de arquitetura aberta da Internet, ou seja, sem que houvesse restrições a arquiteturas ou tecnologias. A comutação de pacotes é explicada por Tanenbaum (2003, p. 126) como bem adequada à manipulação do tráfego interativo, pois os dados trafegam em

pacotes – blocos de tamanho máximo e formatação definidos – assegurando que nenhum usuário monopolize uma linha de transmissão.

Continuando em nossa linha temporal, no início da década de 70, foi desenvolvido mais um conceito que permitia o desenvolvimento de uma Internet de arquitetura aberta: o *Transmission Control Protocol/Internet Protocol* (TCP/IP). Foram Robert Elliot Kahn e Vint Cerf, laureados com o prêmio Turing de 2004, que idealizaram os protocolos. Desde a concepção da ideia, eles deixaram claras quatro regras fundamentais:

> "• As redes devem ser autossustentáveis e nenhuma alteração interna deve ser exigida para conectá-las à Internet.
>
> • As comunicações deveriam observar o princípio do melhor esforço: se um pacote não chega ao destino, deve ser retransmitido pela fonte.
>
> • Caixas pretas deveriam ser usadas para conexão das redes;
>
> futuramente seriam chamadas de *gateways* e roteadores. **Nenhuma informação seria retida pelos gateways sobre os fluxos de pacotes que trafegassem por eles**, mantendo-os, desta forma, simples e evitando adaptações e recuperação de vários modos de falha.
>
> • **Não deveria haver nenhum controle global nos níveis operacionais.**" (LEINER et al., 2009, p. 24, tradução nossa, grifo nosso)

Podem ser tecidas observações sobre os trechos grifados, mas faremos isso em um momento mais apropriado. Por enquanto, vamos nos ater ao fato de que o TCP/IP foi um passo fundamental no desenvolvimento da Internet, pois preservou as ideias de comutação de pacotes e de arquitetura aberta. A relevância do TCP nos é apontada por um dos maiores colaboradores do projeto ARPANET e criador da comutação por pacotes, Leonard Kleinrock:

> “O TCP era a ideia chave de uma arquitetura aberta que permitia que redes de diferentes tipos se interconectassem e computadores trocassem informação fim-a-fim através dessas redes. Essa contribuição de Cerf e Kahn foi um passo crítico no desenvolvimento da Internet.” (KLEINROCK, 2010, p. 34, tradução nossa)

Compreendamos dessa declaração que fim-a-fim se refere à capacidade do protocolo de transporte, rodando nos sistemas finais, permitir que uma máquina se comunique com qualquer outra máquina conectada à Internet. Em outras palavras, que aplicações de um computador enviem mensagens individuais para aplicações de outro computador, sem a necessidade de atuação do protocolo em todos os ativos e passivos da rede que se encontrem entre a origem e o destino da mensagem.

Para compreendermos o propósito da pilha de protocolos TCP/IP, recorremos a James Kurose. Ele explica que o TCP é um protocolo de transporte confiável. E que a conexão TCP é sempre ponto-a-ponto, ou seja, ela acontece entre um único remetente e um único destinatário. Como o protocolo TCP roda apenas nesses dois sistemas, os elementos intermediários da rede (roteadores e switches) são alheios às conexões TCP. (2006, p. 169). Mas como identificar os endereços do remetente e do destinatário? Kurose esclarece que “o endereçamento e o repasse na Internet são componentes importantes do Protocolo da Internet (IP).” (KUROSE, 2006, p. 244). Para consolidação deste entendimento, podemos afirmar, de forma simplificada, que o protocolo TCP é responsável pelo transporte dos dados entre dois pontos, independentemente das divergências de parâmetros entre as redes a que esses pontos pertençam, e o IP pelo endereçamento do remetente e do destinatário.

Novas aplicações foram surgindo e exigindo novos protocolos para um funcionamento correto ou mais seguro. Por exemplo, o *User Datagram Protocol* (UDP) foi implementado como forma de dar suporte a ligações telefônicas sobre o IP. Ele é um protocolo responsável por transporte de dados, assim como o TCP, mas não exige que todos os pacotes cheguem ao destinatário. Permitindo a perda de pacotes, ele

cria um fluxo de dados menos confiável, mas atinge o objetivo de realizarmos ligações telefônicas sobre o IP.

Dessas aplicações que exigiriam novos protocolos, Leiner afirma ser o e-mail a mais disruptiva para aquele período. A motivação para a criação da ARPANET e, posteriormente, da Internet, era o compartilhamento de recursos. E os serviços de e-mail, nas palavras dele “proveram um novo modelo de como as pessoas poderiam se comunicar e alterou a natureza dos processos colaborativos, primeiro na construção da Internet propriamente dita, e depois para a maior parte da sociedade.” (LEINER et al., 2009, p. 25, tradução nossa).

O surgimento de várias aplicações deixou claro o conceito central da Internet. Ela não foi concebida para uma única aplicação, mas como uma infraestrutura sobre a qual outras inúmeras poderiam ser criadas. Leiner frisa que essa característica fica evidenciada com o surgimento da *World Wide Web* (www) (LEINER et al., 2009, p. 25).

CAPÍTULO I – TERRITÓRIO, FRONTEIRA E SOBERANIA

> "Território é uma porção do espaço geográfico que coincide com a extensão espacial da jurisdição de um governo. Ele é o recipiente físico e o suporte do corpo político organizado sob uma estrutura de governo. Descreve a arena espacial do sistema político desenvolvido em um Estado nacional [...]. Ele também serve para descrever as posições no espaço das várias unidades participantes de qualquer sistema de relações internacionais. Podemos, portanto, considerar o território como uma conexão ideal entre espaço e política. Uma vez que a distribuição territorial das várias formas de poder político se transformou profundamente ao longo da história, o território também serve como uma expressão dos relacionamentos entre tempo e política." (GOTTMANN, 2012 [1975], p. 523).

A definição apresentada é bastante apropriada a este texto. Gottmann aborda as expressões políticas e temporais de um território, mas deixa nítida a associação direta do termo território à sua propriedade de ser físico.

Ele descreve a evolução do conceito de território a partir do século XIV, mas afirma ser muito anterior a esse período. Porém, esse foi o momento em que o termo passa a ser utilizado na Europa, referindo-se uma jurisdição ou órbita econômica de um feudo ou um reino. (GOTTMANN, 2012 [1975], p. 523)

Neste trabalho, focaremos apenas nos aspectos conceituais atualmente relevantes, ou que propiciaram a formação das condições hodiernas. Por este motivo, salientaremos as relações entre fronteira, território e soberania observadas a partir do século XV, pois é nesse contexto que "a importância do território como a base e a estrutura essencial da política emerge gradualmente no mapa-múndi, paralelamente às ideias políticas de soberania nacional e autonomia." (GOTTMANN, 2012 [1975], p. 528) Para tal, desenvolveremos os conceitos de Estado, fronteira, soberania e continuaremos a tratar do território, por serem, todos esses, conceitos complementares.

> “Ratzel foi o organizador ou sistematizador de um conjunto de temas e conceitos que, a partir dele, passaram a ser o conteúdo inquestionável de qualquer obra de geografia política, [...] ele construiu um novo campo de estudos, definindo [...] seus temas e conceitos fundamentais: as relações da política com o espaço geográfico, nas quais despontam o estudo do território [...], das fronteiras [...], da política geográfica ou territorial, da circulação pelo território, da importância do “solo” [território] na constituição e na evolução dos Estados.” (VESENTINI, 2010, p. 129)

É com as definições de Ratzel que nos aprofundaremos na temática e observaremos a relação intrínseca que ele nos apresenta entre Estado e território, e como a ideia de soberania se enquadra nesse raciocínio:

> “O homem não é concebível sem o solo terrestre, ainda mais sem a maior obra do homem sobre terra: o Estado. Assim como os termos cidade e estrada expressam, respectivamente, uma fração de humanidade e uma obra humana; quando se fala de Estado, designa-se uma fração de superfície terrestre. O Estado é obrigado a viver do solo. Ele possui invariavelmente apenas as vantagens oferecidas por um solo que lhe é assegurado. É o que exprime a ciência política quando diz que o território pertence à essência do Estado. Ela designa a soberania como *jus territoriale* e estabelece a regra que as mudanças territoriais podem fazer-se apenas por leis. A vida dos Estados faz-nos descobrir relações muito mais estreitas: durante a História, vemos as forças políticas se apreenderem do solo e assim levar à formação dos Estados.” (RATZEL, 2011 [1897], p. 59)

Ratzel (2011, p. 55) defende que as fronteiras, que dão forma ao Estado delimitando seu território, sofrem influências diversas. Desde as mais óbvias, puramente geográficas, até as motivações históricas, religiosas ou nacionais. Ele

propõe, então, uma tipologia de fronteiras que se dá da seguinte forma: três tipos (Políticas, Naturais e Artificiais) que se subdividem em subtipos.

Cataia pode nos ajudar a entender e adaptar a tipologia de fronteiras ratzeliana à atualidade. Passaremos por todos os tipos nos baseando na interpretação dele (CATAIA, 2010, passim). Iniciemos pelas fronteiras **políticas**:

A fronteira **simples** não tem contato com outra área política. Atualmente, essas fronteiras se restringiriam às águas territoriais. Não por essa restrição, seria menos relevante. Esse tipo de fronteira encontra discussão no âmbito das relações internacionais sobre diversas requisições de países sobre extensão dos mares territoriais e zonas economicamente exclusivas. No caso brasileiro, estaríamos tratando da área representada pela Amazônia Azul, com suas proporções ainda em processo de definição. Já a fronteira **dupla** é representada pela contiguidade de dois territórios nacionais.

As fronteiras **fechadas** são os enclaves. Como, por exemplo, o Vaticano. As fronteiras **descontínuas**, assim como as fechadas, são estranhas ao território que as cerca. Ambas se diferenciam, pois aquelas não demarcam a totalidade do território de um Estado. As fronteiras descontínuas estão associadas aos períodos de expansão Colonial e Imperialista. Apesar disso, podemos encontrar exemplo recente de discussão sobre essas fronteiras no caso das Malvinas.

Aquelas que geram conflitos por novas demarcações fronteiriças seriam as fronteiras **deficientes**. No caso brasileiro, temos as demarcações estaduais ainda em discussão no Congresso Nacional. A fronteira **elástica** se assemelha à fronteira deficiente por apresentar uma fronteira ainda mutável, mas se diferencia, pois a causa da elasticidade é a ausência de meios técnicos e cartas precisas que auxiliem na diminuição do erro apresentado na demarcação fronteiriça. O desenvolvimento científico e tecnológico permite que as fronteiras sejam demarcadas como linhas (utilizando metodologia matemática para tal), excluindo a presença das zonas fronteiriças que se debruçam sobre marcos físicos.

Apresentamos as fronteiras políticas e agora explicitaremos as fronteiras **naturais**. Aqui vale salientar que a escolha de um marco natural também é um ato

político, tornando a taxonomia de Ratzel não excludente entre seus tipos. As fronteiras naturais são subdividas em:

Marcos físicos que representariam os limites do ecúmeno: montanhas, desertos, lagos, costas, florestas, etc. Admitem ainda um viés social, podendo ser constituídos por um limite étnico. As fronteiras **boas** apresentam, fisicamente, boas condições de proteção do Estado. Já as **más**, não se prestam à defesa militar de um Estado.

A fronteira **artificial** é o último tipo a ser elencado e possui apenas um subtipo: a fronteira **demarcada**. Esta pode ser alicerçada em um marco físico natural ou artificial, mas sempre é demarcada por um Tratado.

Desse estudo pragmático de tipologia não excludente de Ratzel, podemos depreender que as fronteiras são entidades híbridas de marcos naturais, artificiais e acordos entre Estados, e podem ser classificadas politicamente de seis formas distintas que representam as formas de relacionamento entre os entes políticos envolvidos.

Vimos que o trabalho de Ratzel é focado no traçado geodésico, o que muito condiz com as expectativas envolvidas neste texto. Mas não esgota os temas a serem abordados por nós. Por este motivo, voltemos a buscar auxílio em Cataia (2010, p. 16). Em seu trabalho, ele organiza e sintetiza conceitos de fronteiras de diversos autores. Dentre eles, citaremos apenas aqueles nos quais poderemos nos apoiar, por serem mais pragmáticos em suas definições.

Jacques Ancel afirma que as fronteiras são isóbaras políticas. Daí é possível depreender que elas são estabelecidas em uma região onde dois Estados vizinhos exercem pressão de igual intensidade em direções opostas. Ou seja, linhas permanentes de tensão entre dois campos de força. Um ponto de vista bastante realista das relações internacionais.

Jean Gottmann, base neste texto para a abordagem do conceito de território, é um crítico do pensamento de Ancel. Para ele, o território é o abrigo de um povo, além de descrever o espaço onde um Estado desenvolve seu sistema político. A fronteira, então, é importante para delimitar regimes políticos distintos. Na visão de Gottmann,

não necessariamente há um conflito fronteiriço, pois os acordos e leis internacionais foram desenvolvidos para evitar o uso da força.

Rudolf Kjellen, em uma análise mais política, afirma que as fronteiras são a epiderme dos Estados. Não se atém à geofísica, mas é uma abordagem simples e útil para tratarmos do conceito de soberania.

Por fim, temos a definição de Hildebert Isnard: as fronteiras são a cristalização dos limites da organização do espaço realizado por distintos projetos políticos, inclusive projetos não-estatais. Isto nos chama a atenção para a ações de outras entidades que participam do jogo político mundial.

Procuremos agora entender como se insere a soberania sobre os demais conceitos já estabelecidos.

> “A ideia moderna de soberania foi formulada pela primeira vez na segunda metade do século XVI, e aplicada ao então novo fenômeno do Estado territorial. Ela se referia em termos legais ao fato político fundamental daquela era – o aparecimento de um poder centralizado que exercia a sua autoridade de legislar e fazer cumprir as suas leis no âmbito de um certo território. Esse poder, investido primariamente, mas não necessariamente, em um monarca absoluto, era então superior a quaisquer outras forças que se fizessem sentir naquela extensão de terra. No decorrer de um século, ele se tornou incontestável, tanto no interior como no exterior de seu território. Em outras palavras, ele se tornou supremo.” (MORGENTHAU, 2003, p. 567)

Morgenthau deixa claro que, em sua concepção, o conceito de soberania esteve atrelado a um soberano, possuidor de um poder supremo de criar leis e fazê-las cumprir dentro de determinado território. Posteriormente, o soberano passa a ser reconhecido, também no exterior, por sua capacidade de exercer soberania sobre seu território.

Vamos nos ater aos conceitos atualmente relevantes. Morgenthau (2003, p. 568) nos lembra das modificações ocorridas ao longo dos séculos até a concepção do Estado democrático nacional, com a ideia de soberania popular. A soberania então passa a ser entendida, teoricamente, como a manifestação do desejo de um povo, sobre o território nacional, através de representantes eleitos democraticamente.

É importante relembrar que o direito internacional e os organismos internacionais sempre devem observar a soberania dos Estados. As normas do direito internacional devem ser compulsórias apenas às nações que tenham consentido em aplicá-las, à exceção daquelas necessárias à organização e existência do sistema internacional.

Ainda no âmbito do direito internacional, um conceito importante é o de impenetrabilidade da nação. Morgenthau explica esse conceito e chama nossa atenção para uma situação de exclusão bastante relevante:

> “Isso (A impenetrabilidade da nação) vem a ser uma outra maneira de dizer que, em um determinado território, só uma nação pode exercer sua soberania – a saber, autoridade suprema – e que nenhum outro Estado tem o direito de realizar atos governamentais em seu território sem o seu consentimento. [...] A guerra, como forma extrema de medida coercitiva nos termos do direito internacional, constitui a única exceção a essa regra, visto que é parte inerente da guerra penetrar o território inimigo, enquanto se preserva a impenetrabilidade do seu próprio; e o direito internacional permite ao país ocupante exercer direitos soberanos no território estrangeiro ocupado por forças militares.” (Morgenthau, 2003, p. 571)

Retomando Gottmann (2012 [1975], p. 531), somos apresentados a aspectos mais modernos de soberania. Ele nos leva a pensar sobre como a dependência de suprimentos vindos de outras nações ou a capacidade de se autodefender por meio do controle de suas próprias terras influenciam na soberania.

Além disso, mostra que a soberania foi estendida para outras áreas do espaço antes livres desse controle: as reclamações de extensão do controle soberano sobre a plataforma continental - expandindo os mares territoriais - são provenientes do aumento da acessibilidade aos recursos marítimos. A conquista da capacidade de voar pelo homem forçou a discussão a respeito da jurisdição sobre a coluna de espaço que se estende, em altura, acima dos territórios dos Estados. Esse fato levou o direito internacional a reconhecer a soberania estatal sobre a coluna de espaço aéreo ao infinito. Apesar disso, a questão da soberania sobre o domínio aeroespacial é paradoxal, pois praticamente todos os Estados aceitaram que satélites orbitem sobre seus territórios. Definir como apenas inocentes essas passagens seria, no mínimo, ingenuidade. Tecnologias de espionagem e lançamento remoto ou direcionamento de artefatos explosivos (até mesmo nucleares) são realidade.

Por todos os motivos elencados, Gottmann afirma que a soberania jurídica vem perdendo seu impacto ao passo que outras vertentes ganham relevância. Podemos estender esse raciocínio quando falamos do espaço cibernético. Ele possui peculiaridades antes nunca observadas, tendo sido criado pelos homens. E é nesse momento que muitas vezes temos a apresentação de uma dissociação dos conceitos físicos e virtuais, sem que autores diversos se atenham à noção de que embora as ações no domínio cibernético sejam de cunho virtual, suas capacidades são alicerçadas em elementos reais.

Este trabalho, não por acaso, se inicia detalhando a criação das tecnologias que ajudaram a desenvolver e construir a Internet. Queremos aqui clarear conceitos de infraestrutura de redes de forma a correlacioná-los mais naturalmente ao território físico-geográfico basilar das teorias territoriais. Por este motivo, no próximo capítulo, passaremos por conceitos abstratos do domínio cibernético, não sem fundamentá-los em suas origens técnicas.

CAPÍTULO II – O ESPAÇO CIBERNÉTICO

No capítulo anterior apresentamos conceitos de território, para abordarmos agora, com mais segurança, os conceitos de espaço ou os domínios nos quais os Estados possuem capacidade de exercer influência. Tratamos do território e focamos no terrestre, pois conforme já afirmamos, é ele que confere as condições de habitação à humanidade. Ele sempre foi o objetivo final das ações estatais em qualquer outro espaço, seja o aéreo, o marítimo ou o espacial. Dessa forma, não seria diferente no espaço cibernético.

Para conceituarmos o espaço cibernético tomemos primeiramente a definição do departamento de defesa dos Estados Unidos:

> "Um domínio global dentro do ambiente da informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computação, e microprocessadores e microcontroladores embarcados." (ESTADOS UNIDOS DA AMÉRICA, 2019, p. 56, tradução nossa)

É um conceito bastante direto e bem condizente com a proposta do nosso texto. Ele deixa clara a composição básica do ciberespaço. Outro ponto importante da definição do Departamento de Defesa dos Estados Unidos é que ela considera o domínio cibernético, o ambiente virtual que é criado pela interconexão de infraestruturas de tecnologia da informação e comunicações (TIC). Ou seja, é necessário que haja uma rede de sistemas para que seja configurado o espaço cibernético. Este é um ponto importante, pois não há uma unanimidade quanto a ele. A própria definição apresentada na Doutrina Militar de Defesa Cibernética do Brasil diverge nessa questão: "espaço virtual, composto por dispositivos computacionais conectados em redes **ou não**, onde as informações digitais transitam, são processadas e/ou armazenadas." (BRASIL, 2014, p. 18, grifo nosso)

O ponto de vista apresentado em nossa Doutrina Militar de Defesa Cibernética pode ser questionado. É razoável pensarmos que não havendo uma interconexão entre sistemas, não há espaço a ser gerado, pois não há sequer informação a ser compartilhada. O que há é um ambiente virtual, restrito às capacidades físicas do hardware em questão e aos dados armazenados em suas memórias. Defendemos aqui que não há que se falar, portanto, de um espaço cibernético ou domínio cibernético, onde nações possam exercer influência, em simples máquinas sem conexões com outras máquinas. É coerente dizermos, no entanto, que a partir do momento que essas máquinas forem conectadas a outros sistemas, elas comporão o espaço cibernético.

Talvez por este motivo, o Manual de Campanha do Exército Brasileiro apresente, em seu prefácio, a definição dada pelo Departamento de Defesa dos Estados Unidos (Brasil, 2017), mas mantenha a estruturação hierárquica das normas, utilizando como definição de espaço cibernético a da Doutrina Militar de Defesa Cibernética brasileira (Brasil, p. 2-2, 2017).

Outros autores, atribuem ainda ao domínio cibernético outras dimensões que não a física (infraestruturas interconectadas de TIC) e a virtual criada por essa interconexão. Daniel Ventre, por exemplo, se utiliza de um modelo de espaço cibernético, comumente utilizado, que é dividido em três camadas principais:

> “Uma primeira camada é constituída pela arquitetura material, física, hardware; ela é feita pelo conjunto de computadores, calculadoras, cabos eletrônicos (*hardware layer*). Uma segunda camada, média, denominada *software* ou aplicativa, é constituída pelo conjunto de programas, códigos, dados e algoritmos que dão vida ao ciberespaço (software layer). E uma terceira camada, informacional, é a do sentido, das informações (*news*), dos conteúdos (*meatware layer*).” (VENTRE, p. 77, 2019).

Ventre não limita o ciberespaço às camadas principais, e admite ainda que outras camadas, como a camada operacional e a dimensão humana possam vir a completar essa definição (VENTRE, p. 77, 2019).

A definição apresentada por Ventre também é utilizada por outros autores e, de certa forma, se calca no modelo de referência OSI de arquitetura de redes de computadores de sete camadas ou na pilha de protocolos da Internet de cinco camadas.

Nesses modelos estamos interessados no relacionamento entre as camadas consecutivas, em ambos os sentidos. Toda camada utiliza-se dos serviços providos pela camada inferior para prestar os seus serviços à camada superior. Apresentaremos os modelos (KUROSE, p. 35–41, 2013) para que tenhamos um entendimento técnico maior sobre o assunto e possamos avaliar com mais clareza todas as definições de ciberespaço já apresentadas. Entendemos ainda, ser este um tópico de conhecimento basilar para que se aborde o assunto cibernética, mantendo em mente o que está ocorrendo, de fato, nos sistemas em rede em questão.

O *Open System Interconnection* (OSI) possui sete camadas sequenciais: aplicação, apresentação, sessão, transporte, rede, enlace e física. É o modelo de referência de arquitetura de redes de computadores padronizado pela *International Organization for Standardization* (ISO). Ele foi concebido em um momento inicial de criação dos protocolos que viriam a ser utilizados na Internet e de outros que estavam em desenvolvimento e foram abandonados. Por esse motivo, seu propósito hoje é muito mais educativo do que realmente prático.

Cinco das camadas do modelo OSI possuem equivalência no modelo de pilhas de protocolos de Internet. São elas: camada de aplicação, transporte, rede, enlace e física e realizam os mesmos serviços em ambas as abordagens de arquitetura de redes, por isso, detalharemos cada uma delas quando apresentarmos o modelo de pilhas de protocolos. Quanto às camadas exclusivas do modelo OSI, podemos dizer que a camada de apresentação tem a função de apresentar à camada de aplicação dados traduzidos (descomprimidos ou decodificados, por exemplo) para o entendimento direto da camada superior. E a camada de sessão é responsável pela sincronização da troca de dados.

O modelo de pilha de protocolos é descrito na RFC-3439, possuindo cinco camadas: aplicação, transporte, rede, enlace e física. *Requests for Comments* (RFC) são documentos criados e atualizados pelo IETF (*Internet Enginnering Task Force*), que, por sua vez, é a instituição que especifica os padrões a serem implementados para utilização na Internet. Portanto, dos modelos apresentados, o de pilha de protocolos de Internet é mais voltado à realidade dos sistemas de redes de computadores.

Passaremos pelas camadas rapidamente, em uma abordagem de cima (mais próximo do usuário) para baixo (mais próximo da máquina), iniciando pela camada de **aplicação** da Internet que conforme o próprio nome indica, é a camada mais superior e onde estão as aplicações de rede e seus protocolos. Por estar mais próxima do usuário final, os protocolos presentes nela são mais conhecidos do público geral, como o *Hypertext Transfer Protocol* (HTTP), que é responsável pela transferência de documentos pela *web*; o *Simple Mail Transfer Protocol* (SMTP), para transferência de mensagens via correio eletrônico; e o *File Transfer Protocol* (FTP), que provê a capacidade de transferência de arquivos ponto a ponto. Em termos de sistemas que são aplicações que rodam principalmente nessa camada, podemos citar o *Domain Name System* (DNS) que traduz os apelidos dos endereços (*Uniform Resource Locator* (URL)) para endereços de 32 *bits*, de forma a facilitar a interface do usuário durante a navegação.

A camada de **transporte** é responsável pela transferência, entre cliente e o servidor, das mensagens que lhe forem passadas pela camada de **aplicação**. Nós já vimos os protocolos que são utilizados na camada de **transporte** e como eles foram importantes para o desenvolvimento da internet. O TCP e o UDP são os protocolos responsáveis pelo transporte das mensagens, bem como pelo bom entendimento entre o cliente e o servidor, independentemente das tecnologias que estiverem conversando. O primeiro, provê um serviço orientado a conexão para as suas aplicações, ou seja, não permite a perda dos pacotes, reenviando os pacotes perdidos sempre que necessário. O segundo, não orientado a conexão, é utilizado em aplicações que não demandam a segurança de que todos os pacotes sejam entregues, como por exemplo, aplicações *Voice over IP* (VoIP), em que a perda de poucos trechos de uma palavra em uma chamada telefônica sobre IP não

comprometerão o entendimento da mensagem final, e o não reenvio dos pacotes perdidos impede que sílabas soltas de palavras sobrepostas ocorram durante a conversa.

A camada de **rede** recebe da camada de **transporte** do *host* (máquina onde a aplicação está rodando) de origem o segmento a ser transportado (datagrama) e um endereço de entrega. Ela então provê o serviço de entrega do segmento à camada de **transporte** no *host* de destino. O protocolo IP faz parte dessa camada, para validar a relevância desse protocolo, segue uma afirmação de James Kurose:

> "**Existe apenas um único protocolo IP, e todos os componentes da Internet que têm uma camada de rede devem executá-lo.** A camada de rede da Internet também contém protocolos de roteamento que determinam as rotas que os datagramas seguem entre origens e destinos. A Internet tem muitos protocolos de roteamento. (...) a Internet é uma rede de redes e, dentro de uma delas, o administrador pode executar qualquer protocolo de roteamento. Embora a camada de rede contenha o protocolo IP e também numerosos outros de roteamento, ela quase sempre é denominada apenas camada IP, refletindo o fato de que **ele é o elemento fundamental que mantém a integridade da Internet**." (KUROSE, p. 38, 2013, grifo nosso)

A camada de **enlace** é a hospedeira dos roteadores. Ela que realiza o roteamento, e presta o serviço à camada de **rede** de tramitar determinado pacote da a origem ao destino. Esse processo é realizado sempre aos pares, com passos entre nós origem e nós destino. Os nós serão: o *host* de origem, os roteadores intermediários e o *host* de destino, de forma a concluir a entrega do pacote. Enlaces comumente vistos são *Ethernet*, Wi-fi ou o PPP (Protocolo ponto-a-ponto). É fácil perceber então que um mesmo datagrama será manuseado por diferentes enlaces ao longo de sua rota, e nesse processo, a camada de **rede** receberá um serviço diferente de cada um dos vários protocolos da camada de **enlace**.

Por fim, a camada **física**. Falamos agora dos *bits* fisicamente representados e em que meio físico eles trafegam. O meio físico para o transporte, influenciará no protocolo a ser utilizado na camada de **enlace**. Em cada meio, o *bit* atravessa o enlace de uma forma diferente.

Os meios mais comumente encontrados na camada física são:

a) Cabos coaxiais utilizados para prover acesso à Internet utilizando, na maior parte das vezes, a infraestrutura de provedores de TV a cabo.
b) *Digital Subscriber Lines* (DSL): que basicamente se utilizam dos cabos de par trançado de cobre das linhas telefônicas comuns.
c) Fibra ótica é o meio físico utilizado em larga escala para compor a infraestrutura do *backbone* (parte central de uma rede) da Internet, devido tanto à alta taxa de transmissão admitida, quanto à baixa atenuação do sinal, mesmo a grandes distâncias.
d) *Power Line Communication* (PLC): utiliza a própria rede elétrica como meio de transmissão.

Utilizando-se do espectro eletromagnético, ainda existem o Wi-fi e o WiMAX. O primeiro para redes locais, de uso, muitas vezes, doméstico. E o segundo para provimento de banda-larga a longas distâncias. Além das muito empregadas pelos provedores de acesso à Internet móvel: *Global System for Mobile Communications* (GSM) em suas gerações 3G, 4G e, mais recentemente, 5G. Por fim, a Internet Satelital é bastante usada quando outras tecnologias se tornam excessivamente difíceis de serem aplicadas.

Entendemos agora, que independentemente de qual dos diversos meios (camada **física**) for utilizado, a camada de **enlace** se adaptará e utilizará os protocolos adequados para garantir que o roteamento entre emissor e receptor seja cumprido e permitirá e que a camada de **rede** entregue todos os datagramas recebidos da camada de **transporte**, que, por sua vez, foi a responsável por empacotar as informações recebidas da camada de **aplicação**, que é o mais alto nível e permite a interação humana.

Como este texto busca um tecnicismo mais acurado, perpassamos conceitos básicos de redes de computadores e, a partir deles, podemos tecer algumas observações a respeito de alguns pontos da definição de ciberespaço utilizada por Ventre e outros autores. Vamos então relembrar essa definição e analisá-la:

> “Uma primeira camada é constituída pela arquitetura material, física, hardware; ela é feita pelo conjunto de computadores, calculadoras, cabos eletrônicos (***hardware layer***). Uma segunda camada, média, denominada *software* ou aplicativa, é constituída pelo conjunto de programas, códigos, dados e algoritmos que dão vida ao ciberespaço (**software layer**). E uma terceira camada, informacional, é a do sentido, das informações (*news*), dos conteúdos (***meatware layer***).” (VENTRE, p. 77, 2019, grifo nosso).

A *hardware layer*, primeira camada, constituída pela arquitetura material, pode ser entendida como a junção das camadas física e de enlace do modelo de pilha de pacotes da Internet. A camada média, chamada de *software*, é uma simplificação das camadas de rede, transporte e aplicação. E com isso, esgotamos as camadas do modelo de pilha de protocolos de internet.

E aí aparece um primeiro problema: a terceira camada da definição utilizada por Ventre é a *meatware layer*. Ele dá a essa camada um sentido informacional, relacionando-a ao conteúdo. Mas como relacionar essa camada ao modelo de pilha de pacotes da Internet se já não há mais camadas a explorar?

Nem mesmo a tradução provida pela camada de apresentação, ou a sincronização proporcionada pela camada de sessão, que são camadas exclusivas do modelo de referência OSI, se enquadrariam nessa interpretação de *meatware*.

É razoável pensar que toda informação ou conteúdo no ciberespaço, na verdade são meramente dados, que podem fisicamente serem representados em formato de *bit*. Esse elemento já está contemplado nas outras camadas. Não haveria

necessidade de uma terceira camada para representar a informação, que seria, em última análise a interpretação e o sentido dos *bits*.

Além disso, a terminologia *meatware* possui uma conotação bastante relacionada às terminologias de *peopleware* e *liveware*. Que estão atreladas ao conceito de relacionamento humano com a virtualidade. O que acaba gerando certa confusão com as camadas que complementariam essa definição de espaço cibernético: a operacional e a humana, também citadas por Ventre.

Podemos pensar que esses seriam conceitos mais abstratos que fariam sentido em um entendimento mais geral e menos profundo da situação apresentada. Mas este texto se propõe justamente a fincar as bases técnicas como pressuposto teórico necessário para abordagens do ciberespaço.

Outro ponto que não podemos esquecer, é que, apesar de artificial, estamos falando de um espaço. Assim como os espaços terrestre, marítimo, aéreo e espacial, o espaço cibernético também permite a interação humana. Mas, obviamente, não é exclusividade do ciberespaço essa interação. Por este motivo, não vemos motivação para nomear essa interação com uma terminologia específica.

Em outro artigo, podemos perceber que Ventre ainda chama a nossa atenção para duas outras características que, essas sim, são exclusivas do ciberespaço: a primeira que o espaço cibernético é o único espaço desenvolvido pelo homem e a segunda que ele que perpassa todos os demais espaços geográficos (Ventre, 2011).

Podemos concluir então que, primeiro: sendo uma criação da humanidade, há uma capacidade humana gigantesca de alterar esse espaço quando comparada à capacidade de alterarmos os demais espaços geográficos. No momento que desligamos o nosso computador conectado a uma rede, ou colocamos nosso celular em modo avião, já estamos alterando o ciberespaço. Outros, com maior capacidade técnica, poderão influenciar muito mais, conforme comprovaremos ao longo deste trabalho.

Da segunda parte, podemos depreender que a influência sobre o espaço cibernético, pode implicar em influência nos espaços terrestre, marítimo, aéreo e espacial. Que nação se negaria à utilização de uma capacidade tão versátil?

Por fim, diante de todas as definições de espaço cibernético, com toda informação que colhemos até o momento, e conclusões a que chegamos, já é possível dizermos que entendemos o ciberespaço como um domínio criado pelo homem, interconectado, com propósito de armazenamento, processamento ou trânsito de informação, que apresenta composição passível de ser tecnicamente descrita desde sua infraestrutura física até o nível mais alto de interface com o usuário, que interfere diretamente nos demais espaços geográficos e admite, portanto, um relacionamento entre a realidade e o ambiente virtual tanto por ser formado por uma porção fisicamente tangível, quanto por permitir seu acesso ao usuário final.

De posse de um conceito formado de ciberespaço, o propósito de nosso próximo raciocínio será nos conduzir para um entendimento desse conceito, diante de outros, como território, fronteiras e soberania. Para facilitar, iremos retomar, neste ponto, algumas ideias apresentadas no capítulo anterior.

Gottmann (2012 [1975], p. 523) afirma ser o território “uma porção do espaço geográfico que coincide com a extensão espacial da jurisdição de um governo”. Lembremos que o espaço geográfico hoje se apresenta divido em cinco dimensões: terrestre, marítima, aérea, espacial e cibernética. Há nessa definição, então, o indício necessário para podermos entender o ciberespaço como uma espécie de território, ainda que constituído, em grande parte, de forma virtual. Ainda dela, depreendemos que a jurisdição de um governo, se estende ao ciberespaço.

Podemos corroborar nossa análise quando Gottmann afirma que o poder político se transformou diversas vezes ao longo da história, e por ser o território a “arena espacial do poder político” (2012 [1975], p. 523), este também sofreu modificações ao longo do tempo, como reflexo inerente a essa condição. Daí Gottmann conclui o território como uma expressão dos relacionamentos não apenas da política, mas também do tempo. Podemos depreender então, que as modificações no espaço geográfico, e por consequência, no território, causados pela criação do ciberespaço, implicam em um novo campo de atividade política que deve ser (e está sendo) explorado pelos Estados.

Mas se podemos entender o ciberespaço como um território, conforme já vimos, há a necessidade do estabelecimento de fronteiras pois, ainda que analisemos as fronteiras como Jacques Ancel, utilizando a ideia de isóbaras políticas ou como

Gottmann, que defende que não há necessariamente um conflito em uma fronteira, acordos e leis internacionais são necessários para o bom entendimento nos limites da soberania estatal sobre determinado espaço.

Quanto à tipologia de fronteiras, Ratzel logicamente ainda não previa uma fronteira cibernética. Mas será que podemos entender a soberania sobre a infraestrutura interna ao território geográfico de um país como alguma forma de garantia de segurança da informação?

Sem dúvidas o conceito de impenetrabilidade da nação de Morgenthau nos auxilia a entender essa problemática. “Em um determinado território, só uma nação pode exercer soberania” (MORGENTHAU, 2003, p. 571). Ora, ter a capacidade de colher informações sigilosas de determinado governo, dentro de seus limites territoriais não seria sobrepujar a soberania de quem decretou que tais informações não deveriam ser obtidas por quem não detivesse a devida autorização? Não caracterizaria então uma a violação da impenetrabilidade da nação? Logo, garantir que a infraestrutura interna não possa ser abusada por interesses estrangeiros, e garantir a soberania sobre ela, é sim uma forma de garantir a segurança da informação que por ela trafega. E sendo a infraestrutura física e tangível, seria possível delimitar um espaço interno às fronteiras terrestres acompanhado, até mesmo, pela tipologia ratzeliana.

Daniel Ventre tem uma visão similar à nossa no que diz respeito à necessidade da demarcação de fronteiras no ciberespaço e também se debruça sobre a parcela física que compõe o espaço cibernético:

> “Qualquer território sobre o qual o Estado impõe sua soberania é delimitado por fronteiras. No ciberespaço, elas devem ser imaginadas, inventadas. (...) Sua própria arquitetura (a primeira camada, física) presta-se facilmente a um fatiamento da rede bem próximo do corte do planeta em Estados: os cabos 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 – que poderiam ser os “pontos-fronteiras” (VENTRE, p. 78, 2019)

Ele explica que as funções de uma fronteira possuem características defensivas, como o controle de fluxo humanos, de mercadorias, de capitais e também de dados. E a partir disso, propõe a seguinte definição de fronteira cibernética: “lugar de exercício do poder de controle, de medida, de filtragem dos fluxos de dados, situado no interstício móvel, subjetivo, entre um ciberespaço nacional e o ciberespaço global.” (VENTRE, p. 79, 2019)

E, de fato, essa construção de fronteiras no ciberespaço está se consolidando no mundo:

> “Embora não seja reconhecido como tal nem publicamente endossado pela maioria dos líderes democráticos, um processo de regulação do ciberespaço está acontecendo, construindo os blocos iniciais de cercas virtuais nacionais emergentes. Uma nova “era vestefaliana cibernética” está lentamente emergindo à medida que os líderes de Estado se organizam para proteger seus cidadãos e suas economias individualmente e, inconscientemente, iniciam o caminho para as fronteiras no ciberespaço. (VENTRE, p. 79, 2019, apud DEMCHAK e DOMBROWSKI, 2011, pp. 32-61)

Um exemplo prático de ciber-fronteira estabelecida e, talvez o de maior sucesso no mundo hoje, é o exemplo chinês. A China, além da restrição ao acesso a sites e aplicações estrangeiras que não cooperam com sua política de sigilo de dados privados de usuários, chama a atenção do mundo por possuir arsenais tecnológicos como o sistema defensivo Projeto Escudo Dourado apelidado de *The Great Firewall of China* e outro de carácter ofensivo: The Great Cannon. O primeiro, implementado em 2003, encontra-se consolidado e auxilia no controle do fluxo de informações no país, além de barrar ameaças cibernéticas, baseando-se principalmente na capacidade de identificação global de IP (ENSAFI, 2015, p. 63). E o segundo, mais recente, implementa um sistema dissociado do primeiro, com capacidades ofensivas,

que utiliza máquinas que enviam qualquer tipo de solicitação a servidores chineses, respondem à solicitação com código malicioso que torna o usuário um participante não intencional de um possível ataque distribuído de negação de serviço (DDoS) a algum servidor de interesse (CNN, 2015).

O Projeto Escudo Dourado provê à China a capacidade de desconectar-se completamente da Internet em casos de detecção de ataque cibernético contra o Estado chinês, caracterizando uma fronteira bem delimitada de seu espaço cibernético e provendo a segurança necessária à informação nacional.

Dessa forma, fica claro que aquele Estado está em uma situação muito mais confortável do que a maioria, em relação à soberania sobre seu espaço cibernético, podendo inclusive, exercer grande influência em um espaço cibernético além de suas fronteiras, utilizando-se das capacidades providas pelo *Great Cannon*.

Neste momento, possuímos o embasamento teórico necessário para que no próximo capítulo analisemos o cenário brasileiro e verifiquemos o andamento do estabelecimento das fronteiras nacionais no ciberespaço.

CAPÍTULO III – ASPECTOS DA INFRAESTRUTURA DA INTERNET NO BRASIL

Agora é o momento de voltarmos a um ponto já citado neste texto, dando novamente atenção aos princípios elencados por Kahn e Cerf:

> "• Caixas pretas deveriam ser usadas para conexão das redes;
>
> futuramente seriam chamadas de *gateways* e roteadores. **Nenhuma informação seria retida pelos gateways sobre os fluxos de pacotes que trafegassem por eles**, mantendo-os, desta forma, simples e evitando adaptações e recuperação de vários modos de falha.
>
> • **Não deveria haver nenhum controle global nos níveis operacionais.**" **(**LEINER et al., 2009, p. 24, tradução nossa, grifo nosso)

A motivação que nos leva a focar nos trechos por nós grifados são as evidências recentes de proteção nacional envolvendo tecnologias de rede. Essa proteção, em teoria, se torna paradoxal, pois contradiz os princípios elencados por Robert Elliot Kahn e Vint Cerf.

Os Estados Unidos intervieram nas negociações com a chinesa Huawei impedindo a implementação da tecnologia de 5G chinesa em território norte-americano, alegando possibilidade de espionagem das informações que trafegassem por aquela rede (BBC, 2019).

A tecnologia da Huawei se torna, quando implementada, uma infraestrutura componente da internet e as premissas apresentadas por aqueles que muito contribuíram para o desenvolvimento da rede mundial preveem não haver controle do tráfego nos níveis operacionais, e vão além disso, afirmando que as informações, em forma de fluxo de pacotes, não sejam retidas nos gateways componentes da rede. Se há uma acusação por parte do governo dos Estados Unidos a respeito de espionagem a partir de uma infraestrutura de rede, deduzimos que há o descumprimento dessas premissas. Com essa primeira dedução podemos encadear

um raciocínio que nos conduzirá a três conclusões intermediárias e uma conclusão que nos norteará durante este capítulo.

A primeira: Se há uma acusação sobre a possibilidade de espionagem dos dados que trafegam sobre uma determinada tecnologia de rede, significa que os princípios propostos sobre o não controle global nos níveis operacionais e sobre o não armazenamento dos dados trafegados podem, ambos, serem burlados: ou seja, existe o princípio, mas não há absolutamente nenhuma implementação nos protocolos que garantam o seu cumprimento.

A segunda conclusão: Aquele que acusa, seja por rivalidade econômica, seja por manutenção do sigilo de seus dados, obviamente tem total ciência da situação apresentada na primeira conclusão. Partindo desse princípio, nada garantiria que aquele também não se utiliza das mesmas ferramentas e procedimentos para auferir vantagens estratégicas ao seu Estado.

O raciocínio para expormos a nossa terceira conclusão já foi apresentado e acredito que estaríamos prontos para chegar a ela, mas como forma de fundamentação teórica, antes vamos observar o que nos diz E. H. Carr:

> “É um grande equívoco representar a luta entre as potências saciadas e as insatisfeitas como uma luta entre a moral, de um lado, e a força, do outro. É uma questão na qual, qualquer que seja o envolvimento moral, a política de força predomina de ambos os lados.” (CARR, 1981, p.139).

Tanto os Estados Unidos, quanto a China, agirão de acordo com seus interesses, sobrepujando os interesses dos menos desenvolvidos tecnologicamente. E, além disso, buscarão seus espaços, seja no campo do conhecimento, seja na área mercadológica. Caso seus interesses colidam, ambos buscarão os interesses de seus respectivos Estados.

As afirmações do parágrafo anterior são perfeitamente corroboradas pelo que disse E. H. Carr. De acordo com ele, não há sequer questão moral envolvida nessas

ações. Em toda relação entre Estados, sempre haverá aquele que detém a superioridade de força em relação aos demais, e, por este motivo, imporá sua vontade.

A força pode ser refratada em diversas capacidades. No nosso caso, estamos falando de tecnologia. Mais especificamente de redes de computadores. Já vimos que, em última instância, as redes, independentemente da tecnologia utilizada na implementação, são basilares para a formação do domínio cibernético. Daí, nossa terceira conclusão: os Estados detentores de tecnologias de rede mais avançadas se valerão dessa força para impor suas vontades aos demais.

O que busco evidenciar, e a conclusão conduzirá nosso raciocínio no decurso deste capítulo é: o Estado brasileiro necessita ter a certeza de que suas informações trafegam em uma rede segura. Que a integridade, a confidencialidade, a autenticidade, o sigilo e o não repúdio da informação sejam, de fato, garantidos quando esta está formatada em pacotes e trafegando pela internet, principalmente em território nacional. A dependência das tecnologias e empresas estrangeiras na implementação de nossa rede interna, é a oportunidade que outros Estados precisam para exercerem sua vontade, ao se aproveitarem da vertente tecnológica de sua força.

E é sob essa óptica que analisaremos a infraestrutura de rede nacional neste capítulo. Iremos verificar se estamos abrindo mão da soberania nacional, partindo dos pressupostos apresentados até aqui, avaliando quanto de nossa infraestrutura de rede componente da internet é, de fato, nacional e quanto é uma invasão do território nacional, permitida por meio de contratos de concessão de prestação de serviços de telecomunicações.

Dando prosseguimento à nossa análise, é interessante conhecermos alguns elementos componentes da infraestrutura da Internet. O primeiro deles, os Pontos de Troca de Tráfego (PTT). Vamos dar uma atenção a eles, pois são componentes críticos do modelo atual da Internet.

> “Por definição o **PTT é uma infraestrutura compartilhada que é instalada em uma região para receber a conexão de Sistemas Autônomos** (SA) - através de *peering* - com o objetivo principal de

> otimizar o desempenho da Internet ao manter a troca de tráfego mais localizada entre diferentes redes pertencentes a uma mesma região, diminuindo, assim, o número de saltos entres SAs próximos uns dos outros. Seu núcleo é bastante complexo em termos de quantidade de conexões porque hospeda centenas de membros, por isso requer equipamentos de alto desempenho capazes de processar altas taxas de pacotes por segundo (pps). Apesar dessa complexidade, sua arquitetura é simples de entender, uma vez que o **objetivo do PTT se resume em prover um ponto centralizado de conexão** através de uma *switching-fabric* baseada em tecnologia Ethernet." (BRITO, p. 3, 2015, grifo nosso)

Para avaliarmos o impacto deste componente na rede brasileira, basta observarmos os dados apresentados no artigo intitulado Anatomia do Ecossistema de Pontos de Troca de Tráfego Públicos na Internet do Brasil de Samuel Brito.

Tabela 1. PTTs Públicos em Operação no Brasil (PTTMetro)

-	Cidade	Estado	Código	*Looking Glass*	Gbps	Membros	Obs
01	Americana	SP	**AME**	lg.ame.ptt.br	0,30	9	
02	Belém	PA	**BEL**	lg.bel.ptt.br	1,66	13	
03	Belo Horizonte	MG	**MG**	lg.mg.ptt.br	3,02	34	
04	Brasília	DF	**DF**	lg.df.ptt.br	2,98	24	
05	Campina Grande	PB	**CPV**	lg.cpv.ptt.br	0,20	11	
06	Campinas	SP	**CAS**	lg.cas.ptt.br	2,58	33	(*)
07	Cuiabá	MT	**CGB**	lg.cgb.ptt.br	0,00	7	(*)
08	Caxias do Sul	RS	**CXJ**	lg.cxj.ptt.br	0,07	5	(*)
09	Curitiba	PR	**PR**	lg.pr.ptt.br	14,59	58	(1)
10	Florianópolis	SC	**SC**	lg.sc.ptt.br	1,05	32	(*)
11	Fortaleza	CE	**CE**	lg.ce.ptt.br	0,87	26	
12	Goiania	GO	**GYN**	lg.gyn.ptt.br	0,38	21	
13	Lajeado	RS	**LAJ**	lg.laj.ptt.br	0,00	7	(*)
14	Londrina	PR	**LDA**	lg.lda.ptt.br	1,45	31	
15	Manaus	AM	**MAO**	lg.mao.ptt.br	0,00	7	(*)
16	Maringá	PR	**MGF**	lg.mgf.ptt.br	0,06	14	(*)
17	Natal	RN	**NAT**	lg.nat.ptt.br	0,74	12	(*)
18	Porto Alegre	RS	**RS**	lg.rs.ptt.br	6,30	100	
19	Recife	PE	**PE**	lg.pe.ptt.br	0,03	13	
20	Rio de Janeiro	RJ	**RJ**	lg.rj.ptt.br	19,83	52	(*)
21	Salvador	BA	**BA**	lg.ba.ptt.br	1,78	41	(*)
22	São Carlos	SP	**SCA**	lg.sca.ptt.br	0,00	3	(*)
23	São José dos Campos	SP	**SJC**	lg.sjc.ptt.br	0,47	11	
24	São José do Rio Preto	SP	**SJP**	lg.sjp.ptt.br	0,03	8	(*)
25	São Paulo	SP	**SP**	lg.sp.ptt.br	334,27	550	(1)
26	Vitória	ES	**VIX**	lg.vix.ptt.br	0,22	20	

(1) Há filtros no LG que estão limitando a quantidade de rotas na tabela BGP.
(*) PTT com acesso indisponível ao LG, cujos dados foram fornecidos pelo NIC.br.

Fonte: Brito (2015, p. 6)

Nessa primeira tabela, podemos analisar o vulto do fluxo através dos PTTs no Brasil (coluna Gbps). O PTT de São Paulo, é o maior da América Latina com picos de

500 Gbps. E o PTT.br está entre os 10 que mais realizam trocas de tráfego no mundo (Brito, p. 2, 2015).

A tabela 1 já seria suficiente para tomarmos esse componente como relevante para nossa análise, mas algo muito interessante para nós é saber se os *Internet Service Providers* (ISP) (basicamente os provedores de acesso à Internet) se utilizam desses PTT. Daí observemos a próxima tabela:

Tabela 2. Perfil de SAs nos PTTs do Brasil

Classificação	Brasil (*)	DF	MG	RS	SP	VIX
1. Provedor de Internet	65,1% ± 20%	37,5%	55,9%	68,0%	73,1%	75,0%
1.1 Provedor de Trânsito	8,6% ± 09%	20,8%	14,7%	5,0%	5,6%	10,0%
1.2 Provedor de Acesso	56,5% ± 21%	16,7%	41,2%	63,0%	67,5%	65,0%
2. Provedor de Serviços	10,1% ± 07%	8,3%	8,8%	5,0%	12,5%	5,0%
2.1 Provedor de Conteúdo	3,2% ± 06%	0,0%	2,9%	3,0%	4,7%	0,0%
2.2 Provedor de Hospedagem	6,8% ± 05%	8,3%	5,9%	2,0%	7,8%	5,0%
3. Organização Pública	12,3% ± 21%	37,5%	20,6%	11,0%	4,4%	15,0%
3.1 Universidade Pública	1,8% ± 19%	0,0%	0,0%	2,0%	1,1%	0,0%
3.2 Governo	8,8% ± 13%	33,3%	17,6%	8,0%	2,2%	15,0%
3.3 Outros	1,8% ± 03%	4,2%	2,9%	1,0%	1,1%	0,0%
4. Organização Privada	12,6% ± 09%	16,7%	14,7%	16,0%	10,0%	5,0%
4.1 Universidade Privada	0,7% ± 03%	0,0%	2,9%	4,0%	0,0%	0,0%
4.2 Empresa Privada	10,4% ± 09%	16,7%	8,8%	10,0%	8,9%	5,0%
4.3 Outros	1,5% ± 09%	0,0%	2,9%	2,0%	1,1%	0,0%

(*) Média de todos os 26 PTTs brasileiros.

Fonte: Brito (2015, p. 8)

A média de utilização dos PTTs pelos ISPs é realmente relevante. E tende a aumentar, devido ao baixo custo da utilização da tecnologia e a otimização no tráfego provida por ela. Mas por que estamos apresentando os PTTs neste texto?

Dado o vulto do ecossistema da Internet, precisamos focar em um ponto relevante de sua infraestrutura para retirarmos conclusões gerais a respeito dela. A importância dos PTTs, a forma como ele é entendido ao redor do mundo e o modelo de negócios que se utiliza para sua implementação e manutenção permitem que eles sejam explorados com esse propósito.

> “O modelo de negócios do PTT pode ser de natureza privada - comum nos Estados Unidos - ou aberta, como acontece na Europa e no Brasil. Na maioria dos casos, inclusive no Brasil, o objetivo principal do PTT e prover um ambiente aberto e indiscriminatório de natureza pública para estimular a colaboração e melhorar a troca de tráfego, alavancando a qualidade da Internet na sua região de operação.” (BRITO, p. 4, 2015)

Aí então entramos em uma discussão proposta por Deibert e repercurtida por Walfredo.

> “(...) o modo como solucionar ou evitar conflito nesse novo espaço vai depender em grande parte do regime de governo de cada país. Para ele, Rússia, China e outros países em ascensão defendem uma maior *territorialização* desse espaço, um maior controle por parte do ente estatal, 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), correspondente ao *global common* de Barry Posen (2003, pp. 7-8), de Rodrigues (2012, p. 5) e de Ferreira (2012, p. 70).” (WALFREDO, p. 86, 2013, apud DEIBERT, 2012, grifo nosso)

Um ponto pode ser levantado nessas duas questões. Tomando como base os PTTs, que já virmos serem relevantes para o ecossistema da Internet, e os Estados Unidos serem favoráveis ao seu controle de natureza privada, por que motivo o mesmo Estado seria favorável ao uso global comum do ciberespaço?

A natureza privada da infraestrutura de rede nos Estados Unidos parece óbvia quando falamos do centro mundial do capitalismo hodierno. Mas acaba por contradizer sua postura favorável à manutenção do ciberespaço como um espaço global de uso comum, quando a maior parte das empresas detentoras dos PTTs são nacionais. E se torna ainda mais contraditória quando observamos o Estado interferir no setor privado de infraestrutura de redes, como no caso já citado da Huawei, e impedir o acesso a empresas estrangeiras.

Walfredo, em seu raciocínio, declara enxergar nessa discussão paralelos acerca dos princípios das 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, entre outros, no Direito Internacional a fonte de solução de conflitos." (WALFREDO, 2013, p. 86)

Já dissemos neste texto que não estamos abordando questões morais. O que queremos evidenciar é que o Estado brasileiro precisa observar tanto o protecionismo norte-americano relativo às questões de infraestrutura de redes motivado pela segurança nacional, quanto a postura, por vezes, contraditória dos liberais que defendem a Internet como bem comum global. E, nesse sentido, analisar se a forma que o *backbone* nacional se apresenta é seguro para garantir a soberania nacional sobre o ciberespaço brasileiro, ou seja, aquele compreendido entre as fronteiras nacionais.

AT&T, a Verizon, a Level 3, a Qwest e Sprint. Todas grandes empresas norte-americanas do setor de telecomunicações. Controlam não só o *backbone* nos Estados Unidos, bem como detêm o controle de grande parte do cabeamento submarino ao redor do globo (FEDERAL COMMUNICATIONS COMMISSION, p. 9, 2010). E a situação no Brasil? Quais as maiores empresas do ramo atuando em nosso território? Como se dá nossa conexão ultramarina?

Os Relatórios de acompanhamento do setor de telecomunicações da Agência Nacional de Telecomunicações (Anatel) apresentam um panorama geral do *market share* no Brasil:

Tabela 3: *Market Share* de acessos de SCM por grupo econômico, 2009 a 2019 (1T)

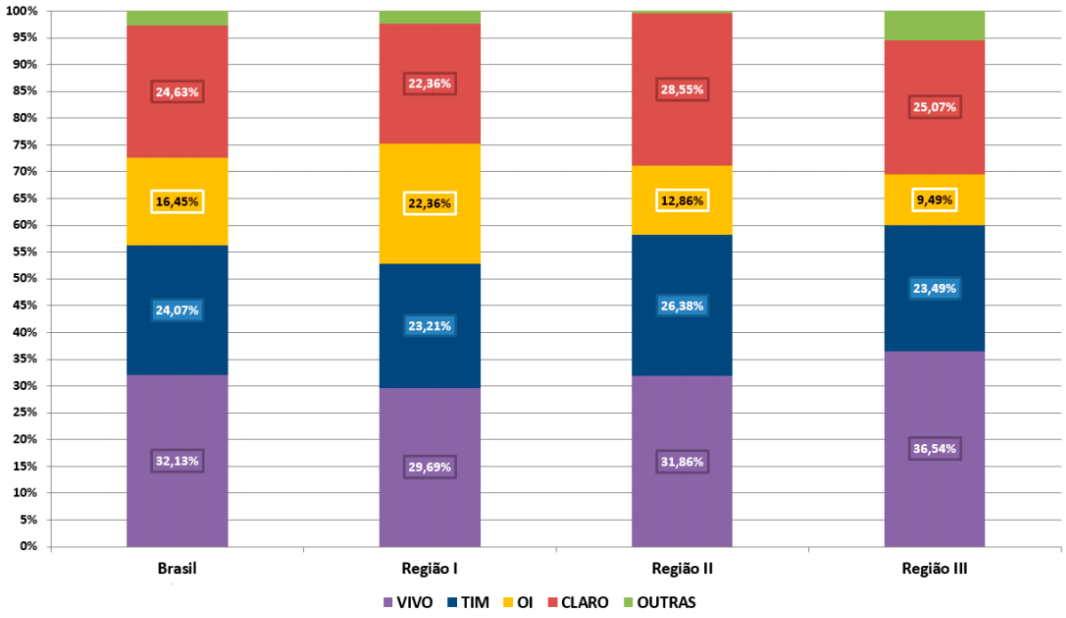
Evolução do *market share* de banda larga fixa, Brasil, 2009-2019 (1T)

Considerando o critério Prestadora de Pequeno Porte (PPPs) até 5% do mercado de varejo

Região	Grupo/Empresa	Anos										
		2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019 (1T)
Brasil	OI	38,2%	32,8%	31,8%	31,5%	29,5%	27,3%	25,0%	24,0%	21,8%	19,2%	18,4%
	VIVO	24,5%	24,3%	22,1%	19,6%	19,4%	17,1%	16,0%	27,9%	26,2%	24,3%	23,6%
	GVT	5,4%	7,3%	9,0%	10,8%	11,4%	12,3%	12,5%	0,0%	0,0%	0,0%	0,0%
	CLARO/NET	12,0%	21,5%	27,7%	28,4%	29,7%	31,4%	31,8%	31,8%	30,8%	30,0%	29,7%
	TIM	0,1%	0,1%	0,2%	0,2%	0,4%	0,6%	1,0%	1,2%	1,4%	1,6%	1,6%
	SKY/DIRECTV	0,0%	0,0%	0,0%	0,0%	0,1%	0,4%	1,0%	1,2%	1,3%	1,1%	1,0%
	Outras (PPPs < 5%)	19,7%	14,1%	9,2%	9,5%	9,6%	10,8%	12,6%	13,9%	18,5%	23,7%	25,6%

Fonte: Anatel – SCM (2019, p. 11)

Figura 1: *Market Share* de acessos de SMP, Brasil e Regiões I, II e III



Fonte: Anatel – SMP (2019, p. 06)

A tabela 3 lista o *market share* dos ISP de banda larga fixa, ao passo que a figura 1 apresenta um gráfico com a mesma informação, mas relativa aos provedores de serviço móvel pessoal (SMP) ou, simplificando, às operadoras de banda larga e telefonia móvel.

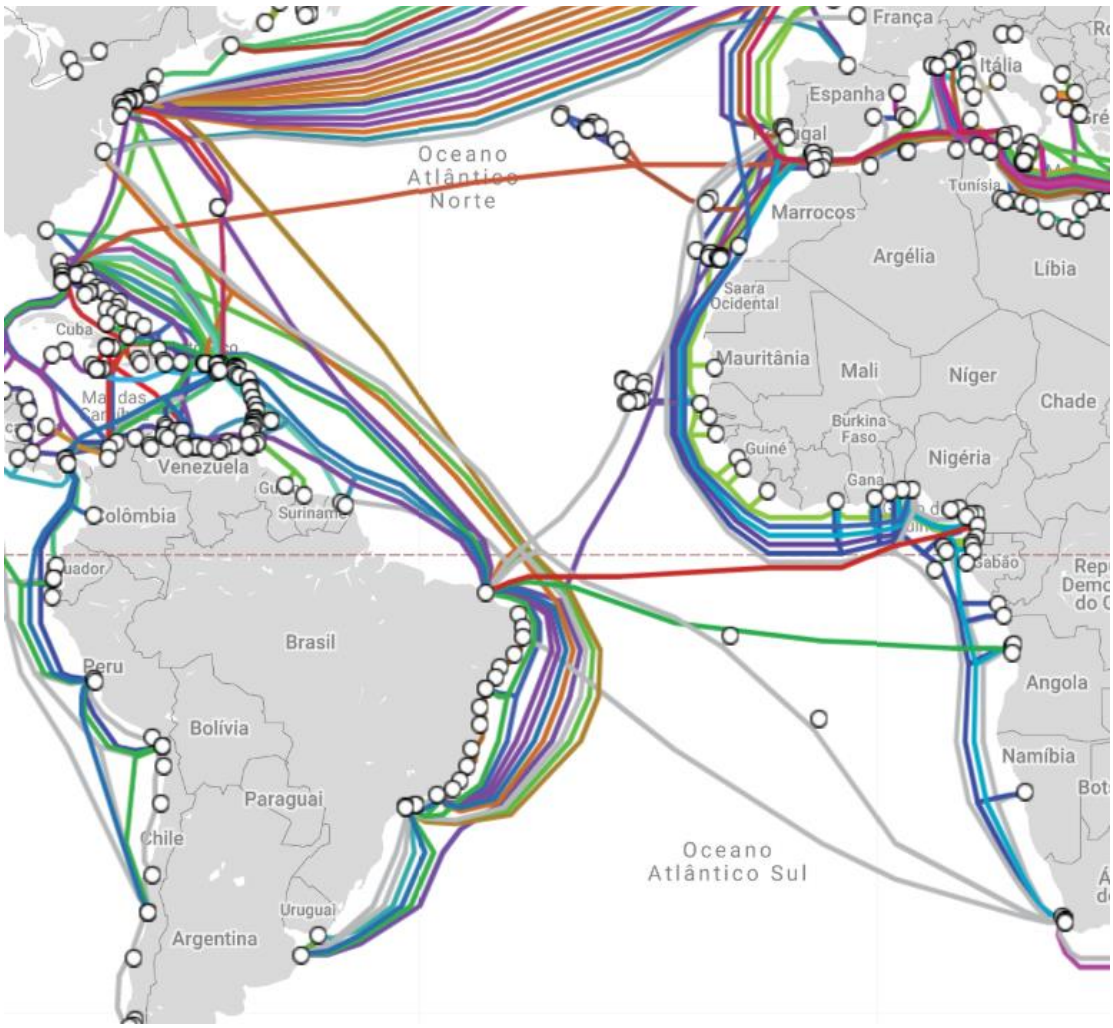
Em ambos os casos podemos observar que os ISPs que se destacam em vantagem avassaladora sobre os demais são: Vivo, TIM, Claro e Oi. No serviço fixo, temos mais de 70% dos contratos sendo operados por esses ISPs. Ao passo que no serviço móvel a situação é ainda mais discrepante, com quase 95% do mercado sob controle de 4 ISPs.

A marca comercial Vivo faz parte da empresa Telefônica Brasil, que por sua vez é uma empresa do Grupo Telefónica, que é uma empresa espanhola. A TIM Brasil é uma subsidiária da Telecom Italia. A Claro é uma marca comercial da América Móvil, que é mexicana. E o Grupo Oi, que dentre as quatro maiores, é a que detém a menor fração dos mercados citados, é uma multinacional luso-brasileira que vem sofrendo para se manter no mercado e corre risco de ser adquirida total ou parcialmente pela Telefônica. (EXAME, 2019)

O *backbone* brasileiro, querendo ou não, está muito mais relacionado a essas empresas do que a instituições nacionais como o PTT.br ou à própria Anatel. Não possuímos uma fronteira bem definida sob nenhum ponto de vista, pois nossa infraestrutura não é de domínio nacional. Mas podemos depreender das figuras que os Provedores de Pequeno Porte (PPP) têm ganhado força nos últimos anos alcançando em 2019 os melhores índices tanto em telefonia móvel quanto em banda larga fixa.

Por fim, analisemos o cabeamento submarino oceânico componente do *backbone* da Internet mundial que passa pelo Brasil. Para essa análise o serviço *Submarine Cable Maps* mantido pela TeleGeography nos auxiliará.

Figura 2. Mapa do Cabeamento Submarino na costa brasileira



Fonte: submarine cable map (2019)

Há dezenove cidades no Brasil com conexões submarinas. Mas destas, quinze são de conexões entre cidades brasileiras. Nos resta como análise em termos de conexão a nível mundial, apenas quatro cidades.

Fortaleza é a cidade com o maior número de cabos submarinos internacionais. São catorze cabos ligando o Brasil a países da América do Norte, Central e do Sul, além da Europa e da África. Recife possui um cabo submarino que nos conecta à África do Sul. Dois cabos em Praia Grande e três em Santos provêm conexão com outros países da América do Sul. Todos os cabos submarinos que tocam a costa brasileira são de empresas estrangeiras.

Ao longo deste texto, tentamos mostrar que a infraestrutura, por ser a base criadora e parte do espaço cibernético, deve ser olhada com cuidado e atenção, para que o país possa realmente garantir sua soberania no ciberespaço, ao menos dentro de suas fronteiras geográficas. Fronteiras essas que podem sim, vir a possuir certa coincidência com a infraestrutura de redes principal do país como acontece na China, ou, como acontece nos Estados Unidos, ao manter sua infraestrutura com empresas primordialmente nacionais.

Os países citados possuem capacidades de projeção no domínio cibernético que talvez não tenhamos pretensão de alcançar. Mas o que não podemos é permitir que outro Estado exerça soberania sobre o nosso território, seja em que dimensão for.

No caso do domínio cibernético, o primeiro passo para garantir essa soberania é garantir um vínculo nacional das empresas que detém o *backbone* do país. Qualquer outra medida de proteção, defesa cibernética ou criação de ciber-fronteiras, se torna fraca e passível de ser até mesmo inócua sem que esse primeiro passo seja dado.

CONCLUSÃO

É necessário o fomento à indústria de tecnologia para que o Brasil crie as condições necessárias que garantam a soberania nacional sobre o ciberespaço intra-fronteiriço. O espaço cibernético é integrado a diversos setores de uma nação e é dessa integração que o Estado brasileiro deve se valer para que a indústria nacional cresça.

A Estratégia de Defesa Cibernética norte-americana deixa clara essa integração logo em seu prefácio: “O Espaço cibernético é componente indissociável dos setores social, financeiro, governamental e político dos Estados Unidos.” (ESTADOS UNIDOS DA AMÉRICA, 2019)

Em termos de estratégias de segurança cibernética, outra nação que aborda de forma holística a temática é a Austrália. Pode-se observar que ela não se limitou a abordar o tema do ponto de vista da Defesa, mas elaborou em 2016 a Estratégia de Segurança Cibernética da Austrália e incluiu diversas áreas do Governo, como a economia e o meio acadêmico. A sinergia dessas áreas em prol de um objetivo único tem obtido resultados excelentes para aquele país (AUSTRÁLIA, 2016).

No que tange à economia, a citada documentação aborda incisivamente a economia digital, abrangendo modelos de negócios disruptivos como *Big Data*, *Internet* móvel e computação em nuvem. A documentação reflete sobre a relevância desse ramo da economia, e prevê a movimentação, a partir de 2030, de 625 bilhões de dólares por ano na região do Pacífico Oriental.

O Governo Australiano deixa clara, em sua documentação, a importância da necessidade de garantir a confiabilidade a nível mercadológico e se propõe a se posicionar como um polo de inovação na segurança cibernética, ao estabelecer um Centro de Desenvolvimento da Segurança Cibernética ao custo de 30 milhões de dólares que, por sua vez é responsável pela criação de uma rede de pesquisa e inovação na área, com a partição do governo, academia, empresas, start-ups de forma que a Australia seja capaz de criar soluções competitivas a nível global. Conta esse novo Centro com uma parceria mais acirrada entre pesquisadores e empresários,

melhoria na gestão e habilidades dos trabalhadores, acesso facilitado ao mercado internacional e reforma regulatória.

Quanto ao foco deste trabalho, o Estado australiano implementou ao custo de 48 bilhões de dólares ao longo de oito anos, a Rede Nacional de Banda-Larga, definindo assim, uma infraestrutura física de rede nacional e garantindo o controle de uma infraestrutura crítica no que tange à segurança cibernética e possibilitando a criação de uma ciber-fronteira que permite que a Austrália exerça soberania sobre seu espaço cibernético.

Daí se observa a evolução da normatização, da infraestrutura de segurança, da interação com outros órgãos e atores a nível nacional e internacional e, principalmente, da cooperação técnica e da capacitação em segurança cibernética a serem promovidas pelo Governo Australiano, em busca da referida meta. O plano integra a segurança cibernética ao desenvolvimento do país e dos cidadãos ao passo que gera oportunidades de negócio, criando empregos e parcerias com instituições acadêmicas com linhas de pesquisa específicas para a segurança cibernética promovendo a cooperação técnica e a capacitação em segurança cibernética. Trata ainda a Segurança Cibernética como um investimento na economia do país, que objetiva atração de novos investimentos, manutenção dos antigos e criação de empregos diretos e indiretos devido ao aumento da confiabilidade da segurança cibernética no país (AUSTRÁLIA, 2016).

Ao observarmos as ações desse país, chegamos à conclusão de que Estratégia de Segurança Cibernética australiana planeja implementação de capacidades cibernéticas defensivas e ofensivas que permitem deter e responder ataques a cibernéticos e que qualquer medida implementada com intuito de dissuadir e responder a atividades cibernéticas maliciosas seria sempre consistente com as regras e leis internacionais, procurando promover a interação com órgãos e atores internacionais. Essas ações colocadas em prática geram um efeito dissuasório extremamente relevante para a soberania australiana e coloca a Austrália na liderança da temática no Indo-Pacífico, sendo fator relevante no equilíbrio de forças naquela porção geográfica.

A superioridade tecnológica denota superioridade de poder na esfera das relações internacionais. A capacidade de projetar poder cibernético é uma realidade irrefutável, e deixar de possuí-la diminui sobremaneira o poder dissuasório do Estado.

Ainda mais perigoso que não possuir capacidade de projeção é permitir que outros Estados se projetem sobre o seu, invadindo as fronteiras nacionais e ferindo a soberania. Desenvolver uma infraestrutura nacional implica em vultosos investimentos em ciência e tecnologia aplicadas nas mais diversas áreas, como vimos no caso australiano. Almejar essas capacidades depende do interesse nacional que, por sua vez, passa pela intenção da sociedade.

Daí se conclui que o conhecimento dos assuntos de interesse nacional, ainda que de forma perfunctória, deve ser disseminado, permitindo assim, que o povo observe a relevância do desenvolvimento tecnológico para a soberania do país. A partir daí, apoie iniciativas do governo que fomentem essa área, gerando os interesses nacionais necessários para que diretrizes governamentais sejam orientadas a criar as capacidades de desenvolvimento da ciência e tecnologia de forma a aproximar determinada nação do patamar de poder das grandes potências.

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Anatel). Assessoria Técnica da Anatel. Relatório de Acompanhamento banda larga fixa 1º trimestre de 2019. Brasília, 2019. Relatório.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Anatel). Assessoria Técnica da Anatel. Relatório de Acompanhamento serviço móvel pessoal (SMP) 1º trimestre de 2019. Brasília, 2019. Relatório.

AMÉRICA, ESTADOS UNIDOS DA. **Department of Defense Dictionary of Military and Associated Terms**. [S.L.]: Departamento de Defesa (DoD), 2008.

AMÉRICA, ESTADOS UNIDOS DA. *National Cyber Strategy of the United States of America*, SETEMBRO DE 2018.Washington, DC, set 2018.

AUSTRÁLIA. *Australia's Cyber Security Strategy*, ABRIL DE 2016. Austrália, abr 2016.

BBC. 5 razões pelas quais os EUA estão tão preocupados com a Huawei. BBC, 21 mai. 2019. Disponível em: https://www.bbc.com/portuguese/geral-48347931. Acesso em: 17 out. 2019.

BRASIL. Exército. **EB70-MC-10.232: Guerra Cibernética**. 1. ed. Brasília, DF, 2017.

BRASIL. **Doutrina Militar de Defesa Cibernética**. Ministério da Defesa.: 1 ed. Brasília, 2014. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 12 out. 2019.

BRITO, Samuel Henrique Bucke et al. Anatomia do ecossistema de pontos de troca de tráfego públicos na internet do brasil. **XXXIII Simpósio Brasileiro de Redes de Computadores (SBRC). Vitória, ES, Brazil**, 2015.

BRUMFIELD, Ben. Study: China cybercensors attack outside its borders with 'Great Cannon'. CNN, 13 abr. 2015. Disponível em:

https://edition.cnn.com/2015/04/12/china/china-cyber-censorship-weapon/. Acesso em: 17 out. 2019.

CARR, Edward H.. Vinte anos de crise: 1919-1939. Brasília, Editora Universidade de Brasília, 1981.

CATAIA, Márcio Antônio. Fronteiras: territórios em conflito. **Geografia em questão**, v. 3, n. 1, 2010.

ENSAFI, Roya et al. Analyzing the Great Firewall of China over space and time. Proceedings on privacy enhancing technologies, v. 2015, n. 1, p. 61-76, 2015.

EXAME. Presidente da Telefônica diz que, se Oi estiver à venda, avalia a compra. EXAME, 15 out. 2019. Disponível em https://exame.abril.com.br/negocios/se-oi-vender-ativo-teremos-que-olhar-diz-presidente-da-telefonica/. Acesso em: 24 out. 2019.

FEDERAL COMMUNICATIONS COMMISSION. Statistics of communications common carriers 2006/2007 edition. 2010.

GOTTMANN, Jean. A evolução do conceito de território. **Boletim Campineiro de Geografia**, v. 2, n. 3, p. 523-545, 2012 (1975).

KLEINROCK, Leonard. An early history of the internet [History of Communications]. **IEEE Communications Magazine**, v. 48, n. 8, p. 26-36, 2010.

KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet. **Uma nova**, 2006.

LEINER, Barry M. et al. A brief history of the Internet. **ACM SIGCOMM Computer Communication Review**, v. 39, n. 5, p. 22-31, 2009.

MORGENTHAU, Hans J. A política entre Nações. 2003.

RATZEL, Friedrich. A relação entre o solo e o Estado-Capítulo I. O Estado como organismo ligado ao solo. **GEOUSP: Espaço e Tempo (Online)**, n. 29, p. 51-58, 2011 (1897).

TANENBAUM, Andrew S. et al. Computer networks, 4-th edition. ed: Prentice Hall, 2003.

VENTRE, D. 2011. Ciberguerra. In: Academia General Militar. Seguridad global y potências emergentes em um mundo multipolar. XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza

VENTRE, Daniel. O dilema da fronteira virtual: Quando os Estados se tornam construtores de ciberfronteiras. **Dilemas-Revista de Estudos de Conflito e Controle Social**, p. 75-96, 2019.

VESENTINI, José William. Repensando a Geografia Política. Um breve histórico crítico e a revisão de uma polêmica atual. **Revista do Departamento de Geografia**, v. 20, p. 127-142, 2010.