Escola de Comando e Estado-Maior do Exército
Escola Marechal Castello Branco
Instituto Meira Mattos
Programa de Pós-Graduação em Ciências Militares

Lucas Soares Portela

Movimentos Centrais e Subjacentes no Espaço Cibernético do século XXI

Rio de Janeiro
2015

LUCAS SOARES PORTELA

Movimentos Centrais e Subjacentes no Espaço Cibernético do século XXI

Linha de Pesquisa: Estudos da Paz e da Guerra

Dissertação apresentada ao Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército para obtenção do título de Mestre em Ciências Militares

Orientadora: Prof.ª Dr.ª Selma Lúcia de Moura Gonzales

Rio de Janeiro

2015

LUCAS SOARES PORTELA

MOVIMENTOS CENTRAIS E SUBJACENTES NO ESPAÇO CIBERNÉTICO DO SÉCULO XXI.

Dissertação apresentada à Escola de Comando e Estado-Maior do Exército como requisito parcial para a obtenção do título de Mestre em Ciências Militares.

Aprovada em 16 de novembro de 2015.

BANCA EXAMINADORA

SELMA LÚCIA DE MOURA GONZALES – Maj (Drª) – Presidente
Programa de Pós-Graduação em Ciências Militares
Escola de Comando e Estado-Maior do Exército

RAFAEL ANTONIO DUARTE VILLA – Prof Dr – Membro
Universidade de São Paulo

ADRIANA APARECIDA MARQUES – Profª Drª – Membro
Programa de Pós-Graduação em Ciências Militares
Escola de Comando e Estado-Maior do Exército

Ciente

LUCAS SOARES PORTELA – Postulante
Programa de Pós-Graduação em Ciências Militares

Dedico essa obra a Deus, razão do meu viver e do meu servir. Além Dele, agradeço principalmente à minha família e à Franciele, pessoas que amo muito e que me apoiaram na realização deste trabalho.

AGRADECIMENTOS

Certa época, o Irmão de Assis disse que o maior desagrado que um homem pode ter não é perder suas riquezas ou bens materiais, mas perder sua honra e orgulho. Da mesma forma, digo que o maior agrado que um homem pode receber de outras pessoas não são bens ou numerários, mas a valorização e dignidade humana. Esse trabalho não foi, dessa forma, fruto de meu esforço próprio, mas resultado do apoio, incentivo e convivência com diversas pessoas. Como o agradecimento a todas elas demandaria maior tempo, sem desmerecer qualquer um deles, gostaria de agradecer particularmente à algumas pessoas que foram marcantes no decorrer do meu mestrado:

- À **Deus**, pela oportunidade de aumentar minha sensibilidade divina e intelecto.
- À Professora Doutora **Selma Lúcia de Moura Gonzales**, por ter me adotado como orientando, pela paciência e interesse pela pesquisa e ideias incomuns.
- À Professora Doutora **Adriana Aparecida Marques**, pela disponibilidade em ler minha dissertação e pelos conselhos dados.
- Ao Professor Doutor **Rafael Duarte Villa**, por ter aceitado o convite de participar da banca e pelas orientações e considerações realizadas, essas foram de muita valia e preciosidade.
- À todos os **professores**, de modo geral, pelos ensinamentos transmitidos, não somente os referentes as matérias cursadas, mas também àqueles que dizem respeito a vida.
- Aos meus **pais**, pelo amor e por todas as vezes que acordaram de madrugada para me levar ou buscar no aeroporto, quando necessitava viajar para assistir aulas.
- Ao meu **irmão**, pelo amor, paciência ao me ver estressado e por estar ao meu lado nos momentos mais importantes e críticos da minha vida.
- A minha **namorada** e companheira, pela paciência de continuar me apoiando e me amando, mesmo quando a distância se demonstrou um problema.
- Ao **Instituto Meira Mattos**, por prover apoio tanto estrutural quanto pessoal durante os cursos realizados e essa pesquisa.
- À **Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)**, pelo fomento de pesquisa e possibilidade de me dedicar exclusivamente às pesquisas.

Para finalizar, desejo que através desses, meus agradecimentos sejam estendidos a todas as demais pessoas que possam ter influenciado essa pesquisa, de forma direta e indireta, pois sem eles o resultado final poderia não ter sido alcançado.

“Não sou come José Américo, que primeiro escreve na cabeça e depois transporta o livro para o papel. A obra de criação, para mim, é quase sempre imprevista. E espontânea. Refaço tudo, depois. Escrever dá muito trabalho. A gente muitas vezes não sabe o que vai fazer. Sai tudo diverso do que se imaginou.”

Graciliano Ramos

“O segredo e a simulação da mentira, que se contrapõem à transparência do poder, interligam-se, como observa Bobbio. Com efeito, as mentiras são parte do arsenal utilizado para resguardar o segredo, e o segredo permite o ocultamento da mentira.”

Celso Lafer

RESUMO

O espaço cibernético foi criado pelos homens e territorializado desde seu princípio. Sua encubação ocorreu dentro dos Estados Unidos, em instituições como o Instituto de Tecnologia de Massachusetts e o Departamento de Defesa estadunidense. Junto com o espaço cibernético surgem diversos dilemas e questões nas diversas ciências existentes. Nas Relações Internacionais, o espaço cibernético introduz questões sobre o Estado, sua existência, a soberania na rede da Internet, fronteiras, direito dos usuários, liberdade de navegação, defesa cibernética, dentre outros. Além das questões relacionadas a conceitos e teorias, o espaço cibernético apresenta uma dinâmica própria e peculiar das relações internacionais. Assim, o foco dessa dissertação são essas dinâmicas entre Estados e o objetivo geral dela é analisar as relações internacionais dentro do espaço cibernético no século XXI, no que tange aos movimentos centrais e subjacentes, especificadamente. Por ser uma dissertação com método de abordagem hipotético-dedutivo, a hipótese que direcionou a pesquisa foi: o espaço cibernético foi criado em território dos Estados Unidos, sendo esse o Estado com maior domínio e autonomia sobre ele. Para restringir este domínio ou garantir o exercício da soberania, os demais Estados formam movimentos subjacentes (alternativos e reacionários). Estes movimentos não se limitam somente aos atores estatais, também sendo observado nos demais atores. Desta forma, existe uma correlação entre movimento central dos Estados Unidos e movimentos subjacentes. Por meio desta, a dissertação identificou sete centros no espaço cibernético, a saber: Estados Unidos; Alemanha; China; França; Japão; Reino Unido; Rússia. Além da identificação dos países, os movimentos centrais mapeados foram o acordo *Safe Harbor* e o *Five Eyes Group.* Por sua vez, os principais movimentos alternativo e reacionário abordados foram o grupo BRICS e a proposta Brasil-Alemanha sobre privacidade no espaço cibernético, respectivamente. Esses movimentos subjacentes surgiram em resposta às revelações do Wikileaks e Edward Snowden sobre as atividades da *National Security Agency*. Logo, a relação entre os movimentos centrais e subjacentes foram comprovadas ao final da pesquisa, confirmando a hipótese proposta.

Palavras-Chave: Relações internacionais; movimentos centrais; movimentos subjacentes; espaço cibernético.

ABSTRACT

The cyberspace was created by men and territorialization happened since its inception. It was built in United States by institutions such as the Massachusetts Institute of Technology and the US Department of Defense. This cyberspace gives us many dilemmas and issues of various sciences. In International Relations, cyberspace introduces questions about the State, its existence, sovereignty in the internet, borders, rights of users, freedom of browsing, cyber defense, among others. In addition to issues, cyberspace has its own peculiar dynamics of international relations. Thus, the focus of this dissertation is these dynamics between States. The its goal is to analyze the international relations within the cyberspace in the twenty-first century, regarding the central and underlying movements, specifically. This dissertation work with hypothetical-deductive method of approach and the hypothesis that directed the research was: cyberspace was created in US territory, which is the State with greater control and autonomy over it. To restrict this domain or guarantee the exercise of sovereignty, other States form underlying movements (alternative and reactionary). These movements consist of State and other actors. Thus, there is a correlation between central movement of the United States and underlying movements. Through this, the dissertation identified seven centers in cyberspace: the United States; Germany; China; France; Japan; United Kingdom; Russia. In addition to the identification of countries, the central movements were mapped according the Safe Harbor and the Five Eyes Group. In turn, the main alternative movement was the BRICS group and the main reactionary movement was the Brazil-Germany proposal in the UN General Assembly about privacy in cyberspace. These underlying movements emerged in response to case of Wikileaks and Edward Snowden about the activities of the National Security Agency. Therefore, the relationship between the central and underlying movements were confirmed at the end of the study, claim the hypothesis proposed.

Keywords: International relations; center movement; underlying movement; cyberspace;

LISTA DE ILUSTRAÇÃO

LISTA DE GRÁFICOS E TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ArpaNET	Advanced Research Projects Agency Network
BRIC	Brasil, Rússia, Índia e China
BRICS	Brasil, Rússia, Índia, China e África do Sul
CCNSO	Code Names Supporting Organization
CFC	Comissão Federal do Comércio dos Estados Unidos
CGI.br	Comitê de Gestão da Internet do Brasil
CNUDM	Convenção das Nações Unidas sobre o Direito do Mar
CSCSS	Centro para Estratégias do Ciberespaço e Ciência de Segurança
DNS	Domain Name and System
EUA	Estado Unidos da América
FARCs	Forças Armadas Revolucionárias Colombianas
FMI	Fundo Monetário Internacional
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	Fórum de Governança da Internet
IPs	Internet Protocols
ISSO	Organização Internacional para Padronização
ISOC	Internet Society
MIT	Instituto de Tecnologia de Massachusetts
NSA	National Security Agency
OCDE	Organização para Cooperação e Desenvolvimento Econômico
OMC	Organização Mundial do Comércio
OMPI	Organização Mundial de Propriedade Intelectual
ONU	Organização das Nações Unidas
PIB	Produto Interno Bruto
TICs	Tecnologias de Informações e Comunicações
TOR	The Onion Router
UIT	União Internacional de Telecomunicação
W3C	World Wide Web Consortium
EZLN	Exército Zapatista de Libertação Nacional

SUMÁRIO

INTRODUÇÃO

O espaço cibernético é compartilhado por governos, organizações, empresas e indivíduos. Nele, as decisões de alguns dos atores citados interferem nas ações dos demais (BRASIL, 2010). Outras características importantes desse meio que podemos citar dizem respeito à sobreposição de soberanias e a insuficiência dos instrumentos de controle, que o torna o espaço cibernético ideal para a prática de crimes. Dado isto, os Estados e demais atores se articulam entre eles para tentarem garantir suas soberanias e seus interesses.

Embora os estudos sobre ciberespaço estejam evoluindo nesse século XXI, poucos se aventuraram especificamente sobre a questão das relações internacionais dentro do Espaço Cibernético. A maioria dos estudos, como no caso de Otávio Barros (2011), aborda essa problemática em pesquisas mais ampla sobre estratégia de defesa e segurança cibernética. Estas pesquisas reforçam a importância de se pensar defesa e segurança cibernética e tentam retratar a situação da realidade de alguns países e as tendências globais nesse espaço.

No entanto, outras pesquisas, como a de Mandarino Jr (2010), apresentam algumas questões especulativas, gerando reflexões sobre dilemas e desafios do espaço cibernético. Entretanto, em sua maioria, esses trabalhos abordam apenas aspectos teórico-conceituais da discussão. Por outro lado, existem estudos que analisam as possíveis formas de ataques e defesas cibernéticas de forma mais empírica, como nas pesquisas do coronel da Força Aérea Americana, Forrest Hare (2009).

A criação de regras e entendimentos entre os Estados no espaço cibernético permite uma relação mais pacífica entre eles, impedindo choques de soberanias e disputas excessivas de poder no cenário internacional (DINH, 2003; BARROS, 2011). Dentro dessa lógica, esta dissertação aborda a temática do espaço cibernético, sendo o objeto da pesquisa as relações internacionais. Sobre essas relações, a pesquisa focou os movimentos centrais e subjacentes.

Diante disto, o objetivo geral desta dissertação foi *analisar as relações internacionais dentro do espaço cibernético no século XXI, no que tange aos movimentos centrais e subjacentes*. Tal objetivo resultou da seguinte problemática: *quais as relações internacionais existentes dentro do espaço cibernético no século XXI, no que tange os movimentos centrais e subjacentes?* A não especificação sobre a abrangência das relações internacionais vislumbradas, ou seja, se contempla somente os Estados ou outros atores, foi assim optada porque todos os atores têm papeis importantes dentro do espaço cibernético.

Para responder tal pergunta e nortear essa pesquisa dissertativa, a hipótese de estudo foi: *o espaço cibernético foi criado pelos Estados Unidos, sendo esse o Estado com as principais empresas que detém o domínio e abrangência sobre esse espaço. Para restringir este domínio ou garantir o exercício da soberania, os demais atores formam movimentos subjacentes (alternativos e reacionários). Desta forma, existe uma correlação entre movimento central dos Estados Unidos e movimentos subjacentes.*

Essa hipótese nos instiga face aos últimos acontecimentos relacionados à invasão cibernética e a captação clandestina em massa de dados sensíveis de atores estatais pelos Estados Unidos, como aqueles evidenciados por Edward Snowden (HARDING, 2014). Ademais, as pesquisas referentes ao espaço cibernético podem explicar como os Estados são caracterizados em meio virtual; podem interpretar os elementos políticos e estratégicos envolvidos nas operações militares cibernéticas. Elas também exploram os sistemas de defesa desse espaço como instrumentos da capacidade dissuasória dos países e analisam como os fatores nacionais, transnacionais e internacionais colaboram para moldar a política e a estratégia de Estado.

Para verificar a hipótese apresentada e responder à problemática proposta, a dissertação perseguiu cinco objetivos: (I) Contextualizar o espaço cibernético e debater conceitos importantes como Fronteira, Regime Internacionais, Soberania e Espaço Cibernético; (II) Avaliar elementos teóricos sobre centros e poder cibernético, englobando as relações do tabuleiro de Joseph Nye; (III) Descrever empiricamente os conceitos de centros e a caracterização do poder desses Estados no espaço cibernético; (IV) Compreender os movimentos centrais e subjacentes no espaço cibernético.

Esta pesquisa, como demonstrado anteriormente, apresentou foco nas relações internacionais, em especial, nos movimentos centrais e subjacentes do espaço cibernético. Sendo o universo considerado os Estados e atores com maiores envolvimentos com questões do espaço cibernético. Diante deste universo, a dissertação utilizou uma amostragem teórica[1], que são os atores estatais envolvidos em arranjos internacionais específicos sobre espaço cibernético.

Dentre eles, podemos citar Estados Unidos, Alemanha, China, Reino Unido, França, Japão, Rússia, a União Europeia e o grupo BRICS. Junto com esses Estados encontramos também envolvimentos de outros atores não estatais, que embora não citados

[1] Em pesquisas de fundamentação teórica, de acordo com Antonio Gil (2010), o pesquisador deve selecionar uma amostra especifica que tenha efetivo envolvimento com o processo investigado, sendo chamada de amostragem teórica. O objetivo desta amostragem é encontrar variações entre os conceitos que permitam fortalecer a teoria que está sendo discutida (GIL, 2010).

como amostra, apresentam relações diretas com ela. Em virtude disso, outros exemplos que temos dessa relação com a amostra são: o caso da Irlanda e Estônia com o apoio da Microsoft contra o acesso ilegal a dados pessoais pelos Estados Unidos, os casos do Wikileaks e de Edward Snowden, dentre outros.

Sobre o recorte temporal, ele pode ser enquadrado em três categorias distintas: recorte longitudinal[2]; recorte transversal[3]; ou transversal com perspectiva longitudinal[4], de acordo com Richardson (1999). Dentre estas categorias de recorte, a utilizada na delimitação temporal desta dissertação é a transversal. Isto porque ela analisa mudanças que estão acontecendo nas relações internacionais sobre segurança e defesa cibernética, principalmente com as constantes revelações de espionagens, como no escândalo do Wikileaks (2010)[5] e no caso Snowden (2013)[6].

Considerando que a resposta da problematização foi sintetizada por uma hipótese, o método de abordagem utilizado foi o hipotético-dedutivo[7]. Em relação à abordagem de pesquisa, essa dissertação teve predominância de dados qualitativos (VAN EVERA, 1997). O tratamento desses dados ocorreu no nível de análise internacional.

Além disto, embora para cada objetivo de pesquisa aconselha-se um método de procedimento específico, essa escolha pode variar conforme o pesquisador (MARCONI & LAKATOS, 2003). Sendo assim, nessa dissertação utilizamos apenas um método de procedimento, o comparativo. Embora a aplicação deste método tenha sido utilizada mais efetivamente no final da dissertação, ele foi importante para os demais degraus. Isto porque para se realizar uma comparação é necessário compreender a realidade em que os fenômenos sociais estão inseridos.

Dessa forma, a primeira fase da dissertação analisou o espaço cibernético. Para tal foi necessário conceituar este espaço, compreender o conceito de soberania aplicado nele, como são delimitadas suas fronteiras, e os interesses que suportam a criação ou não de um regime internacional do espaço cibernético. Ao conceituar o espaço cibernético, a pesquisa

---

[2] O pesquisador delimita um período temporal para avaliar, por exemplo, o entre guerras (1918-1939) (RICHARDSON, 1999).

[3] Analisa um momento especifico da história, por exemplo, a promulgação da Constituição de 1988. Nessa categoria, parte considerável dos pesquisadores comparam os períodos anterior e posterior ao fato para confirmar suas hipóteses (RICHARDSON, 1999).

[4] Ela é a combinação dos recortes transversal e longitudinal, ou seja, o pesquisador delimita um ponto histórico especifico conjugado com a noção de mudanças ao longo de um período (RICHARDSON, 1999).

[5] Ocasião em que o fundador do Wikileaks, Jullian Assange, tornou público uma série de documentos secretos do Exército dos Estados Unidos que demonstravam as atividades de espionagem realizadas por aquele Estado.

[6] Caso semelhante ao do escândalo do Wikileaks em 2010, mas desta vez as revelações de espionagens foram feitas pelo ex-funcionário da Agência Nacional de Segurança (NSA – sigla em Inglês), Edward Snowden.

[7] Esse método testa a hipótese adotada com a geração de novos conhecimentos científicos (GIL, 2010).

retomou o histórico da construção do espaço cibernético, juntamente com seu processo de territorialização, e também abordou esse espaço como objetivo científico.

A abordagem da soberania dentro desse espaço foi possível por meio da compreensão das ameaças e fragilidades dos Estados nesse ambiente e os principais litígios existentes entre eles. Nisto, notamos a relativização da soberania em face da percepção dos Estados no século XXI e a demanda deles por uma soberania responsável. A necessidade de reavaliar a soberania no espaço cibernético é semelhante ao debate do conceito de fronteiras e de regimes internacionais nesse espaço.

Nessa perspectiva, para compreender tais inquietações, a dissertação analisou as características das fronteiras e como elas são notadas no espaço cibernético. A dissertação também observou os principais acordos e organismos internacionais sobre espaço cibernético. Ela adentrou também na teoria crítica para compreender a função dos regimes internacionais e verificou a percepção dos Estados Unidos sobre esse fenômeno na temática do espaço cibernético.

A segunda fase da pesquisa pretendeu teorizar os centros, os raios, os movimentos centrais e subjacentes. Para isso, além de analisar os Estados centros e os Estados raios do sistema internacional, também vislumbrou o poder cibernético e a sua difusão mundial. Ao abordar os centros e os raios, a pesquisa demonstrou que o mundo é historicamente formado por esses dois conceitos e debateu o que caracteriza um Estado como centro do sistema.

Na terceira fase, a pesquisa trabalhou na identificação e caracterização dos centros do espaço cibernético. Com pretensão de alcançar isto, o capítulo foi divido em dois momentos, a identificação dos centros e a caracterização deles. Para identificar os centros, o estudo abordou os dados referentes à penetração da internet no mundo; os controladores da internet e suas origens geográficas; e os principais produtores de conhecimentos. Na segunda parte, a dissertação avaliou o contexto sócio econômico; os marcos legais e regulatórios; e as infraestruturas tecnológicas de cada centro.

A quarta fase da dissertação utilizou o método comparativo mais enfaticamente. O objetivo desta fase foi comparar empiricamente os movimentos centrais, alternativos e reacionários. Esta fase foi dividida de acordo com os movimentos e com os atores envolvidos em cada um deles. Assim, cada seção analisa os movimentos centrais; alternativos e reacionários em três composições: com participação de Estados centrais, com participação de Estados raios e com participação de atores não estatais.

A técnica de pesquisa predominante em toda a dissertação foi a Documentação Indireta[8]. Além dessas técnicas, essa dissertação também utilizou a "Análise Interpretativa e Crítica"[9] e "Tomada de Apontamento"[10]. A partir delas, de acordo com Marconi & Lakatos (2003), o pesquisador tem a possibilidade de fazer críticas sobre os argumentos apresentados, retendo o mais significativo para a proposta da dissertação. Em ambas as técnicas, a coleta de dados é realizada, principalmente, por meio das "Fichas de Apontamento"[11].

Por fim, cabe evidenciar que as etapas descritas acima são fundamentais para a fase final da dissertação. A compreensão do espaço cibernético; a teorização dos centros e do poder cibernético; a identificação dos Estados centros e dos Estados raios do espaço cibernético; e a comparação entre movimentos centrais; alternativos e reacionários possibilitaram um debate final sobre a pesquisa. Este debate permitiu responder ao propósito da dissertação apresentado anteriormente: analisar as relações internacionais dentro do espaço cibernético no século XXI, no que tange os movimentos centrais e subjacentes, especificadamente.

[8] De acordo com Marconi & Lakatos (2003), esta técnica permite reunir material-fonte, sejam primários ou secundários, que servem de antecedentes ao campo de interesse, ou seja, permitem criar um panorama teórico conceitual do tema tratado.

[9] Essa técnica, também chamada de "Leitura Analítica", é composta por uma leitura integral das obras; identificação das ideias-chaves; hierarquização e sintetização de cada uma delas (GIL, 2010).

[10] A "Tomada de Apontamento" é uma técnica complementar da "Análise Interpretativa e Crítica", que serve como forma de reter as partes mais importantes de uma leitura (GIL, 2010)

[11] Existem fichamentos de diversas finalidades: fichas bibliográficas; fichas de resumo; fichas de sumário; fichas de citações entre outras (GIL, 2010). Nas "Fichas de Apontamento", o pesquisador tem a liberdade de anotar apenas o que é pertinente à proposta da dissertação, poupando tempo e gerando produtividade, pois os recursos intelectuais economizados são utilizados na etapa reflexiva.

1 PENSANDO O ESPAÇO CIBERNÉTICO

Quando falamos no dia-a-dia sobre espaço cibernético as pessoas costumam associar seu uso com os computadores. Entretanto, esse espaço alcançou dimensões maiores, estando presente em todos os lugares. Isso foi possível devido ao aumento da conectividade entre as pessoas.

A compreensão da relação entre movimentos centrais e subjacentes no espaço cibernético dependem diretamente do significado desse próprio espaço. Em virtude disso, o objetivo desse capítulo é compreender algumas questões sobre o espaço cibernético. Para tanto, realizamos aqui uma abordagem que está além da conceituação do espaço cibernético, interpelando também a questão da soberania, fronteiras e regimes internacionais.

Cada uma dessas questões auxilia para o restante do desenvolvimento da pesquisa, pois compreender a soberania no espaço cibernético permite entender os pontos de conflitos e o papel dos Estados nesse novo espaço. A compreensão das fronteiras favorece o entendimento de que além dos aspectos físicos, o espaço cibernético também é conectivo. Por fim, a discussão sobre regimes internacionais nos ajuda a compreender como eles vêm sendo organizados e qual a perspectiva sobre uma regulação mais abrangente acerca do espaço cibernético.

1.1 CONCEITUANDO O ESPAÇO CIBERNÉTICO

1.1.1 Histórico do Espaço Cibernético

Os espaços geográficos tradicionais sempre existiram, mas a exploração deles pelo ser humano ocorreu com o passar do tempo. Diferente desses espaços geográficos, o espaço cibernético foi criado pelo próprio homem. Em virtude disto, desde sua concepção, este espaço cibergeográfico sempre foi explorado e territorializado.

Por ser uma obra das mãos humanas, o espaço cibernético por vezes é percebido como uma região abstrata e resultante do imaginário de uma sociedade. Inclusive, de acordo com Richard Clarke (2010), diante do conceito de espaço cibernético, algumas pessoas recordavam e imaginavam algo semelhante ao filme *Matrix*[12]. Entretanto, este espaço apresenta tanto aspectos informacionais e virtuais como também aspectos estruturais e físicos.

[12] O filme retrata o Espaço Cibernético como uma dimensão negra com letras verdes flutuando alternadamente de cima para baixo e de baixo para cima.

Por causa do caráter abstrato e do ineditismo do espaço cibernético, encontramos uma variedade de autores tentando conceituá-lo de forma universal. Cada um deles se atém mais especificadamente a um aspecto distinto. Assim, encontramos autores que utilizam como referência para conceituação os aspectos informacionais e virtuais e outros que mais se aproximam dos aspectos estruturais e físicos.

O próprio Richard Clarke (2010), por exemplo, conceitua o espaço cibernético como toda a rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles. Ainda, conforme ele, o espaço cibernético não pode ser confundido com a conceituação de Internet, pois essa é o conjunto de redes menores e equipamentos conectados a ela. Assim, para esse autor, o conceito de espaço cibernético é mais abrangente, pois, além da Internet, ele também engloba todos os demais computadores não conectados e também seus equipamentos.

A adição das estruturas desvinculadas da Internet ao conceito de espaço cibernético é justificada pelo autor por meio da propriedade informacional. De acordo com ele, todos os computadores não conectados à Internet e as demais redes privadas[13] também dispõe de informações e dados que moldam o mundo. Por exemplo, neles encontramos flutuações de dinheiro, transações de créditos, comércio, e até sistemas de controle de elevadores, geradores e outras estruturas críticas.

Sob a perspectiva nacional, Rafael Mandarino Jr (2010) conceitua o espaço cibernético como o conjunto de infraestruturas críticas, os locais de armazenamento e processamento de dados e o conjunto de pessoas que interagem com esses sistemas. Para ele, as infraestruturas críticas são todos os *hardwares, softwares* e equipamentos que estão conectados por meio de fibras óticas ou ondas eletromagnéticas. Além dessas, ele também coloca dentro do conceito de espaço cibernético a própria informação.

Este autor apresenta uma visão de conceito semelhante àquela apresentada por Richard Clarke (2012) quando discorre sobre os elementos da infraestrutura crítica. Entretanto, Mandarino Jr (2010) considera mais dois elementos no conceito de espaço cibernético: as informações e os usuários. Devido a isso, enquanto Clarke (2012) vislumbra os meios em que a informação trafega como parte do espaço cibernético, Mandarino Jr (2010) considera a própria informação como fragmento desse espaço.

Sobre os usuários, Mandarino Jr (2010) considera os recursos humanos como parte do espaço cibernético. Esta é uma visão ousada, pois os usuários são operadores do

[13] Redes privadas são chamadas de intranets e não apresentam ligação com a rede mundial ou essa ligação é controlada e monitorada.

espaço e não componentes. Uma visão mais ilustrativa sobre o papel dos recursos humanos no espaço cibernético é aquela oferecida por Daniel Ventre (2011), em que divide o espaço cibernético em três camadas.

Esse pesquisador afirma que o espaço cibernético é composto por três categorias de elementos principais: *hardware, software e peopleware*. Ao definir essas categorias, Daniel Ventre (2011) deixa transparecer sua percepção sobre o conceito de espaço cibernético. A categoria *hardware* diz respeito a toda a estrutura física do espaço cibernético e a categoria *software* à dimensão virtual.

Por sua vez, a categoria *peopleware*, na percepção de Ventre (2011), é a camada cognitiva do espaço cibernético, ou seja, os operadores desse espaço. Assim, embora os usuários estejam englobados na definição de espaço cibernético, eles são diferenciados das outras duas categorias. Caso essa distinção não seja realizada, também poderíamos englobar como recurso do espaço terrestre, analogamente, as pessoas e até mesmo os veículos.

Cada um desses conceitos apresentam focos diferentes e também particularidades, como dito anteriormente. Embora Clarke (2012) faça distinção entre a Internet e o espaço cibernético, este somente se concretizou como espaço cibergeográfico por meio da rede mundial. Por isso, a história do espaço cibernético e da Internet por vezes se confundem.

O computador já existia quando a Internet começou a ser projetada. A história da invenção do computador começa com a própria Matemática, conforme demonstrado pela obra de Cléuzio Fonseca Filho (2007) intitulada "História da Computação". Além disto, este autor explica que os primeiros computadores eletromecânicos surgiram na década de 30 e o primeiro computador eletrônico comercialmente disponível surgiu em 1951 (FONSECA FILHO, 2007).

O trabalho que originou a Internet surgiu durante a segunda geração de computadores eletrônicos, na década de 1960. Nesta geração, além de um avanço tecnológico nos próprios computadores, foram desenvolvidos também dispositivos para uso conjunto, como impressoras, fitas magnéticas e discos de armazenamento (FONSECA FILHO, 2007). Enquanto isso, no Instituto de Tecnologia de Massachusetts (MIT), um grupo de pesquisadores tentavam criar uma rede para interconectar os computadores e permitir a troca de informação (KNIGHT, 2014).

Conforme Peter Knight (2014), o conceito de computadores conectados em redes surgiu no trabalho de Joseph Carl Robnett Licklider em 1962. Esse autor explica que o primeiro livro sobre o assunto somente foi publicado depois de dois anos de pesquisa. Entretanto, a idealização da Internet não se limitava à Massachusetts.

Outro pesquisador que também é considerado um dos pioneiros da Internet foi Paul Baran da RAND Corporation (KNIGHT, 2014). Esse pesquisador foi financiado pela Força Aérea dos EUA para desenvolver um sistema de comunicação descentralizado que garantisse a resiliência da força durante um ataque nuclear, conforme apontado por Knight (2014). Ainda de acordo com ele, este trabalho resultou em uma série de artigos em 1964 que desenvolvia uma arquitetura de rede.

Esses trabalhos resultaram no primeiro protótipo da Internet em 1969, chamado *Advanced Research Projects Agency Network* (ArpaNET). Ele era composto de quatro computadores localizados em universidades estadunidenses (KNIGHT, 2014). Peter Knight (2014) nos alerta que embora se entenda a Internet como um resultado de um projeto militar, ela surgiu como um projeto do Pentágono para induzir trocas de informação entre essas universidades.

A partir de então, novas inovações, teorias e conceitos foram incorporadas à Internet e aos Computadores. Em 1974, os pesquisadores Vint Cerf e Robert Kahn publicaram um artigo criando o TPC/IP (KNIGHT, 2012). Essa inovação permitiu a conexão de computadores com tecnologias distintas e que não faziam parte do projeto ArpaNET a Internet, ou seja, foi uma abertura daquela rede ao mundo (KNIGHT, 2014).

Desta forma, o espaço cibernético não é natural, como por exemplo, os espaços terrestre e aéreo, mas um espaço criado pelo próprio homem. Por ser um produto da ação humana desde sua origem, o espaço cibernético já surge territorializado. Essa territorialização é realizada através da rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles.

1.1.2 Territorializando o Espaço Cibernético

Os espaços geográficos clássicos – terrestre, marítimo e aéreo – apresentavam processos paulatinos de territorialização e com certa espontaneidade. A territorialização dos espaços contemporâneos – sideral e cibernético – são mais complexos e sistêmicos. Nesse tópico trabalharemos mais profundamente a territorialização do espaço cibernético.

De acordo com Raffestin (1993), o território é um espaço trabalhado pelos homens. O processo em que permite ao homem agir dentro de um território é chamado de territorialização. Entretanto, Robert Sack (1986) não aborda a territorialização como um conceito, mas como uma ferramenta política. Para ele, a territorialização é uma estratégica

geográfica poderosa, pois pode ser utilizada para controlar pessoas e coisas dentro de uma área, como também para interligar o espaço e uma sociedade.

A premissa de Sack (1986) pode ser vislumbrada nas histórias de todos os países, pois em algum momento delas existiram questões territoriais, de limites e fronteiras. Essas questões são tão complexas que alguns Estados responderam a elas com construções de muros para demarcar seus limites. Entre tais exemplos, encontramos a Grande Muralha da China e o Muro de Berlin.

Embora esses muros apresentem como principal função separar estados-nações, as tecnologias avançaram e aproximaram essas mesmas sociedades, superando cercas e muros. Isso já era notada quando o telégrafo era considerado tecnologia de ponta, pois a comunicação instantânea já acontecia (NYE JR, 2012). Atualmente, além da instantaneidade, a Internet possibilitou um aumento constante no volume de informação trocada por segundo, conforme apontado por Nye Jr (2012), ou seja, velocidade e quantidade.

O avanço tecnológico provocado pela globalização nos faz questionar sobre a validade da clássica ligação entre geografia e relações sociais. Um símbolo marcante de como essa relação era íntima pode ser visualizado no poema intitulado "*Mending Wall"*. Nele, Robert Frost escreve "boas cercas fazem bons vizinhos", demonstrando uma íntima ligação entre o território natalício e as relações sociais.

Sobre a permanência ou não do vínculo entre a geografia e as relações sociais, Bauman (1999) argumenta que a relevância da geografia está cada vez mais comprometida pela globalização. Para ele, as fronteiras e limites são cada vez mais insustentáveis, devido, principalmente, pelo aumento da mobilidade provido pelo avanço tecnológico. Contrário a ele, Robert Kaplan (2013) defende a relevância da geografia mesmo neste mundo globalizado. Debate similar acontece dentro das mudanças provocadas pela Internet.

Com o surgimento da chamada "Era da Internet", houve uma aclamação generalizada sobre o fim da geografia (CASTELLS, 2003). Alguns observadores, de acordo com Joseph Nye Jr (2012), acreditam que a "Era da Internet" marca o declínio do Estado soberano. No entanto, Nye Jr (2012) defende a continuidade dos Estados como atores dominantes das relações internacionais, mesmo com a oposição de outros autores. Logo, embora o espaço cibernético cause a sensação de abolição fronteiriça e fim da geografia, os limites geográficos e o poder estatal continuam sendo preponderantes na perspectiva de alguns autores emblemáticos das Relações Internacionais.

Para melhor compreender a territorialização do espaço cibernético é necessário entender também outros conceitos, como espaço, território, limites e fronteiras. Cabe

ressaltar, ainda, que a conceituação de cada um desses termos não é produto de um consenso ou de uma aceitação universal. Assim, não é pretensão desta dissertação explorar as discussões sobre cada um desses conceitos, mas fornecer parâmetros para os estudos do espaço cibernético.

Sobre as definições de "espaço", as que melhor satisfazem este trabalho são aquelas utilizadas por Milton Santos (1986) e Claude Raffestin (1993). De acordo com Santos (1986), o espaço é um campo em que atuam forças sociais. Diferente dele, Raffestin (1993) acredita que o espaço é algo dado e preexiste a qualquer ação, como se fosse uma matéria-prima. A principal diferença entre as duas definições é a relação do espaço com as forças sociais, enquanto para Santos (1986) o espaço é produto das interações sociais, para Raffestin (1993) ele pode existir sem tais interações.

Embora o conceito de "espaço" seja utilizado como sinônimo de "território" por parte de alguns autores, esse erro deve ser evitado. A diferença fica mais clarificada nos estudos de Raffestin (1993), pois enquanto ele observa o espaço como algo cru e preexistente ao território, este é vislumbrado como o local em que a ação humana se desenrola. Assim, ao passo que Milton Santos (1986) enxerga as ações como primordiais para a existência do Espaço, Raffestin (1993) considera essas ações apenas dentro do conceito de território.

Por ser um produto humano, o território é um dos três elementos básicos de um Estado-Nação, juntamente com o povo e a soberania (SANTOS, 1986). A utilização desse território é o que gera o local chamado Estado-Nação, conforme Milton Santos (1986). Cabe acrescentar que além de ser a porção terrestre do Estado, ele também abrange o subsolo e o céu acima dele (HUSEK, 2000).

Para delimitar um território, o ser humano utiliza limites e fronteiras. Esses dois conceitos não podem ser confundidos, como aponta Marcelo Varella (2012). Para ele, o limite é o ponto de intercessão entre os territórios de dois Estados e a fronteira é a região em torno dos limites. Devido a isto, também encontramos o termo zona fronteiriça ou zona de fronteira. O conceito de fronteira ou zona de fronteira é primordial para garantir a segurança dos limites de um Estado.

Com as conceituações realizadas anteriormente, a definição de Sack (1986) de que a territorialização é uma ferramenta política utilizada para controlar pessoas e interligar sociedade fica nítida. Embora essa primeira definição apresentada por Sack (1986) seja prática para compreender o processo de territorialização, ela é criticada pelo próprio autor. Ele se critica, pois considera que uma conceituação simples como essa é insuficiente para abarcar todas as consequências e implicações desse conceito.

Por isso, não cabe descartar a breve conceituação, mas abordar uma versão de sua definição mais complexa, também proposta por Sack (1986, p. 19). De acordo com essa segunda versão, a territorialização é "a tentativa de um indivíduo ou grupo de afetar, influenciar, ou controlar pessoas, fenômeno, e relações, por meio da delimitação e afirmação do controle sobre uma área geográfica" [tradução nossa][14]. Dessa forma, a territorialização serve para um indivíduo ou grupo e também para diversos propósitos.

A compreensão dessa nova versão do conceito de Sack (1986) é prática apenas quando visualizamos um pequeno espaço. Entretanto, quando pensamos em um grande espaço sofrendo um processo de territorialização, como o espaço cibernético, o que podemos observar é um vasto choque de interesses de diversos indivíduos e grupos. Todavia, a pergunta surge: qual o propósito de territorializar o espaço cibernético.

À vista disso, alguns autores apresentam anseios sobre o que fazer com o espaço cibernético, que podem ser divididos em dois extremos. O primeiro extremo é composto por aqueles autores que querem territorializá-lo e o segundo extremo por aqueles que querem evitar esse fenômeno. Ora, como dito anteriormente, territorializar é apropriar-se de um espaço, assim, desterritorializar o espaço cibernético é limitar as suas formas de controle.

Como dito anteriormente, o espaço cibernético foi criado e territorializado simultaneamente. Logo, ele foi criado com algumas ferramentas de controle, mesmo que insuficientes, como por exemplo, os quatro princípios que conduziu o ingresso de novas instituições na rede ArpaNET (CLARKE, 2012). O grupo que se posiciona contra o processo de territorialização, luta pelo uso livre do espaço cibernético, sem a influência e o controle de qualquer ator.

Assim, a territorialização do espaço cibernético pode ser figurada nos propósitos apresentados por alguns autores. Mandarino Jr (2010), por exemplo, explica a necessidade de se delimitar o espaço cibernético para se aplicar políticas de segurança e defesa. Outro propósito que podemos citar é aquele abordado por Ferreira Neto (2014), em que a territorialização do espaço cibernético permite também um maior controle de todos os demais espaços.

Peter Knight (2014), por sua vez, fala da necessidade de desenvolvimento de Tecnologia, Informação e Comunicação. Mas para isso, ainda de acordo com ele, é necessário consenso entre todos os envolvidos no processo político, de forma a criar regras e políticas

[14] *"The attempt by an individual or group to affect, influence, or control people, phenomena, and relationship, by delimiting and asserting control over a geographic area"* (SACK, 1986, p. 19).

eficientes. Desse autor infere-se a necessidade de consenso para se territorializar o espaço cibernético.

Logo, a territorialização esteve presente como uma tentativa de regulamentar o espaço, tanto com regras de utilização, quanto também com arranjos para seu funcionamento. Assim, a territorialização do espaço cibernético é traduzida pelos propósitos de todos os envolvidos nessa área geográfica. Isto resulta no dilema do espaço cibernético: territorializar ou desterritorializar.

1.1.3 Espaço Cibernético como Objetivo Científico

O espaço cibernético não é somente planejado pelo homem, mas também um espaço geográfico que perpassa todos os demais (VENTRE, 2011). Essa característica é um exemplo da abrangência desse espaço. Por isso, pensar no espaço cibernético como objeto exclusivo das ciências da computação é visualizá-lo limitadamente.

Da mesma forma que o espaço cibernético perpassa os espaços terrestre, aéreo, marítimo e sideral, ele também perpassa por todas as ciências, de forma generalizada, como objeto científico. Assim, analisar toda a historiografia sobre os estudos do espaço cibernético necessitaria de uma pesquisa tão abrangente que nem mesmo uma tese de doutorado conseguiria abarcar. Em virtude disso, este tópico pretende apenas demonstrar as principais questões sobre o espaço cibernético e algumas vertentes de pesquisas.

A primeira área de pesquisa sobre espaço cibernético que merece atenção é a teórica e conceitual. Como essa dissertação já demonstrou, as pesquisas sobre esse objeto são recentes e por isso ainda faltam debates e estudos para universalizar teorias e conceitos sobre espaço cibernético. Diante disto, Mandarino Jr (2010) nos apresenta a taxionomia como uma demanda acadêmica.

Ademais, o autor também evidencia a necessidade de compreender os impactos das novas tecnologias para o espaço cibernético. Essas tecnologias servem para reterritorializar o espaço cibernético, como foi o caso dos satélites e a rede wi-fi. Embora essas tecnologias pareçam acessíveis, aquelas de última geração somente são disponíveis por um custo elevado, ou seja, as tecnologias também impactam e são impactadas pela distribuição de poder no globo.

O impacto das tecnologias, somado à necessidade de compreender a configuração do espaço cibernético, formam outra área de pesquisa desse espaço. De acordo com Richard Clarke (2012), o espaço cibernético lembra o período feudal. A complexidade desta

configuração, entretanto, não está em compreender o período feudal cibernético, mas entender a influência de um espaço nessa fase de maturação que perpassa o mundo globalizado em que estamos inseridos.

Esse embate de realidades causa também litígios entre soberanias. Parte das questões de soberanias no espaço cibernético surge da sua própria configuração, em que é complexo delimitar fronteiras e limites de Estados. Em virtude disso, os pesquisadores desta linha tentam clarificar formas de delimitar esses limites e evitar novos litígios.

Essa mesma vertente também gera pesquisas sobre regulamentações e marcos legais internacionais. Por ser um tema recente, não existe ainda uma regulamentação universal e um reconhecimento global (MANDARINO JR, 2010). Esses tratados regulariam e organizariam a configuração do espaço cibernético, como também evitariam guerras cibernéticas (CLARKE, 2012).

As pesquisas sobre a dimensão e a configuração desses tratados abarcam também as consequências ou não de suas existências. Assim, além de abordarem os litígios visíveis do espaço cibernético, elas também versam sobre questões de segurança, como os crimes cibernéticos (CLARKE, 2012). Dessa forma, encontramos mais uma categoria de pesquisa: segurança e defesa cibernética.

Embora a segurança e a defesa cibernética confundam-se por vezes, por isso a demanda por pesquisas sobre isso, em alguns casos o limiar desses dois conceitos é claro. Enquanto na questão de segurança perpassam debates sobre crimes cibernéticos e privacidade, a defesa apresenta questões próprias das relações internacionais. Dentre elas, cabe destacar, poder cibernético e guerra cibernética.

Sobre a problemática do poder cibernético, podemos citar a forma como o poder é utilizado, seu alcance e sua mensuração. Assim, encontramos recursos de poder físico ou virtual. Por sua vez, dentro do âmbito da guerra cibernética, além dos próprios estudos de casos, as pesquisas também tentam compreender as principais abordagens de uma guerra cibernética, como se defender e como garantir a resiliência de uma nação.

Para finalizar, cabe ressaltar novamente que existem diversas abordagens do espaço cibernético como objeto científico. Richard Clarke (2012), por exemplo, explica as pesquisas sobre esse espaço por meio de uma tríade, que abarca os endereços de computadores e as regulamentações adicionais do espaço cibernético. O terceiro elemento da tríade abordado por Clarke (2012) é um objeto que impacta indiretamente no espaço cibernético, a energia elétrica. Assim, esse breve tópico apresentou a abrangência do objeto

científico espaço cibernético e justificou a abordagem delimitada dessa dissertação aos assuntos referentes aos Estados.

1.2 SOBERANIA RESPONSÁVEL PARA O ESPAÇO CIBERNÉTICO

1.2.1 Fragilidades e Ameaças no Espaço Cibernético

Assim como nos demais espaços geográficos, os Estados competem entre si pelo domínio do espaço cibernético, seja de forma direta ou indireta. Entretanto, Joseph Nye Jr (2012) afirma que diferente dos demais, o espaço cibernético não pode ser dominado por um único Estado, pois o aumento do poder nele também gera dependências e fragilidades. Este tópico pretende discorrer sobre as fragilidades e possíveis ameaças do espaço cibernético.

A impossibilidade de domínio desse espaço é devida sua exploração facilitada e a difusão de poder propiciada pelo próprio espaço cibernético (NYE JR, 2012). Enquanto precisamos de recursos consideráveis para adquirir um barco ou navio para explorar o mar, ou então para comprar um avião e poder voar, no caso do espaço cibernético essa verba é irrisória. Os poucos recursos necessários para utilizar o espaço cibernético, o torna acessível a qualquer pessoa (NYE JR, 2012).

Em virtude disso, Nye Jr (2012) afirma haver uma vantagem preponderante do ataque em relação à defesa cibernética. Um indivíduo que acessa um computador ligado na rede, mesmo sem recursos, apresenta capacidade de desenvolver um vírus para atacar outros indivíduos ou até mesmo alguns Estados. Enquanto isso, para manter a resiliência e a segurança dos servidores, um grande banco necessita de investimentos maciços.

Além de tentar garantir uma resiliência nos sistemas, outro fator para o encarecimento da defesa cibernética é a tentativa de identificação do autor dos ataques. De acordo com Nye Jr (2012), a dificuldade de se identificar as fontes de onde surgem os ataques ou definir os agentes que os efetuam torna complexa a própria dissuasão dentro do espaço cibernético. Isso porque uma defesa dissuasória pressupõe um contra-ataque ou consequências negativas ao agressor, sendo difícil realizá-las quando a fonte dos ataques é desconhecida.

Ademais, como visto anteriormente, a definição do espaço cibernético apresenta duas dimensões: uma virtual e uma física. Devido a essa abrangência, o poder cibernético também apresenta duas dimensões: o poder intraespaço e o poder extraespaço (NYE JR, 2012). Como o nome de cada uma das dimensões sugere, a primeira dimensão desse poder diz respeito ao poder utilizado no meio virtual e a segunda aquele utilizado no mundo físico.

Embora a conceituação e caracterização desse poder cibernético seja realizada em uma seção própria dessa dissertação, nesse momento uma pequena abordagem quanto à propagação do poder no meio virtual e físico é necessária. As ameaças e fragilidades do espaço cibernético respondem à propagação do poder cibernético tanto na dimensão virtual quanto na dimensão física, conforme Nye Jr (2012). Além disso, os ataques realizados em meio virtual também impactam em alvos físicos, sendo o inverso também possível (NYE JR, 2012).

Em âmbito virtual, um ataque pode direcionar milhares de computadores controlados por vírus para acessarem simultaneamente uma página de serviço, como de um banco ou de um governo, causando uma sobrecarga nos servidores e impedindo temporariamente seu funcionamento (GAMA NETO & LOPES, 2014). De acordo com Nye Jr (2012), um exemplo de ataque ao espaço cibernético com origem no meio físico seria o corte de cabos de uma rede ou sabotagem de roteadores, que impediriam o funcionamento da Internet. De acordo ainda com ele, outro exemplo seria um vírus enviado ao sistema de uma hidroelétrica, que poderia impedir o fornecimento de energia em uma região, ou seja, um ataque no espaço cibernético gera consequências reais.

Os ataques cibernéticos, entretanto, não podem ser confundidos com os crimes cibernéticos. Conforme apontado por Joseph Nye Jr (2012) é costume dos autores tratarem equivocadamente os ataques cibernéticos e os crimes cibernéticos como sinônimos. Em virtude disso, cabe realizar uma distinção conceitual dessas duas atividades.

Os crimes cibernéticos apresentam baixas consequências ao Estado (NYE JR, 2012), como por exemplo, desfiguração de páginas eletrônicas ou escaneamento de portais. Por sua vez, os ataques cibernéticos são aqueles que causam consequências diretas e com grandes impactos ao Estado (NYE JR, 2012), como por exemplo, vírus desenvolvidos para invadir e controlar sistemas *SCALAS*, que são responsáveis pelo controle de usinas nucleares, hidroelétricas e outras instalações críticas. Cabe ressaltar ainda, que dentre os crimes cibernéticos e ataques cibernéticos, há aqueles de maiores e menores intensidades.

Para auxiliar na distinção dos ataques cibernéticos e crimes cibernéticos, McGuire & Dowling (2013) explicam que todos os atos que são crimes fora do espaço cibernético (*off-line)*, também são crimes no espaço cibernético (*online).* Assim, esse crimes englobam toda a gama de atos ilícitos de possível aplicação em computadores ou a rede de internet. Essa conceituação, por exemplo, entende como crimes cibernéticos as fraudes por meio de e-mails; o roubo de informações de empresas e governos; a pirataria e quebra de direitos autorais; as

ofensas não monetárias; o roubo de banco por meio de acesso ilegal a contas e transferências; e a espionagem industrial (NCPC, 2012).

No que diz respeito à defesa cibernética, as ameaças podem interromper e degenerar o funcionamento da estrutura de defesa de um Estado (OLIVEIRA, 2011). Nesse caso, os ataques são desferidos contra "os recursos informatizados que controlam a utilização dos modernos equipamentos militares, que compõem os sistemas de comando e controle, de armas e de vigilância" (OLIVEIRA, 2011, p. 108). Assim, os ataques cibernéticos são realizados não somente contra estruturas do funcionamento do Estado, mas também contra os próprios recursos da defesa.

As ameaças cibernéticas, de forma geral, apresentam características que as tornam tão atraentes quanto os crimes de tráfico. A primeira delas é a possibilidade de retornos financeiros consideráveis, assim como no tráfico. Outra característica que as tornam atraente é o anonimato e o alcance transnacional garantidos pelo espaço cibernético.

Esse espaço permite não somente o anonimato do usuário, mas também o disfarce, pois é possível mascarar uma máquina quanto à sua localização (MANDARINO JR, 2010). Ademais, a velocidade de comunicação e as interconexões existentes no mundo, permitem que uma pessoa possa aplicar um golpe em um país sem se quer estar nele (SOFAER & GOODMAN, 2001). Essas características garantem uma maior integridade ao agente responsável pelo ato, diferente de uma invasão ou crime *in loco.*

Essas duas características também ajudam a compreender esse costume de tratar crimes cibernéticos de maneira vaga. Essa dificuldade é mais notada empiricamente, pois percebemos a dificuldade de definir a origem ou as motivações por de trás de cada ofensiva. Por isso, quando analisamos dados fornecidos por empresas de segurança da internet, como a Norton e a McAfee, encontramos crimes cibernéticos e ataques cibernéticos dentro da mesma estatística.

Por isso, uma pesquisa mais empírica sobre ameaças e fragilidades não encontraria fontes e recursos mais específicos para compreender a atual conjuntura do mundo. Logo, as ameaças e fragilidades do espaço cibernético, somando as dificuldades de identificá-las, explicam o porquê de alguns autores chamarem a guerra cibernética de guerra invisível. Assim, não estamos falando em um espaço em que os Estados dispõem de suas soberanias como nos demais espaços, mas de um espaço que até o conceito de soberania necessita ser revisto.

1.2.2 Relativização de Soberania

Assim como nas demais ciências sociais, a ciência das Relações Internacionais sofre mudanças teóricas e conceituais. Com a emergência de novos cenários e interações entre Estados, alguns conceitos e teorias são revistas e repensadas. Dessa forma, com o surgimento da globalização, encontramos autores advogando sobre o fim do conceito de soberania e outros defendendo a necessidade de sua reformulação, devido à nova realidade do sistema internacional.

A noção de que o conceito de soberania é dinâmico não é tão recente, ela remete ao próprio autor responsável pelo cerne dos debates sobre esse termo, ou seja, Jean Bodin (2011). De acordo com esse autor, a soberania muda seu significado com a evolução da história. Para demonstrar isso de forma prática, ele explica que o conceito de soberania é tão antigo quanto à criação da própria civilização.

Jean Bodin (2011) defende essa visão ao apontar para a abordagem deste conceito pelos reis no contexto bíblico. Ele exemplifica isso abordando a passagem de Daniel 2,44: "no tempo desses reis, o Deus dos céus suscitará um reino que jamais será destruído e cuja soberania jamais passará a outro povo". De acordo com Bodin (2011), o antigo testamento compreende que a soberania era associada ao divino.

Essa condição muda com o tempo, sendo associada, na época de Bodin (2011), século XVI, não mais a Deus, mas ao soberano. Desta forma, independente do período analisado, trabalhar com a soberania requer uma revisão conceitual no que diz respeito à percepção da sociedade vislumbrada. Este tópico tem este objetivo.

Ao falar em soberania, percebe-se uma interação entre âmbito doméstico e externo. Assim, para repensar esse conceito é importante abordar alguns pensadores das Relações Internacionais e da Ciência Política. Alguns desses autores, como é o caso de Maquiavel (1994), não discutem diretamente o conceito de soberania, mas o observam quando analisam os conflitos de suas épocas.

Em sua obra intitulada "Discursos", Maquiavel (1994) explica a política como resultado de forças provenientes das ações concretas da sociedade. Por meio dessa colocação, é possível inferir que a soberania engloba a possibilidade de se agir em prol dos interesses dela própria. Em virtude disso, Maquiavel (2010) traduz o conceito de soberania na figura do soberano e na vontade dele.

Enquanto esse autor vislumbra a soberania por meio das ações do príncipe na vida dos principados, autores contratualistas discutem sobre a soberania no início da sociedade.

Dentre os autores contratualistas encontramos Hobbes (2003); Locke (1994); e Rousseau (1996). Todos estes concordam que a soberania resulta do contrato firmado entre a sociedade e o seu soberano.

Sobre os contratualistas, algumas características da concepção de soberania se distinguem ou se complementam no pensamento dos três autores citados anteriormente. Isso porque mesmo dentro de escola especifica, autores apresentam perspectivas distintas sobre um mesmo problema. Assim, a abordagem individual de cada um deles traz questões relevantes sobre o conceito de soberania.

Hobbes (2003), igualmente a Maquiavel (2010), também não discorre especificadamente sobre o conceito de soberania em suas obras. Para compreender como este autor observa a soberania é necessário visualizar a figura do soberano. Dessa forma, na perspectiva dele, o soberano é o titular da liberdade e do direito de sobrevivência dos demais indivíduos da sociedade, características concedidas pela realização do contrato social.

Essas características garantem a titularidade da soberania, conforme aponta Hobbes (2003). Isto permite ao soberano a utilização do Leviatã, ou seja, do Estado e do monopólio legitimo da força (HOBBES, 2003). A utilização da força é uma ferramenta de controle que garante a autonomia do soberano dentro de seu território, ou seja, garante a soberania.

Quando se pensa no plano internacional nos termos da teoria hobbesiana, encontramos um cenário do estado de natureza em que não há um soberano. Desta forma, se observa um embate de soberanias no cenário internacional, em que cada uma delas tenta garantir o monopólio da força dentro de seus territórios e, por vezes, além deles. Ademais, atualmente se visualiza também ensaios de Leviatãs no cenário internacional, em virtude do crescente aumento de organismos internacionais.

Diferente de Hobbes (2003), os clássicos de Locke (1994) e Rousseau (1996) abordam diretamente o conceito de soberania. Enquanto Hobbes (2003) delimita a soberania em virtude do monopólio da força dentro de um território, Locke (1994) não acredita na maldade natural do homem, definindo a soberania na própria cessão dos indivíduos ao contrato social. Assim, enquanto na teoria hobbesiana a soberania é garantida pelo monopólio legitimo da força, em Locke (1994) o soberano garante ela por meio da legislação do Estado.

A partir do momento em que a sociedade concede ao indivíduo a titularidade de seus interesses, direitos e deveres, a soberania é constituída e garantida (LOCKE, 1994). A soberania como garantia do exercício do interesse e da vontade também é percebida por

Rousseau (1996). De acordo com ele, a soberania de um Estado é traduzida pela vontade geral, ou seja, pela capacidade de satisfazer a vontade do Estado.

Entretanto, cabe ressaltar que vontade geral e a vontade de todos não são sinônimos. Enquanto a vontade de todos ou vontade coletiva resulta da somatória de todas as vontades, a vontade geral advém da convergência das vontades de um povo (ROUSSEAU, 1996). Logo, a soberania diz respeito a esta convergência, sendo natural a contestação da soberania de um Estado por parte de alguns nacionais e também de outros Estados.

O referencial que pauta uma soberania, como mencionado por Jean Bodin (2011), evolui conforme o avanço de uma sociedade. Sobre a relativização da soberania, também encontramos argumentos em Montesquieu (1996). De acordo com ele, a soberania respeita um referencial que varia conforme a categoria de governo adotada. Assim, caso o governo seja uma monarquia, a soberania é pautada pela honra; caso seja despotismo a soberania está embasada no medo; e no caso da república é referenciada pela virtude (MONTESQUIEU, 1996).

Outra divisão realizada quanto à soberania é aquela feita por autores como Hegel (1997), que divide a soberania em duas dimensões: interna e externa. A primeira, conforme demonstra o autor, é aquela que diz respeito à vontade emanada do povo e do soberano. Enquanto a dimensão externa, para ele, é aquela em que cada Estado é autônomo e a soberania está fundada no soberano.

Tal visão também é percebida em Kant (apud ANDRADE, 1998), que diferencia soberania do povo e soberania do indivíduo. Ela também é realizada em Tocqueville (2005), que trabalha com a soberania do povo. Embora a ideia de uma variação conceitual de soberania seja aceita por alguns autores, conforme demonstrado anteriormente, a ideia de uma soberania relativizada no espaço cibernético precisa ser discutida com cautela.

Primeiramente, pode-se pensar em relativização quanto à sua abrangência e em um segundo momento n a relativização quanto à sua abordagem. Em relação à abrangência, a relativização da soberania ocorre quando ela é reconhecida ou não por um Estado, por exemplo, os Estados Unidos não reconhecem a soberania compartilhada em alto-mar. Sobre a relativização quanto à abordagem, ela ocorre sob os temos de Montesquieu, ou seja, a conceituação dela resulta da percepção de cada Estado e por isso pode ser distinta dependendo de cada um.

1.2.3 Espaço Cibernético e a Soberania Responsável

A distinção entre ciências duras e leves não diz respeito apenas à manipulação das pesquisas e metodologias aplicadas, mas também à durabilidade de conceitos e teorias. Assim, conceitos como soberania sofrem rápidas modificações com o decorrer da história. Isso foi demonstrado anteriormente, quando Jean Bodin (2011) explicou a mudança da soberania associada ao divino para um conceito associado ao soberano.

Essa conceituação menos sacralizada é estudada por Norberto Bobbio (1994). Para ele, a soberania pode ser conceituada de forma *lato sensu* e *stricto sensu*. No que diz respeito ao *lato sensu*, a soberania é o poder de decidir em última instância (BOBBIO, 1994). Em relação ao *stricto sensu*, Bobbio (1994) trabalha a soberania no âmbito do Estado, em que ela é o poder do soberano em decidir sobre as questões do Estado, ou seja, ele trabalha a soberania absoluta.

Ademais, de acordo novamente com Bodin (2011), o conceito de soberania tem ligação com o cargo e não com a pessoa que está à frente do cargo. Caso haja uma mudança neste cargo, a soberania é transferida para o novo titular. Jean-Jacques Rousseau (1996) defende uma perspectiva semelhante, pois ele afirma que a soberania muda com a troca da titularidade do cargo. Entretanto, ele explica que a soberania também muda espontaneamente, de forma paulatina, pois ela também é constituída pelo interesse nacional.

A definição realizada por Rousseau (1996), na "Teoria da Soberania Popular", é o ponto inicial para compreender a soberania no mundo atual. Como visto, para este autor, um Estado tem como limite da soberania a própria vontade geral, e não deve se alienar aos objetivos de outrem, pois isso acarretaria na perda da soberania. Assim, para compreender o que é soberania para Rousseau é necessário compreender o que é a vontade geral.

A vontade geral, de grosso modo, é a convergência de todas as vontades particulares em uma vontade única, que busca o melhor para todos (ROUSSEAU, 1996). No entanto, por ser resultante das relações entre as vontades particulares, a vontade geral pode representar apenas a vontade de uma parcela da sociedade, devido à divisão de forças, vontades sociais e políticas (ROUSSEAU, 1996). Dessa forma, a soberania definida por Rousseau se assemelha à soberania popular construída por Immanuel Kant (2008).

A diferença destas conceituações de soberania para aquela absoluta, definida por Bodin (2011) e por Bobbio (1994), está na fonte do poder soberano. Na soberania absoluta, o poder tem como base o soberano e é exercida por ele. Já a origem da soberania popular é o

povo (KANT, 2008), mesmo sendo exercida por um soberano. Assim, as ações do Estado são respostas às vontades do povo.

A utilização pura da teoria de Rousseau (1996) apresenta certos entraves de aplicação, principalmente quando se pensa nos Estados Modernos. Isso porque estes Estados apresentam densidades demográficas exorbitantes. Isso impede a sintetização de todas as vontades particulares em uma vontade geral.

Essa complexidade aumenta, principalmente, quando se pensa em uma vontade geral em nível de comunidade internacional. Entretanto, no âmbito das relações entre Estados é mais fácil compreender as dinâmicas de uma Soberania Popular por meio da vontade geral. Por exemplo, no BRICS é necessário considerar a opinião de apenas cinco Estados, facilitando a convergência de interesses. Assim, a contribuição desta teoria está na relação entre a soberania e a convergência de interesses dos principais Estados atuantes no espaço cibernético.

Independente da soberania ser absolutista ou popular, o monopólio do poder e o uso da legislação pelos titulares dela é algo comum. Isto é evidenciado por Miguel Reale (2002) ao afirmar que o direito é a emancipação da soberania e que está por sua vez é a forma jurídica da vontade do Estado. Assim, podemos inferir que a soberania para Reale (2002) é o exercício de ações visando à vontade do Estado, ou seja, é o poder de defender os interesses nacionais.

Além da relação entre direito e soberania, outra característica comum aos estudos desses autores é a relação entre soberania e território. Conforme aponta Raymond Aron (1979):

> O soberano - o rei ou seus sucessores democráticos- pode impor sua vontade sobre todo o território do Estado. Em outras palavras, tem o monopólio da força militar dentro desse território. Por outro lado, visto de fora das fronteiras do Estado, ele é o representante da coletividade em nome da qual tem o direito e o dever de falar, e cuja independência protege com uma força militar, contra os rebeldes e os inimigos externos. (ARON, 1979)

Este autor enxerga a soberania dentro dos limites territoriais de um Estado. Para ele, a soberania é o poder de imposição da vontade do Estado em seu território, ou seja, é uma característica do comportamento estatal. Ademais, ele enxerga a soberania em âmbito interno e externo. Internamente, soberania é o poder de usar a força e externamente ela é o poder de representar legalmente uma sociedade nacional.

Percebemos, por meio desses autores, uma relativização do conceito de soberania conforme o tempo e o espaço em que ela foi estudada. No entanto, qual é o conceito de soberania na globalização?

Até o final da Guerra Fria, a configuração do sistema internacional evoluiu juntamente com as relações entre os atores internacionais. Conforme esse novo desenho ia se concretizando, havia um consenso sobre as novas problemáticas do sistema. Após o final da Guerra Fria, os autores começaram novamente a discutir o que seria o sistema globalizado, alguns discutindo polaridade, outros debatendo a regionalização e mais uns tantos as relações em redes.

Com o início do século XXI percebeu-se que a principal característica da globalização era a ausência de uma definição unificada. Ademais, também notaram na globalização relações mais complexas do que as dos sistemas anteriores. Assim, outra característica são os conceitos abrangentes, em que todas as percepções de mudanças convergem em uma noção de indefinição.

Tal problema conceitual sobre a globalização também ocorre com a soberania. No decorrer da história, houve mudanças conceituais sobre a soberania. Cada uma dessas novas variações conceituais recebia de seus pesquisadores uma denominação própria, como visto anteriormente.

Na própria obra de Aron (1979), "Paz e Guerra entre as Nações", encontramos uma diversidade conceitual sobre soberania. Dentre elas, podemos citar por exemplo, a soberania difusa; a soberania concentrada; a soberania transnacional; e a soberania imperial. Assim, no século XXI, lidar com o conceito de soberania é apreender a considerar todas as faces que ela apresenta no contexto da globalização e o momento em que ela converge de uma definição para a outra.

A soberania responsável, referência deste estudo, é uma destas variações conceituais. De acordo com o Relatório do Desenvolvimento Humano de 2013, desenvolvido pelo Programa das Nações Unidas para o Desenvolvimento (PNUD, 2013), a soberania responsável é fundamentada no contexto atual:

> Embora a maioria dos governos apoie os princípios do multilateralismo, a verdade é que se preocupam, e compreensivelmente, com a preservação da soberania nacional. Uma excessiva observância do primado da soberania nacional pode incentivar rivalidades transfronteiriças e o "pensamento de soma zero". Os países, por si só, são menos capazes de se defenderem dos efeitos de contágio das crises financeiras ou dos efeitos nocivos do aquecimento global. As medidas nacionais não garantem aos cidadãos dos

> países o acesso a bens públicos globais. Alguns governos não são capazes de proteger suficientemente os direitos humanos dos seus cidadãos. A melhor estratégia passa por uma soberania responsável, ou seja, a formulação das políticas nacionais deve ter em conta os interesses do mundo, no seu todo, e em longo prazo. (PNUD, 2013, p.120-121)

Infere-se desse relatório que a soberania responsável difere das variações clássicas vistas anteriormente. Isto porque, além de considerar os interesses nacionais em suas ações, o Estado também deverá considerar os interesses globais, ou seja, agir por meio de ética global. Cabe ressaltar, no entanto, que a soberania responsável não deve ser encarada como uma forma de intervenção em outro país, mas que haja uma ação solidária de um conjunto de países para solucionar problemas que estão além das capacidades nacionais de outro Estado.

Ademais, esse relatório nos submete ao jogo de dois níveis proposto por Putnam (1988). Isso permite perceber que para algumas questões, a ação unilateral de um Estado não é capaz de satisfazer as necessidades dos nacionais. Dessa forma, para conceder acesso aos seus nacionais de determinados bens públicos globais, um Estado necessita da cooperação dos demais países. Além disto, manter uma soberania responsável "exige que se tenha em conta, de forma criteriosa e conscienciosa, as consequências do comportamento nacional em nível global e regional" (PNUD, 2013, p. 109-110).

Assim, a importância da população para a soberania responsável é notada. Essa importância pode ser contextualizada nos debates anteriores, principalmente, nas visões dos autores que versam sobre a constituição do Estado e o contrato social. Ademais, o papel da população para a conceituação da soberania pode ser sintetizada inclusive pela obra do "Pequeno Príncipe" de Antoine de Saint-Exupéry (1999), quando o pequeno príncipe questiona o real poder do rei sobre um planeta desabitado. Assim, não há soberania sem uma base populacional que a garanta.

Logo, a soberania evoluiu com o decorrer da história para um conceito multifacetado, em que varia conforme a ocasião e o ator. Além disso, se a soberania é o exercício do interesse nacional, relativizá-la, como muitos autores colocam, é inviável e impraticável, pois necessita de reconhecimento de outros atores, podendo impossibilitar a ação de um Estado. Desta forma, o que ocorreu com a soberania foi uma evolução, em que o titular dela exerce ações em prol do interesse nacional em âmbito doméstico e internacional, podendo interpretá-la de formas distintas, dependendo do fórum em que está atuando.

1.3 FRONTEIRAS CIBERNÉTICAS MULTIFACETÁRIAS

Tradicionalmente, os principais espaços geográficos em que a guerra se alastra são terrestre, marítimo e aéreo. Com o desenvolvimento tecnológico, novos espaços vêm sendo explorados estrategicamente pelos Estados, como o espaço extra-atmosférico e o espaço cibernético. De todos esses espaços, o único que foi construído pelo homem é o cibernético, sendo explorado em potencial por atores não estatais antes mesmo dos próprios Estados.

Para entender como atores estatais e não estatais se comportam no espaço cibernético, precisamos compreender como esse espaço é construído. Isso nos permite perceber os pontos fortes e fracos da defesa e segurança cibernética. Dessa forma, esta seção apresenta como objetivo compreender o conceito de fronteiras cibernéticas.

Para tal, a compreensão das fronteiras tradicionais também é necessária. Essa necessidade é justificada quando Daniel Ventre (2012) explica que o espaço cibernético perpassa por todos os demais espaços, influenciando-os continuamente. Por isso, compreender as fronteiras do espaço cibernético requer também compreender esse conceito nos demais espaços.

1.3.1 Fronteiras nos demais Espaços Geográficos

Os espaços geográficos podem ser divididos em duas categorias: clássicos e contemporâneos[15]. A primeira categoria diz respeito aos espaços cuja exploração pelo homem é evidente, como terrestre, marítimo e aéreo. A segunda categoria diz respeito àqueles espaços cuja delimitação ainda é prematura e desafiadora ou cujas ações do Estado necessitam ser regulamentadas, como é o caso do espaço extra-atmosférico e do espaço cibernético.

O espaço terrestre compreende a superfície terrestre e o subsolo que estão localizados dentro dos limites do Estado, conforme visão do direito internacional (VARELLA, 2012). Esse subsolo tem ligação direta com a camada da superfície, por isso também compõe o espaço terrestre, independentemente da sua profundidade (CASELLA,

[15] A divisão entre os espaços geográficos não corresponde a nenhum critério que não seja o interesse humano e o seu uso. Isso diz respeito ao processo de territorialização de um Estado, ou seja, nos conceitos anteriormente discutidos, é criar territórios nos espaços. O processo de territorialização depende diretamente do interesse dos Estados por dado espaço e do nível tecnológico de cada um deles, pois isso determinará as condições e capacidade de uso do espaço. Em virtude disto, chamou-se aqui de espaços geográficos contemporâneos os espaços extra-atmosférico e cibernético, pois somente vieram a ser debatidos na segunda metade do século XX.

2012). Além desses locais, o espaço terrestre também é caracterizado pelas as ilhas fluviais (CASELLA, 2012).

Sobre a água doce encontrada dentro do espaço terrestre de um Estado, encontramos diferentes posicionamentos entre diversos autores. Alguns destes consideram essas águas como um domínio distinto dos espaços citados anteriormente, ou seja, constituindo o espaço fluvial, conforme apontado por Paulo Casella (2012). Outros consideram o domínio fluvial como composição do espaço terrestre, sendo assim considerado também um domínio terrestre, entre os autores dessa visão, nós encontramos a de Valério Mazzuoli (2011).

Além de Casella (2012) e Mazzuoli (2011), a Convenção das Nações Unidas sobre o Direito do Mar vislumbra os domínios fluviais como pertencentes ao espaço marítimo (ONU, 1982). Outro direito que privilegia a adoção dessa visão é o consuetudinário, que atribui a responsabilidade por esse recurso à mesma força armada responsável pelo espaço marítimo. Em virtude disso, essa dissertação privilegia essa última abordagem, ou seja, os recursos fluviais como derivados do espaço marítimo.

De todos os espaços existentes, o espaço terrestre é aquele em que as fronteiras são mais bem consolidadas pelo direito internacional (MATTOS, 1990). Mesmo assim, conforme aponta Robert Kaplan (2013), ainda hoje existem consideráveis conflitos envolvendo as fronteiras desse espaço. Por isso, o General Meira Mattos (1990) explica que nenhuma delimitação territorial deve ser realizada sem um marco fronteiriço, ou seja, marcas que determinam a exata localização do limite de um Estado.

Um limite pode ser delimitado por meio naturais[16] ou artificiais[17] (REZEK, 2011). No caso do espaço terrestre, os meios naturais que marcam as suas fronteiras são rios, lagos interiores; ilhas fluviais; montanhas, cordilheiras e pontes[18] (MATTOS, 1990). Por sua vez, as fronteiras demarcadas artificialmente são delimitadas utilizando métodos astronômicos; geodésicos; matemáticos; ou mesmo linhas imaginárias, sendo instalados demarcadores nos limites, como por exemplo, placas (MATTOS, 1990).

Como dito anteriormente, devido a sua antiga maturação, o espaço terrestre apresenta delimitações de fronteiras mais práticas e de fácil regulamentação pelo direito

[16] A demarcação natural diz respeito aos traços físicos encontrados dentro de um dado território, como por exemplo, rios e cordilheiras.
[17] A delimitação artificial é aquela feita pelo próprio homem por meio de acordos, acontecimento ou por regras internacionais de delimitação de fronteiras.
[18] Embora as pontes sejam obras criadas pelo homem, de acordo com Meira Mattos (1990), elas são consideradas como demarcações naturais de limites, pois elas perpassam rios e lagos.

internacional. Diferente desse espaço, os limites e fronteiras dos espaços marítimo e aéreo são de maior complexidade. Tal dificuldade existe, pois os marcos limítrofes são imateriais.

Sobre o espaço marítimo, sua definição pode ser realizada nos termos da Convenção das Nações Unidas sobre o Direito do Mar (CNUDM) de 1982. Embora essa convenção não utilize a nomenclatura espaço marítimo, ela utiliza a definição similar de área marítima. Desta forma, o espaço marítimo deve ser definido como "leito do mar, os fundos marinhos, e o seu subsolo além dos limites da jurisdição nacional" (ONU, 1982, p. 02). Além desses, o espaço marítimo também inclui os estreitos de navegação internacional, ilhas e mares fechados ou semifechados (MATTOS, 2014).

Enquanto o direito internacional utiliza os conceitos de limite territorial e de zona fronteiriça no espaço terrestre, os conceitos utilizados por esse direito no espaço marítimo são: mar territorial, zona contígua, zona econômica exclusiva, plataforma continental, e alto-mar (MATTOS, 2014). Na medida em que as delimitações do espaço terrestre são demarcadas por aspectos físicos, as delimitações do espaço marítimo são demarcadas em função da exploração econômica (VARELLA, 2012). Em virtude disto, as suas demarcações são resultantes de acordos e convenções internacionais de abrangência multilateral, como a já citada CNUDM de 1982.

Acerca do mar territorial[19], ele é localizado entre a costa e o alto mar, em que o Estado exerce soberania (MUNIZ, 2009). Assim, o mar territorial é uma extensão do território do qual um Estado exerce sua soberania em *stricto sensu*[20] (SOUZA, 1999). Cabe salientar que a camada do fundo marítimo que segue ao território por dentro do mar territorial e acaba em um grande declive às profundezas do mar é chamada de plataforma continental e pertence ao território de um Estado (VARELLA, 2012).

A área que se segue ao mar territorial recebe o nome de zona contígua, ela tem função semelhante às zonas fronteiriças, ou seja, garantir a segurança do mar territorial. Por isso, ela é definida como a zona em que o Estado pode realizar ações de fiscalização para garantir a segurança nacional (MATTOS, 2014). Cabe frisar que esta zona já não faz mais parte do território de um Estado, por isso tem início após o mar territorial (VARELLA, 2012).

Da mesma forma, parte da zona econômica exclusiva também não pertence ao território de um país, pois ela tem extensão de 200 milhas náuticas da costa (MATTOS, 2014). Além da distância das duas zonas, outra diferença entre elas é que na zona econômica

[19] No mar territorial, todos os demais Estados têm direito de passagens inocentes (REZEK, 2011).
[20] Norberto Bobbio (1994) divide o conceito de soberania em *lato sensu* – poder de decidir em última instância – e *stricto sensu* – poder do soberano em decidir sobre as questões do Estado.

exclusiva, o Estado pode explorar economicamente a região, e aos demais somente é permitido a passagem, implementação de cabos submarinos e instalação de oleodutos (VARELLA, 2012). Entretanto, se o Estado não tiver capacidade para explorar toda a oferta dessa zona, os demais Estados podem desfrutar do que não foi aproveitado (VARELLA, 2012).

A última zona de importante menção trata-se do alto-mar ou comumente chamada de águas internacionais. Esta região é de uso comum de todos os Estados, desde que utilizado de forma pacífica (MUNIZ, 2009). Ademais, nela, os Estados praticam uma soberania compartilhada. Isso significa que os Estados que usufruírem dos recursos em alto mar devem sempre pensar na preservação dessa zona e do comum uso entre todos os atores (ONU, 1982). Entretanto, essa característica de soberania compartilhada não é percebida por alguns autores, como por exemplo os Estados Unidos, que vislumbra a lei do mais capacitado.

No caso do espaço aéreo, ele pode ser definido como toda área que vai da superfície terrestre e marítima até o final da atmosfera, onde encontramos o início do espaço extra-atmosférico. Apesar da dificuldade de se delimitar um marco fronteiriço neste tipo de espaço, as regras limítrofes são mais simplórias do que as referentes ao espaço marítimo. O espaço aéreo pode ser dividido em dois ambientes, o espaço aéreo nacional e o espaço aéreo internacional (REZEK, 2011).

O primeiro espaço é de exclusividade do Estado para exercer sua soberania, sendo que os demais somente podem usufruir dele com prévia autorização ou acordos realizados, conforme demonstra Paulo Casella (2012). Ele é composto, como afirma Francisco Rezek (2011, p. 372), pelos “ares situados acima de seu território e de seu mar territorial”. No entanto, essa massa de ar tem o limite de 100 km de altitude, extensão considerada antes do fim da camada atmosférica (FERREIRA NETO, 2011).

O espaço aéreo internacional, por sua vez, é um patrimônio da humanidade comum, em que todos têm direitos de transitar (REZEK, 2011). Cabe ressaltar que embora não apresente tantos recursos naturais exploráveis como o mar internacional, o espaço aéreo internacional é permeado por questões ambientais. Dessa forma, ele é tratado como o mar internacional, mas com grau de preocupação e relevância diferenciado.

Acima dos 100 km de altitude, como dito anteriormente, encontramos o início do espaço extra-atmosférico. Esse espaço geográfico é considerado contemporâneo, pois demandou de tecnologias para sua exploração que somente surgiram no século XX. O interesse pela exploração desse espaço nos remete, especialmente, para o final da década de 1950 e da década de 1960 (SOBREIRA, 2005).

Ao final da década de 1950, a União Soviética lançou o primeiro satélite do mundo, chamado de *Sputnik* (REZEK, 2011). Já em 1969, os Estados Unidos enviaram uma missão tripulada de sucesso para aterrissar na Lua (REZEK, 2011). Esses dois fatos, além de marcantes, também referenciam os dois principais marcos do espaço extra-atmosférico.

Ainda assim, não há um consenso entre os autores e pesquisadores deste espaço sobre suas delimitações. Quando falamos disso, não nos referimos à extensão do espaço extra-atmosférico, mas sobre os espaços geoestacionário e sideral como componentes únicos ou como espaços distintos do espaço extra-atmosférico. Marcelo Varella (2012), por exemplo, trabalha separadamente esses dois espaços.

Para ele, o espaço geoestacionário compreende a região ao redor da terra, numa altura de aproximadamente 36 mil quilômetros acima do Equador. Essa região é destinada aos lançamentos de satélites. O espaço sideral, por outro lado, é definido por ele como as demais regiões do universo.

Enquanto isso, outros autores, como Rezek (2011), trabalham o espaço sideral e geoestacionário como um único espaço, o chamando de extra-atmosférico. De acordo com ele, o espaço extra-atmosférico é convencionado pelo Tratado da ONU sobre Espaço Exterior de 1967. Esse tratado regulou tanto o uso comum do espaço geoestacionário como o do espaço sideral. Sobre esses espaços, Paulo Sobreira (2005) ressalta que embora haja regras para o espaço extra-atmosférico isso não significa afirmar que logo o homem terá capacidade exploratória do espaço externo e tampouco imaginar que tal exploração é impossível.

Dos espaços geográficos, podemos inferir que alguns referenciais são comuns a todos eles: a proteção da nação e seus interesses; e também o uso dos demais Estados. Ao sinalizar os limites e fronteiras de um espaço, deve-se refletir se eles garantem a segurança da população, de seus bens e de seus interesses, traduzidos na própria atuação da soberania. Ademais, deve-se garantir que aquele espaço possa ser utilizado pelos demais, sem comprometer a soberania do titular do espaço nacional. Por fim, os espaços clássicos por si só demonstram duas características: a interdependência dos espaços e a complexidade de marcos limítrofe.

1.3.2 Conceituando Fronteira Cibernética

Apesar do espaço cibernético desafiar os conceitos tradicionais de fronteira, sua delimitação é possível, como notamos em pesquisas das diversas ciências. Esse tópico deseja abordar algumas definições sobre fronteiras cibernéticas. Cabe relembrar, no entanto, que as

obras citadas aqui não abordam exclusivamente essas fronteiras, mas admitem a necessidade de defini-las para o estudo sobre espaço cibernético.

Essa falta de especificidade está na dificuldade de delimitar algo que pode parecer intangível e complexo. Por isso, encontramos autores que abordam fisicamente as fronteiras cibernéticas e outros que as observam na dimensão virtual. Devido a isto, podemos classificar as definições de fronteiras cibernéticas em materiais e imateriais.

Cabe ressaltar que tais tentativas de delimitação fronteiriça ainda são tímidas e requerem mais debates e reflexões. Para começar, vale conhecer as pesquisas de Mandarino Jr (2010), que abordam a fronteira cibernética da seguinte forma:

> Como, então, identificar as fronteiras cibernéticas do território nacional? Se lembrarmos que as interconexões com outros estados se dão por meio de cabos óticos submarinos transoceânicos, que adentram o território nacional pelo litoral ou pelo espectro eletromagnético, através de conexões de satélites, que tipo de fronteira devemos proteger? As fronteiras dos mares territoriais, as fronteiras terrestres ou as do espaço aéreo? (MANDARINO JR, 2010, p. 67)

Ao delimitar as fronteiras cibernéticas, esse autor pensa em estruturas físicas do espaço cibernético. Dessa forma, para proteger o espaço cibernético brasileiro, por exemplo, o Brasil precisaria proteger as fronteiras nas quais realiza comunicação com os demais países. Isso engloba a defesa tanto de cabos ultramarinos quanto de torres receptoras de sinais.

Ao contrário do autor anterior, Hosang (2011) acredita na necessidade de proteção das máquinas que suportam o espaço cibernético. Assim, a defesa deveria focar nas máquinas que recebem os dados pelos cabos e satélites. Entretanto, uma pessoa pode interceptar dados importantes diretamente dos cabos e sinais de satélites, ou seja, a defesa das máquinas não garantem o interesse nacional e a soberania de um Estado.

Outro conceito de fronteira cibernética é a Fronteira-Ponto. Esse conceito foi proposto por Ferreira Neto (2014). Para tal, esse autor desenvolveu uma pesquisa baseada na noção de evolução das fronteiras, resultado dos estudos sobre processos de territorialização.

A territorialização de um espaço é realizada por etapas, por isso é apropriado falar em “evolução fronteiriça”. O General Meira Mattos (1990), ao escrever sobre a Teoria de Fronteira, afirma que as fronteiras evoluem com o decorrer da história. Para ele existem quatro estágios de evolução de uma fronteira, conforme o quadro abaixo:

Quadro 1.1 – Evolução Fronteiriça

Etapa de Evolução		Descrição
1	Vazios de Ecúmeno	Característica do mundo antigo, pouco povoado, quando os núcleos geohistóricos eram separados por enormes vazios demográficos.
2	Zonas inocupadas ou fracamente ocupadas	Estas zonas não abrigavam nenhum poder político capaz de perturbar os interesses dos núcleos geohistóricos de que eram separados.
3	Faixas relativamente estreitas, as chamadas fronteiras-faixas	Nas áreas em que o povoamento dos países limítrofes não chega a pressionar um sobre o outro.
4	Fronteira linha, estabelecida sob critérios vários (natural, artificial, astronômico, étnico)	Nas áreas em que a densidade populacional colocou em contato permanente o interesse das partes.

Fonte: Elaborado com base em Carlos Meira Mattos (1990).

Pelo quadro do autor, podemos inferir que a evolução de uma fronteira não diz respeito a sua idade. Ela está associada com a relação entre espaço e sociedade. Dessa forma, podemos verificar momentos históricos em que encontramos fronteiras em etapas diferentes de evolução.

Exemplificando, na obra de Michel Foucher (2009), o autor explica que sucedeu apenas um ano após o descobrimento das Américas para que o papa Alexandre VI emitisse três bulas papais sobre aqueles territórios. Elas delimitavam aquela área como território espanhol. Isso mostra que no período das grandes navegações havia regiões no globo com fronteiras linha e outras com vazios de ecúmeno, como no caso da Europa e das Américas, respectivamente.

Além das etapas apresentadas por Meira Matttos (1990), Ferreira Neto (2004) propõe uma etapa posterior, chamada de Fronteira-Ponto. De acordo com ele, essa fronteira é exclusiva do espaço cibernético e pode ser caracterizada como os "nós" da rede, ou seja, os pontos de conexão da rede pelos quais trafegam os pacotes de informações. Ademais, ainda de acordo com ele, a fronteira cibernética recebe esse nome de ponto, porque o espaço cibernético pode ser utilizado para afetar pontos escolhidos nos outros espaços geográficos.

Outros autores que trabalham indiretamente o conceito de fronteiras cibernética realizam debates mais operacionais. Por exemplo, o coronel da Força Aérea Americana, Forrest Hare (2009), analisa o controle das Fronteiras Cibernéticas. Ao fazer isto, ele contribuiu para a definição dessas fronteiras, como podemos ver no trecho seguinte:

> The symbolic gestures to "regain control" can be reified by technological border control points, attempting to thicken the cyber borders, or both. For example, a border control point could be established at the terminus between undersea cables and fiber optic lines. At these points, customs, law

> enforcement, or other agents of the federal government could employ any of several technical solutions such as deep packet inspection devices or Anagran flow management devices. Other solutions suggest labeling traffic to identify countries of origin and destination. The intent here is not to debate the technical or practical feasibilities of such measures. (HARE, 2009, p. 96).[21]

De acordo com ele, um Estado tem três opções de controle desse tipo de fronteira: monitorar os pontos de conexão entre as fronteiras; engrossar as fronteiras para garantir a resiliência do espaço; ou os dois anteriores simultaneamente. Em uma analogia com as fronteiras terrestres, essas ações seriam: controlar as fronteiras em comum com os países vizinhos; engrossar as faixas de fronteiras e instalar aparelhos de monitoramento para detectar penetrações não autorizadas no território; ou todas as anteriores.

No trabalho de Hare (2009), como notado, o conceito de Fronteira Cibernética surge quando ele aborda a vigilância dos cabos ultramarinos e de fibras óticas. Assim, para Hare (2009), as fronteiras cibernéticas são os pontos de ligação entre o espaço cibernético nacional e o internacional. Nesses pontos ocorre a entrada e saída dos dados que trafegam na rede.

Cabe ressaltar que as fronteiras cibernéticas também apresentam uma face imaterial, baseado na fonte do poder cibernético: a informação (NYE JR, 2012). Frisamos ainda que os pesquisadores das fronteiras cibernéticas que vislumbram a dimensão imaterial também a observam além da abstrata "Matrix"[22]. Assim, eles se apoiam tanto no aspecto virtual quanto nas consequências operacionais dessa face das fronteiras.

Igualmente o que ocorre no debate sobre fronteiras cibernéticas materiais, a face imaterial delas é abordada por diferentes aspectos. Um desses referenciais, para compreender as fronteiras cibernéticas imateriais, é a divisão de responsabilidade. Essa possibilidade é embasada em experiências dos Estados Unidos por dividir seus domínios de acordo com a função, conforme explica Barros (2011). Exemplos dessas referências são os domínios ".mil" e ".gov", que são de incumbência das forças armadas e do departamento de segurança do governo, respectivamente.

---

[21] O simbólico gesto para "recuperar o controle" pode ser refinado por pontos de controle das fronteiras tecnológicas, tentando engrossar as fronteiras cibernéticas, ou ambas. Por exemplo, um ponto de controle fronteiriço pode ser estabelecido no terminal entre os cabos submarinos e as linhas de fibra óptica. Nesses pontos, costumes, aplicação da lei, ou outros agentes do governo federal podem empregar qualquer uma das várias soluções técnicas como pacotes de inspeção de dispositivos ou dispositivos de gerenciamento de fluxo Anagran. Outras soluções sugerem tráfego rotulagem para identificar os países de origem e destino. A intenção aqui não é debater as técnicas viáveis ou práticas dessas medidas. [tradução nossa]

[22] Ambiente idealizado pelo filme Matrix produzido por Joel Silver em 1999. A Matrix era uma dimensão virtual composta por um infinito com luzes verdes, colunas de números e símbolos fluindo constantemente na vertical.

Seguindo a mesma linha de Barros (2011), temos o especialista americano em segurança doméstica Kristin Finklea (2013). Entretanto, ele não analisa os domínios em relação às responsabilidades, mas observa a posição geográfica. De acordo com ele, cada endereço que acessamos tem um Estado responsável pela informação que ali trafega. Os exemplos que ele utiliza são os ".us", atribuídos aos EUA, e os ".au", atribuídos à Austrália.

Essa visão é criticada pelos juristas David John e David Post (1996). Eles afirmam que uma pessoa pode adquirir um endereço ".us" de uma máquina localizada no Brasil. Outro exemplo dado é a possibilidade de se registrar um ".fr" por meio de um laptop durante uma conexão no aeroporto de Paris. Em virtude disso, para esses juristas, as fronteiras cibernéticas são as informações ou pacotes de dados.

Ademais, conforme explica Richard Clarke (2012), os pacotes de dados apresentam registros de origens e destinatários. Assim, utilizar os próprios dados como fronteiras, permite imputar responsabilidades sobre os Estados. Isso é justificado pela soberania responsável visto anteriormente, em que um Estado deve responder por todas as consequências dos dados originados em seu território. Entretanto, existem atualmente programas de computador capazes de mascarar esses registros, como o navegador TOR (CHACOS, 2012).

Cada um desses conceitos apresenta impactos distintos sobre a forma como o monitoramento de determinada fronteira será realizada e sobre os limites soberanos de cada Estado no espaço cibernético. Ademais, o monitoramento das fronteiras também depende da tecnologia que cada país dispõe. Diante disto, os autores aqui tratados podem ser sintetizados no quadro seguinte:

Quadro 1.2 – Conceituações acerca das Fronteiras Cibernéticas

CATEGORIA	AUTOR	DEFINIÇÃO	EXEMPLO	MONITORAMENTO
Fronteiras Cibernéticas Imateriais	John & Post (1996)	As informações são a própria fronteira do espaço cibernético; assim proteger a informação é proteger o espaço cibernético em questão.	Pacotes de dados; E-mails; arquivos.	Defesa por meio de softwares
	Barros (2010)	As fronteiras cibernéticas são caracterizadas pela competência dos responsáveis pela rede em questão.	Domínios como os ".com"; ".gov"; ".br".	Defesa por meio de softwares
	Finklea (2013)			

Fronteiras Cibernéticas Materiais	Hare (2009)	As fronteiras cibernéticas equivalem às estruturas físicas que conectam as redes entre os países.	Cabos ultramarinos; e sinal dos satélites.	Filtros ligados juntamente aos cabos para monitorar os dados
	Mandarino Jr (2010)			Fronteiras simultâneas das quais as interconexões são feitas
	Hosang (2011)	Assim como o espaço cibernético, as fronteiras cibernéticas resultam dos sistemas das próprias máquinas.	Computadores e servidores.	Ferramentas de segurança dos equipamentos por meio de softwares e das estruturas físicas
	Ferreira Neto (2014)	Pontos de conexões da rede (nós) em que trafegam os pacotes de informações.	Roteadores; Pontos de Trocas de Dados	Filtros ligados juntamente aos pontos de conexões

Fonte: Elaboração própria embasado em Mandarino (2010); Hare (2009); Hosang (2011); Barros (2010); Finklea (2013); John & Post (1996); Ferreira Neto (2014).

Portanto, não há uma definição padronizada sobre as fronteiras cibernéticas. Cada pesquisador aponta para um referencial como fronteira do espaço cibernético. O que cabe notar é que cada autor se ocupa de um aspecto material ou de um aspecto imaterial dessa fronteira. Assim, na perspectiva dessa dissertação, as fronteiras cibernéticas são multifacetárias, sendo dividias em duas categorias: fronteiras materiais e imateriais.

1.3.3 Fronteira Cibernética como Espaço Conectivo

O espaço cibernético, como mencionado anteriormente, perpassa todos os demais espaços geográficos. Em virtude disso, o mundo virtual permeia toda a vida da sociedade atual. Por isso, na mídia ou em algumas pesquisas, comumente encontramos pessoas enquadrando nosso período histórico como a “Era da Informação” ou a “Era da Internet”.

Embora essas fontes queiram fazer referência à imersão tecnológica, a nomenclatura utilizada pode interferir na compreensão da história atual. Conforme aponta André Lemos (2004), nós não estamos vivenciando a “Era da Informação” ou a “Era da Internet”, mas estamos na “Era da Conectividade”. A ideia da “Era da Conectividade” surgiu com o conceito de computação ubíqua.

Ainda de acordo com Lemos (2004), o pesquisador Mark Weiser explorou o conceito de computação ubíqua em um artigo no ano de 1991. Nele, Weiser explica que as tecnologias possibilitariam aos homens estarem em vários lugares simultaneamente por meio

dos computadores (LEMOS, 2004). André Lemos (2004) utilizou esse conceito para explicar que estamos constantemente conectados ao espaço cibernético, independe da hora e lugar.

Nessa "Era da Conectividade", cada pessoa transita no espaço cibernético por meio de perfis ou identidades. Embora tenhamos a percepção de que a conectividade e a possibilidade de se criar identidades acabaram com os laços territoriais, Manual Castells (2003) explica que essa crença é falaciosa.

De acordo com ele, o ineditismo das relações sociais dentro do espaço cibernético não impediu que estudos sobre identidades e laços territoriais fossem realizados. Tais estudos demonstram que embora a internet facilite a criação de identidades falsas ou fantasiosas, a maioria das pessoas sempre utiliza sua identidade real como base de inspiração, conforme Castells (2003). Geralmente o que se observa são algumas distorções entre o perfil virtual e a identidade real, dependendo do nível de maturidade desta última (CASTELLS, 2003).

Sobre isso, Castells (2003) explica que as maiores distorções são encontradas entre os adolescentes. Para ele, a identidade nessa faixa etária ainda está em construção, por isso apresenta instabilidades. Assim, quando um adolescente cria um perfil no espaço cibernético, ele é carregado de tendências e culturas em desenvolvimento.

Outra falácia que Manuel Castells (2003) aponta é o isolamento social causado pelo espaço cibernético. De acordo com ele, ao vivenciarem na dimensão virtual, as pessoas não desintegram seus laços com o mundo real, mas os fortalece ao exercitarem traços de sua identidade. Ademais, as relações sociais no espaço cibernético não anulam as relações no espaço real, somente as complementam.

Além disso, André Lemos (2004) demonstra que quanto maior a conectividade de um Estado, mais forte serão as instituições dele. Da mesma forma, quanto maior a conectividade de um indivíduo, mais forte será sua identidade. Por outro lado, quanto maior a conectividade das pessoas, menor será a distorção entre identidade real e identidade virtual, pois ela por vezes é validada pelos demais indivíduos.

Embasado nisso, uma pessoa com alta conectividade, ou seja, conectado em redes sociais, profissionais, e-mails, noticiários e outras redes, terá sua vida constantemente monitorada tanto por usuários conhecidos como também por indivíduos desconhecidos. Em virtude disso, ela poderia ver comprometida uma oferta de emprego se em algum desses perfis dela fosse distorcido ou fantasioso, como por exemplo, utilizar o nome de "Garoto Festeiro". Assim, quanto maior for a exposição de uma pessoa na rede, geralmente mais fidedigna será sua identidade.

Essa conexão entre a vida no espaço cibernético e a vida no mundo real se revela no sentimento de "topofilia". Essa palavra, de acordo com Roca *et al* (2006), faz referência aos laços afetivos entre um indivíduo e um território, ou seja, fundamenta o sentimento de pertencimento e nacionalidade. Assim, por mais que um indivíduo esteja em território estrangeiro, ainda sim se autoproclamará pertencente ao seu território de origem.

Dessa forma, se uma pessoa estiver utilizando a Internet, o sentimento de pertencimento ao seu território de origem não é omitido. Por outro lado, ele é aflorado, pois as páginas acessadas estão carregadas de aspectos territoriais, como cultura, idioma e signos. Por exemplo, por mais que um brasileiro acesse a rede francesa, ele continua ligado ao território brasileiro, mesmo se o *tablet* utilizado tiver sido comprado em algum aeroporto britânico, pois as configurações utilizadas em seu computador e navegador o remeterá ao Brasil.

De acordo ainda com esses autores, o sentimento de afinidade entre indivíduo e território não é menos importante do que a capacidade de um indivíduo de gerar riquezas para seu Estado nacional. Neste caso não estamos mais falando de topofilia, mas sim de "terrafilia". Dessa forma, além de englobar a ligação entre o indivíduo e o seu território, esse segundo conceito também versa sobre a produção de riquezas que essa pessoa gera para seu território de origem, mesmo não estando nele (ROCA *et al*, 2006).

A remessa de riqueza ou o simples ato de navegar nas redes do país de origem é resultado da racionalidade humana. De acordo com Miguel Reale (2002), a racionalidade de uma pessoa é moldada pela formação de condutas. Ainda conforme ele, as principais condutas que formam a racionalidade humana são: conduta religiosa; conduta moral; conduta costumeira; e conduta jurídica.

Na conduta religiosa, o indivíduo age com base na sua crença ou motivação transcendental. Por sua vez, a conduta moral é formada pela percepção de bem ou mal avaliada pela consciência de um indivíduo. Por conseguinte, a conduta costumeira é aquela em que o homem não pauta suas ações em sua própria consciência, mas no conjunto de regras e costumes estabelecidos pela sociedade.

No que diz respeito à conduta jurídica, ela é formada pela combinação da conduta moral e a conduta costumeira, sendo esta a principal referência. Assim, o indivíduo pauta seu agir dependendo do seu conhecimento sobre o arcabouço jurídico. Cada uma dessas condutas interfere com maior ou menor grau no agir de uma pessoa.

Dessa forma, todas essas condutas são formadas pela história do indivíduo. Ademais, dependendo do contexto em que a pessoa está inserida, uma conduta poderá impactar mais do que as demais. No caso do espaço cibernético, por exemplo, quando um

usuário consegue mascarar seu sistema ao ponto de garantir o anonimato, a conduta jurídica quase não apresenta relevância em sua racionalidade.

Portanto, embora o espaço cibernético apresente fronteiras multifacetárias, não podemos esquecer que ele é um espaço conectivo. Isso significa que mesmo superando as fronteiras de um Estado, a racionalidade de um indivíduo estará vinculada ao seu território, por meio das condutas que referenciam seu agir. Tais condutas, por serem formadas pela história de cada pessoa, se revelam nos conceitos de topofilia e terrafilia.

1.4 REGIMES INTERNACIONAL DO ESPAÇO CIBERNÉTICO

Para manter a liderança das relações internacionais e satisfazer seus interesses nacionais, um Estado forte e com grande centralidade geopolítica no mundo utiliza normas, regras e outras ferramentas de poder. Tais ferramentas podem resultar em regimes internacionais, caso recebam suficiente atenção dos centros e demais estados. Assim, a existência dos regimes internacionais e sua manutenção estão vinculadas a convergência de interesses entre os Estados, em especial daqueles que são considerados os centros das relações internacionais vigentes.

A teoria que versa sobre os Regimes Internacionais surge dentro do debate sobre cooperação internacional. Por ser um debate muito amplo, existem diversos teóricos de diferentes escolas das Relações Internacionais discutindo esse objeto, inclusive das escolas majoritárias. Assim, temos, por exemplo, os realistas Mearsheimer (2000) e Krasner (2012) e os liberais Keohane (1984) e Nye Jr (2012).

Além disto, não há um consenso sobre a definição dos Regimes Internacionais. Por isto, esta seção serve não somente para abordar conceitualmente e empiricamente esse tema, mas para contextualizar o espaço cibernético dentro da perspectiva futura de um regime internacional. Assim, o leitor conhecerá os principais organismos internacionais que versam sobre o espaço cibernético, como também compreenderá o significado de um regime internacional do espaço cibernético para o centro.

1.4.1 Defesa e Segurança Cibernética

Para os Estados Unidos e a Colômbia, as Forças Armadas Revolucionárias da Colômbia (FARCs) eram consideradas como grupos terroristas. Outros países como Equador, Bolívia e Brasil não percebiam esse grupo da mesma forma (CUNHA, 2010). O

reconhecimento de uma atividade terrorista por um Estado significa reconhecer um problema de defesa e não de segurança.

Essa pequena abordagem sobre as percepções que alguns Estados apresentam sobre as FARCs serve para exemplificar como um mesmo problema pode ser interpretado sob a percepção da segurança ou da defesa. Se a percepção de uma questão tangível como defesa ou segurança já é complexa, imaginar uma fácil distinção entre esses dois conceitos no espaço cibernético é um ato enganoso. Afinal, como visto anteriormente, os conflitos dentro do espaço cibernético são considerados por alguns como a "guerra invisível".

Embora essa dificuldade, a distinção entre segurança cibernética e defesa cibernética é necessária para esse estudo. Compreendendo a diferença dessas duas abordagens, podemos entender se os principais organismos internacionais do espaço cibernético versam sobre defesa ou sobre segurança. Para tal, cabe nesse momento, abordar os conceitos clássicos de defesa e segurança para compreender a sua aplicabilidade no espaço cibernético.

O conceito de defesa apresenta diversas dimensões, por isso sua utilização, por vezes, pode induzir-nos ao erro (BOBBIO, 1994). Sob a perspectiva política, por exemplo, defesa significa conservar as estruturas políticas e jurídicas do território, do povo e da soberania, conforme apontado por Bobbio (1994). Por sua vez, na esfera militar, a defesa é o emprego de recursos visando prevenir o Estado de possíveis agressões (BOBBIO, 1994).

Entretanto, cabe ressaltar que a defesa não se confirma apenas no momento da agressão, mas anteriormente. Assim, a defesa também emprega recursos para dissuadir possíveis agressões e ameaças. Em virtude disso, o conceito de defesa na visão de Clausewitz (1982) é diferenciado em tempos de paz e em tempos de guerra.

Conforme demonstrado por ele, em tempos de paz, a defesa constitui em esperar e preparar formas de aparar um possível ataque. Por outro lado, em tempos de guerra, a defesa não é constituída apenas da espera, ela prevê a utilização de atos ofensivos. Para compreender qual categoria de defesa um Estado deve seguir, é necessário conhecer os inimigos e quando este irá atacar.

No caso do espaço cibernético, esse reconhecimento não é possível. Por isso, nesse espaço, um Estado deve estar sempre em alerta, ou seja, comportar-se como em estado de guerra. Seguindo esta lógica, e compreendendo que as armas cibernéticas utilizadas no espaço cibernético são frutos de informações, a defesa cibernética depende também de gestão de dados (NETO & LOPES, 2014).

Assim, o conceito de defesa cibernética é abordado por Paulo Sérgio de Melo Carvalho (2011) da seguinte forma:

> Defesa Cibernética – 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 operacional, tais ações caracterizam a Guerra Cibernética. (CARVALHO, 2011, p. 18)

Enquanto a defesa tem uma relação direta com a guerra, defesa dos interesses nacionais, garantia da sobrevivência e da soberania, a segurança pública tem referência às questões de ilícito, conforme inferido pela obra de Moisés Naím (2006). Dessa forma, segurança pública é composta das ações de prevenção e repressão de ilícitos. Assim, ao passo que a defesa nacional garante a sobrevivência de um Estado, a segurança pública garante ao indivíduo viver em harmonia com os demais.

Sendo assim, a segurança cibernética é referenciada por Oscar Medeiros Filho (2014) da seguinte forma:

> Considerando-se os objetivos do presente artigo, torna-se interessante desde já diferenciar a dimensão cibernética de defesa (ligado à noção de guerra) da dimensão de segurança pública (ligado mais a noção de ilícitos). Para tanto, usaremos as tipologias *"cybercrime"* para designar o tipo de violência cibernética aplicado notadamente no campo de segurança pública e *"cyberwar"* para designar a violência exclusiva às relações entre unidades políticas, típicas da guerra clássica. (MEDEIROS FILHO, 2014, p. 54).

Infere-se desse autor que a segurança cibernética existe para combater os crimes cibernéticos. De acordo com ele, para compreender a segurança cibernética é necessário entender a conceituação de crimes cibernéticos. Assim, cabe nesse momento recordar a conceituação realizada nesta dissertação no tópico 1.2.1, intitulado "Fragilidades e Ameaças do Espaço Cibernético".

Para McGuire & Dowling (2013) crimes cibernético são todos os atos realizados *online* que quando realizados *off-line* são considerados ilegais. Assim, para compreender o que são crimes cibernéticos é necessário realizar analogias com os crimes tradicionais. Exemplificando, a extorsão em ambiente virtual seria considerado um crime cibernético, como também o roubo de informação.

Por fim, essa analogia facilita a distinção entre defesa cibernética e segurança cibernético. Distinção essa necessária para o mapeamento das organizações que controlam o espaço cibernético. Tal entendimento nos ajuda perceber se a estrutura existente considera um problema latente somente a segurança cibernética, ou se considera a defesa cibernética, ou os dois juntos.

1.4.2 Instituições e Organismos Internacionais do Espaço Cibernético

Os regimes internacionais são utilizados pelos Estados para resguardarem seus interesses nacionais face aos demais atores. Quando comparamos com outras questões, como comércio internacional, meio ambiente e assuntos nucleares, o regime internacional do espaço cibernético inexiste. Entretanto, alguns acordos, organismos internacionais e organizações não governamentais são importantes para a manutenção desse novo espaço.

As instituições ligadas ao gerenciamento do espaço cibernético podem ser divididas em três categorias quanto sua natureza: organizações não governamentais (ONGs), empresas e organismos internacionais. Cabe ressaltar que as instituições abordadas aqui são aquelas que têm relação direta e praticamente exclusiva com o espaço cibernético. Entretanto, isso não exclui a importância de organização que tratam a temática de forma indireta.

As três principais ONGs zeladoras do espaço cibernético são: *Internet Corporation for Assigned Names and Numbers (ICANN); Internet Society (ISOC); World Wide Web Consortium (W3C).* Cada uma dessas organizações nasceram dentro do projeto da ArpaNET. Ademais, elas estão subordinadas a legislação estadunidense (NYE JR, 2012).

A ICANN tem a função de distribuir números de *internet protocols* (*IPs)* e a identificação de cada um deles (ICANN, 2015). O número de IP tem como principal funcionalidade identificar cada máquina conectada na rede, analogicamente, ele seria o número de CPF de uma máquina. Ademais, essa organização também é responsável pelos nomes de domínios de primeiro nível, por exemplo, os “.com”, “.info”, “.org” e outros.

Dos departamentos da ICANN, vale abordar a *Internet Assigned Numbers Authority (IANA).* Esse departamento é responsável pela coordenação global do endereçamento IP e *Domain Name System (DNS)*, e outros recursos de protocolos da Internet (IANA, 2015). Embora parece exercer a mesma função da entidade maior, a IANA é mais especifica, pois além dela existem dentro da ICANN outros departamentos, com por exemplo, o *Country Code Names Supporting Organization (CCNSO)*, responsável pelos endereços de países, como os “.br”, “.fr”, “.de”.

Outra organização não governamental que também trata de um aspecto técnico do espaço cibernético é o *World Wide Web Consortium (W3C).* Igualmente como o ICANN, a W3C é uma organização subordinada à legislação dos Estados Unidos. Ela é responsável por desenvolver padrões de navegação (NYE JR, 2012). Enquanto a ICANN é responsável pelo aspecto organizacional da rede, o W3C é responsável pelo aspecto tecnológico da navegação.

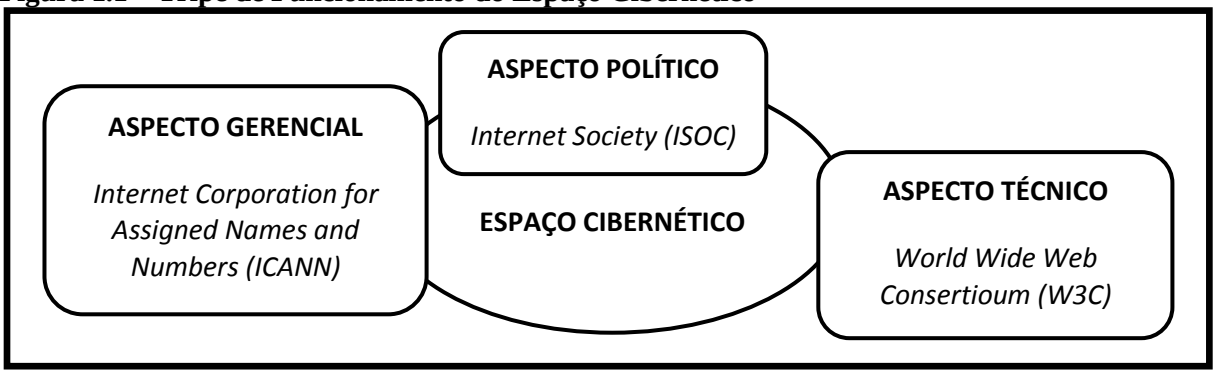
A organização não governamental responsável pelos aspectos políticos, tecnológicos, de desenvolvimento e governança é a *Internet Society (ISOC).* Essa organização responde por um amplo espectro de assuntos do espaço cibernético. Ela é responsável por "estabelecer e promover princípios que se destinam a convencer os governos a tomar decisões que são certas para os seus cidadãos e futuro de cada nação" (ISOC, 2015).

A ISOC também se dedica a garantir que a Internet permaneça aberta, transparente e definida pelos usuários. Embora trabalhe juntamente com os governos, essa organização preza pela não intervenção deles. Cabe ressaltar que a ISOC também está subordinada as leis dos EUA, como as ONGs anteriormente citadas (NYE JR, 2012).

Por ser uma organização que realiza trabalhos no espectro político, ela apresenta um departamento responsável por pesquisas e relatórios sobre espaço cibernético, a *Internet Engineering Task Force (IETF).* Este produz documentos técnicos e de alto nível para auxiliar nas tomadas de decisões sobre espaço cibernético por Estados (IETF, 2015). De acordo com a página virtual da IETF (2015), essas produções servem também para orientar profissionais de design, uso e gestão de rede.

Essa organização conta ainda com uma comissão, chamada *Internet Architecture Board (IAB).* Ela supervisiona o desenvolvimento técnico e de engenharia do IETF (IAB, 2015). Assim, ela garante que a IETF seja uma organização não somente da produção técnica, sendo também um laboratório de engenharia de rede. Essas três grandes organizações não governamentais formam um tripé, que pode ser sintetizado pela figura abaixo:

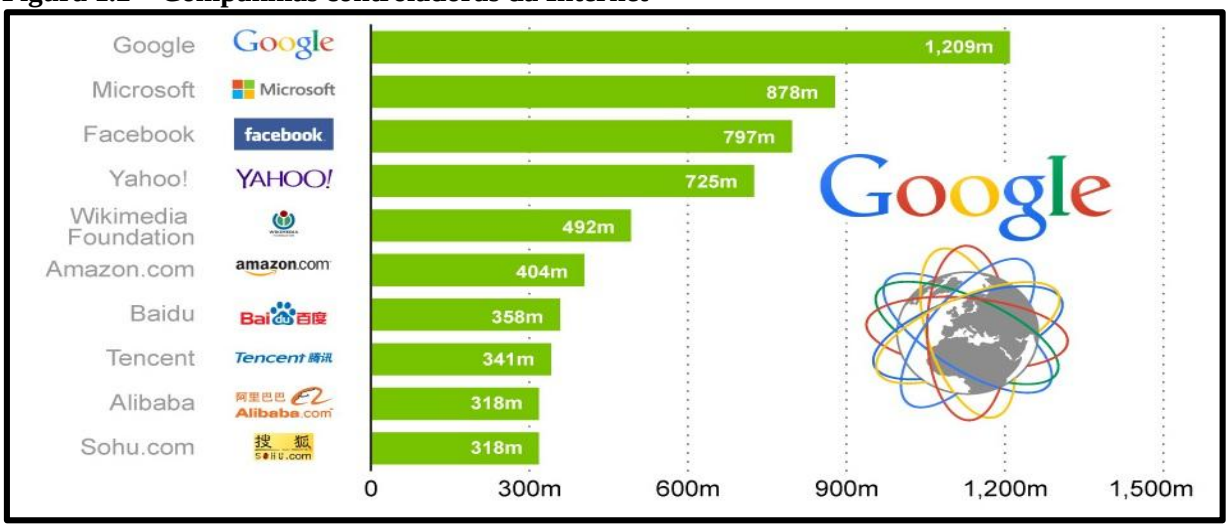
Figura 1.1 – Tripé de Funcionamento do Espaço Cibernético



Fonte: Elaboração própria com base em ISOC (2015); ICANN (2015); W3C (2015); Nye Jr (2012).

Como dito, algumas organizações não governamentais são responsáveis pelo funcionamento do espaço cibernético. Entretanto, não é somente esse grupo que conduz a exploração desse espaço. Diferente das ONGs, as empresas têm como principal objetivo o lucro por meio do espaço cibernético. As empresas que mais impactam sobre o espaço cibernético são aquelas com maiores penetrações de usuários, podendo ser organizadas conforme a figura abaixo:

Figura 1.2 – Companhias controladoras da Internet



Fonte: Fox (2013)

Embora sejam empresas privadas, pelo conceito de terrafilia visto em seções anteriores, parte dos lucros delas é submetida ao Estado de localização da sede. Além disso, mesmo sendo empresas transnacionais, a sede de cada uma delas responde à legislação do país em que está situada. Por isso, a análise das empresas acima, quando realizada sob a perspectiva das nacionalidades, demonstra o domínio dos Estados Unidos sobre o espaço cibernético.

Das dez empresas apresentadas na figura, as seis com maior penetração de usuários são estadunidenses e as outras quatro são chinesas. Quando divididos em nacionalidades, as empresas dos Estados Unidos detém 4,505 milhões e as chinesas detém 1,335 milhões de usuário, ou seja, mesmo com a presença chinesa, o poderio estadunidense persevera. Ademais, esses dados demonstram que a divisão de poder no mundo entre Estados Unidos e China também é refletida quando falamos em empresas que controlam o espaço cibernético.

Sobre os organismos internacionais, cabe ressaltar que aqui são abordados apenas aqueles diretamente associados à temática do espaço cibernético. Isso porque encontramos

questões do espaço cibernético também em organismos de temas mais abrangentes, como na Organização Mundial do Comércio (OMC) e a Organização Mundial de Propriedade Intelectual (OMPI). Os organismos internacionais que apresentam relações diretas com a temática do espaço cibernético são: União Internacional de Telecomunicação (UIT); e a Organização Internacional para Padronização (ISO).

A UIT é responsável por estruturas de comunicações, pela cooperação internacional nessa área e por temas de emergências mundiais (ONU, 2014). Sobre a infraestrutura, ela é responsável pelo uso global compartilhado do espectro de radiofrequência, pelos satélites orbitais, pela infraestrutura de telecomunicação e pela interconexão entre vários sistemas de comunicação

Ela também promove cooperação internacional na área de satélites orbitais, trabalhando na melhoria da infraestrutura de telecomunicações junto a países em desenvolvimento. Além disso, ela se dedica a temas especiais como acessibilidade e fortalecimento da segurança cibernética.

Além dessa, dentro do sistema ONU ainda encontramos o Fórum de Governança da Internet (IGF). Esse encontro tem como principal objetivo unir pessoas com interesses semelhantes e de diversas áreas afins ao debate do espaço cibernético (IGF, 2015). Dentre as temáticas tratadas no fórum, as questões de políticas públicas ganham maior destaque (IGF, 2015).

O último trabalho que consideramos aqui é aquele executado pela Organização Internacional para Padronização (ISO). No âmbito dessa organização foi criado o chamado ISO 3166, que padroniza os códigos de países e suas subdivisões (ISO, 2015). Dessa forma, por exemplo, a ISO contribuiu para que os endereços ".br" fossem utilizados somente em domínios brasileiros.

Cabe ressaltar ainda que todas as organizações não governamentais e organismos internacionais abordados estão vinculados à segurança cibernética. Ademais, embora existam empresas exclusivas de segurança cibernéticas quanto de defesa cibernética, nenhuma delas apresenta imersão de usuários suficientes para serem consideradas controladoras da internet. Isso pode ser causada por dois fatores, ou porque existem diversas empresas dividindo esses usuários, ou devido à baixa percepção dos usuários sobre a relevância desses temas.

Por fim, o conjunto de instituições responsáveis pelo espaço cibernético é divido em empresas, organizações não governamentais e organismos internacionais. Enquanto a primeira apresenta foco sobre o comércio virtual e a prestação de serviços, as organizações não governamentais se ocupam de manter o funcionamento do espaço cibernético e garantir a

segurança cibernética. Assim, resta aos organismos internacionais promover a cooperação nessa área, como também o debate sobre a governança desse novo espaço. Cabe ressaltar, entretanto, que tanto as empresas quanto as organizações não governamentais estão majoritariamente condicionadas ao arcabouço jurídico dos Estados Unidos.

1.4.3 Regimes Internacionais: instituições que servem a quem

A Teoria dos Regimes Internacionais apresenta autores das diversas correntes dominantes das Relações Internacionais e uma falta de consenso quanto às definições e conceitos. Cada uma dessas escolas tende a adaptar a existência dos regimes internacionais à suas premissas teóricas. Este tópico demonstra como teorias, conceitos e discursos são utilizados para algum propósito e para alguém.

De acordo com Hasenclever, Mayer e Rittberger (2000), as principais percepções teóricas aplicadas aos regimes internacionais são: Realismo Estrutural; Neoliberalismo; e Cognitivismo. Essas percepções também são identificadas por Krasner (2012). No entanto, ele utiliza os termos: estrutural tradicional (Realismo estrutural); estrutural modificada (Neoliberalismo); e grociana.

Embora essa variação teórica interfira na avaliação dos regimes internacionais, a sua conceituação apresenta uma aceitação universal. O primeiro conceito de regimes internacionais surgiu em 1975 com o pesquisador John Ruggie (KEOHANE, 1984). O conceito de Ruggie, abordado por Keohane (1984), define os regimes internacionais como conjuntos de regras, regulamentos, normas, expectativas, compromissos e sinergias organizacionais que tenham sido aceito por um grupo de Estado.

A aceitação universal, entretanto, somente surgiu com a definição realizada por Krasner em 1983 (KEOHANE, 1984). De acordo com ele, os regimes internacionais são:

> Os regimes podem ser definidos como princípios, normas e regras implícitos ou explícitos e procedimentos de tomada de decisões de determinada área das relações internacionais em torno dos quais convergem as expectativas dos atores. Os princípios são crenças em fatos, causas e questões morais. As normas são padrões de comportamento definidos em termos de direitos e obrigações. As regras são prescrições ou proscrições específicas para a ação. Os procedimentos para tomada de decisões são práticas predominantes para fazer e executar a decisão coletiva. (KRASNER, 2012, p. 94).

Essas definições apresentam duas diferenças primordiais quanto à intenção e a abrangência dos regimes internacionais. Na definição de John Ruggie, apenas Estados podem

participar dos regimes internacionais, não necessitando de convergência entre os interesses desses atores. Por outro lado, na definição de Stephen Krasner, todos os atores internacionais podem participar de um regime internacional, desde que haja uma convergência de interesses entre eles.

Quando comparada as duas visões conceituais, podemos afirmar que a definição de Krasner garante uma especificidade na identificação dos regimes internacionais. A centralidade desta inferência está na convergência ou não de interesses. Caso desconsiderada a convergência de interesses como requisito ao estabelecimento dos regimes, qualquer acordo multilateral entre Estados com pretensões globais poderia ser considerado um regime internacional, mesmo aqueles que não apresentam sinergia entre os Estados assinantes.

Mesmo optando por uma definição de regime internacional, ao interpretar a realidade percebemos diferenças entre eles. Por isso, a aceitação universal de um conceito não é suficiente para compreender os interesses dos atores na formação dos regimes internacionais. Ao estudar essas distinções, Oran Young (1982) definiu algumas categorias de regimes internacionais quanto à origem de cada um deles, classificando-os em: espontâneos, negociados e impostos.

Os regimes internacionais espontâneos surgem da ação de diversos atores, que não necessariamente apresentam sinergias intencionais entre eles. Esse tipo de regime não é resultado de um desenho prévio, pois não envolve a coordenação consciente dos seus participantes. Além disso, eles surgem com baixa convergência de interesses e vão se fortalecendo em uma relação proporcional direta. Igualmente, esta categoria de regime é altamente resistente aos esforços da opinião pública.

Os regimes internacionais negociados são aqueles caracterizados pelo diálogo e consentimento entre as partes envolvidas. Nesses regimes, os atores estatais produzem acordos formais sobre diversas áreas das relações internacionais. De acordo com Young (1982), a forma como esses acordos são construídos produzem também diferenças dentro da própria categoria, podendo ser agrupadas em subcategorias: regimes de negociação constitucional; de negociação legislativa; de negociação compreensiva; ou de negociação parcial.

A subcategoria de negociação constitucional diz respeito aos regimes internacionais que versam sobre um assunto em que todos envolvidos participam da sua criação. Na subcategoria de negociação legislativa somente uma parcela de países que são envolvidos no regime respondem pela sua criação. Essas duas categorias versam sobre a abrangência dos participantes do acordo.

Na terceira subcategoria, denominada regimes internacionais de negociação compreensiva, os acordos firmados somente entram em vigor com o consenso dos participantes. Por outro lado, na subcategoria de negociação parcial, basta uma parcela do apoio dos participantes para que um acordo entre em vigor. Essas duas subcategorias versam sobre os escrutínios dentro dos regimes internacionais negociados. Cabe ressaltar ainda que quanto maior for o apoio dos atores, maior a legitimidade de um acordo firmado.

Por sua vez, os regimes internacionais impostos são aqueles criados por um Estado central ou conjunto de Estados centrais. Neles, o consentimento dos atores subordinados não é explicito e o centro proponente utiliza métodos de coerção, cooptação e manipulação de incentivos para concretizar a instituição do regime internacional. Por isso, eles são fomentados pela potência ou potências dominantes para promover regimes internacionais favoráveis aos seus interesses.

Além de categorizá-los, Oran Young (1982) afirma que os regimes internacionais não são estáticos, mas dinâmicos. De acordo com ele, os regimes internacionais podem mudar de uma categoria para outra, ou seja, eles são flexíveis. Essas alterações contínuas são frutos das mudanças ocorridas nos ambientes político, econômico e social dos Estados envolvidos. Ademais, para Young (1982), essas transformações estruturais ocorrem nas regras e nas normas que regem os regimes internacionais.

Dessa forma, a categorização criada por Oran Young (1982) clarifica a noção de que os regimes internacionais são criados para servirem aos propósitos de algum ator específico, geralmente dos centros do mundo. Os regimes internacionais negociados ou impostos sempre dependerão da vontade política dos atores envolvidos, caso alguma potência não pretenda que o regime se concretize, ela pode utilizar do seu poder econômico, político ou militar para impedir as negociações. Essa influência também é percebida nos regimes internacionais espontâneos.

Cabe ressaltar que é possível a criação de regimes internacionais sem o apoio da potência dominante ou dos demais centros do mundo. Entretanto, eles somente conseguem espaço no sistema internacional na medida em que seus projetos não contrapõem os interesses desses centros. Caso isso ocorra, a potência dominante e demais centros utilizam o poder deles para garantir seus interesses.

Sobre a estrutura internacional vigente, essa foi construída principalmente após a II Guerra Mundial, sob a perspectiva dos vencedores da guerra. Esses acordos definiram as principais bases das relações internacionais atuais. As instituições criadas para garantir essas

bases foram: a Organização das Nações Unidas; o Banco Mundial; o Fundo Monetário Internacional; e o Acordo Geral de Tarifa e Comércio.

De acordo com Fareed Zakaria (2008), embora essas instituições tenham sido criadas inicialmente como uma forma de evitar conflitos da dimensão das Grandes Guerras Mundiais, as organizações internacionais também serviam como ferramentas de poder estadunidense, principal centro daquele período. Para ele, o fortalecimento ou enfraquecimento dessas organizações respondiam a demanda dos Estados Unidos. Tal demanda era traduzida na necessidade de controle do sistema internacional ou da estabilidade desse centro.

Assim, quando o mundo entrava em crise e ameaçava os objetivos estadunidenses, a legitimidade dessas instituições era reafirmada. Por outro lado, quando elas mesmas poderiam atrapalhar os interesses dos Estados, as organizações eram ignoradas. Dessa forma, a legitimidade das instituições internacionais estava diretamente relacionada com o interesse do principal centro da época, os Estados Unidos.

Por meio dessa visão, Zakaria (2008) ainda explica que para garantir sua posição de *global player* após uma possível decadência da *Pax Americana*, os Estados Unidos, enquanto centro do mundo, deveriam fortalecer as organizações internacionais. Ao aumentar e fortalecer as ferramentas de controle das organizações internacionais, os Estados Unidos evitariam uma supressão de sua nação face o surgimento de um novo centro do mundo. Dessa forma, caso se sentisse ameaçado, os Estados Unidos poderiam recorrer a alguma instituição internacional.

Em virtude disso, percebemos que os regimes internacionais atuais evoluem com maior agilidade quando apoiados pelos Estados Unidos. Por exemplo, o regime internacional de Armas Nucleares evoluiu consideravelmente com a aplicação do Tratado de Não-Proliferação Nuclear, pois este acordo satisfazia as ansiedades dos Estados Unidos e da União Soviética, que são Estados centrais. Por outro lado, os acordos vinculados ao regime internacional do meio ambiente sempre permearam a não aplicabilidade, pois eles reduzem o potencial de desenvolvimento dos Estados Unidos e outros centros.

Igualmente como ocorre com o regime internacional do meio ambiente, os Estados Unidos não estão interessados em um regime internacional do espaço cibernético, pois detém as instituições mantenedoras desse ambiente. Por exemplo, conforme apontado por Nye Jr (2012), não existe uma governança sobre espaço cibernético e sim um grupo de instituições dispersas que controla esse espaço. Ao realizar essa afirmação, Joseph Nye Jr (2012) cita algumas ONGs que controlam esse espaço, como a *W3C* ou o *ICANN*.

Embora essas instituições sejam não governamentais, elas apresentam laços com o território dos Estados Unidos. A W3C e a ICANN nasceram dentro do projeto da ArpaNET e foram criadas no âmbito do Instituto de Tecnologia de Massachusetts e da Universidade da Califórnia do Sul, respectivamente. Assim, ambas as instituições estão sob o domínio estadunidense. Isso significa que a criação de um regime internacional sobre espaço cibernético requer a redução do controle sobre essas instituições pelos Estados Unidos.

Logo, embora os regimes internacionais possam surgir de diversas formas aquém da potência central, essa pode ser considerada um motor para o regime. Isto porque, como visto, um regime pode mudar de espontâneo para imposto, dependendo da vontade e capacidade desse centro. Como o espaço cibernético foi construído dentro de instituições estadunidenses e as principais controladoras desse espaço estão dentro dos Estados Unidos, a criação de um regime internacional depende diretamente dos interesses desse centro.

2 TEORIZANDO OS CENTROS E O PODER CIBERNÉTICO

Os Estados são interconectados por cabos ultramarinos e satélites no espaço cibernético. Dessa forma, para que uma informação gerada no Brasil, por exemplo, possa chegar a algum destinatário no estrangeiro, torna-se necessário transitar por redes e satélites de outros países, como os Estados Unidos. Assim, a configuração física desse espaço se assemelha a uma configuração de centro-raios.

O nomenclatura “centro-raios” surgiu em 1951 com John Foster Dulles. Naquela ocasião, Dulles era chanceler dos Estados Unidos e negociava o Tratado de Paz de São Francisco. Ele utilizou o termo “centro-raios” para sugerir uma configuração de segurança na Ásia Oriental, em que os Estados Unidos seriam o centro, enquanto China, Coréia e Japão seriam os raios. Na proposta dele, os Estados Unidos celebrariam acordos bilaterais com essas nações, que deveriam sempre envolver os Estados Unidos nas discussões sobre defesa asiática.

A posição de centro do sistema por um Estado não é exclusiva do cenário asiático ou da temática de segurança e defesa. A observação de um mundo formado por centros e raios também pode ser notada em outras temáticas, como é o caso do espaço cibernético. Ademais, os termos centros e raios não são conceitos únicos dessa percepção de mundo.

As vontades dos Estados resultam em ações ou movimentos. Assim, os interesses dos centros ou dos raios são traduzidos em movimentos centrais e subjacentes, respectivamente. Os movimentos subjacentes, por sua vez, são subdivididos em reacionários e alternativos.

O objetivo desse capítulo é realizar uma breve teorização do que seria a percepção de um mundo formado por centros e raios. Nessa etapa, a dissertação realiza uma conceituação do que seriam os centros, os raios e os movimentos deles derivados. Posteriormente ela realiza uma curta revisão histórica sobre a formação dos centros e raios no decorrer da história.

A revisão história demostra que embora os debates sobre o espaço cibernético sejam recentes, a configuração de um mundo formado por centro-raios é mais antiga. Ademais, este capítulo também mostra que a percepção de um mundo formado por centros e raios não é estadocêntrica. Isto porque essa visão também considera a atuação de atores não estatais nas relações internacionais.

Os conceitos de centros e raios podem ser utilizados para compreender as relações de políticas externas e de poder no mundo. Em virtude disso, torna-se também necessário

abordar o conceito de poder cibernético. Para isso, a dissertação aborda a noção clássica de poder e as categorizações delas propostas por Joseph Nye Jr (2012).

2.1 CENTROS E RAIOS NAS RELAÇÕES INTERNACIONAIS

2.1.1 Conceituando Movimentos Centrais e Subjacentes

De acordo com Amado Cervo (2008), a política exterior de um Estado é resultado de sua percepção de mundo, que por vezes pode ser resumida e encontrada nas próprias teorias das Relações Internacionais. Ele afirma que uma teoria apresenta seis etapas de maturação, em que uma delas é tornar-se uma política exterior. Como exemplo desta constatação, ele cita "O Choque de Civilizações", que inspirou a guerra no Afeganistão e Iraque, e a "Teoria da Estabilidade Hegemônica", que sugeriu o unilateralismo americano.

Quando Amado Cervo (2008) aborda as teorias sobre o aspecto da maturação, ele se posiciona dentro da Teoria Crítica. Um dos grandes teóricos desta corrente de pensamento é Robert Cox (1981) e sua principal visão de mundo pode ser resumida em sua frase celebre: "a teoria é sempre para alguém e para algum propósito". Esta frase de Cox (1981) foi norteadora de parte do trabalho de Cervo (2008), intitulado "Teorias de relações internacionais: quais e para quê?".

Diante disso, quando uma teoria ocupa a posição de uma política externa, significa que ela serve a algum propósito específico de algum ator. Entretanto, sendo a teoria uma percepção de mundo e a política externa a instrumentalização dessa visão, o processo de maturação reverso também é possível. Assim, algumas políticas externas deram origens a algumas teorias, como por exemplo, as Teorias de Integração que surgiram embasadas na integração europeia.

A visualização de um mundo formado de centros e raios surgiu dentro dessa engenharia reversa no processo de maturação de uma teoria. Como dito anteriormente, o termo centro-raios foi citado pela primeira vez em 1951 por John Foster Dulles, ele abordou o termo duas vezes no seu discurso sobre o Tratado de Paz de São Francisco, que deu origem ao acordo pós-guerra entre Estados Unidos e Japão (HEMMER & KATZENSTEIN, 2002). Esse primeiro tratado deu origens a acordos semelhantes com outros atores asiáticos, como por exemplo, com a Coréia em 1953 e com a China em 1954.

A ideia desses tratados bilaterais era garantir a influência estadunidense no tema de defesa na Ásia Oriental. Esse conjunto de tratados é caracterizado como uma política de

centro-raios por Ikenberry, Mastanduno & Wohlfort (2011). Essa estratégia era baseada em uma lógica de poder, que viria ser chamada posteriormente de *"Powerplay"* por Victor Cha (2001).

Este autor define *"Powerplay"* como o ato de criar alianças assimétricas com países que poderiam se envolver em guerras de grandes proporções. Essas guerras provavelmente resultariam em um efeito *spill over*, que envolveria os Estados Unidos em uma guerra indesejada (CHA, 2001). Para evitar isso, as alianças bilaterais realizadas pelos Estados Unidos na Ásia eram tentativas de garantir o controle estadunidense sobre as decisões desses aliados e impedir esse efeito (CHA, 2001).

Ademais, a estratégia era chamada de centro-raio, pois as alianças realizadas resultavam em uma relação em que os Estados Unidos, como centro, negociavam diretamente com os raios – Coréia, Japão e China – e estes Estados não apresentavam relações aparentes entre eles próprios (CHA, 2001). Assim, a China não podia discutir as questões de defesa diretamente com a Coreia, para isso deveria falar também com os Estados Unidos. De acordo ainda com Victor Cha (2001), as relações centro-raio ainda perduram na Ásia Oriental nesse século XXI, pois esse continente é caracterizado pela ausência de uma arquitetura multilateral de defesa.

Teorizar a política externa estadunidense para a Ásia Oriental permite compreender a aplicação da visão centro-raio nas demais regiões do globo. Além disso, essa teorização também possibilita entender as consequências da visão centro-raios para os agentes que a aplicam e também para os países que sofrem o efeito dessa abordagem. Ademais, a análise da política exterior estadunidense para a Ásia nos ensina sobre a própria dinâmica do centro.

Além de usarem a teorização para compreender fatos, de modo geral, os pesquisadores também utilizam leis específicas, que tem a função de resumir grande quantidade de fatos e prever outros novos. Visando isto, a 3ª Lei de Newton – toda ação gera uma reação – pode ser aplicada em vários campos científicos, não somente na Física. A existência de centros no sistema internacional é exemplo disto, pois as ações deles geram reações.

Alguns desses movimentos são definidos pela Teoria da Estabilidade Hegemônica e são classificados por ela como movimentos contra hegemônicos e anti-hegemônicos. De acordo com William Carroll (2006), os movimentos contra hegemônicos são aqueles que reúnem forças sociais com interesses comuns em criar um projeto alternativo e emancipatório ao modelo hegemônico. Por sua vez, ainda de acordo com ele, os

movimentos anti-hegemônicos são aqueles que buscam construir projetos singulares dispersos, que são antagônicos ao modelo hegemônico, com o objetivo de desestruturá-lo, como por exemplo, o chavismo[23].

William Carroll (2006) trabalha esses movimentos com a existência de uma hegemonia como referência e sob o ponto de vista do jogo entre ideologias. Entretanto, as hegemonias, diferente dos centros, não permeiam todos os períodos históricos. Desta forma, adotar o conceito de hegemonia e centro como sinônimos gera questões operacionais contraditórias.

Uma dessas questões que podemos citar como exemplo é: os movimentos trabalhados por Carroll (2006) não existem em todos os períodos, inclusive nos que não existe claramente uma hegemônica, como em uma configuração multipolar e bipolar. Isto nos remete às críticas realizadas por Suzan Strange (1996) sobre a Teoria da Estabilidade Hegemônica. De acordo com ela, o foco excessivo que alguns autores concedem ao poder hegemônico chega ao ponto de negar a existência dos demais poderes nas relações internacionais.

Por causa disso, a ideia dos movimentos de não alinhamento e alinhamento dentro do sistema internacional necessita de uma caracterização operacional. Essa necessidade enxerga um suporte conceitual na visão de um mundo formado por centro e raios. Ademais, de acordo com Rubens Ricupero (2008), quando um Estado se resigna a ordem internacional vigente, ele atua dentro do sistema internacional para modificá-lo ou destruí-lo. Dessa forma, quando um centro ou centros do mundo dispõe de suas ações, isso pode gerar movimentos que objetivam destruir a estrutura internacional vigente (reacionários) e outros que pretendem modificá-la (alternativos).

Os movimentos reacionários são aqueles em que os participantes não concordam com a liderança dos centros, tão pouco com a estrutura do sistema internacional operacionalizada por eles. Desta forma, esse tipo de movimento pretende desestruturar o sistema internacional vigente. Enquanto isso, os movimentos alternativos não visam o antagonismo ao sistema, mas somente desejam substituir os atores centrais nos papeis de jogadores globais.

Esses dois movimentos são chamados aqui de movimentos subjacentes e resultam da deficiência de controle dos temas da agenda pelos atores centrais. Em outras palavras, os

[23] Nome dado às ideologias pregadas pelo ex-presidente da Venezuela, Hugo Chaves. Essas ideias resultavam em uma política externa que instigava o estabelecimento de um bloco de repúblicas americanas resistentes à influência externa na região, em especial dos Estados Unidos.

movimentos subjacentes são sintomáticos de um sistema centro-raios imperfeito. Isso é nítido na crítica que Fareed Zakaria (2008) faz à colocação do Secretário de Estado americano James Baker:

> O secretário de Estado James Baker sugeriu em 1991 que o mundo estava avançando para um sistema de *hub-and-spoke* [centro e raios], em que cada país teria de passar pelos Estados Unidos para chegar ao seu destino. O mundo do século XXI talvez seja mais bem descrito como um mundo de rotas ponto a ponto, com novos padrões de voos sendo mapeados todos os dias. (Isso é verdade até no sentido físico: em apenas dez anos, o número de visitantes russos à China aumentou mais de quatro vezes, de 489 mil em 1995 para 2,2 milhões em 2005). O foco mudou. Os países estão cada vez mais interessados neles mesmos – a história de sua ascensão – e dão menos atenção ao Ocidente e aos Estados Unidos. Em consequência, as discussões obrigatórias da campanha presidencial americana ao longo de 2007 sobre a necessidade de se diminuir o antiamericanismo erram um pouco de alvo. O mundo está mudando de raiva para a indiferença, do antiamericanismo para o pós-americanismo. (ZAKARIA, 2008, p. 47)

No contexto desta colocação, observamos tanto os dois movimentos estudados por Carroll (2006) quanto os movimentos subjacentes abordados por essa dissertação. Sobre os movimentos analisados por Carroll (2006), encontramos os movimentos anti-hegemônico, quando Zakaria (2008) afirma que antigamente os países apresentavam uma raiva e uma cisma contra os Estados Unidos. Encontramos também os movimentos contra hegemônicos, quando o autor afirma que o mundo mudou do repúdio para indiferença e aponta a criação de conexões que não passam pelos EUA (Rússia-China).

Sobre os movimentos subjacentes, esses sentimentos descritos por Zakaria (2008) também os regem, mas com certa diferença. Enquanto o sentimento de indiferença impera nos movimentos contra hegemônicos, no caso dos movimentos alternativos encontramos não somente indiferença, mas casos também de repúdio.

Além dessa diferença, cabe ressaltar a premissa de que os movimentos subjacentes são caracterizados pelas relações raios-raios, com pouco envolvimento dos Estados centrais. Estes somente participam desses movimentos quando há o interesse de debilitar algum outro centro que possa interferir em seus objetivos. Entretanto, esse apoio se limita aos movimentos alternativos, pois os movimentos reacionários também comprometeria o próprio poder do Estado central participante.

Outra premissa é que as dinâmicas entre centro-raios e raios-raios podem ser vislumbradas também no âmbito regional das relações internacionais. De acordo com Buzan & Wæver (2003), cada região do globo apresenta dinâmicas de segurança próprias com

lideranças regionais específicas, por isso são chamadas por eles de complexos de segurança. Algumas dessas lideranças apresentam assimetrias relativamente grandes em relação aos demais atores estatais regionais, como no caso da América do Sul e do Brasil. Esse desequilíbrio de poder gera dinâmicas de centro-raios e também de raios-raios.

Desta forma, enquanto os movimentos reacionários são formados apenas para contrapor as ações do centro, os movimentos alternativos pretendem regular alguma temática conforme a vontade própria dos Estados proponentes. Tal ambição pode permitir a estes Estados moldar as normas do sistema internacional em favor dos próprios interesses. Assim, eles substituiriam os centros sem gerar mudanças estruturais no sistema internacional vigente.

2.1.2 Um Mundo historicamente formado por Centros e Raios

O Estado que conhecemos atualmente, ou seja, o Estado Contemporâneo é uma instituição relativamente recente, datada do final do século XIX (BOBBIO, 1994). Um sistema formado por centros e raios, entretanto, não é tão recente quanto aos Estados contemporâneos. Isto porque esse sistema pode ser observado em outros períodos históricos, como no império Egípcio e em Roma.

Nas primeiras dinastias egípcias (2800 a 2400 a.C.), a unidade política central, aquela em que o faraó tinha sede, era contornada por outras unidades políticas, chamadas "nomo". Essas unidades tinham um papel fundamental na defesa do império egípcio, pois naquele período o faraó não tinha um exército formado ou milícia (BURNS, 1948). Para se defender, o faraó recorria a cada nomo, que cedia o comando de suas milícias locais à unidade central (BURNS, 1948).

No caso do império Persa (550 a.C – 330 a.C), podemos encontrar uma estrutura clara das relações entre centro e raios, caracterizadas inclusive por estruturas físicas. Esse reino era composto por quatro capitais imperiais – Susa, Persépolis, Babilônia e Ecbátana – e outras diversas cidades nas circunvizinhanças, que eram ligadas a uma ou a outra dessas capitais por estradas (BURNS, 1948). Com esta configuração viária, os mensageiros reais, comerciantes ou viajantes necessitavam transitar por uma ou mais capitais para chegar aos destinos pretendidos, nunca tendo uma opção viária direta.

Por sua vez, durante seu período de república (509 a.C – 27 a.C), Roma administrava suas unidades políticas conforme sua utilidade. Desta forma, ela era formada por um governo central e várias províncias, que eram administradas por governadores a serviço do governante de Roma (BURNS, 1948). Por si só, o funcionamento das províncias seria um

exemplo da relação entre centros e raios, pois toda a sua administração deveria estar voltada ao governo central. Entretanto, quando pensamos na relação do governo central com os chamados Estados-Clientes, encontramos um dos primeiros exemplos históricos de raios que não faziam parte da mesma esfera política do Centro, conforme apontado abaixo:

> [O Estado-Clientes eram] regiões ou cidades que se mantinham relativamente autônomas se respeitassem os acordo feitos com os romanos, que tinham que apoiar seus soberanos. Qualquer troca de chefes sem o acordo de Roma era encarada como declaração de guerra aos romanos (GONÇALES, 2005, p. 15)

Os Estados-Clientes não somente tinham que realizar suas trocas políticas com a aprovação de Roma, como também dependiam dela militarmente e economicamente. Exemplos de centro e raios semelhantes aos do império romano, em que a relação se dava entre duas unidades políticas distintas, podem ser visualizados com mais veemência quando pensamos no mercantilismo. Entretanto, os exemplos encontrados após a idade média não são tão enfáticos como os apresentados no início deste tópico.

Além disso, em alguns casos, as relações centro-raios podem ser classificadas quanto a outras temática, por exemplo, religião, comércio, poder absolutista e revoluções intelectuais. Dessa forma, encontramos dentro do mercantilismo, por exemplo, as reformas e contrarreformas da Igreja Católica. Quando observamos a questão religiosa entre 1571 a 1600, encontramos um movimento central e também movimentos reacionários.

Por sua vez, ao observamos o período colonial nos séculos XV e XVI, logo recordamos das grandes navegações e as relações entre colônias e metrópoles. Pensamos também em um mundo dividido entre Portugal e Espanha, que eram percebidos como centros das relações internacionais naquele período (FURTADO, 2007). Entretanto, com o século XVII, assistimos a debilidade da potência militar espanhola, enquanto ela era observada por três potências em ascensão na época: Holanda, França e Inglaterra (FURTADO, 2007).

Estes países também utilizaram em algumas regiões do globo um modelo colonizador distinto daquele aplicado pela Espanha e Portugal para exploração, ou seja, aqueles países também empregavam o modelo de colônia de povoamento. Dentro do sistema colonial vigente, o povoamento de colônias era notado como um movimento alternativo, pois não previa a desestruturação do sistema colonial, mas apenas o desenvolvimento de seus Estados. Caso as ações adotadas por esses países visassem o fim do sistema colonial, elas seriam exemplos de movimentos reacionários.

Assim, as colônias de povoamento empreendidas, pelas três potências citadas anteriormente, em algumas regiões do globo eram próprias dos movimentos alternativos ao movimento central, empreendido por Portugal e Espanha. Os movimentos reacionários, neste caso, eram as tentativas das colônias de se livrarem do Pacto Colonial. Ademais, este pacto ilustra corretamente como as relações centros e raios ocorriam naquele período, pois as colônias eram obrigadas a negociar apenas com as metrópoles, sem interferência do mercado externo. Desta forma, as mercadorias que saiam do Brasil, por exemplo, somente chegariam à outra potência europeia se passassem primeiramente por Portugal (FAUSTO, 2006).

Através dessa prévia revisão histórica, percebemos que as relações entre centros e raios podem ser observadas no decorrer de toda história. O século XIX não é uma exceção, pois as dinâmicas entre os impérios europeus e seus territórios extracontinentais são semelhantes àquelas do período colonial. Isso foi mostrado anteriormente e observado também nos escritos do historiador Eric Hobsbawm (2014).

Igualmente, durante toda a história existiram movimentos que se rebelaram contra este modelo de organização com maior ou menor efetividade. As revoltas contra o império romano, os movimentos de independência das Américas no século XVIII e XIX, e de forma mais contemporânea no século XX, quando encontramos antagonismos que caracterizam movimentos reacionários. Exemplo disso é o embate entre ideologia capitalismo e comunismo. Nesse período também é notado movimentos alternativos, como o movimento dos não alinhados.

Entretanto, percebemos uma mudança na forma em que estes movimentos se manifestam no contexto do século XX. Anterior à este século, os movimentos, sejam eles centrais ou subjacentes, se posicionavam por meio da política e diplomacia. Com o advento e inovação das tecnologias de informações e comunicações, estes movimentos começam a utilizar do espetáculo ou sensacionalismo para enfatizar seus objetivos e angariar membros.

Diversos exemplos do uso de TICs para promover esses movimentos podem ser encontrados no decorrer do século XX. Destes podemos citar a utilização das propagandas como ferramentas dentro de conflitos, tais como as campanhas publicitárias realizadas por Hitler contra os Aliados e vice-versa, que associavam os inimigos a figuras demoníacas, ignorantes ou outros estereótipos negativos. Um exemplo mais recente de movimento que utilizou as TICs como instrumento pode ser vislumbrado já no final do século XX e pós-queda do muro de Berlim, e diz respeito ao levante do Exército Zapatista Libertação Nacional (EZLN) em 1994, no México.

O EZLN foi o primeiro movimento reacionário a utilizar as TICs sistematicamente para se opuser ao movimento central (FIGUEIREDO, 2006). Ele é considerado aqui como reacionário, devido ao levante ocorrido em 1994 em resposta às mudanças constitucionais realizadas pelo presidente Salinas. Além disso, o EZLN sistematizou o uso da internet para denunciar abusos do governo (movimento central) e angariar simpatizantes (FRANCHI, 2004), ou seja, foi o primeiro movimento subjacente a utilizar as TICs sistematizadas e formalmente.

Somente o fato do EZLN usar a internet de forma sistêmica não configura uma mudança significativa no *modus operandi* dos movimentos subjacentes. A relevância do uso da rede para realizar o movimento reacionário apresenta significado na medida em que as operações na Internet se demonstraram mais eficiente do que a própria guerrilha armada. Inclusive, de acordo com Guilherme Figueiredo (2006), o *modus operandi* via internet substituiu por completo o uso da guerrilha armada naquela ocasião. Ademais, conforme aponta estudo de Franchi (2004), o uso da rede permitiu a internacionalização da reivindicação do EZLN, gerando poder e apoio à causa defendida por eles.

Os movimentos centrais e subjacentes são tão remotos quanto às relações entre centros e raios. Entretanto, esses movimentos aparecem mais claramente com o decorrer da história. Sobre essa discussão, as relações entre centros-raios e os movimentos deles derivados apresentam dois momentos de evolução. O primeiro diz respeito à internacionalização dos movimentos, ou seja, momento em que os atores componentes são de nacionalidades distintas. O segundo momento é aquele em que o uso do espaço cibernético permite maior eficiência e abrangência de atores.

2.1.3 Atores Não-Estatais e os Tabuleiros de Joseph Nye

As relações entre centro-raios, raios-raios e os movimentos derivados deles vêm sendo tratadas até este momento como estadocêntricas, mas na verdade essas relações abrangem outros atores. Limitar qualquer discussão sobre política externa do século XXI aos atores estatais é ignorar os deslocamentos de poder existentes atualmente no mundo. De acordo com Nye Jr (2012), neste século estamos assistindo constantemente dois deslocamentos de poder: transição de poder e difusão de poder.

De acordo com ele, a transição de poder é mais comumente conhecida, pois esse fenômeno é notado em toda a história civilizatória. Por outro lado, conforme apontado por Nye Jr (2012), a difusão de poder é um evento recente. Os avanços nas tecnologias de

informação e comunicação causaram uma difusão do poder tanto horizontal quanto vertical, ou seja, o poder se desloca também para os atores não estatais.

Para ilustrar como as relações internacionais são constituídas atualmente, Joseph Nye Jr (2002) utiliza a figura de um tabuleiro de xadrez. Este tabuleiro, entretanto, não é semelhante aquele tradicional, de um nível apenas, mas composto de três níveis de jogo. Cada um desses níveis apresenta uma temática específica, com uma distribuição de poder distinta.

Dessa forma, como ainda demonstra Nye Jr (2002), o tabuleiro superior é formado pelo poder militar e apresenta um cenário internacional unipolar, com os Estados Unidos no centro. No tabuleiro do meio, encontramos o nível econômico e um cenário multipolar, em que não somente os Estados Unidos tem destaque, mas alguns outros Estados também, como a China. Finalmente, no tabuleiro inferior estão todos os demais atores, sejam transnacionais, internacionais ou locais.

Assim, a imagem que vislumbramos nessa metáfora de Nye Jr (2002) são três cenários de três jogos distintos. Sobre essa metáfora, cabe ressaltar que os movimentos realizados em qualquer um dos tabuleiros podem impactar nos demais níveis de jogo. Por exemplo, Gilberto Dupas (2002) explica que o terceiro tabuleiro é decisivo para a manutenção da posição isolada dos Estados Unidos no primeiro tabuleiro.

Em virtude disso, a metáfora do tabuleiro de xadrez tridimensional de Joseph Nye Jr (2005) ainda é uma representação simplificada de um jogo mais complexo. Isso porque se observarmos a complexidade dos assuntos envolvidos no terceiro tabuleiro, como por exemplo, questões ambientais, sociais, humanitárias entre outras, perceberemos que um único tabuleiro não é suficiente para abarcar tantos temas. Em virtude disso, uma representação mais significativa, seria um jogo de xadrez multinível e de multitabuleiros, como aquele representado pelo tabuleiro "*Star Trek"*.

Esse tabuleiro foi elaborado com base na série de ficção cientifica "Jornada nas Estrelas" da década de 60. Embora esse tabuleiro tenha sido utilizado na série como objeto decorativo daquele programa de televisão, diversos fãs tentaram operacionalizar o jogo de forma a torná-lo real. Dentre essas tentativas, o conjunto de regras mais famoso foi aquele criado por Andrew Bartness em 1976.

As regras de Bartness se tornaram famosas principalmente devido ao consentimento de Franz Joseph Schnaubelt, responsável pelos objetos da série. O Tabuleiro *Star Trek* é composto por três tabuleiros principais e maiores (4x4 casas) e mais quatro menores (2x2 casas), chamados de tabuleiros de ataque. Esses tabuleiros menores são moveis, e podem ser anexados em qualquer um dos tabuleiros principais.

As peças utilizadas por esse tabuleiro condiz com a mesma composição do jogo de xadrez tradicional. Entretanto, como os tabuleiros principais são menores quando comparados com um tabuleiro tradicional, o posicionamento das torres e dos cavalos é realizado nos tabuleiros de ataques, que inicialmente são dispostos dois em cada lado do jogo. Embora nessa distinta forma de se jogar xadrez a partida começa com o posicionamento e as mesmas movimentações do xadrez tradicional, as regras são diferenciadas no decorrer dos turnos.

A principal mudança é referente a movimentação dos tabuleiros de ataques. Esses tabuleiros somente podem ser anexados a outro nível se estiverem vazios ou com a presença apenas de peões, a peça de menor graduação no jogo. No caso das relações internacionais essa regra seria um pouco diferente e flexibilizada.

Isso porque abordagem de um tema da agenda dentro de outro, como por exemplo, o meio ambiente relacionado com a economia, depende do ator que realiza essa transição. Assim, para que um tabuleiro de ataque migre para outro nível não poderia estar vazia e dependeria do grau das peças e da rigidez do tema. Por exemplo, em temáticas flexíveis, como por exemplo, o próprio espaço cibernético, os peões conseguiriam realizar a transição dos tabuleiros, como veremos posteriormente. Diante dessas considerações, resta agora uma representação gráfica da distinção entre o tabuleiro do Nye Jr (2005) e o tabuleiro *Star Trek*:

Figura 2.1 – Tabuleiro Tridimensional de Joseph Nye Jr

NOVA PROPOSTA DE TABULEIRO	**TABULEIRO DE NYE**
	
TABULEIRO STAR TREK 3D CHESS	TABULEIRO STRATO CHESS

Fonte: Elaboração própria com base em Nye Jr (2005)

No tabuleiro proposto por Nye Jr (2005), somente conseguimos distinguir com precisão as agendas militar e econômica. As demais agendas ficam presentes no tabuleiro inferior e não conseguimos realizar uma distinção clara entre elas. Ademais, esse tabuleiro não considera os temas securitizados, que em algumas ocasiões são mais relevantes do que os tabuleiros econômico e militar.

Em contrapartida, o tabuleiro do modelo *Star Trek* possibilita compreender a securitização dos temas da agenda e a influência que um assunto pode ter dentro de outra temática. Assim, encontraríamos os mesmo tabuleiros militar (superior) e econômico (meio) de Nye Jr (2002), mas no nível inferior encontraríamos o tabuleiro político, em que a diplomacia está presente. Nesse modelo, além destes três tabuleiros de níveis, também encontramos tabuleiros móveis menores que podem ser anexados em cada um dos níveis conforme o contexto do jogo. Dessa forma, temas como o espaço cibernético é vislumbrado dentro do ambiente militar, econômico e político, simultaneamente.

Ademais, no modelo *Star Trek* é perceptível que atores não estatais também podem estar presentes dentro de tabuleiros predominantemente estatais, como o militar. Para compreender isso, basta recordarmos as fragilidades do espaço cibernético abordadas no primeiro capítulo. De acordo com o debate realizado, um indivíduo pode utilizar o espaço cibernético para afetar a defesa de um Estado.

Em virtude disso, mesmo com o poder significativo dos Estados Unidos no tabuleiro militar, uma pessoa ou empresa pode realizar um ataque cibernético e tirar do ar um sistema de comunicação estadunidense. O tabuleiro *Star Trek* permite vislumbrar essa possibilidade. Utilizando este tabuleiro como metáfora, ficam claras as visões de Timothy Garton Ash (2009) e Nye Jr (2012) de um mundo não somente multipolar, mas também de um mundo não polar.

Compreendendo a importância que os atores não estatais têm no espaço cibernético, enfatizada diversas vezes no primeiro capítulo dessa dissertação, cabe aqui afirmar a abrangência que os movimentos centrais e subjacentes apresentam. Estes movimentos não são exclusivos dos Estados, mas também apresentam participação de atores não governamentais, sejam eles empresas ou até grupo de indivíduos, como já dito anteriormente.

Dessa forma, encontramos exemplos de atuação de atores não estatais dentro dos movimentos centrais, como por exemplo, a Google. Ela aparece como uma defensora do movimento central quando tenta operar na China. Como esse país asiático dispõe de uma

configuração desvinculada da rede mundial, ele consegue obstruir o acesso de algumas páginas do Google dentro de seu território.

Encontramos também a atuação de atores não estatais dentro dos movimentos alternativos, como por exemplo, o navegado *The Onion Router* (TOR). Este navegador prevê o acesso à rede mundial desvinculada dos controladores da Internet e permitindo o acesso anônimo às páginas. O navegador TOR é administrado por um grupo de voluntários anônimos e recebe apoio de um grupo de atores não estatais autoproclamados "*The Internet Defense League"*[24].

Sobre os movimentos reacionários, o ator não estatal que podemos citar como exemplo é o *Wikileaks*. Essa organização tinha em sua propriedade uma série de documentos secretos dos Estados Unidos, que comprometia a imagem estadunidense nas relações internacionais. O *Wikileaks* tentou comprometer a estrutura de poder estadunidense por meio dessas informações, divulgando-as na rede.

Por fim, cabe ressaltar, que de todos esses movimentos, encontramos uma maior gama de exemplos da participação de atores não estatais nos movimentos reacionários. Isso ocorre devido ao que Nye Jr (2012) escreve sobre os recursos financeiros necessários para atuar no espaço cibernético, sobre a acessibilidade de se criar vírus e sobre a complexidade de se criar armas cibernéticas de alto nível. Em virtude disso, os atores não estatais tem maior possibilidade de questionar o poderio estadunidense do que custear o sistema vigente no lugar dos Estados Unidos.

2.2 PODER CIBERNÉTICO

2.2.1 Poder e suas Categorias

O mundo pode ser interpretado por meio de diferentes visões, dentre elas podemos interpretá-lo pela perspectiva de centros e raios. Os movimentos centrais e subjacentes são pautados pela disputa de poder nas relações internacionais. Em virtude disso,

[24] Grupo atualmente composto por 45 atores: Mozilla; Reddit; Cheezburger Network; Participatory Politics Foundation; EFF; WordPress; BoingBoin0067; Tor; Access Now; Avvo; Us Representative Darrell Issa; Open Technology Institute; CREDO Mobile; 4chan; HotspotShield; Fark.com; Public Knowledge; Tech Dirt; Imgur; Citizens for Self Governance; Doll Divine; Song Meaning; CDT; Grooveshark; Dutch Member of the European Parliament Marietje Schaake; Free Press; Personal Democracy Media; Torrentfreak; Zoe Lofgren; OverBlog; Indenti.ca; Statusnet; ECA; ROFLCon; Hypermachine; Craigs Connect; Ruckus.; Politihacks; Computer and Communications Industry Association; Open Media (Canada); Demand Progress; La Quadrature; PHP; Private Internet Access; e Piwik.

compreender o conceito de poder e suas categorias é preponderante para entender esses movimentos dentro das relações internacionais do espaço cibernético.

A compreensão do poder, entretanto, é complexa, pois se trata de um conceito impreciso e de difícil mensuração (NYE JR, 2012). Compreender o conceito de poder se assemelha a entender o conceito de tempo. Por causa disso, a frase de Santo Agostinho sobre o tempo também pode ser aplicada ao poder:

> Quando dele falamos, compreendemos o que dizemos. Compreendemos também o que nos dizem quando dele nos falam. O que é, por conseguinte, o tempo? Se ninguém me perguntar, eu sei; se o quiser explicar a quem me fizer a pergunta, já não sei. (AGOSTINHO, 1996, p. 265).

Na colocação de Santo Agostinho, se trocarmos a palavra "tempo" pelo termo "poder", a citação não apresentaria prejuízo de veracidade. Isso ocorre porque, como na definição de tempo, o conceito de poder é uma ideia básica, conforme apontado por Joseph Nye Jr (2012). De acordo ainda com ele, toda ideia básica é contestada, ou seja, de difícil consenso.

Assim, não há uma definição universalmente aceita por todos que utilizam o termo "poder", sendo a predileção por uma definição reflexo dos valores pessoais de cada pesquisador e de seus interesses (NYE JR, 2012). Sobre essas variações conceituais, algumas pessoas definem o poder como a capacidade para fazer ou resistir às mudanças (NYE JR, 2012). Ademais, há também quem o defina como a capacidade para conseguir o que se quer (NYE JR, 2012).

Por outro lado, Nye Jr (2012) relaciona poder com duas vertentes: os recursos e a questão comportamental. Dessa forma, para ele, o poder pode ser definido como recursos e também pode ser definido como resultados comportamentais. Na primeira definição, o poder de um Estado é definido pelos seus recursos, que por meio de estratégias, conseguem alcançar resultados pretendidos. Na segunda definição, por outro lado, poder significa afetar outros por meio da coerção, recompensa e atração, visando alcançar resultados preteridos.

Ademais, pelo estudo de poder realizado por Joseph Nye Jr (2012), podemos inferir que o poder é: elástico; rígido; relacional; e perceptível. O poder é elástico, pois se refere às relações sociais mais efêmeras, que mudam constantemente, dependendo da circunstância, conforme apontado por Nye Jr (2012). Isso porque o poder pode estar traduzido em recursos militares, mas também pode ser observado como recursos financeiros.

Por outro lado, ele também é rígido, pois os recursos que produzem poder em um relacionamento ou contexto social podem não produzir efeitos em outros (NYE JR, 2012). Dessa forma, uma nação não consegue projetar seu poder militar em todas as esferas de atuação, pois ele não se aplica aos demais contextos sociais. Por exemplo, o poder advindo da posse de tanques não pode ser aplicado dentro da dimensão virtual do espaço cibernético.

Além disso, o poder também é relacional, pois tê-lo significa influir sobre alguma coisa ou alguém para conseguir um resultado esperado. Em virtude disso, não é correto dizer que algo ou alguém é poderoso sem um aspecto referencial (NYE JR, 2012). Assim, um país é poderoso quando comparado com outro país e uma pessoa tem poder sobre as demais, quando estas não apresentam recursos e capacidades para evitarem mudanças.

De acordo com Nye Jr (2012), a característica relacional do poder gera três aspectos, chamados de faces e demostrados pelo quadro abaixo:

Quadro 2.1 – Três aspectos do poder nacional

PRIMEIRA FACE: A usa ameaças ou recompensas para mudar o comportamento de B contra as preferências e estratégias iniciais deste. B sabe disso e sente o efeito do poder de A.
SEGUNDA FACE: A controla a agenda das ações de uma maneira que limita as escolhas de estratégias de B. B pode ou não saber disso e estar consciente do poder de A.
TERCEIRA FACE: A ajuda a criar e moldar as crenças, percepções e preferências básicas de B. É improvável que B tenha consciência disso ou entenda o efeito do poder de A.

Fonte: Nye Jr (2012, p. 36)

Essas faces demonstram que o poder também é perceptível, ou seja, o seu uso depende da imagem que ele projeta sobre demais atores. Essa capacidade de projeção é o que permite a dissuasão. Em algumas vezes, essa aparência de dispor de poder é suficiente para impedir um comportamento rival, mas outras vezes não. Nye Jr (2012) exemplifica que atores não estatais conseguem enfrentar potências com grande poder militar mesmo sem dispor de poder comparável, como por exemplo, os grupos terroristas.

Nas relações internacionais, a projeção de poder pode ser realizada, de acordo com Nye Jr (2012), de três formas distintas: poder duro; poder brando; e poder inteligente. O primeiro diz respeito à projeção tradicional de poder, ou seja, meios essencialmente militares e uso da força, enquanto o segundo diz respeito à utilização de meios como diplomacia, economia e informação, ou seja, sem o uso direto da força. A terceira categoria de poder diz

respeito à mescla do poder duro e brando, ou seja, o uso da força com base nos recursos informacionais.

Independente da categoria utilizada, o poder é definido como recursos ou/e como resultados comportamentais. Mediante isso, cabe compreender o que é o poder cibernético. Ademais, cabe também abordar como as faces do poder se revelam dentro do espaço cibernético.

2.2.2 Abordagem Conceitual sobre Poder Cibernético

O advento do espaço cibernético não significa o fim da geografia espacial ou do Estado, como aparentou alguns pesquisadores. Por isso, um Estado consegue utilizar o monopólio da força e exercer seu poder também nesse novo espaço. Em virtude disto, este tópico tem como objetivo central debater parâmetros existentes sobre o espaço cibernético, que são utilizados como indicadores comparativos de poder cibernético.

Esses indicadores são definidos como comparativos, pois de acordo com Nye Jr (2012), o poder é relacional. Essa característica do poder, ainda conforme ele, deriva das duas definições que compõe esse conceito: poder como resultado de comportamentos e poder como recursos. Assim, os recursos que serão abordados como indicadores de poder cibernético servem para comparar os poderes cibernéticos dos Estados.

De acordo com Nye Jr (2012), o poder cibernético é algo novo, pois somente recentemente foram criados a banda larga e os parques de servidores. Além disso, quando Nye Jr (2012, p. 162) fala do poder cibernético, o define como "um conjunto de recursos que se relacionam à criação, ao controle e à comunicação da informação eletrônica e baseada em computadores – infraestrutura, redes, software, habilidades humanas". De acordo com essa definição, além da banda larga e dos servidores, o autor engloba como recursos do poder cibernético a infraestrutura, redes, software e as habilidades humanas.

Apesar de ser recente e de definição complexa, alguns institutos de pesquisa já vêm tentando mensurar o poder cibernético. Isso também é feito com outras categorias de poder, como o poder militar, mensurado pelo *Stockholm International Peace Research Institute (SIPRI).* Entretanto, os índices de mensuração de poder, de modo geral, devem ser observados com cautela.

Isso porque as características do poder e a sua variação conforme o contexto, o torna complexo para mensuração (NYE JR., 2012). Entretanto, mesmo assim, Nye Jr (2012) explica que vários analistas tentaram quantificar o poder nos assuntos internacionais.

Exemplificando isso, ele nos recorda de Ray Cline, que foi um funcionário da CIA e fornecia informações sobre o poder americano e soviético durante a Guerra Fria.

Esse especialista era muito influente e suas opiniões afetaram opiniões políticas e colocaram em jogos bilhões de dólares. De acordo com Nye Jr (2012), em 1977, Cline divulgou a formula que utilizava para avaliar o poder das nações naquele período. Assim, o poder era mensurado por ele com a seguinte equação:

Quadro 2.2 – Equação para Mensuração de Poder de Ray Cline

PODER PERCEBIDO = (POPULAÇÃO + TERRITÓRIO + ECONOMIA + MILITARES) X (ESTRATÉGIA + VONTADE)

Fonte: Nye Jr (2012, p. 24)

Entretanto, essa equação começou a ser descartada com o final da Guerra Fria. Isso porque ela demonstrava uma superioridade soviética sobre o poder americano e como sabemos, a União Soviética colapsou em 1991. Outro exemplo citado por Nye Jr (2012) sobre um possível cálculo de poder considera as variáveis: recursos de um país e desempenho nacional.

Dentre os recursos de poder de um país, ele aponta para as tecnologias, empresas, recursos humanos, recursos de capitais e recursos físicos. Por sua vez, o desempenho nacional é pautado pelas restrições externas, infraestruturas e ideias. Além disso, os pesquisadores que utilizavam esse cálculo também consideravam como um país determinava a sua capacidade militar e a sua proficiência no combate (NYE JR, 2012). Entretanto, essa formula somente era utilizada sobre o poder militar, não sobre as demais categorias (NYE JR, 2012), o que evidencia a característica rígida do poder.

No caso do espaço cibernético, o instituto que atualmente mensura o poder cibernético nas relações internacionais é o *Booz Allen Hamilton* (BAH). Ele é um grupo de consultoria estadunidense que criou um *"Cyber Power Index".* Embora atualmente esse seja o único índice publicado sobre poder cibernético, já identificamos outros projetos de mensuração em fase inicial, como por exemplo, o Centro para Estratégias do Ciberespaço e Ciência de Segurança (CSCSS), que está localizado no Reino Unido.

Sobre a mensuração realizada pelo BAH (2011), o índice criado trabalha quatro categorias de analises: marco regulatório e legal; contexto socioeconômico; infraestrutura tecnológica; e aplicação industrial. As duas primeiras variáveis da metodologia do BAH (2011) estão relacionadas com a vontade de causar ou moldar um comportamento, ou seja, o

poder como resultados comportamentais. Por sua vez, a infraestrutura tecnológica e a aplicação industrial estão relacionadas com o conceito de poder como recursos.

Dessa forma, o poder cibernético apresenta tanto uma parcela de recursos, como também a parcela da burocracia e dos contextos sociais. A parcela dos recursos compõe o potencial do poder cibernético e a parcela da burocracia e dos contextos sociais compõe a capacidade desse poder. Sem a segunda parcela, um Estado não consegue utilizar seus recursos tecnológicos.

2.2.3 Poder Cibernético Factual e Especulativo

Uma das consequências do poder é a projeção de percepções. Assim, um poder pode ser notado ou não pelos demais atores. Ademais, um poder também gera percepções nos próprios titulares, pois encorajam ou desencorajam comportamentos. Dessa forma, um poder gera autoimagens e anti-imagens.

A relação entre autoimagem e anti-imagem surge com a percepção de interesse nacional como algo positivo ou negativo. De acordo com Jervis (1970), a percepção de uma imagem pode gerar cooperações ou conflitos. Para ele, mesmo que uma imagem projetada seja intencionalmente cooperativa, quando mal projetada pode gerar uma situação de percepção enganosa.

A partir dessa percepção enganosa, um país pode interpretar uma atitude imperialista do proponente, gerando assim uma anti-imagem negativa. Mesmo tal decisão sendo imposta por meio do poder brando, ainda assim será considerada negativa. Isso porque ela se choca com o interesse nacional do país que se sente ameaçado.

Por outro lado, a anti-imagem também surge da autoimagem negativa. Para Kaplowitz (1990), existe uma relação entre negatividade e comportamentos totalitaristas. A partir dessa ideia, o Estado pode se comportar de quatro formas, conforme abaixo:

Quadro 2.3 – Relações Entre Posturas e Categorias de Imagens

Posturas	Consequência da Autoimagem	Anti-imagem
Totalista	Percepção negativa do outro	Extremista, virtude da necessidade de sobrevivência
Totalista de Longo Prazo	Percepção negativa do outro, mas respaldada devido à limitação de poder	Flexível, concedendo abertura para negociação
Competitiva	Percepção positiva ou negativa dependendo da convergência de objetivos	Leve na percepção negativa e inexistente na positiva
Firme, mas cooperativa	Percepção positiva de si e do outro	Existente somente se há um monopólio de agenda

Fonte: Elaboração própria baseada em Kaplowitz (1990)

Dessa forma, a anti-imagem está vinculada com a autoimagem de um país e as estratégias de comportamento adotadas por ele. Assim, quando o país A se percebe positivamente e o país B negativamente, o país B também adotara a mesma percepção em relação ao país A. Além disto, as estratégias de comportamento adotadas geram também anti-imagens, que surgem de uma reação entre a estratégia adotada e a percepção negativa.

Essas posturas são adotadas mediante a auto percepção de poder que um Estado apresenta de si mesmo. Teoricamente, quanto maior é o poder percebido pelo ator estatal, mais rígida será a postura adotada. Essa relação de postura e poder é tão íntima, que conseguimos notá-la nas faces do poder de Joseph Nye Jr (2012).

Essa postura também influencia as pesquisas de Nye Jr (2012) sobre o poder cibernético. Embora ele não tenha abordado as relações entre imagens e percepções dentro do espaço cibernético, ele aborda o comportamento resultante do emprego do poder cibernético. Para tal, ele também nomeia essas relações de "faces".

Dessa forma, Nye Jr (2012) nos apresenta três faces do poder cibernético. Na primeira face, os demais atores percebem as intenções do Estado, enquanto na segunda podem perceber ou não. Na terceira face, os atores não percebem a intenção dos Estados, conforme mostra o quadro abaixo:

Quadro 2.4 – As três faces do poder no domínio cibernético

PRIMEIRA FACE **(A induz B a fazer o que B inicialmente não faria)** Duro: ataques de negação de serviços, inserção de *malwares*, interrupções de sistema Scala, prisões de *bloggers*. Brando: campanha de informação para mudar as preferências iniciais dos *hackers*, recrutamento de membros de organizações terroristas.
SEGUNDA FACE **(A impede a escolha de B excluindo as estratégias de B)** Duro: *firewalls*, filtros e pressão sobre as companhias para excluir algumas ideias. Brando: automonitoramento de ISPs e *sites* de busca, regras do ICANN sobre os nomes de domínios padrões de *software* amplamente aceitos.
TERCEIRA FACE **(A molda as preferências de B para que algumas estratégias não sejam nunca consideradas)** Duro: ameaças de punir *bloggers* que disseminam material censurado. Brando: informações para criar preferências (como estimulação do nacionalismo e *hackers* patrióticos), desenvolvimento de normas de repulsa (como o caso da pornografia infantil).

Fonte: Nye Jr (2012, p. 171)

Quando observamos os dois quadros sobre faces do poder (Quadro 2.1 e Quadro 2.4), percebemos uma divergência quanto às percepções dos atores. No primeiro quadro sobre os três aspectos do poder, notamos uma degradação de clara percepção dos atos dos Estados

para um desconhecimento de suas ações na última face. Por sua vez, nas faces do poder cibernético, as ações exemplificadas no quadro 2.4 revelam um progresso na percepção, de um desconhecimento na primeira face para uma percepção clara na terceira face.

Isto ocorre, porque ações de negação, inserção de *malware*, interrupção de sistemas ou campanhas de informação somente são percebidas após o ataque. Por outro lado, ações de punição de *bloggers* e desenvolvimento de normas de repulsa dos crimes cibernéticos são facilmente notadas. Assim, a percepção do poder cibernético está mais ligada à identificação dos ataques, do que aos ataques em si.

Em virtude dessa dificuldade na percepção das ações no espaço cibernético, poderíamos considerar que o poder cibernético apresenta duas categorias: poder cibernético factual e poder cibernético especulativo. O poder cibernético factual é aquele que o Estado realmente apresenta recursos tangíveis, como por exemplo, número de satélites, servidores, *hackers*, estratégias, dentre outros. Por sua vez, o poder cibernético especulativo está mais associado ao discurso sobre capacidades e habilidades, ou seja, aos recursos intangíveis.

Essa categorização do poder cibernético não é aplicada plenamente nas outras categorias do poder. Isso porque é difícil para um Estado esconder uma esquadrilha de caças ou um grupo de cavalaria pesada em um território estrangeiro, mas é possível para um Estado espionar outro ator dentro do espaço cibernético sem que ele saiba. Da mesma forma, um Estado não conseguiria omitir um ataque direto realizado a um território inimigo, no máximo talvez negar a autoria, mas é possível realizar uma invasão a um sistema de governo sem que ele saiba que tal ataque tenha ocorrido.

Um exemplo factível do uso do poder cibernético especulativo ocorreu em 2013, por ocasião das revelações de Eduard Snowden sobre a espionagem aos líderes mundiais pelos Estados Unidos. Naquela ocasião, o presidente dos Estados Unidos, Barack Obama, se pronunciou sobre as acusações de espionagem e afirmou que teriam capacidade de realizar a espionagem, mas não o fizeram (TERRA NOTÍCIAS, 2013). Dessa forma, ele negou o uso do poder cibernético factual, mas não refutou o uso do poder cibernético especulativo.

3 ESTADOS UNIDOS E OS DEMAIS CENTROS DO ESPAÇO CIBERNÉTICO

O mundo visualizado sob a perspectiva dos centros e raios pode ser vislumbrado também no âmbito do espaço cibernético. No mundo, os Estados centrais são aqueles capazes de moldar as relações internacionais conforme seus interesses nacionais. Entretanto, esses Estados não são homogêneos, mas apresentam distinções e assimetrias, o que justifica a caracterização dos centros no espaço cibernético.

A caracterização possibilita o mapeamento dos principais movimentos centrais e subjacentes do espaço cibernético. Em virtude disso, este capítulo identifica quais os centros do espaço cibernético. Para isso, a primeira seção observa a penetração do espaço cibernético no mundo, como também os controladores desse espaço e os principais países produtores de conhecimento sobre esse tema.

Compreendendo quem são os centros do espaço cibernético, o capítulo realizou a caracterização de cada um deles. O intuito de caracterizar um país é compreender padrões que os tornam distinto dos Estados raios, facilitando a separação das duas categorias. Para tanto, observou-se o âmbito do espaço cibernético nos contextos socioeconômicos, infraestruturas de tecnologias e marcos regulatórios de cada centro.

3.1 QUEM SÃO OS CENTROS NO ESPAÇO CIBERNÉTICO

3.1.1 Penetração do Espaço Cibernético no Mundo

O espaço terrestre apresenta diversas vias de conectividade para as pessoas: calçadas, ruas, rodovias, ferrovias, etc. No espaço cibernético não é diferente, para que as pessoas possam se conectar uma com as outras, precisam acessar as vias da Internet. Em virtude disso, o indicador de penetração da Internet auxilia para identificarmos os centros do espaço cibernético.

Como o próprio nome diz, esse indicador mensura o quanto a Internet perpassa uma sociedade. Ademais ele também mensura o recurso de poder da terceira camada do espaço cibernético: o componente cognitivo. De acordo com Daniel Ventre (2011), o componente cognitivo é composto por todos os usuários do espaço cibernético.

Dessa forma, o índice de penetração da Internet nos remete a Nye Jr (2012), quando esse discorre sobre a importância do indivíduo no espaço cibernético e a difusão de poder para esse ator. Assim, quanto maior a penetração da Internet, maior será o número de

usuários de um país no espaço cibernético. Cabe ressaltar que a quantidade de usuários no espaço cibernético pode ser tão benéfica quanto maléfica para um Estado.

Isso resulta do fato de cada estação de acesso à Internet ser um alvo em potencial de ataques cibernéticos. Assim, por um lado, muitos usuários conectados à Internet permite ao Estado ter massa cognitiva familiarizada com o espaço cibernético, que pode ser usada como recurso de poder cibernético. Em contra partida, um alto número de usuários significa maiores canais de acesso para ameaças externas à rede nacional.

Trabalhar com o índice de penetração da Internet não é algo tão recente ou escasso. Além do índice de poder cibernético da Booz Allen Hamilton (2011), encontramos também trabalhos de discussões acadêmicas, como os artigos de Chinn e Fairlie (2006) e de Kiiski e Pohjola (2002). Enquanto o primeiro artigo utiliza a penetração da Internet para comparar a disparidade do uso dessa tecnologia entre países, o segundo abordar as causas da penetração.

Kiiski e Pohjola (2002) utilizam como amostragem os países da Organização para Cooperação e Desenvolvimento Econômico (OCDE). Dentre as determinantes para o aumento da penetração da Internet nesses países, os autores elencaram como as principais: o Produto Interno Bruto (PIB) per capita e o custo de acesso à Internet. Assim, percebemos que além de impactar em todos os demais espaços, o espaço cibernético também é impactado por eles, isso é evidente quando pensamos no PIB per capita, que é uma variável indireta que impacta no espaço cibernético.

No trabalho de Chinn e Fairlie (2006) também observamos variáveis indiretas que impactam no espaço cibernético. Eles abordam variáveis econômicas – renda per capita, tempo de escolaridade, analfabetismo e abertura comercial –, variáveis demográficas – taxa de urbanização, dependência da juventude e idosos – e indicadores de infraestrutura – densidade telefônica e consumo de eletricidade. Por outro lado, esses autores também abordaram variáveis diretas, como por exemplo, preços das telecomunicações, regulamentação da qualidade delas e especificações para uso de computadores.

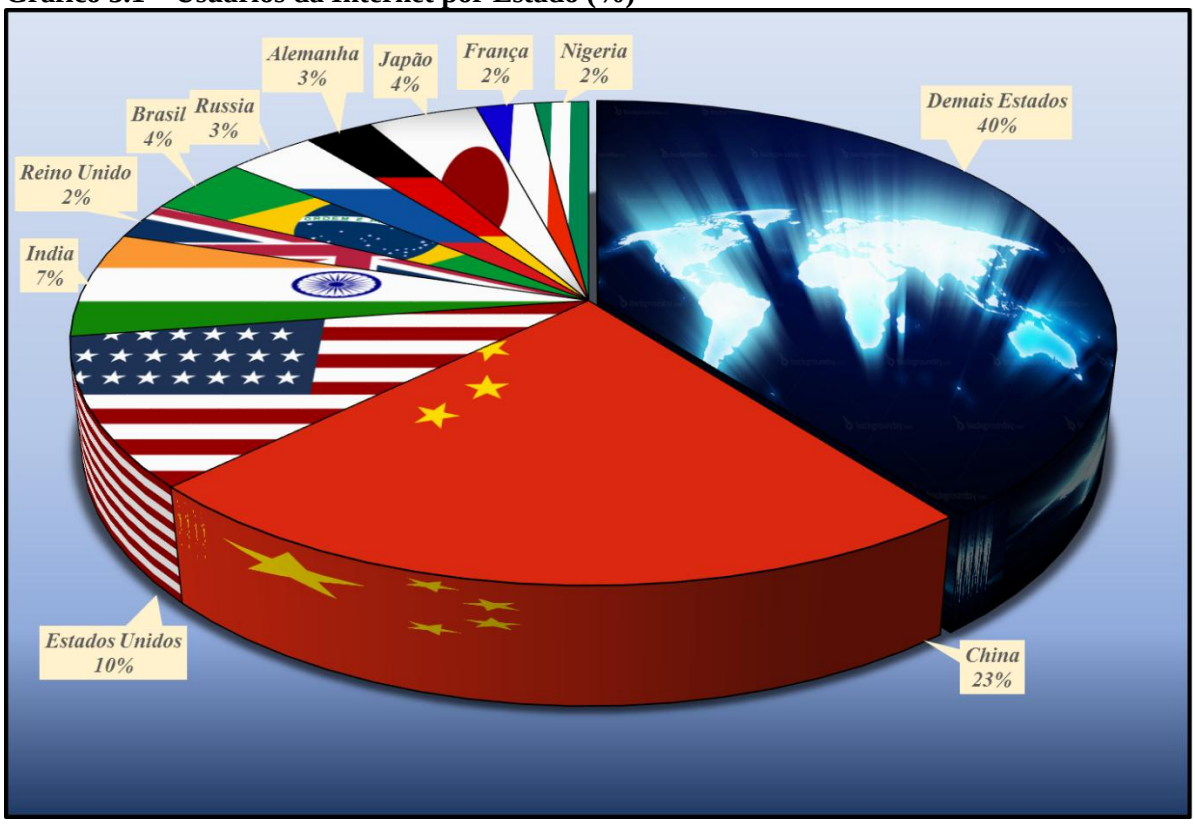
Na pesquisa realizada pela Booz Allen Hamilton (2011), a penetração da Internet é colocada dentro de uma categoria maior, chamada de "Acesso à Informação e Tecnologias de Comunicação". Dentro desta categoria, além da penetração da Internet, essa empresa mensurou a penetração da telefonia móvel e a penetração das redes sociais. Além disso, ela também considerou os pontos de acesso Wi-Fi de um país.

Para mensurar a penetração do espaço cibernético no mundo, essa dissertação segue um método semelhante ao da Bozz Allen Hamilton (2011). Assim, ela vislumbra a

penetração da Internet, que engloba todo o tipo de conexão, sejam aquelas feitas em computadores ou aquelas realizadas por dispositivos móveis e pontos de acesso Wi-Fi. Ademais, também vislumbra o preço da Internet, como uma variável prospectiva, e o PIB per capita, para averiguar o poder de neutralizar as consequências negativas de se ter um elevado número de usuários nesse espaço.

A quantidade de usuários da Internet por países pode ser sintetizada pelo gráfico abaixo:

Gráfico 3.1 – Usuários da Internet por Estado (%)



Fonte: Elaboração própria com base em World Bank (2015; 2015a)

Embora a China apresente quase 25% do total de usuários da Internet, ela é classificada como um Buraco Negro do Espaço Cibernético (RSF, 2006). Tal classificação ocorre, porque ela suprime o livre acesso à Internet (RSF, 2006). Isso significa que alguns sites são inacessíveis da China, como a própria lista dos países que são considerados Buraco Negro do Espaço Cibernético (RSF, 2006).

O fato de a China apresentar uma filtragem mais contundente do conteúdo que trafega em seu espaço cibernético facilita o controle dos crimes cibernético. Entretanto, o custo da liberdade é alto para tal. Ademais, a filtragem chinesa não visa o controle

cibernético, mas a manutenção do governo chinês. Dessa forma, o filtro da rede pode ser uma ferramenta de controle do espaço cibernético em um Estado.

Em virtude disso, o indicador de PIB demonstra não somente a predisposição para o aumento da penetração no espaço cibernético, como também a capacidade de um Estado de neutralizar as consequências negativas da penetração. Isso porque ele dispõe de recursos para investir em defesa e segurança cibernética. Além disso, mesmo com poucos usuários, quanto maior o PIB per capita, maior é a percentagem da população de um país com acesso ao espaço cibernético, como demonstrado pela tabela abaixo:

Tabela 3.1 – Relação entre PIB e Usuários da Internet (2013)

Países	PIB per capita (US$)	Usuários (% da população)	Usuários (Total)
Estados Unidos	52.980,0	84,2	266.490.921,10
Alemanha	46.255,0	84,0	67.711.179,00
Reino Unido	41.776,8	89,8	57.596.158,63
França	42.631,0	81,9	54.001.779,56
Japão	38.633,7	86,3	109.829.560,61
Rússia	14.487,3	61,4	88.113.243,35
Brasil	11.938,9	51,6	103.386.753,30
China	6.991,9	45,8	621.680.040,00
Nigéria	2.966,1	38,0	65.973.831,10
Índia	1.486,9	15,1	189.073.079,00

Fonte: Elaboração própria com base em World Bank (2015; 2015a; 2015b)

Por meio dessa tabela percebemos a relação entre PIB per capita e penetração na Internet, evidenciada anteriormente. Como também é possível observar que não existe uma relação direta entre PIB e quantidade de usuários do espaço cibernético total. Entretanto, podemos evidenciar que países como Estados Unidos, Alemanha e Reino Unido dispõem de maior capacidade financeira para lidar com a defesa cibernética.

Abordar o número de usuários que acessam a rede em um país nos fornece uma análise sobre quantidade do poder cibernético de um Estado. Entretanto, não basta ter o maior arsenal de bombas do mundo se elas não são ativadas quando necessário, ou seja, não adiante ter um grande poder cibernético se ele não apresentar qualidade. Para mensurar a qualidade desse poder, observaremos a velocidade da Internet disposta em cada país e o seu custo.

A velocidade é um indicador da qualidade da penetração, pois quanto mais rápido a conexão com a Internet, melhor será o tempo de reposta aos ataques. O custo da rede, por sua vez, serve como um indicador de controle, pois nos mostra se essa velocidade é acessível a todos os usuários. Sendo assim, a relação entre velocidade e custo pode ser observada pelo gráfico abaixo:

Tabela 3.2 – Relação entre Custo e Velocidade da Internet por País (2013)

Países	Preço de 1 Mbps (USD)	Velocidade Média (Mbps)	Velocidade Média (USD)	% do PIB per capita
Estados Unidos	3,52	37,7	132,704	0,25
Alemanha	2,65	31,7	84,005	0,18
Reino Unido	2,45	30,9	75,705	0,18
França	6,19	44,0	272,36	0,64
Japão	0,27	103,1	27,837	0,07
Rússia	0,61	30,1	18,361	0,13
Brasil	3,32	14,1	46,812	0,39
China	1,36	30,5	41,48	0,59
Índia	8,57	7,6	65,132	4,38

Fonte: Elaboração própria com base em World Bank (2015b); Ookla (2015; 2015a).

Pela percentagem do PIB per capita necessária para se adquirir uma Internet de velocidade mediana, podemos inferir que o espaço cibernético é acessível com qualidade nacional em todos os Estados analisados. Entretanto, a qualidade nacional varia consideravelmente em alguns casos. Exemplificando, encontramos o Japão, com velocidade maior que o dobro do segundo país com Internet mais veloz, e o Brasil e Índia, com velocidades consideravelmente abaixo dos outros Estados.

Dessa forma, quando analisamos a penetração do espaço cibernético pela quantidade de usuários, encontramos um domínio chinês-estadunidense, pois esses países detém 1/3 dos usuários desse espaço. Entretanto, quando analisamos também a relação entre PIB per capita e percentagem da população nacional com acesso ao espaço cibernético, destacam-se outros países. Além dos Estados Unidos, também encontraríamos a Alemanha, o Reino Unido, a França e o Japão, pois mais de 80% da população acessa a Internet.

3.1.2 Controladores do Espaço Cibernético do Setor Privado

A composição demográfica do espaço cibernético não demonstra por si só os Estados Centrais desse ambiente. Para isso, também é necessário observar os controladores desse espaço. Entretanto, este tópico somente engloba dados referentes ao setor privado, pois os atores não-governamentais ou setores estatais já foram observados no primeiro tópico, quando abordamos as instituições e organizações internacionais do espaço cibernético.

Dentre os dados utilizados, observaremos os navegadores. Eles são utilizados para acessar as páginas virtuais, mas eles não são o único recurso de acesso ao espaço cibernético. Além deles, existem compartilhadores de arquivos, mensageiros e outros programas que permitem o envio e a recepção de informação. Entretanto, parte considerável do espaço

cibernético é acessada por esses navegadores, cujos principais podem ser classificados quanto à nacionalidade e o valor de mercado:

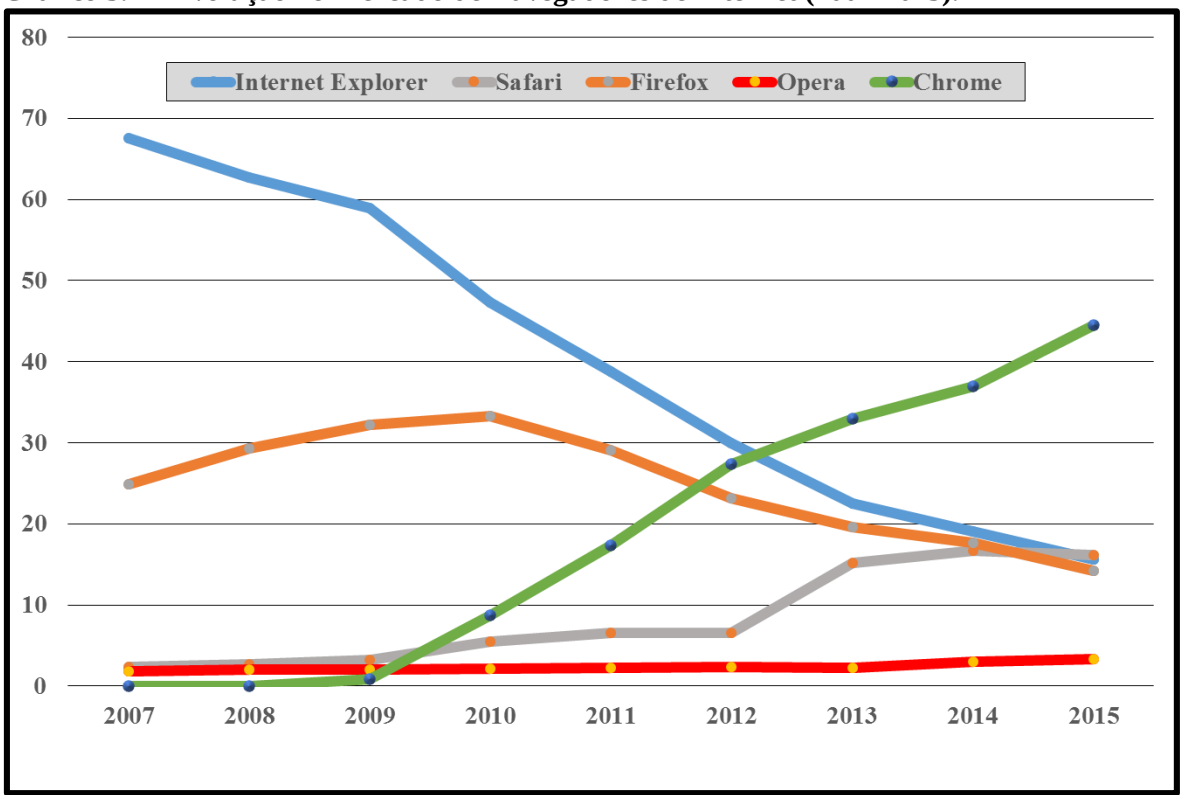
Quadro 3.1 – Nacionalidade e Valores dos Principais Navegadores de Internet

Navegadores	Empresas	Países	Valor de Mercado (USD)
Internet Explorer	Microsoft	Estados Unidos	343,8 bilhões
Safari	Apple	Estados Unidos	483 bilhões
Firefox	Mozilla Foundation	Estados Unidos	Sem fins lucrativos
Opera	Opera Softwares	Noruega	1 bilhão
Chrome	Google	Estados Unidos	382,5 bilhões

Fonte: Elaboração própria com base em Exame (2014) e TI Inside Online (2012).

Dos principais navegadores de Internet, somente um deles é de uma empresa sediada fora dos Estados Unidos, o Opera da Opera Software, na Noruega. Entretanto, o valor dessa empresa é irrisório quando comparada com os demais. Esse valor reflete inclusive a baixa popularidade que esse navegador apresenta, conforme gráfico abaixo:

Gráfico 3.2 – Evolução no Mercado de Navegadores de Internet (2007-2015).



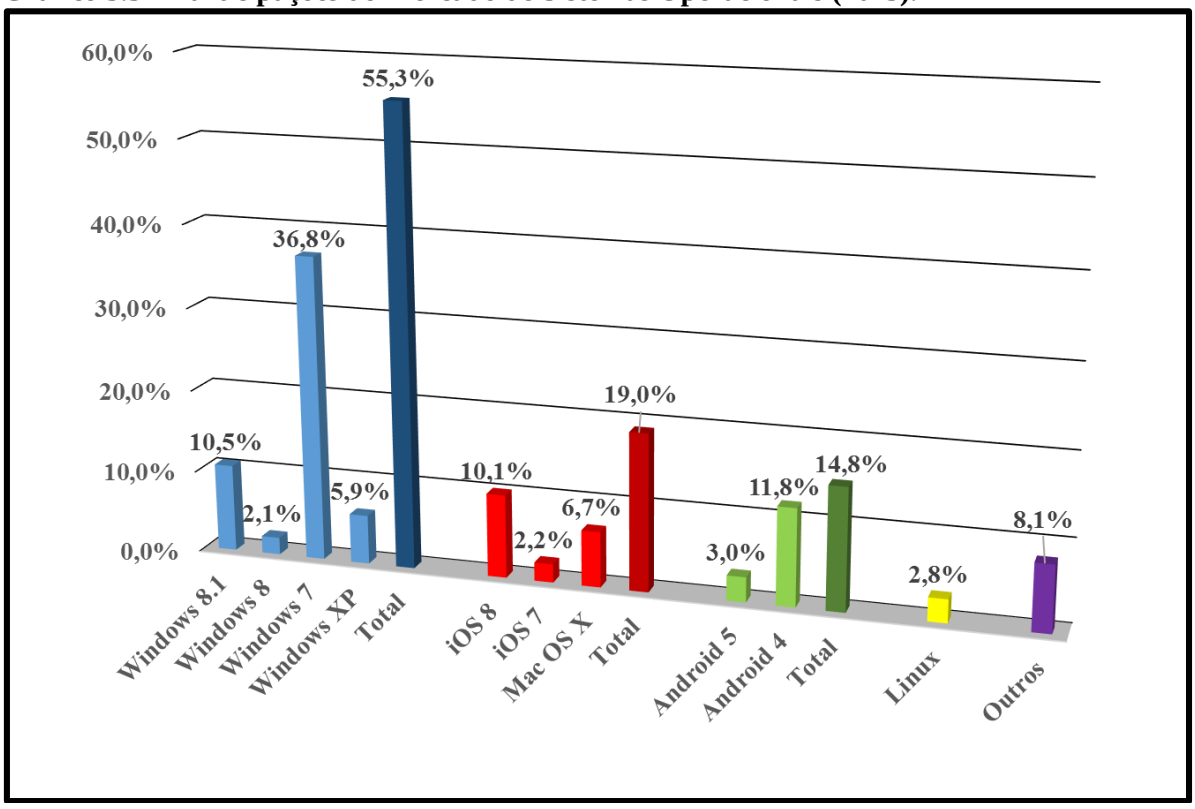
Fonte: Elaboração própria com base em W3Counter (2015).

Apesar de ser um nicho recente, o mercado de navegadores já apresenta mudança de liderança. Entretanto, cabe ressaltar, que a mudança de liderança da Internet Explorer para o Chrome não afeta o controle estadunidense dos navegadores. Isso fica patente quando

observamos a evolução da participação de mercado do navegador norueguês Opera, que sempre foi discreta.

Algumas das empresas responsáveis pelos navegadores, como a Microsoft, Apple e o Google, também são responsáveis por parte significativa do mercado de sistemas operacionais. Esses sistemas são compostos por programas que operacionalizam os *hardwares* [25] dos aparelhos de acesso ao espaço cibernético. O mercado de sistemas operacionais pode ser divido conforme gráfico abaixo:

Gráfico 3.3 – Participações do Mercado de Sistemas Operacionais (2015).



Fonte: Elaboração própria com base em W3Counter (2015a).

Diferente do mercado de navegadores, o mercado de sistemas operacionais é mais restrito. Isso porque os navegadores são criados por meio dos próprios sistemas operacionais, ou seja, estes demandam maiores investimentos e pesquisas. Em virtude disso, os navegadores com maior participação no mercado são de propriedade das empresas com maior valor de mercado (Quadro 3.1).

Dessa forma, a Microsoft, que responde pelo Internet Explorer, é a proprietária dos sistemas operacionais Windows. Por sua vez, a responsável pelo navegador Safari, a

[25] *Hardware* são os componentes físicos que formam os computadores e outros aparelhos tecnológicos. Eles são compostos por componentes eletrônicos.

Apple, também é proprietária dos sistemas operacionais OS. Outro exemplo é a Google, que é responsável pelo navegador Chrome e dona dos sistemas Android.

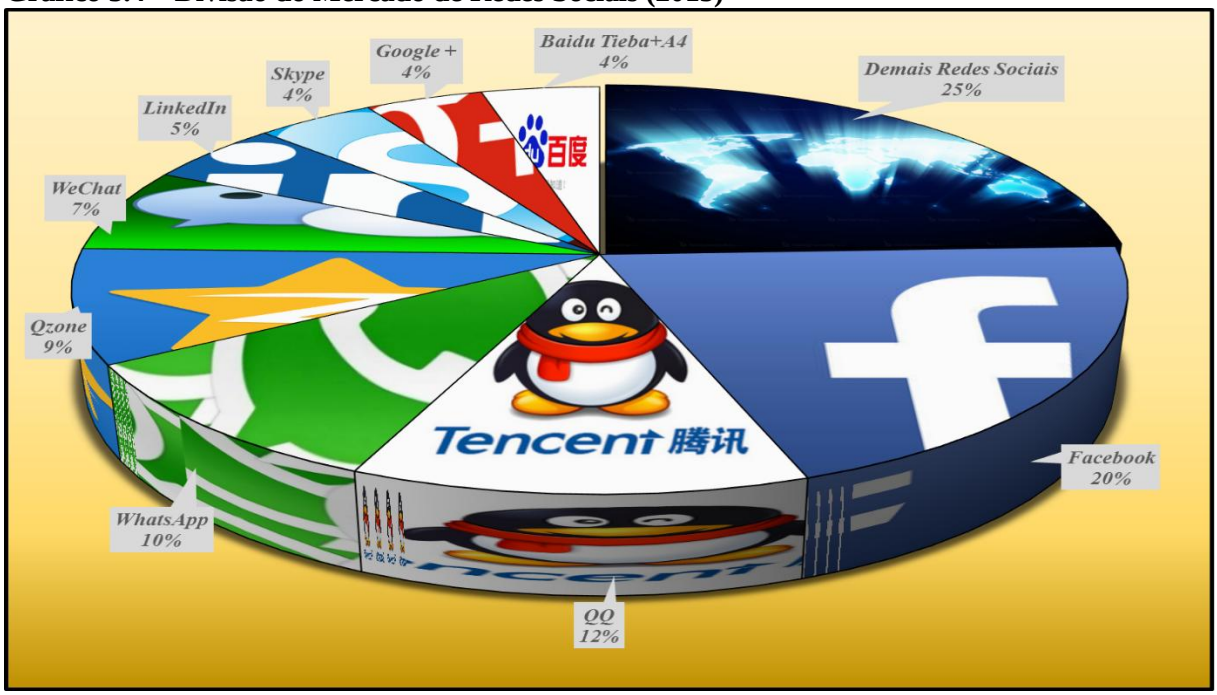
Igualmente como ocorre no mercado de navegadores, nos sistemas operacionais também encontramos iniciativas de códigos abertos. Assim, encontramos o navegador Mozilla e também o sistema operacional Linux. Essas duas iniciativas são utilizadas como exemplos pelos grupos que defendem um espaço cibernético livre do poder estatal.

Os navegadores e sistemas operacionais são utilizados para troca de informações no espaço cibernético. Essas informações, por vezes, podem ser interceptadas pelas empresas responsáveis por cada um desses programas. Cabe ressaltar nesse caso, que praticamente todo o mercado de sistemas operacionais são estadunidenses.

Entretanto, o navegadores e sistemas operacionais não são as únicas formas de captação de informações, pois as redes sociais também podem ser utilizadas para tal. As redes sociais são os principais produtores de perfis e identidades no espaço cibernético, pois neles os indivíduos divulgam não somente informações pessoais como também fotos, vídeos e outras formas de comunicações. Dessa forma, as empresas responsáveis pelas redes sociais apresentam um grande número de informações armazenadas em seus servidores.

Essas informações são armazenadas principalmente nos países em que cada empresa sedia. Por isso, apesar de serem atores privados, essas informações podem ser utilizadas por Estados indevidamente. Esse mercado pode ser dividido da seguinte forma:

Gráfico 3.4 – Divisão do Mercado de Redes Sociais (2015)



Fonte: Elaboração própria com base em Statista (2015).

Diferente dos mercados de navegadores e de sistemas operacionais, o mercado de redes sociais apresenta uma maior variação de nacionalidades. Enquanto o Facebook, o WhatsApp, o LinkedIn, o Skype e o Google + são empresas americanas, as demais empresas que apresentam participação significativa no mercado de redes sociais são chinesas. Em um contexto geral, o Facebook detém 30% do mercado, pois o Whatsapp também é de sua propriedade.

Dessa forma, os controladores do espaço cibernético do setor privado também podem ser divididos predominantemente em duas nacionalidades: estadunidense e chinesa, com a penetração de usuários do espaço cibernético. Entretanto, cabe ressaltar que as empresas estadunidenses apresentam maior predileção do que as chinesas, pois estas são predominantemente escolhidas por usuários da China, não apresentando uma projeção mundial semelhante às das empresas dos Estados Unidos.

3.1.3 Produtores de Conhecimento sobre Espaço Cibernético

Alguns pesquisadores, como visto anteriormente, utilizam algumas variáveis como sugestivas de estudos prospectivos. Igualmente, visualizar os produtores de conhecimento permite não somente compreender os países com foco acadêmico na questão do espaço cibernético, como também compreender quais nações apresentam potenciais futuros. Para tal, não basta analisar somente as produções cientificas, mas também a propriedade intelectual dos países e seus investimentos em Produção e Desenvolvimento (P&D).

A propriedade intelectual é utilizada como uma forma de proteção de conhecimento (BUAINAIN, 2005). Em virtude disso, ela pode quantificar a geração de conhecimento de um Estado. Ademais, ela também permite compreender os benefícios econômicos da geração de conhecimento para um Estado:

Tabela 3.3 – Balança de Pagamento em Propriedade Intelectual (2014)

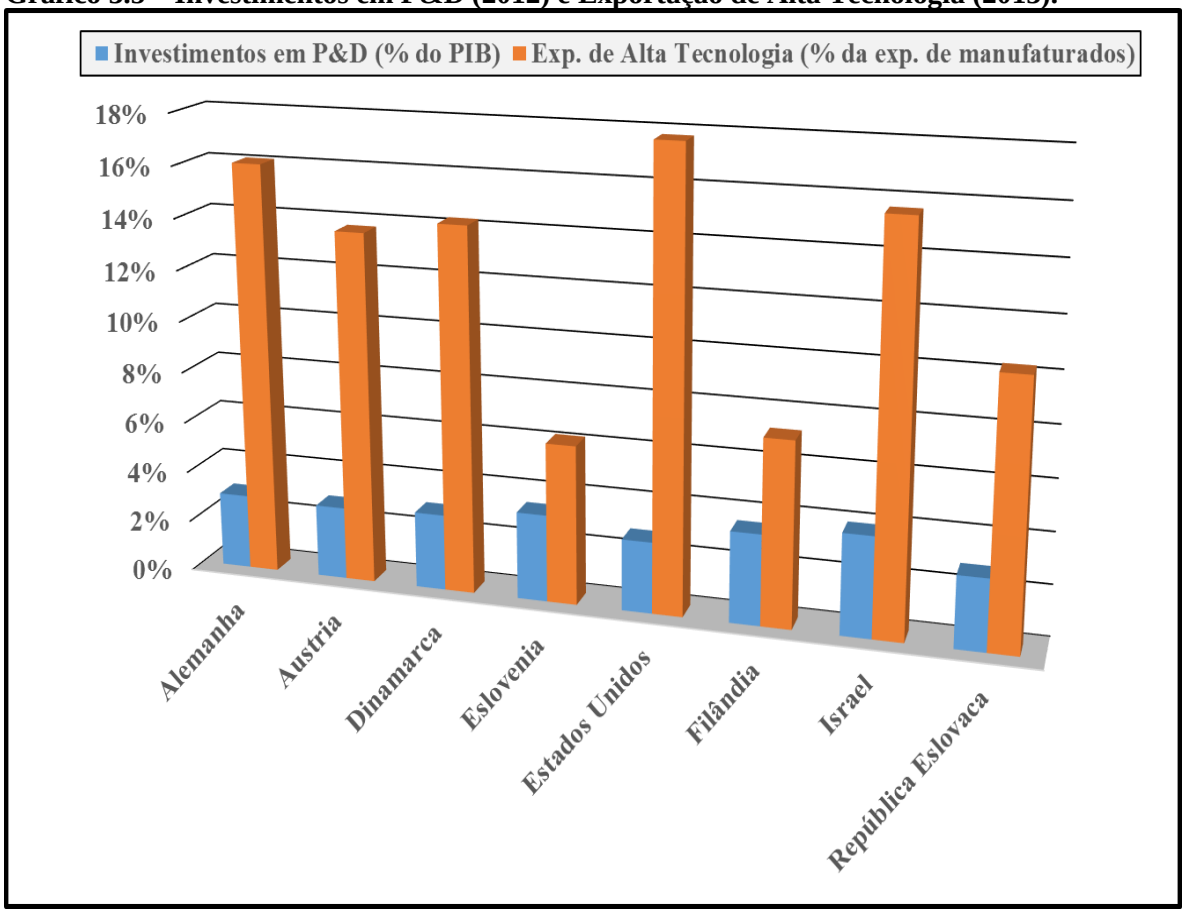
Países	Recebimento (USD)	Pagamentos (USD)	Saldo Final (USD)
Estados Unidos	132.653.000.000,00	41.940.000.000,00	*90.713.000.000,00*
Japão	36.825.091.036,70	20.923.212.289,38	*15.901.878.747,32*
Reino Unido	20.002.922.361,36	10.837.125.075,63	*9.165.797.285,73*
Alemanha	13.797.145.696,25	8.122.212.953,69	*5.674.932.742,56*
Suíça	16.627.790.848,02	12.351.406.707,94	*4.276.384.140,08*
França	11.917.478.827,53	10.233.725.383,89	*1.683.753.443,64*
Hungria	2.091.229.670,10	1.728.192.134,84	*363.037.535,26*
Islândia	163.297.958,94	110.796.021,65	*52.501.937,29*

Fonte: Elaboração própria com base em World Bank (2015c; 2015d).

Esses oito países são os que mais lucram com propriedade intelectual do mundo. Cabe ressaltar que esses dados não englobam somente o conhecimento referente ao espaço cibernético. Entretanto, mesmo sendo dados abrangentes, eles demonstram que os Estados Unidos, Japão e Reino Unido apresentaram maior capacidade de gerar conhecimentos, inclusive sobre o espaço cibernético.

Outro dado importante são os investimentos relacionados à pesquisa e desenvolvimento de um país. Esses investimentos podem gerar também lucros, além da detenção de novas tecnologias. Em virtude disso, cabe observar qual percentagem do PIB é investida em P&D e a quantidade que é exportada:

Gráfico 3.5 – Investimentos em P&D (2012) e Exportação de Alta Tecnologia (2013).



Fonte: Elaboração própria com base em World Bank (2015e; 2015f).

Assim, os principais países que investem em P&D apresentam percentuais relativos quando comparados. Entretanto, os Estados Unidos, Alemanha e Israel apresentam maiores exportações de alta tecnologia. Como o espaço cibernético é altamente tecnológico, a propriedade intelectual e os investimentos em P&D revelam o potencial dos Estados Unidos, Alemanha e Reino Unido nesse campo.

Como dito anteriormente, o espaço cibernético foi territorializado recentemente pelo homem, quando comparado com os demais espaços geográficos. Por isso, os estudos sobre ele também são recentes e de pouco volume. Para ilustrar isso, quando pesquisamos o termo "cyber", no banco de dados da JSTOR (2015), encontramos 14.379 artigos científicos.

Esse número é relativamente baixo quando comparado com os temos *"international relations"* (806.600 resultados), *"foreign policy"* (730.990 resultados), "*defense"* (730.501 resultados). A limitação de produção não está relacionada apenas aos artigos. Quando observamos as revistas cientificas e os livros específicos sobre esse assunto catalogados no banco de dados da SJR (2015) e JSTOR (2015) encontramos uma limitação semelhante:

Tabela 3.4 – Principais Produtores de Conhecimento sobre Espaço Cibernético

	Revistas Científicas				**Livros**			
Países	1961-1989	1990-2000	2001-2013	***Total***	1998-2005	2006-2010	2011-2015	***Total***
Austrália						1		***1***
Bélgica	1		2	***3***				
China			2	***2***	2		1	***3***
Estados Unidos	4	3	8	***15***	7	2	17	***26***
Países Baixos			1	***1***		1		***1***
Reino Unido			1	***1***		3	5	***8***

Fonte: Elaboração própria com base em SJR (2015); JSTOR (2015).

Embora as revistas científicas e livros acadêmicos sobre espaço cibernético apresentem relevância semelhante, percebemos uma discrepância entre as produções americanas e inglesas face às demais. Assim, em termos de produtores de conhecimento, os principais centros vislumbrados são: Estados Unidos; Reino Unido e Alemanha. Enquanto os Estados Unidos se destacaram em todos os pontos analisados, o Reino Unido se destacou tanto nos lucros com propriedade intelectual como na produção de revistas e livros científicos. Por sua vez, a Alemanha se destacou em propriedade intelectual e investimentos em P&D.

3.2 ESTADOS UNIDOS NO ESPAÇO CIBERNÉTICO

3.2.1 Contexto Socioeconômico

Observar o contexto socioeconômico de um país requer a construção de um retrato de todas as extensões da vida de um povo. Quando a BAH (2011) selecionou os critérios para análise do contexto socioeconômico dos países, ela utilizou variáveis diretas e

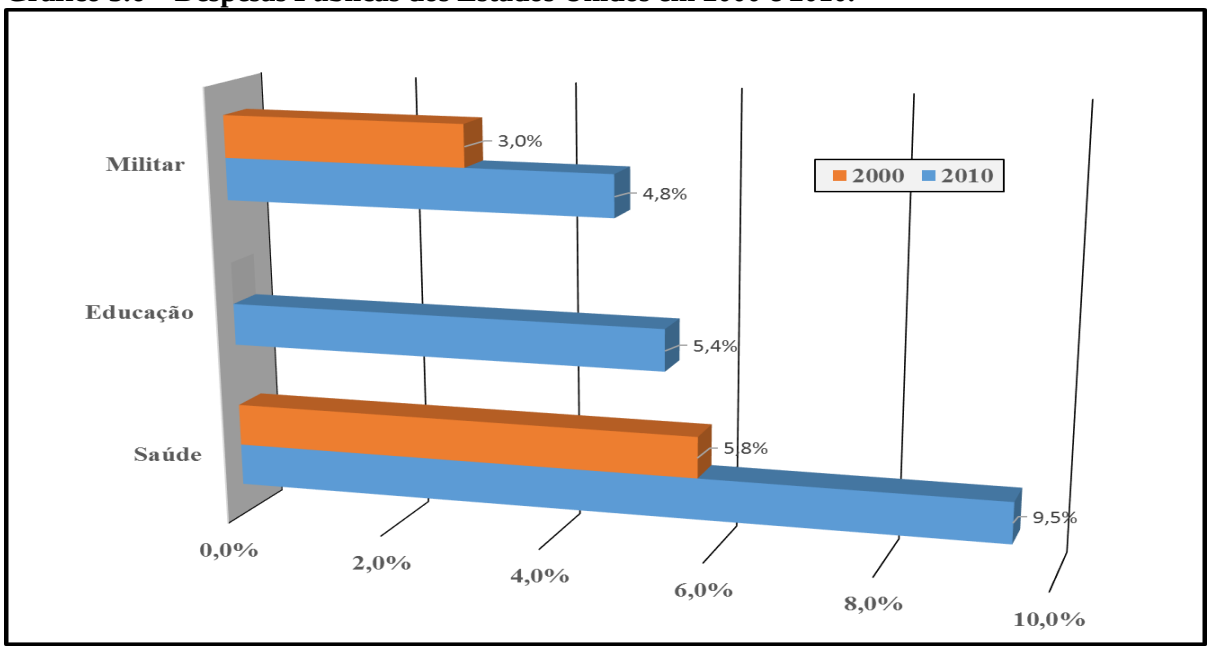
indiretas. Como o foco dessa seção é conhecer os principais centros do espaço cibernético serão avaliadas apenas as variáveis diretas.

Dentre os Estados analisados anteriormente como centros do espaço cibernético, os Estados Unidos demonstraram destaque em todas as variáveis vislumbradas. Macroeconomicamente falando, ele apresenta investimentos prioritários no setor de serviço, conforme observado no relatório do PNUD (2000). Enquanto no setor agrícola e industrial os Estados Unidos investem, respectivamente, 1,7% e 26,2% das aplicações, sendo investido em serviços 72%. De acordo ainda com esse relatório, de todo esse total investido nesses setores, os Estados Unidos aplicaram 67,7% na iniciativa privada.

A percentagem investida no setor de serviço é considerada alta quando comparada com a média global. Isso porque a média global de investimentos em serviços é de 62,1%, enquanto a média de investimento em agricultura e indústria é de 4,8% e 30,6%, respectivamente. Embora não se revele como um investimento muito acima da média, as aplicações dos Estados Unidos no setor privado são também superiores à média global de 62,6%.

Os investimentos públicos de um país podem ser alocados em três principais áreas para o desenvolvimento humano: saúde, educação e militar. Para mensurar as despesas públicas nessas áreas, o PNUD (2013) observou a percentagem do PIB cada país aplicou nessas três áreas, que pode ser resumida pelos gastos abaixo:

Gráfico 3.6 – Despesas Públicas dos Estados Unidos em 2000 e 2010.



Fonte: Elaboração própria com base em PNUD (2013).

Embora o espaço cibernético perpasse por todas as áreas do conhecimento, as áreas de maior interesse aqui são: o militar e a educação. A educação nos fornece um quadro sobre as possíveis inovações e aprofundamentos do conhecimento sobre espaço cibernético. Por sua vez, os investimentos na área militar permitem compreender o preparo dos Estados Unidos para lidar com ameaças do espaço cibernético.

De acordo com o gráfico apresentado acima, os investimentos no setor militar aumentaram mais de 50% em 10 anos. Mesmo em 2000, quando os investimentos eram de 3,0% do PIB, esse país já investia mais do que a média global de 2,3% (PNUD, 2013). Em 2010, esses investimentos chegam próximo ao dobro da média global de 2,6% (PNUD, 2013).

Embora não disponhamos de dados para verificar o aumento nos investimentos públicos em educação entre 2000 e 2010 dos Estados Unidos, a média global pode ser utilizada como supressora dessa ausência estatística. A média global de investimentos em educação no ano de 2010 era de 2,3%, enquanto os Estados Unidos investia 5,4%. Além de serem valores superiores às médias globais, o valor bruto é muito superior, pois os Estados Unidos dispõe de um dos maiores PIBs do mundo.

A relação desses dados com o espaço cibernético se dá na medida em que o setor de serviço, militar e educação impactam nessa temática. De acordo com Sérgio Ribeiro (2011), os ataques cibernéticos realizados tanto nas infraestruturas críticas quanto nas empresas comprometem os serviços aos cidadãos. Ademais, ainda conforme ele, esses mesmos ataques também afetam os aspectos sociais, políticos e econômicos de um país. Assim, os investimentos em serviços, educação e área militar fortalecem o espaço cibernético sob o domínio dos Estados Unidos.

Os dados analisados até esse momento dizem respeito a uma parcela do contexto socioeconômico atribuído aos tomadores de decisões estadunidenses. Entretanto, cabe abordar também o contexto socioeconômico relativo à sociedade. Para isso, analisaremos algumas percepções da população dos Estados Unidos sobre ela própria.

Conforme demostrado anteriormente, Castells (2003) explicou que os perfis virtuais apresentam similaridades com as identidades reais de cada usuário. Da mesma forma, a satisfação e percepção de cada pessoa em relação ao mundo real também são projetadas no mundo virtual. A satisfação de cada pessoa pode ser mensurada quanto ao bem-estar individual e quanto à sociedade, conforme abaixo:

Tabela 3.5 – Auto Percepção Social da População dos Estados Unidos (2007-2011)

Percepções do Bem-Estar Individual		
Variáveis	2007-2011	Média Global
Satisfação Global com a Vida (0=insatisfeitos; 10=muito satisfeitos)	*7,1*	*5,3*
Satisfação com a Liberdade de Escolha (% de satisfeitos)	*85%*	*73,9%*
Satisfação com o Emprego (% de satisfeitos)	*87,4%*	*73,2%*
Percepções da Sociedade		
Variáveis (% de respostas sim)	2007-2011	Média Global
Confiança nas Pessoas	*37%*	*29,8%*
Satisfação com a Comunidade	*83,8%*	*79%*
Percepção de Segurança	*75%*	*66%*

Fonte: Elaboração própria com base em PNUD (2013).

De acordo com a tabela apresentada acima, a percepção do bem-estar estadunidense está acima da média global. Dentre as variáveis que determinam essa percepção, a mais interessante para o debate sobre espaço cibernético é a satisfação com a liberdade de escolha. Isso porque alguns dos dilemas sobre espaço cibernético dizem respeito à liberdade de uso dele e a privacidade dos seus usuários.

Sobre a percepção da sociedade, a população dos Estados Unidos confia mais nas pessoas do que a média global. Essa confiança pode tornar o usuário mais vulnerável no espaço cibernético, pois a maioria dos crimes cibernéticos depende do fator confiança da vítima. Cabe ressaltar, por último, que essa vulnerabilidade do *peopleware* é acentuada pela percepção das pessoas sobre a segurança e a satisfação com a própria sociedade.

3.2.2 Infraestrutura Tecnológica

Embora o contexto socioeconômico dos países impacte indiretamente no espaço cibernético, a infraestrutura tecnológica dos Estados impacta diretamente nele. Para realizar a caracterização da infraestrutura tecnológica dos atores estatais, poderíamos observar os dados referentes à propriedade intelectual, mercado de navegadores, empresas tecnológicas. Entretanto, esses dados já foram vislumbrados na delimitação dos centros do espaço cibernético, por isso, aqui analisaremos apenas o comércio de partes, componentes e serviços, como também a adoção de novas tecnologias.

O comércio de partes e componentes é aquele referente a produtos intermediários utilizados na produção de produtos transformados para o consumo final (PNUD, 2013). Todos os equipamentos utilizados para o acesso ao espaço cibernético – celulares, notebooks, computadores – são produtos finais de partes e componentes. Nesse ponto da fabricação

desses produtos encontramos a ligação entre o comércio de partes e componentes e o espaço cibernético.

Sobre os Estados Unidos, o comércio de partes e componentes pode ser caracterizado pela tabela abaixo:

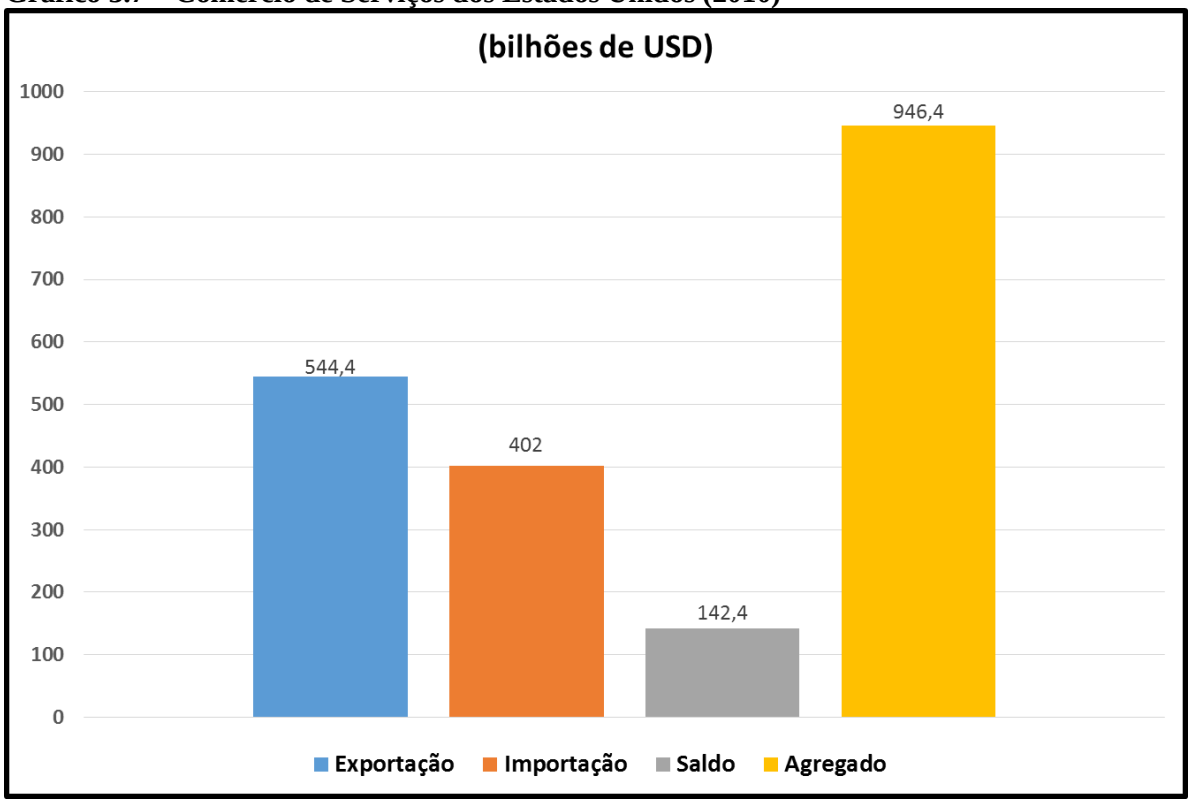
Tabela 3.6 – Comércio de Partes e Componentes dos Estados Unidos (2010)

	Estados Unidos (% do total)	Média Global (% do total)
Exportações	30,3%	29,2%
Importações	28,8%	31,6%
Valor Agregado	59,1%	60,8%

Fonte: Elaboração própria com base em PNUD (2013).

Como visto, enquanto o comércio de componentes do mundo é deficitário, no caso dos Estados Unidos, ele é superavitário. Ainda sobre isso, o valor agregado do comércio dessas partes, tanto em âmbito mundial quanto estadunidense, compõe maior parcela da balança comercial. Além do comércio de serviço, outro fluxo internacional importante para o espaço cibernético é o comércio de serviço. Sobre esta categoria comercial, os Estados Unidos apresentam os seguintes dados:

Gráfico 3.7 – Comércio de Serviços dos Estados Unidos (2010)



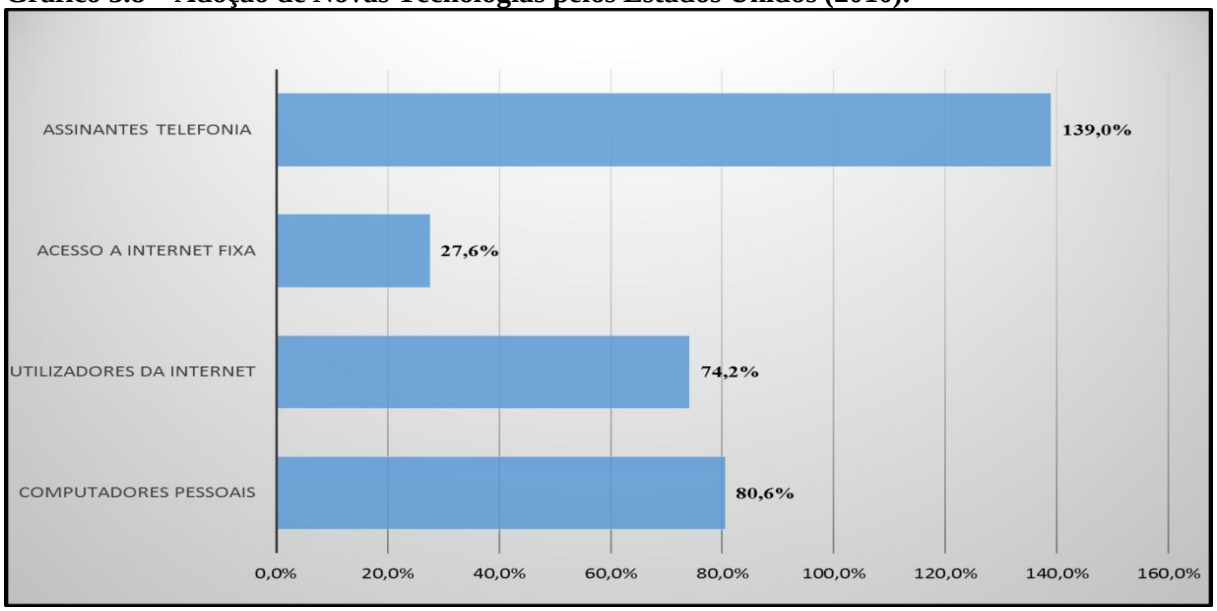
Fonte: Elaboração própria com base em PNUD (2013).

Igualmente ao comércio de partes e componentes, o comércio de serviço estadunidense apresenta saldo superavitário. A diferença na análise que encontramos no comércio de serviços é em relação ao globo. De acordo com o relatório do PNUD (2013), os Estados Unidos apresentaram superávit equivalente ao do mundo como um todo, que seria de 143 bilhões de dólares.

Sobre a participação desse país em todo o comércio global de serviços, os Estados apresentam apenas 14% dele. Enquanto o agregado de importações e exportações de serviço no mundo soma um total de 6721,9 bilhões de dólares, os Estados Unidos movimenta somente 946,4 bilhões de dólares em 2010. Cabe ressaltar que em um universo de cerca de 190 países, contribuir com um décimo de um comércio é relativamente significativo.

Quando relacionamos o comércio de partes e componentes ou de serviços com espaço cibernético, estamos falando sobre inserção de tecnologia. Sobre essa, o PNUD (2013) realiza mensurações observando quatro categorias de inserção: Telefonia; Banda Larga Fixa; Internet; e Computadores Pessoais. A inserção de tecnologia nos Estados Unidos pode ser representada pelo gráfico abaixo:

Gráfico 3.8 – Adoção de Novas Tecnologias pelos Estados Unidos (2010).



Fonte: Elaboração própria com base em PNUD (2013).

De acordo com esse gráfico, com exceção do acesso à Internet Fixa, todas as outras quatro tecnologias já foram adotadas por mais da metade da população dos Estados Unidos. Cabe ressaltar que o baixo índice de adoção da internet fixa pode ser reflexo do aumento do acesso à Internet Móvel. Em virtude disso, compreendemos a elevada percentagem dos utilizadores da Internet concomitantemente o baixo acesso à Internet Fixa.

3.2.3 Marcos Regulatórios

O espaço cibernético teve sua territorialização recentemente, quando comparado com os demais espaços. Entretanto, como esse é um espaço cuja velocidade e fluxos de interações são demasiadamente altos, algumas regulamentações por parte dos Estados não demoram a surgir. Isso se aplica ao principal centro desse espaço, os Estados Unidos.

A regulamentação nos Estados Unidos não é somente real, como também excessiva. De acordo com DLA Piper (2015), um escritório multinacional anglo-americano de advocacia, os Estados Unidos dispõem de centenas de leis sobre proteção de dados e privacidade. Isso é justificado devido à dinâmica entre leis federais e leis estaduais nesse país.

Dentro dos Estados Unidos, as leis sobre proteção de dados e privacidade no espaço cibernético podem ser criadas tanto em âmbito federal quanto em âmbito estadual, o que gera uma quantidade excessiva de leis sobre essa temática. Além dessa grande quantidade de legislação sobre dados e privacidade, os Estados Unidos também dispõem de cerca de 20 setores que tratam do assunto, conforme apontado pela DLA Piper (2015). Esses setores são específicos sobre esse assunto, mas também existem alguns semi-específicos (DLA PIPER, 2015).

Apesar da existência desses setores, os Estados Unidos não dispõem de uma autoridade máxima sobre segurança de dados. De acordo com DLA Piper (2015), essa ausência de uma autoridade máxima é suprimida parcialmente pela Comissão Federal de Comércio daquele país. De modo geral, essa comissão tem autoridade sobre práticas comerciais desleais ou enganosas de empresas estadunidenses. Dentro do âmbito dos dados, essa comissão também requer das empresas algumas medidas mínimas para a segurança e privacidade desses dados.

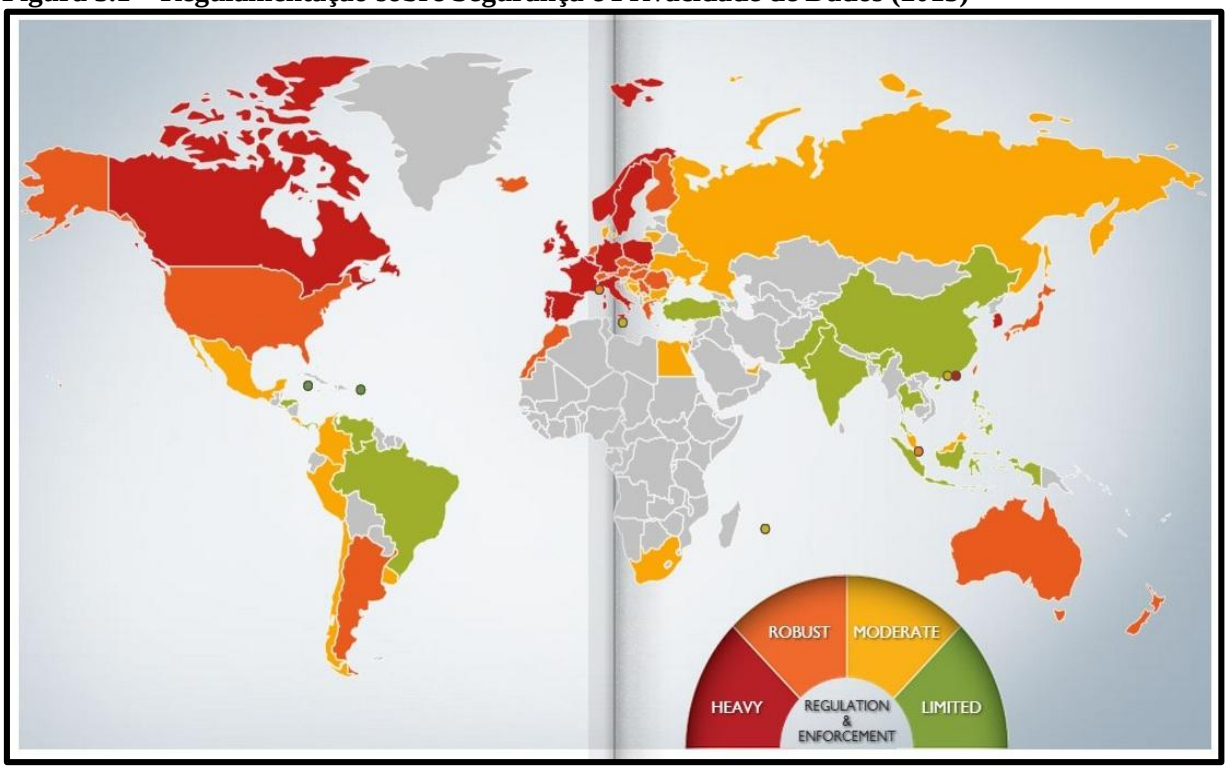
A Comissão Federal de Comércio também é utilizada como referência nas definições de dados pessoais e de dados pessoais sensíveis dentro dos Estados Unidos, conforme apontado pela DLA Piper (2015). De acordo com essa comissão, os dados pessoais são aqueles que podem ser utilizados para contato ou para distinguir uma pessoa, como por exemplo, endereços IP e identificadores de dispositivo. Cabe ressaltar que mesmo com tal definição, ainda existem algumas leis federais e estaduais nos Estados Unidos que consideram como dados pessoais àquelas informações que não abrangem a possibilidade de identificação de pessoas.

Os dados pessoais sensíveis para os Estados Unidos, por sua vez, são aqueles que possibilitam o roubo ou o uso de uma identidade sem autorização (DLA PIPER, 2015).

Dentre os exemplos sobre dados pessoais sensíveis citados pela Comissão Federal de Comércio, encontramos os dados de saúde pessoal, dados de qualidade de crédito e informações pessoais coletadas on-line de crianças menores de 13 anos. Sobre a transferência dos dados pessoais e pessoais sensíveis, os Estados Unidos não apresentam restrições, exceto para aqueles dados referentes ao governo estadunidense (DLA PIPER, 2015).

Embora o controle das transferências seja baixo e tenha um grande número de leis e normas sobre dados, os Estados Unidos não são classificados pela DLA Piper (2015) como um país de alta regulamentação, mas um Estado robusto no que tange a segurança e privacidade de dados, conforme demonstrado pela figura abaixo:

Figura 3.1 – Regulamentação sobre Segurança e Privacidade de Dados (2015)



Fonte: DLA Piper (2015).

A classificação dos Estados Unidos nesse mapa é justificada pela mescla entre alta regulamentação e a baixa restrição para transferência de dados. Dessa forma, a alta regulamentação não significa, no caso dos Estados Unidos, um cenário de altas restrições, mas reflexo de sua estrutura organizacional. A liberdade legislativa que os Estados Unidos dispõem contribui para o grande número de legislações sobre segurança e privacidade de dados.

3.3 DEMAIS CENTROS NO ESPAÇO CIBERNÉTICO

3.3.1 Contexto Socioeconômico

Os mesmos centros do mundo no espaço cibernético são aqueles das demais temáticas das relações internacionais, mas com alguns atores distintos. Ademais, não há um consenso sobre esses centros no espaço cibernético. Por exemplo, enquanto a Bozz Allen Hamilton (2011) analisa um grupo de 20 centros, Samuel Cruz Júnior (2013) observa os Estados Unidos, Rússia e Índia. Para esta dissertação, além dos Estados Unidos, os demais centros do mundo identificados são: Alemanha, China, França, Japão, Reino Unido e Rússia.

Para a Bozz Allen Hamilton (2011) dos 20 países analisados, os setes principais são: Reino Unido, Estados Unidos, Austrália, Alemanha, Canadá, França e Coréia do Sul. Por outro lado, Samuel Cruz Júnior (2013) vislumbra os Estados Unidos, a Rússia, Índia e China, mas esse quarto centro não foi abordado em seu estudo, devido à ausência de dados. Sobre as escolhas desta dissertação, elas foram realizadas por meio dos critérios observados no início desse capítulo.

Embora essas escolhas não estejam de acordo com a abordagem feita por Samuel Cruz Júnior (2013), quando comparadas com o índice da Bozz Allen Hamilton (2011) são parcialmente convergentes. O desacordo com o primeiro autor ocorre sobre a inclusão da Índia como centro do mundo, pois ela não apresentou destaques nos critérios observados. Enquanto isso, os países designados por essa dissertação como centros do espaço cibernético estão dentro do grupo de 20 países da Bozz Allen Hamilton (2011).

Sobre a distribuição macroeconômica dos recursos desses seis centros, ela pode ser sintetizada conforme tabela abaixo:

Tabela 3.7 – Estrutura Macroeconômica dos demais Estados Centrais (1998)

Países	**Agricultura (% do PIB)** *Média Global: 4,8%*	**Industrial (% do PIB)** *Média Global: 30,6%*	**Serviços (% do PIB)** *Média Global: 62,1%*
Alemanha	1,1	54,8	44,1
China	18,4	48,7	32,9
França	2,3	26,2	71,5
Japão	1,7	37,2	61,1
Reino Unido	1,8	31,5	66,7
Rússia	7,3	35,3	57,4

Fonte: Elaboração própria com base em PNUD (2000).

Quase todos esses centros apresentam estruturas macroeconômicas voltadas para o setor de serviços. Dessa forma, podemos afirmar que essa é uma característica comum aos países centrais do espaço cibernético estruturas macroeconômicas focadas no setor de serviços. Além disso, essa conclusão nos faz questionar a validade da relação países agrícolas e países industriais com a pobreza e o desenvolvimento, respectivamente.

No mais, somente o Reino Unido e a França apresentam uma estrutura de serviço superior à média global. Sendo que destes dois, somente a França chega próximo da estrutura dos Estados Unidos de 72%. Entretanto, cabe novamente relembrar que essa percentagem é relacionada ao PIB, ou seja, enquanto a França investiu naquele ano somente 1,08 trilhões de dólares em serviço, os Estados Unidos investiram cerca de 6,5 trilhões de dólares (WORLD BANK, 2015g).

Sobre a priorização que a defesa cibernética pode receber dos Estados, os dados analisados demonstram um aumento das despesas com o setor militar apenas dos Estados Unidos. As despesas dos demais centros permaneceram relativamente inalteradas. Entretanto, quando pensamos em inovação, pesquisa e desenvolvimento, cuja base é a educação, o cenário é diferente, conforme tabela a seguir:

Tabela 3.8 – Despesas Públicas dos Estados Centrais (2000/2010)

Países	**Saúde (% do PIB)**		**Educação (% do PIB)**		**Militar (% do PIB)**	
	2000	2010	2000	2010	2000	2010
Estados Unidos	*5,8*	*9,5*	-	*5,4*	*3,0*	*4,8*
Alemanha	*8,2*	*9,0*	-	*4,6*	*1,5*	*1,4*
China	*1,8*	*2,7*	-	-	*1,9*	*2,1*
França	*8,0*	*9,3*	*5,7*	*5,9*	*2,5*	*2,3*
Japão	*6,2*	*7,8*	*3,7*	*3,8*	*1,0*	*1,0*
Reino Unido	*5,6*	*8,1*	*4,5*	*5,6*	*2,4*	*2,6*
Rússia	*3,2*	*3,2*	*2,9*	*4,1*	*3,7*	*3,9*

Fonte: Elaboração própria com base em PNUD (2013).

Esse quadro revela ainda um aumento nas despesas de educação por parte da Rússia e Reino Unido. Este último, inclusive superando a percentagem investida em educação pelos Estados Unidos. A Rússia, por sua vez, apesar de não ter superado as despesas estadunidenses, é o único centro em que as despesas com Educação e setor Militar superam as da Saúde. Ademais, cabe ressaltar que embora não tenha um aumento relativamente grande nas despesas em educação, a França apresenta números superiores aos dos Estados Unidos.

Sobre a abordagem social do contexto socioeconômico dos centros do espaço cibernético, mais uma vez observamos as percepções. A população de cada Estado central do espaço cibernético apresenta a seguinte percepção sobre si mesma:

Tabela 3.9 – Auto Percepção Social da População dos Estados Centrais (2007-2011)

Percepções do Bem-Estar Individual						
Variáveis	Alemanha	China	França	Japão	Reino Unido	Rússia
Satisfação Global com a Vida (0=insatisfeitos; 10= satisfeitos)	*6,7*	*5,0*	*7,0*	*6,1*	*6,9*	*5,4*
Satisfação com a Liberdade de Escolha (% de satisfeitos)	*89%*	*77%*	*90%*	*78%*	*90%*	*54%*
Satisfação com o Emprego (% de satisfeitos)	*89%*	*70%*	*87,4%*	*76%*	*88,3%*	*67,9%*
Percepções da Sociedade						
Variáveis (% de respostas sim)	Alemanha	China	França	Japão	Reino Unido	Rússia
Confiança nas Pessoas	*31,1%*	*57%*	*20%*	*33%*	*35%*	*24%*
Satisfação com a Comunidade	*93,9%*	*77%*	*89,4%*	*85%*	*86,6%*	*69,4%*
Percepção de Segurança	*78%*	*80%*	*63,0%*	*69%*	*70%*	*40%*
**** Abaixo da média global***						

Fonte: Elaboração própria com base em PNUD (2013).

De acordo com a tabela apresentada acima, as percepções de bem-estar individual da China e Rússia estão abaixo da média global. Dos países avaliados, damos destaque à Rússia, pois sua população não se percebe como livre para escolhas. Cabe ressaltar que essas percepções são refletidas dentro do espaço cibernético, como explicado quando da análise da percepção da sociedade estadunidense.

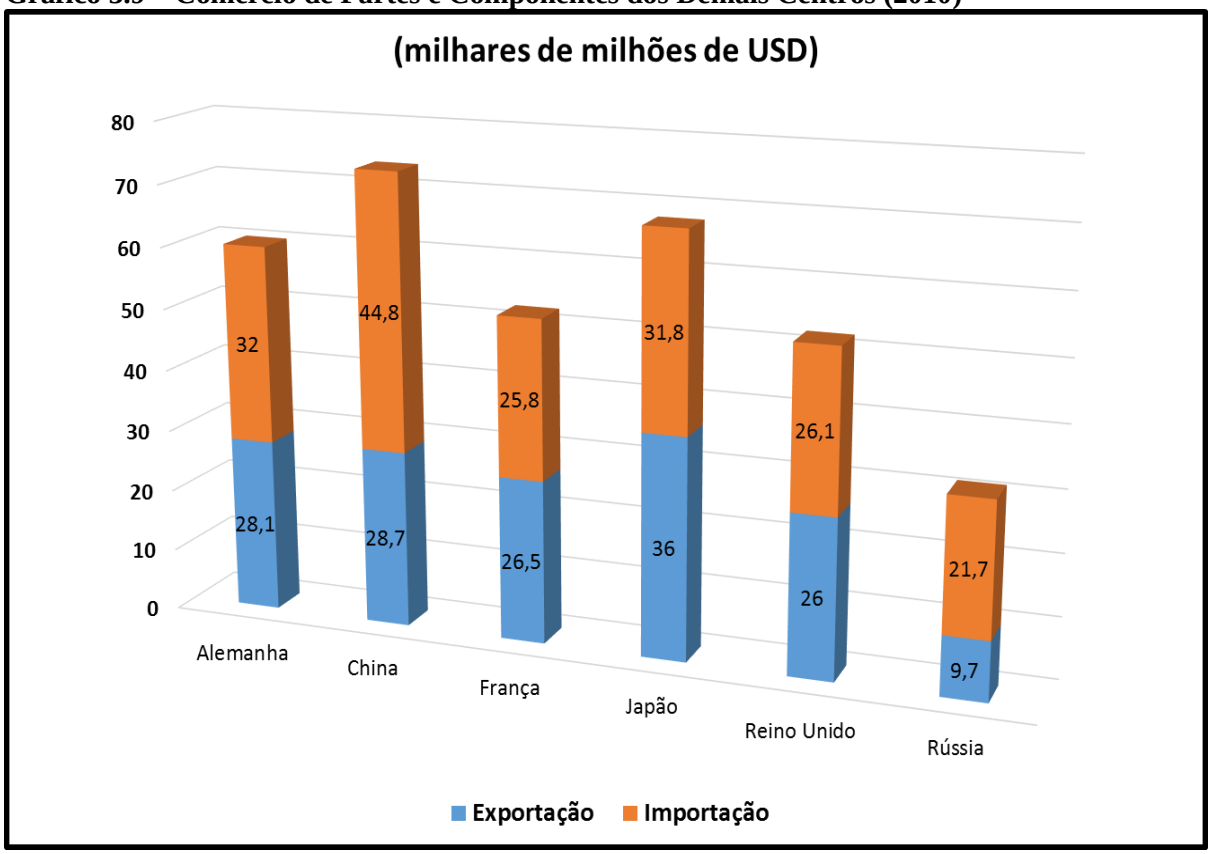
Sobre a percepção da sociedade, a Alemanha, Japão e Reino Unido tem uma caracterização semelhante àquela vislumbrada para os Estados Unidos. Apesar da percepção acima da média tornar os usuários da rede um possível alvos de ataques, ela também é reflexo de uma sociedade autoconfiante. Da mesma forma, com percepções abaixo da média, a população não confiará em armadilhas do espaço cibernético. Entretanto, essa baixa percepção também pode resultar de uma sociedade fragilizada. Sendo assim, a percepção da sociedade em relação à média global pode apresentar dúbia interpretação.

3.3.2 Infraestrutura Tecnológica

Como dito no tópico sobre a Infraestrutura Tecnológica dos Estados Unidos, o comércio de partes e componentes configura parte significativa da balança comercial estadunidense e mundial. Essas partes se relacionam com o espaço cibernético na medida em

que resultam em produtos finais de ponto de acesso, como celulares, computadores e *tablets*. Sobre o comércio de partes e componentes dos demais centros do espaço cibernético do mundo, ele pode ser resumido conforme gráfico abaixo:

Gráfico 3.9 – Comércio de Partes e Componentes dos Demais Centros (2010)

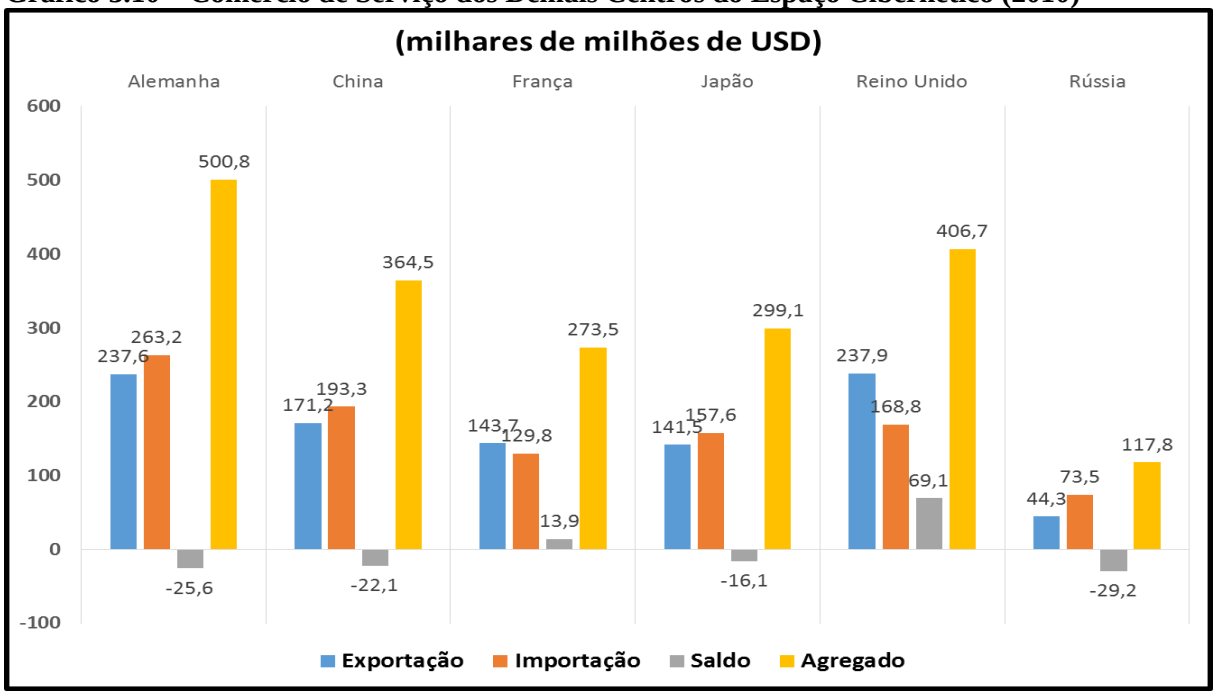


Fonte: Elaboração própria com base em PNUD (2013).

Com exceção da Rússia, todos os demais Estados considerados aqui como centros do espaço cibernético apresentam na balança comercial maior participação do comércio de partes e componentes. Ademais, enquanto há maior parte das importações do que exportação em partes e componentes na Alemanha, China e Rússia, no caso da França e Japão a exportação tem maior parte desse comércio. Ademais, notamos a China como um destaque especial, pois 70% da balança comercial dela são compostas das partes e componentes.

Quando comparamos o valor agregado do comércio de serviços dos centros do espaço cibernético com o dos Estados Unidos, aqueles países somente investem cerca de 50%. Ademais, dos seis centros analisados somente dois acompanham o saldo americano quanto à qualidade, ou seja, somente dois países apresentam o comércio de serviço superavitário. Além disso, esses centros juntos detêm 29% do comércio de serviço ou 43%, quando observarmos também o comércio dos Estados Unidos, conforme abaixo:

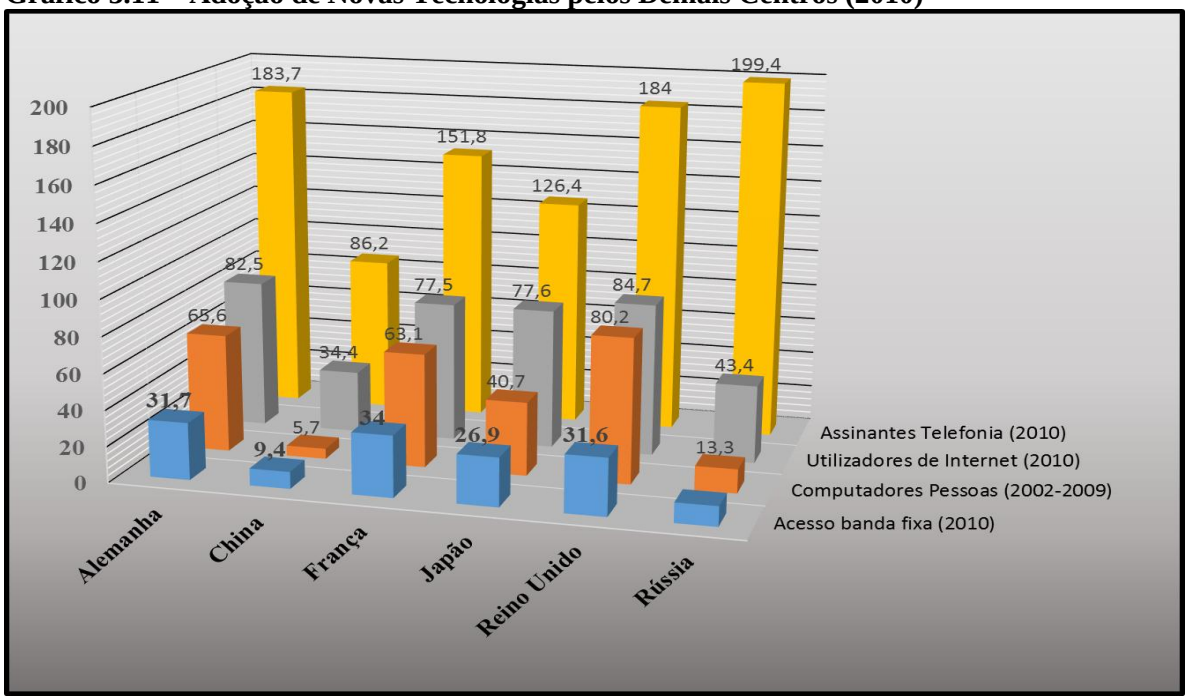
Gráfico 3.10 – Comércio de Serviço dos Demais Centros do Espaço Cibernético (2010)



Fonte: Elaboração própria com base em PNUD (2013).

Por sua vez, a adoção de tecnologia pelos centros pode ser demonstrada conforme gráfico abaixo:

Gráfico 3.11 – Adoção de Novas Tecnologias pelos Demais Centros (2010)



Fonte: Elaboração própria com base em PNUD (2013).

Os dados referentes à adoção de novas tecnologias pelos centros do Espaço Cibernético devem ser observados com cautela. Isto porque não podemos considerar a baixa percentagem de acesso à banda fixa como resultado da internet móvel. Outra comprovação disso é o alto índice de assinantes de telefonia em detrimento dos computadores pessoais em alguns Estados.

Nesse quadro, somente a Alemanha, França, Japão e Reino Unido apresentam números comparáveis aos dos Estados Unidos. Por outro lado, a China e a Rússia apresentam baixa adoção de computadores pessoais e de Internet. Entretanto, mesmo com baixos números, a Rússia ainda apresenta maior número de assinantes de telefonia.

3.3.3 Marcos Regulatórios

Embora o espaço cibernético seja demandante de uma regulamentação desde sua criação, não é possível observar uma padronização sobre a segurança e privacidade de dados. Em virtude disso, encontramos países com centenas de legislações, como os Estados Unidos, e outros com apenas uma norma, como no caso do Reino Unido. Esse tópico demonstra como cada um desses centros lida com os dados pessoais do espaço cibernético e suas diferenças.

A Alemanha é outro país em que há apenas uma regulamentação federal sobre a segurança e privacidade de dados. Embora seja uma lei federal alemã, essa regulamentação segue as diretrizes europeias de proteção de dados (DLA PIPER, 2015). Ademais, essa lei não é abrangente, abarcando apenas os dados das autoridades públicas e de organismo privados nacionais. Entretanto, cabe ressaltar, que essa lei federal não é a única regulamentação sobre dados na Alemanha, pois cada unidade política deste país dispõe de leis próprias sobre essa temática, assim como ocorre com os Estados Unidos.

A principal diferença entre as unidades políticas alemãs para as estadunidenses é que aquelas dispõem não somente de leis próprias sobre a segurança de dados, mas também de autoridades locais que versam sobre esta temática (DLA PIPER, 2015). Dessa forma, a autoridade nacional alemã é pulverizada em cada um dos seus estados. Outra especificidade da Alemanha é as definições sobre dados pessoais e pessoais sensíveis pela lei federal sobre o tema.

Conforme a DLA Piper (2015), a Alemanha define os dados pessoais como informações sobre as circunstâncias pessoais ou materiais de uma pessoa singular identificada ou identificável. A definição de dados pessoais sensíveis, por sua vez, são informações pessoais especiais. Exemplos destes dados são informações sobre origem racial e étnica,

opiniões públicas, crenças religiosas ou filosóficas, filiações sindicais, saúde ou vida sexual (DLA PIPER, 2015).

A definição alemã de dados pessoais sensíveis não considera somente as informações que podem gerar fraude, mas também aquelas relacionadas a opiniões e liberdades de expressão. Outra diferença da Alemanha para os Estados Unidos é que ela distingue as transferências de dados em território europeu daquelas realizadas com o estrangeiro. Assim, de acordo com a DLA Piper (2015), a Alemanha não restringe as transferências de dados em território europeu, mas somente com o território extraeuropeu, que deverão seguir critérios específicos de segurança para serem efetuadas.

No caso da China, não há uma lei nacional abrangente sobre a segurança e privacidade de dados, mas pequenas menções encontradas em várias leis e regulamentações chinesas (DLA PIPER, 2015). Ainda com tais menções, a DLA Pìper (2015) afirma que as interpretações dadas pelas legislações chinesas não são explícitas. Cabe ressaltar ainda que embora não haja uma regulamentação especifica para essa temática, a China vem apreciando há algum tempo um projeto de lei referente à segurança de dados, mas não há previsão de aprovação (DLA PIPER, 2105).

A falta de legislações específicas sobre essa temática também acarreta em uma ausência de autoridade que verse sobre a segurança de dados. Entretanto, essas mesmas carências não impediram uma definição de dados pessoais e pessoais sensíveis pelo Estado chinês. De acordo com DLA Pipper (2015), os dados pessoais são definidos por ele como informações relacionadas com indivíduos específicos, que podem ser utilizados para identificá-los, seja de forma individual ou conjunta.

Por sua vez, os dados pessoais sensíveis são aquelas informações que podem gerar algum impacto negativo para o indivíduo de referência das informações (DLA PIPPER, 2015). Conforme a DLA Pipper (2015), a classificação de um dado pessoal sensível depende diretamente do consentimento do titular dos dados e a característica especifica de cada dado. Sobre a transferência de dados, a China permite essa ação desde que resguardado alguns requisitos, como consentimentos das partes e sigilo dos dados transferidos (DLA PIPPER, 2015).

Na França, a regulamentação se assemelha à da Alemanha, em que somente há uma única legislação nacional, que versa sobre a segurança e a privacidade de dados. Esta matéria é regulada pela Lei francesa nº 78/1978, que versa sobre tecnologia da informação, arquivo de dados e liberdade civil (DLA PIPPER, 2015). O interessante nessa lei é sua idade, pois foi criada anterior à década de 1990, antes mesmo da “Era da Conectividade”.

Juntamente com essa lei, a França dispõe de uma autoridade nacional chamada de "Comissão Nacional da Informação e das Liberdades". A principal função dessa comissão é garantir que a tecnologia da informação continue disponível para o cidadão, conforme apontado pela DLA Pipper (2015). Ainda de acordo com essa multinacional de consultoria, a comissão francesa zela para que a tecnologia da informação não comprometa a identidade humana, os direitos humanos, a privacidade, a liberdade pública ou individual.

A definição francesa para dados pessoais é semelhante à alemã, ou seja, informações que nos remete a uma pessoa singular que possa ser identificada. Igualmente, podemos relacionar a definição alemã e a francesa de dados pessoais sensíveis, pois ambas os define como informações referentes à raça, origem étnica, política, opiniões filosófica ou religiosa, filiações sindicais, condições de saúde ou vida sexual. Outro ponto de semelhança entre Alemanha e França diz respeito à transferência de dados, que não apresenta restrições dentro do território europeu, mas deve seguir algumas condições quando feita para os territórios que não pertencem à União Europeia.

Por fazer parte dessa união, o Reino Unido apresenta definições sobre dados pessoais, pessoais sensíveis e regras de transferência de dados iguais às da França e da Alemanha. Ainda por ser membro da União Europeia, o Reino Unido aderiu à Diretiva de Proteção de Dados europeia em 2000, sendo essa a lei máxima sobre segurança e privacidade de dados. O organismo responsável pela aprovação dessa diretiva foi o Gabinete do Comissário de Informação, órgão nacional responsável pela segurança e privacidade de dados no Reino Unidos (DLA PIPPER, 2015).

No caso do Japão, a segurança e privacidade de dados são garantidas pela Lei sobre Proteção de Dados Pessoais. Essa lei exige que os operadores comerciais que utilizam banco de dados de informações pessoais com abrangência superior a cinco mil pessoas identificáveis nos últimos seis meses, adotem medidas de proteção dos dados (DLA PIPPER, 2015). Assim, o Japão difere dos demais países abordados aqui ao criar uma lei de abrangência parcial, ou seja, somente as organizações com banco de dado de mais de 5000 pessoas identificáveis.

Sobre a autoridade nacional, o Japão se assemelha aos Estados Unidos. Isso porque não dispõe de uma autoridade especifica para tratar da segurança e privacidade de dados. Essa função, no entanto, é exercida por uma entidade responsável especificadamente por outra área, que seria a Agência de Negócios japonesa (DLA PIPPER, 2015). Além dessa agência, o ministro da Saúde, Trabalho e Bem Estar, como também o ministro com jurisdição

sobre as operações de negócios também são responsáveis por essa segurança (DLA PIPPER, 2015).

Embora a definição japonesa de dados pessoais se assemelha aquela observada na União Europeia, há uma distinção quanto às pessoas englobadas no caso japonês. De acordo com a DLA Pipper (2015), na definição japonesa, os dados pessoais são informações que possibilitem a identificação de um indivíduo específico, como por exemplo, data de nascimento. Entretanto, a diferença é que a definição japonesa somente considera dados pessoais àquelas informações que fazem referência a pessoas vivas, desconsiderando as que já morreram.

Sobre os dados pessoais sensíveis, a lei japonesa de Proteção de Dados Pessoais não apresenta uma definição. Entretanto, a DLA Pipper (2015) afirma que para diferenciar dados pessoais de dados pessoais sensíveis, o Japão utiliza definição estabelecida pela Agência de Serviços Financeiros do Japão. Esta define dados pessoais sensíveis como informações relacionadas à opinião pública, crenças religiosas, participação em sindicatos, raça, etnia, entre outras. Por último, a transferência de dados a terceiros somente é permitido no Japão mediante permissão do proprietário da informação.

Por sua vez, a Rússia se assemelha aos Estados Unidos quanto às leis que norteiam a segurança e a privacidade de dados. De acordo com a DLA Pipper (2015), além de convenções internacionais como a de Estrasburgo[26], a Rússia também apresenta legislações especificas, incluindo o Ato de Proteção de Dados. Além dessas, os russos também dispõe de diretrizes publicadas pela autoridade nacional russa responsável pela proteção de dados, o Serviço Federal de Supervisão das Comunicações, Tecnologias da Informação e Meios de Comunicação.

Sobre as definições de dados pessoais e de dados pessoais sensíveis, a legislação russa se assemelha à europeia. Assim, para eles, dados pessoais são informações que se relacionam direta e indiretamente a uma pessoa específica ou definida. Por sua vez, os dados pessoais sensíveis são informações referentes à raça, identidade nacional, opiniões políticas, crenças religiosas e filosóficas, estado de saúde, intimidades e dados biométricos.

Entretanto, as transferências de dados da Rússia para outro Estado devem seguir alguns critérios. Dentre eles podemos citar a necessidade do país destinatário ter também ratificado a convenção de Estrasburgo. Outra requisição é que o requerente deve se assegurar que o destinatário forneça a proteção adequada do dado sobre sua tutela.

[26] Convenção Internacional para Proteção de Pessoas face o Tratamento Automatizado de Dados de Caráter Pessoal.

Finalmente, podemos notar uma distinção quanto à existência ou não de leis federais sobre a segurança de dados e a existência ou não de autoridades nacionais. Ademais, mesmo quando tais leis existem, alguns Estados apresentam um número excessivo de normas e outros somente uma. Entretanto, de uma forma geral e resguardada algumas distinções, podemos considerar um consenso entre esses países sobre as definições de dados pessoais, dados pessoais sensíveis e regras de transferência de dados.

4 MOVIMENTOS CENTRAIS E SUBJACENTES

Os movimentos centrais e subjacentes são derivados da visão de um mundo formado por centros e raios. Essa visão de mundo pode ser aplicada nas diversas temáticas das relações internacionais, pois ela é inerente às disputas de poder, em que sempre existe um país comparavelmente superior aos demais. Em alguns casos, os centros são bem evidenciados pela configuração do próprio sistema, como no caso do espaço cibernético.

Embora existam diversos movimentos centrais e subjacentes, no caso do espaço cibernético, eles não são de fácil acessibilidade. Isso porque os movimentos que ocorrem no espaço cibernético podem também se apoiar no anonimato, não permitindo uma compreensão factível dos mesmos. Em virtude disso, este capítulo se propôs analisar apenas aqueles movimentos tangíveis e mais representativos para a exemplificação e compreensão dos movimentos centrais e subjacentes no espaço cibernético.

Em todos os movimentos – centrais, alternativos e reacionários – abordaremos três exemplos. O primeiro exemplo aborda um movimento com atuação predominante dos centros e o segundo com composição predominantemente de raios. Por último, com o terceiro exemplo, a dissertação aborda a participação direta e indireta de atores não estatais nesses movimentos.

4.1 MOVIMENTOS CENTRAIS

4.1.1 Safe Harbor (Estados Unidos – União Europeia)

Quando essa dissertação considerou os movimentos centrais no segundo capítulo, compreendemos que estes são grupos originados pela vontade de um ou mais centros. Ademais, também entendemos que eles resguardam a estrutura internacional vigente para garantir a manutenção do poder dos centros envolvidos. Por isso, os movimentos centrais são conduzidos pelo interesse nacional dos principais centros participantes.

Esses movimentos centrais podem ser homogêneos ou heterogêneos. Os movimentos centrais homogêneos são aqueles em que o grupo é constituído apenas por Estados centrais. Por sua vez, os movimentos centrais heterogêneos são compostos por Estados centrais cooperando com Estados raios.

O acordo "*Safe Harbor"* entre Estados Unidos e União Europeia versa sobre a transferência de dados entre esses atores (CONNOLLY, 2009). Esse acordo é composto por

sete princípios sobre proteção e privacidade de dados. Os princípios protegidos pelo acordo são: os proprietários das informações devem ser informados sobre a coleta delas; os proprietários podem optar pela não coleta ou transferência de dados; transferências de dados a terceiros somente podem ocorrer com organizações que também contemplem esses princípios; os dados coletados não podem ser aleatórios; os proprietários dos dados podem acessá-los; e deve haver meios para respaldar esses princípios.

Somente respeitando esses princípios, as empresas estadunidenses podem transferir e manter dados de europeus. Esse acordo foi necessário aos Estados Unidos, devido aos requisitos impostos pelos países da União Europeia. Como já abordado no capítulo 3, sobre os marcos regulatórios dos centros do espaço cibernético, a legislação dos países da União Europeia garante a livre transferência de dados apenas entre os europeus, enquanto a transferência para países estrangeiros está sujeita a adequações.

Cabe ressaltar que a União Europeia em si é um arranjo dos países europeus composto por centros e raios. Inclusive, os principais países dessa união também são centros do mundo: França, Alemanha e Reino Unido. Estes três países são primordiais para a política externa da União Europeia e também centros do espaço cibernético. Em virtude disso, tratar a União Europeia por si só como ator central desse espaço não acarreta prejuízo de análise.

Dessa forma, quando falamos no acordo *"Safe Harbor"* estamos tratando de um movimento predominantemente homogêneo, pois os principais negociadores são Estados Unidos, França, Alemanha e Reino Unido, conforme demostrado por Henry Farrel (2002). Inclusive, cabe ressaltar que o acordo *"Safe Harbor"* foi resultado de um desacordo entre esses centros europeus. Enquanto não havia objeções do Reino Unido sobre a transferência automática de dados para os Estados Unidos, a França e Alemanha apresentavam desconfianças (FARREL, 2002).

Em virtude disso, embora o primeiro rascunho desse movimento tenha surgido em 1998, ele foi aceito pela União Europeia somente em 2000. As divergências não ocorreram somente dentro da União Europeia, mas também dentro dos Estados Unidos. Alguns congressistas estadunidenses, como Ira Magaziner, criticavam as restrições para transferências de dados impostas pelos países europeus, sugerindo, inclusive, uma ação dentro da Organização Mundial do Comércio (FARREL, 2002).

Assim, a formação de um movimento que regulamentasse a troca de informação entre Estados Unidos e União Europeia foi necessária para evitar litígios que comprometesse a posição desses centros. Em virtude disso, esse movimento é caracterizado nesta dissertação como um movimento central. Cabe ressaltar que embora negociado principalmente entre

centros, ele também impacta nas relações internacionais com os raios europeus, que também sofrem influência da *"Safe Harbor".*

Entretanto esse acordo vem sendo comprometido desde o final de 2013. Depois das revelações de Edward Snowden sobre as ações estadunidenses da *National Security Agency (NSA),* as relações firmadas pela *"Safe Harbor"* foram abaladas. Isso porque os dados da União Europeia que transitavam para os Estados Unidos estavam sendo utilizados em desconformidade com as normas europeias de transferência de dados (SIMPSONS, 2015).

Essa crise não engloba somente as relações entre os Estados do acordo, mas também o envolvimento do setor privado. Isso porque a autoridade nacional responsável pela segurança de dados irlandesa entrou com uma ação legal no Tribunal de Justiça da União Europeia contra o Facebook. Nesta ação, a Irlanda acusa o Facebook de transferir dados de irlandeses para os Estados Unidos e disponibilizá-los à NSA (SCHECHNER & POP, 2015).

Os advogados de acusação constantemente afirmam que um acordo de vigilância mista, como o *"Safe Harbor"*, não garante a segurança e a privacidade dos dados dos usuários da União Europeia (SCHECHNER & POP, 2015). Entretanto, eles não conseguem provas evidentes das ações da NSA, exceto as exposições públicas anteriormente abordadas sobre as atividades da agência (SCHECHNER & POP, 2015). Independente da veracidade da acusação, o importante é a percepção negativa gerada sobre a *"Safe Harbor".*

A ação descrita acima surgiu de um Estado raio, a Irlanda, que pode comprometer um acordo realizado especialmente entre Estados centrais. Ademais, os envolvidos nessa crise são atores não estatais: os indivíduos que se sentem lesados e o Facebook, uma empresa privada estadunidense. Esse exemplo mostra como os movimentos centrais podem ser agredidos por Estados raios ou por atores não estatais.

Assim, percebemos a complexidade das relações internacionais como o sugerido tabuleiro Star Trek, citado no capítulo 2. Dessa forma, mesmo sendo um movimento caracterizado por Estados centrais, o acordo *"Safe Harbor"* é impactado por atores com baixo poder cibernético e também empresas e indivíduos. Por fim, ainda como dito no capítulo 2, de abordagem teórico-conceitual dos movimentos centrais e subjacentes, todo movimento advindo dos Estados centrais geram reações, no que chamamos aqui de movimentos subjacentes.

4.1.2 Five Eyes Group

De maneira geral, Estados centrais podem se envolver ou constituir movimentos centrais com a participação de Estados raios. Isso ocorre quando o movimento tem como principal objetivo suprir uma necessidade do Estado central que dependa da cooperação de outros países. O grupo chamado de "*Five Eyes"* é um exemplo desse tipo de movimento.

De acordo com General canadense James Cox (2012), esse grupo constitui a mais exclusiva associação de países para o compartilhamento de inteligência do mundo. De acordo com ele, fazem parte desse grupo os Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia. A função de inteligência requer a constante vigilância, que juntamente ao fato do grupo ser composto por cinco Estados justificam o nome desse movimento central de "*Five Eyes Group".*

Embora esse grupo não conte somente com Estados centrais, ele é caracterizado como movimento central devido à sua origem. Esse projeto surgiu em uma cooperação sobre inteligência entre dois Estados Centrais durante a segunda guerra mundial, os Estados Unidos e o Reino Unido (COX, 2012). De acordo com Cox (2012), essa cooperação se intensificou principalmente durante a Guerra Fria, em especial sobre a matéria de comunicação e codificação. Também nesse período a cooperação entre Estados Unidos e Reino Unido se tornou abrangente e englobou os outros três olhos (COX, 2012).

Conforme Carly Nyst e Anna Crowe (2014), esse movimento central não é somente para intercâmbio de informações de inteligência entre os países participantes, mas realmente um grupo de vigilância transfronteiriça. Assim, os participantes do "*Five Eyes Group"* cooperam na obtenção de informações de inteligência pelo mundo. Cabe ressaltar que nesse grupo é proibida a espionagem entre os membros, mas somente de atores que não participam do grupo (MCGREGOR & DYER, 2013).

Como podemos notar em diversas partes dessa dissertação, o maior fluxo de informação do mundo transita atualmente via espaço cibernético por meio de dados. Em virtude disso, o *"Five Eyes Group"* observa atualmente a maioria da comunicação do globo (NYST & CROWE, 2014). Para isso, esse movimento utiliza um sistema de vigilância chamado de ECHELON.

Por meio desse sistema, o *"Five Eyes Group"* consegue interceptar sinais de satélites e radio fusão (AMARAL, 2014). Ademais, de acordo com Roberto de Amaral (2014), o ECHELON também consegue detectar possíveis testes nucleares. Ainda de acordo com ele, esse sistema de monitoramento global está disposto em algumas regiões do globo,

como por exemplo, na Ilha de Assunção no Oceano Atlântico Sul, de onde são monitoradas a América do Sul e a África.

Ademais, quando o jornalista e escritor americano James Bamford compareceu ao Brasil para palestrar no Comitê Gestor da Internet do Brasil (CGI.br), ele evidenciou as atividades desse grupo ao falar sobre o *"Five Eyes Group"*. Conforme sua colocação, a participação estadunidense é realizada por meio da NSA e seus *workshops* juntos com os outros quatro Estados (MATSU, 2015). Além disso, ele explica que a atividade do *"Five Eyes Group"* está além da interceptação de sinais, pois eles também coletam dados em cabos submarinos e em empresas como a Google e a Microsoft.

Embora quando falamos em espionagem, interceptação de informação e monitoramento de Estados, nossos pensamentos nos remetam as questões de guerra e consequentemente aos assuntos militares, os assuntos abordados por essa rede de monitoramento não se limitam aos "temas de generais". Encontramos exemplos na mídia das ações desse movimento tanto em âmbito de defesa quanto na esfera industrial.

Sobre a ação em defesa, podemos citar como exemplo alguns compartilhamentos de informações do Canadá sobre terrorismo para os demais membros do grupo (LJUNGGREN & HOSENBALL, 2014). Entretanto, cabe ressaltar que a reportagem de Ljunggren e Hosenball (2014) também evidencia falhas na cooperação. Isso porque a reportagem trata do não compartilhamento de informações de suspeitos canadenses de terrorismo, devido à lei de privacidade deste Estado.

O exemplo sobre a ação do "*Five Eyes Group"* no âmbito da esfera industrial pode ser encontrado nas revelações do Wikileaks. Esta é uma organização transnacional que revelou documentos e informações sensíveis e confidenciais de Estados e organizações sem a autorização dos proprietários (HARDING, LEIGH & PILKINGTON, 2011). Dentre as revelações realizadas pela Wikileaks, encontramos um documento sobre a espionagem da empresa japonesa Mitsubishi por esse movimento central (BBC NEWS, 2015).

Como vimos, o grupo é composto pelos Estados Unidos, Reino Unido, Austrália, Canadá e a Nova Zelândia. Dessa forma, o *"Five Eyes Group"* tem dois centros do espaço cibernético, os Estados Unidos e o Reino Unido, que detém essa posição desde a II Guerra Mundial. A ausência de mais centros do espaço cibernético nesse movimento ocorre em virtude da necessidade dos membros de se submeterem à coordenação estadunidense (MCGREGOR & DYER, 2013).

Assim, o *"Five Eyes Group"* é formado por países centrais do espaço cibernético – Estados Unidos e Reino Unido – e por países raios – Canadá, Austrália e Nova Zelândia.

Em virtude desse grupo ter se originado pela cooperação dos dois países centrais e ser coordenado pelos Estados Unidos, ele é considerado um movimento central. Portanto, ele é caracterizado desta forma, haja vista garantir a continuidade do controle estadunidense e britânico sobre os recursos de poder informacional da estrutura internacional vigente.

4.1.3 Google na China.

A figura das relações internacionais como um tabuleiro *Star Trek*, em que os atores não estatais apresentam capacidade de impactar no sistema internacional, nos instiga a compreender alguns atores não estatais sediados nos Estados centrais. Embora na operacionalização dos movimentos centrais e subjacentes sobressaia os Estados, no espaço cibernético eles apresentam interdependência com o setor privado. Em virtude disso, a estabilidade dos Estados Unidos como centro do espaço cibernético depende diretamente da atuação de suas empresas.

Dentre os atores não estatais relevantes ao espaço cibernético observado, os sediados nos Estados Unidos são Microsoft, Apple, Facebook e Google. Esta última empresa lidera o mercado de navegadores, além de ser a segunda maior empresa em termos de valor de mercado dessa área. Mesmo com tais números, esta empresa vem tendo dificuldades na penetração de mercados restritos, como o chinês.

A China faz parte do grupo de países que comumente tem sido chamado de Buracos Negros da Internet. Eles são assim apelidados devido às altas restrições que impõe tanto na transferência de dados com o estrangeiro, como também no acesso a dados dentro do próprio território. A abordagem sobre esses Buracos Negros da Internet será realizada posteriormente, pois nesse instante o foco são as ações da Google visando à entrada no marcado chinês.

O Google negociou a sua entrada na China em 2006, com fortes questionamentos da comunidade internacional, conforme apontado por Daniel Oppermann (2010). Para tanto, esse autor explica que a Google teve de se adequar à política de filtros e restrições do governo chinês. Assim, alguns termos que poderiam causar constrangimentos aos governantes da China foram censurados, como por exemplo, a palavra Tibet, Falun Gong e Tiananmen (OPPERMANN, 2010).

Os questionamentos em torno da entrada da Google na China, conforme ainda Oppermann (2010), diziam respeito à contradição entre ação e missão da empresa estadunidense. Ela aceitou as restrições chinesas impostas para sua entrada mesmo com a

missão de organizar as informações do mundo e torná-las acessíveis e úteis. Isso significa que sua missão na China não vislumbrava a acessibilidade e a utilidade da informação, mas somente a conquista de mercado.

O motivo pelo qual uma das maiores empresas estadunidense de tecnologia da informação se submeteu às restrições chinesas é o tamanho do mercado da China. Como demonstrado no início do capítulo 3, sobre os centros do espaço cibernético, a China detém a maior quantidade de usuários desse espaço cibergeográfico. Sendo que as principais empresas controladoras do espaço cibernético são estadunidenses e chinesas.

A entrada da Google na China representa, dessa forma, a influência dos Estados Unidos dentro do território do seu principal concorrente no controle do espaço cibernético. Isso não seria uma ação unilateral dos Estados Unidos, pois as empresas chinesas também já penetram no território estadunidense com maior facilidade, devido à ausência de restrição de transferência de dados deste país. Entretanto, mesmo com a entrada da Google na China, essa empresa somente deteve cerca de 30% do mercado, sendo uma empresa chinesa a maior detentora do espaço cibernético chinês, a Baidu, com 58% (OPPERMANN, 2010).

Embora a percepção de abandono de um mercado como o chinês aparente perda de influência da Google no mundo, o que ocorreu na verdade foi um fortalecimento de sua projeção mundial. Isso porque a saída dessa empresa da China reverteu um cenário caótico que ela vivenciava, como por exemplo, um suposto roubo de dados da empresa pelo governo chinês, a invasão de contas da Google de ativistas chinesas; e a restrição termos em sua busca (NYE JR, 2012). Esses empecilhos provocavam mais prejuízos significativos para o Google em âmbito mundial do que dentro do próprio mercado chinês (NYE JR, 2012).

De acordo ainda com Nye Jr (2012), naquele momento o mercado chinês ainda não representava muitos ganhos a Google devido ao domínio da concorrente chinesa Baidu. Ademais, ele explica que em âmbito mundial, a Google estava disputando com a Microsoft para ser o principal servidor de armazenamento de dados em nuvem. Dessa forma, continuar na China poderia lhe custar sinergia e credibilidade necessárias para a disputa com a Microsoft (NYE JR, 2012).

Embora um único ator não possa constituir isoladamente um movimento central, cabe ressaltar que a tentativa de penetração do território chinês não é exclusiva da Google. Muitas outras empresas estadunidenses realizaram negociações para a entrada na China, se submetendo também às restrições impostas. Dentre essas empresas, Oppermann (2010) nos apresenta como exemplo a Yahoo e a Microsoft.

Assim, as ações desses atores não estatais somente poderiam ser consideradas parte de um movimento central, caso houvesse uma convergência nas ações deles e uma sinergia sistematizada com os Estados Unidos. Mesmo que não possam ser consideradas próprias do movimento central, as ações dessas empresas estão associadas às ações dos Estados Unidos no espaço cibernético. Em virtude disso, elas contribuem de forma indireta com os movimentos centrais empreendidos pelos Estados Unidos nesse espaço.

Isso porque as informações coletadas, transferidas e armazenadas em território estadunidense podem ser utilizadas por agências como a NSA. Tal fato ficou evidente quando analisamos, no início desse capítulo, os litígios envolvendo o movimento central da *"Safe Harbor".* Também, isso fica mais notório ainda quando observamos o contexto que levou a Google a anunciar sua retirada da China em 2012.

4.2 MOVIMENTOS ALTERNATIVOS

4.2.1 BRICS Cable

Os movimentos alternativos são aqueles em que os Estados participantes almejam a posição de *global players* das relações internacionais, substituindo os centros vigentes. Podemos observar movimentos dessa categoria constituídos apenas por Estados raios, como também por Estados centrais. Apesar de ter a participação de ambos os tipos de atores, os movimentos alternativos diferem dos centrais quanto à participação dos Estados e quanto aos objetivos de cada movimento.

Como dito, tanto os movimentos centrais, quanto os movimentos alternativos podem apresentar a presença de Estados centrais e Estados raios. Entretanto, nos movimentos centrais sempre teremos a presença de Estados centrais e a participação de Estados raios não é constante. Nos movimentos alternativos, por sua vez, a participação de Estados ré evidente, enquanto à participação de Estados centrais nem sempre é vislumbrada.

Sobre o objetivo desses movimentos, enquanto aqueles centrais visam à manutenção do poder dos Estados centrais, os movimentos alternativos objetivam a ascensão dos Estados raios. Assim, nos movimentos alternativos, a participação de Estados centrais ocorre quando estes apoiam a substituição de Estados centrais concorrentes, externos ao movimento. Cabe ressaltar que os movimentos alternativos não visam à desestruturação do sistema internacional, mas apenas a substituição dos Estados centrais nas relações internacionais.

Por meio dessas premissas sobre os movimentos alternativos, o grupo do BRICS pode ser caracterizado como um exemplo da participação de países centrais. Ele pode ser caracterizado como um movimento alternativo em virtude da sua origem no artigo de Jim O'Neill (2001). De acordo com este artigo, o Brasil, Rússia, Índia e China (BRIC) poderiam se tornar dominantes até 2050.

As previsões realizadas por esse artigo foram posteriormente adotadas por esses países como interesse nacional e condensado em um grupo, que se reuniu formalmente em 2009 na Rússia. A África do Sul, representada pelo "S" do acrônimo, somente se apresenta oficialmente como membro do grupo na terceira cúpula, ocorrida em 2011. Em todas as cúpulas e reuniões do BRICS, os principais assuntos tratados referiam-se a algum problema que afetava a estabilidade desses países ou temas que poderiam gerar o desenvolvimento necessário para serem centros do mundo, como havia previsto O'Neill (2001).

Sendo assim, o grupo do BRICS é caracterizado como movimento alternativo por não apresentar pretensões de alterar a estrutura do sistema internacional, mas apenas de se tornarem os países influentes do sistema. Isso fica nítido quando observamos a instituição do Banco de Desenvolvimento do BRICS. Desde o anuncio da criação desse banco, economistas tem vislumbrado essa iniciativa como uma alternativa ao Banco Mundial e ao Fundo Monetário Internacional (FMI), como demonstrado em reportagem de Alessandra Corrêa (2014).

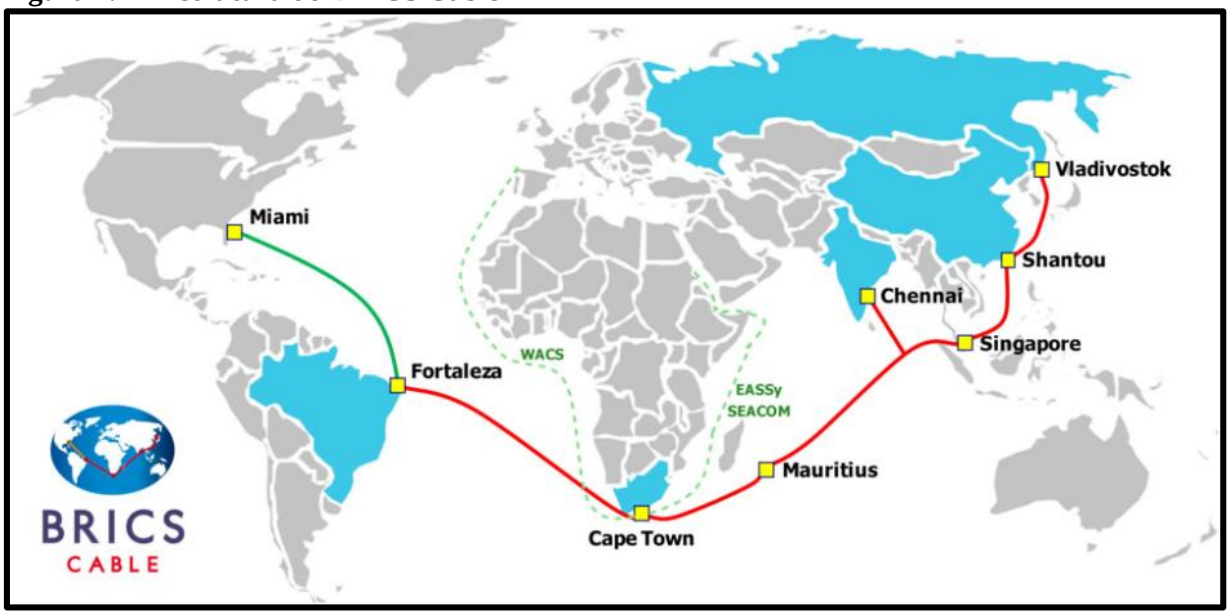
Sob o aspecto do espaço cibernético, esse grupo também pode ser caracterizado como um movimento alternativo. Após as revelações de Snowden em 2013, sobre as atividades de espionagem estadunidense da NSA, alguns países do BRICS se perceberam ameaçados pelo poder cibernético dos Estados Unidos. A reação desse grupo face essas revelações é a criação de um cabo submarino exclusivo para o grupo, chamado "*BRICS Cable"*.

O projeto desse cabo foi apreciado pelos países membros do BRICS em 2013, ocasião da Cúpula de Fortaleza (LESAME, 2014). Além de assegurar uma independência da rede dos Estados Unidos, o *BRICS Cable* pretende também reduzir custos (BISSIO, 2015). Juntamente com a instituição desse cabo, a Cúpula de Fortaleza resultou ainda na assinatura de um memorando de cooperação em Inovação, Ciência e Tecnologia. Tal cooperação fortalece o projeto de emancipação da rede e a instalação do *BRICS Cable.*

O objetivo desse cabo é a instalação de cerca de 34.000 km de fibra óptica interligando os cinco países componentes do BRICS (LOPES, 2013). Ademais, ele não conectaria somente os países do BRICS, mas também Singapura e Maurícia (LOPES, 2013).

Além disso, após o último ponto de conexão em Fortaleza, o cabo conectará o BRICS à Miami, como podemos constatar pelo mapa abaixo:

Figura 4.1 – Estrutura do BRICS Cable



Fonte: Gill Lopes (2013).

De acordo com Gill Lopes (2013), esse cabo vinha sendo implementado e sua conclusão estava prevista para meados de 2015. Entretanto, essa iniciativa não tem conseguido angariar fundos e colaboradores para o projeto original, mesmo com o apoio de outros Estados Emergentes (NIELSEN, 2014). Isso nos faz refletir sobre a eficiência na projeção dos movimentos alternativos dentro do espaço cibernético.

Mesmo com a concretização desse cabo, cabe relembrarmos algumas considerações sobre o espaço cibernético realizadas no primeiro capítulo dessa dissertação. A primeira delas, sobre as fronteiras cibernéticas, que são multifacetárias, ou seja, ainda que ocorra a construção de um cabo submarino exclusivo para os Estados do BRICS, os dados da Internet que trafegariam por satélites e ondas de rádios ainda estariam vulneráveis. A outra reflexão é sobre a defesa dos próprios cabos, que de acordo com Forrest Hare (2009) podem ser acessados por meio de um terminal conectado a eles.

Dessa forma, apenas o estabelecimento de uma estrutura de rede própria dos BRICS não pode prevenir esses Estados de futuras ações de espionagem. Entretanto, essa iniciativa pode servir de inspiração para ações mais eficazes nesse sentido, caso haja uma vontade política para tal. Independente da eficiência, o anuncio desse cabo é visto por essa dissertação como uma alternativa ao domínio estadunidense do espaço cibernético.

4.2.2 Estônia, Irlanda e o Armazenamento de Dados

O tempo de territorialização do espaço cibernético é extremamente pequeno quando comparado com os demais espaços geográficos. Entretanto, esse espaço já surge com alguns poucos centros dominando-o, sendo os Estados Unidos o principal destaque, como visto em capítulos anteriores. Como o domínio estadunidense somente começou a ser questionado recentemente, com as acusações de uso indevido de informações pessoais, não houve muitas iniciativas visando movimentos alternativos para o espaço cibernético.

Em virtude disso, atualmente vislumbramos a fase de ensaios individuais de alguns Estados, visando à proteção de ataques cibernéticos. Algumas iniciativas mais abrangentes para constituir um movimento alternativo significativo, como por exemplo, o do *BRICS Cable*, não tem encontrado financiamento devido (NIELSEN, 2014). Entretanto, cabe ressaltar aqui que, antes da formação de movimentos centrais ou subjacentes, é natural o ensaio de projetos no cenário doméstico dos Estados, dinâmica própria do jogo de dois níveis proposto por Putnam (1988).

Um exemplo sobre esse tipo de ensaio para um futuro movimento alternativo espontâneo no espaço cibernético pode ser vislumbrado na Estônia. Para se proteger de ataques cibernéticos, a Estônia pretende se basear no conceito de resiliência. De acordo com o ICANN (2013, p. 06), resiliência é "a capacidade de resistência/tolerância/sobrevivência do sistema de identificadores exclusivos a ataques maliciosos e outros eventos que causam interrupções sem resultar na interrupção ou paralisação do serviço".

Dessa forma, a Estônia tem interesse em criar um sistema que continue funcionando mesmo após um ataque cibernético que vise à queda da rede estoniana. Esse conceito é demasiadamente similar ao que se convencionou chamar dentro do debate de guerra nuclear de sistema de Destruição Mútua Assegurada. A diferença entre os dois conceitos é que enquanto na Destruição Mútua Assegurada, o sistema destruído também elimina o adversário, na resiliência um sistema atacado tende a continuar em funcionamento.

A necessidade que a Estônia percebe em garantir uma resiliência surge de alguns ataques cibernéticos recebidos em 2007. Os ataques constituíram em uma negação de serviço nos sistemas bancários da Estônia, ou seja, os bancos pararam de funcionar, o que causou um caos urbano (ZUCCARO, 2011). Esse ataque ocorreu em resposta à decisão do governo estoniano de remover um memorial soviético de sua capital (ZUCCARO, 2011).

Os efeitos desse ataque poderiam ser evitados caso a Estônia tivesse um sistema com resiliência adequada na ocasião. Para evitar novos ataques dessa natureza, esse Estado

pretende realizar um *backup* de si mesmo, conforme reportagem do *The Economist* (2015). De acordo ainda com a reportagem, o *backup* estoniano consistiria em garantir que o governo funcionasse digitalmente, caso sofresse algum tipo de sabotagem, como um ataque de outro Estado. Em virtude disso, o projeto é chamado de "continuidade digital" (THE ECONOMIST, 2015).

De acordo com a reportagem do *The Economist* (2015), para que a "continuidade digital" funcione, a Estônia pretende criar vários elementos de resiliência. O primeiro elemento consistiria em manter os serviços do governo funcionando em servidores secundários dentro do território estoniano. Caso isso falhasse, o serviço migraria para fora do país e estaria amparado por nuvens em computadores dentro de embaixadas estonianas espalhadas pelo mundo.

Cabe ressaltar que o principal parceiro da Estônia para o estabelecimento da "continuidade digital" é a Microsoft. Um experimento real desse projeto foi realizado em conjunto com a Microsoft durante a guerra da Geórgia em 2008 (THE ECONOMIST, 2015). Naquela ocasião, hackers tentaram atacar o website do presidente estoniano Toomas Ilves, mas esse foi movido tranquilamente para a "nuvem" da Microsoft em Dublin e Amsterdã e continuou funcionando.

A Estônia não é o único Estado que busca parceria juntamente com a Microsoft. Outro ator apoiador dessa empresa estadunidense é a Irlanda. A ação conjunto entre a Microsoft e a Irlanda ocorre no âmbito do acesso de dados em território estrangeiro.

Embora a Microsoft seja uma empresa estadunidense, ela mantém servidores com dados em outros países, assim como qualquer multinacional de tecnologia. Como vimos nos movimentos centrais, os Estados Unidos utilizam os dados de empresas como a Microsoft em seu monitoramento da Internet. Entretanto, quando os Estados Unidos requisitaram à Microsoft dados de um usuário de seu serviço de e-mail em 2014, a empresa negou o acesso (ROHR, 2014). Ao receber essa resposta negativa, os Estados Unidos acionaram a justiça estadunidense contra a Microsoft, conforme reportagem de Altieres Rohr (2014).

De acordo com Rohr (2014), a justificativa da Microsoft para não conceder os dados requeridos foi que eles estavam armazenados em um servidor na Irlanda. Em virtude disso, a empresa não se considerou obrigada a ceder os dados, até porque esse ato poderia violar as normas europeias para a transferência de dados. Os Estados Unidos, por outro lado, considerou que a empresa tinha a obrigação de fornecer os dados, pois a sede da Microsoft estava localizada em território estadunidense.

Dentro dessa disputa, a Irlanda surgiu como apoiadora do Microsoft. A Irlanda enviou uma carta para corte americana recordando que os meios apropriados para a obtenção de dados armazenados em seu território era por meio de um acordo legal previamente estabelecido entre os dois Estados. Dessa forma, a requisição via Microsoft violaria a confiança depositada sobre esse acordo.

Além da Irlanda, outras empresas estadunidenses apoiaram a Microsoft. Essa coalização de empresas e Estados contra os Estados Unidos ocorreu devido as possíveis consequências de uma derrota da empresa estadunidense. Conforme apontado por Rohr (2014), caso a Microsoft perdesse na justiça, haveria nos Estados Unidos um precedente legal para a requisição de dados no estrangeiro, o que tornou o caso polêmico.

Como dito anteriormente, embora esses casos não sejam um exemplo de movimentos alternativos, eles podem ser considerados ensaios para futuros movimentos. No caso da Estônia, se o projeto com a Microsoft resultar em um sucesso, outros Estados podem utilizar suas representações diplomáticas para garantir a resiliência de sistemas críticos, ou seja, criando "embaixadas virtuais". Na questão do apoio da Irlanda à Microsoft, caso resulte em ganhos para empresa estadunidense, outras empresas podem retirar seus dados de território estadunidense para garantir maior autonomia sobre os armazenamentos. Logo, os movimentos que surgirem desses casos são alternativos, pois não mudam a estrutura vigente, mas somente redirecionam o armazenamento de um centro para outros atores.

4.2.3 Deep Web e FreeNet

Como vimos no primeiro capítulo da dissertação, os regimes internacionais podem surgir pela força, negociação ou espontaneidade. Embora a distinção entre regimes internacionais, movimentos centrais e subjacentes esteja claro, estes também são constituídos de forma semelhante. Assim, eles podem ser frutos da força, de uma negociação ou surgirem como produtos do acaso.

Os atores envolvidos em movimentos espontâneos não apresentam ações formais visando um fim, mas suas ações individuais coincidem e contribuem para um mesmo resultado. Os movimentos espontâneos no espaço cibernético são mais notados entre atores não estatais, pois geralmente estão focados em um objetivo consequencial da estrutura internacional vigente. Os atores privados, por exemplo, apresentam como objetivo comum o lucro, por isso agem semelhantemente em prol dele.

O debate sobre a regulamentação do espaço cibernético apresenta dois extremos: liberalizar ou restringir. Geralmente atores não estatais se posicionam em favor da liberalização, em especial os indivíduos. Assim, enquanto os atores privados visam ao lucro, o objetivo desses indivíduos é a liberdade e privacidade no espaço cibernético.

Um movimento alternativo e espontâneo advindo desses atores pode ser exemplificado pela chamada *Deep Web* e por alguns navegadores alternativos de código aberto. A *Deep Web* é definida como uma parte do espaço cibernético que por algum motivo não está indexada nas ferramentas de busca, como o Google (CIANCAGLINI *et al*, 2015). A indexação consiste em incluir determinados endereços, documentos e materiais nas ferramentas de busca, facilitando o acesso por todos os usuários.

Os principais usuários que recorrem a *Deep Web* são aqueles que buscam garantir seu anonimato na rede. Em virtude disso, de acordo com Ciancaglini *et al* (2015), encontramos na *Deep Web* tanto pessoas que querem proteger suas comunicações, como usuários de drogas, assassinos, *hackers,* jornalistas em busca de informações privilegiadas entre outros. Essas pessoas buscam termos, assuntos e informações ilegais, que são geralmente bloqueados e também filtrados pelos veículos tradicionais (CIANCAGLINI *et al*, 2015).

Dentre as explicações que tornam um conteúdo virtual livre de indexação temos: as páginas são dinâmicas, os sites são bloqueados, eles são privados ou são conteúdos restritos e com acessos limitados (CIANCAGLINI *et al*, 2015). Embora haja diversos motivos para que um conteúdo virtual não seja indexado nas ferramentas de busca, a razão que mais torna a *Deep Web* atraente para essas categorias de pessoas é o desligamento das instituições responsáveis pela gestão da Internet. Por isso, geralmente as páginas publicadas sem vinculação com as principais entidades do espaço cibernético apresentam, por exemplo, nomes de domínios próprios ou fora dos padrões oficiais.

A ausência de regulamentação da *Deep Web* apresenta também um lado negativo, o que faz com que ela seja também conhecida como *Dark Web*. Essa fama negativa não se dá somente pelas categorias de usuários já descritas anteriormente. Ela é conhecida como *Dark* em virtude da dificuldade que os seus usuários tem de discernir quais conteúdos são seguros ou não, por isso, se aconselha aos aventureiros da *Deep Web* não realizarem transferência de dados para seus computadores, conforme alerta estudo de Lívia Vidal e Rafael Santos (2014).

Para acessar essa rede, o usuário utiliza um navegador chamado *TOR,* sigla para *The Onion Router*. Esse navegador foi desenvolvido inicialmente pelo Laboratório de Pesquisa Naval dos Estados Unidos em 2002 para comunicações anônimas (CIANCAGLINI

et al, 2013). Ele permite o anonimato, pois sua programação utiliza pontos aleatórios espalhados na rede, impossibilitando o monitoramento dos dados (CIANCAGLINI *et al*, 2013).

Outra iniciativa similar à *Deep Web* chama-se *FreeNet* e foi desenvolvida por Ian Clarke, quando este ainda era universitário na *Edinburgh University*. Enquanto a *Deep Net* é vislumbrada como um conjunto de conteúdos que não podem ser indexados, a *FreeNet* foi criada com o objetivo de tornar a rede livre e sem restrições (MONTEIRO & FIDENCIO, 2013). Em virtude disso, ela é menos associada a atividades ilícitas do que a *Dark Web.*

A segurança da *FreeNet* está fundada na própria forma de acesso dos conteúdos. Enquanto a *Deep Web* é acessada por meio de navegadores alternativos, como o *TOR*, a *FreeNet* funciona por meio do compartilhamento *people to people* (P2P). Isso significa que não utiliza um navegador específico, mas o compartilhamento entre usuários. Assim, caso conheça o dono do conteúdo, um usuário consegue discernir sobre a segurança de um conteúdo mais facilmente.

Além da Deep Web e da FreeNet, outras diversas iniciativas com o mesmo sentido vêm sendo aplicadas. Dentre elas podemos citar Web Oculta; Web Opaca; Dark Net entre outras (MONTEIRO & FIDENCIO, 2013). Esses movimentos são frutos de uma indiferença, eles visam tornar a Internet livre, sem controle estatal. Assim, esses projetos não foram necessariamente criados em virtude de uma ação especifica do centro, mas como resultado do processo de territorialização do espaço cibernético, que já visava o controle.

Esses projetos são chamados de movimentos alternativos de atores não estatais, pois são compostos por um grupo de atores aquém dos Estados. O próprio navegador Mozilla, visto em capítulos anteriores, também foi criado por um grupo de atores que apoiavam a liberdade. Em virtude disso, ele também poderia ser classificado como parte indireta desse movimento alternativo, não somente pelo seu objetivo, mas também pelo apoio de diversos atores.

Embora o qualifiquemos dessa forma, essas iniciativas aparentam ser mais reacionárias do que alternativas, principalmente quando comparadas com o Mozilla, por exemplo. Entretanto, cabe ressaltar mais uma vez que elas não são consequências de uma ação especifica do centro, mas espontânea. Logo, aprendemos com os exemplos da Deep Web e do Mozilla de que a linha entre os movimentos alternativos e os movimentos reacionários é bem tênue.

4.3 MOVIMENTOS REACIONÁRIOS

4.3.1 Proposta Brasil-Alemanha nas Nações Unidas

A linha que separa os movimentos subjacentes é bem tênue, o que vai diferenciá-los é a intensidade dos sentimentos de indiferença ou amargura para com as ações dos centros. Outra forma de diferenciar é observando se as ações desses movimentos são reacionárias às ações dos centros. Assim, para diferenciá-los devemos pensar nas relações entre movimentos centrais, subjacentes e a Teoria dos Jogos.

De acordo com Ronaldo Fiani (2006), existem dois modelos tradicionais de jogos, a saber: jogos simultâneos e jogos sequenciais. Os jogos simultâneos são aqueles em que os jogadores ignoram as ações dos demais ao tomarem suas decisões, sem se preocuparem com as consequências de suas escolhas. Ao contrário do jogo simultâneo, nos jogos sequenciais, os jogadores tomam decisões em ordem predeterminada, ou seja, eles têm a oportunidade de analisar a jogada anterior dos demais atores para determinar qual será a sua ação.

Os movimentos alternativos seguem o padrão de jogo simultâneo, pois suas ações são regidas principalmente pelo sentimento de indiferença. Assim, esses movimentos não precisam considerar as ações dos centros para agirem. Por sua vez, os movimentos reacionários seguem a lógica dos jogos sequenciais, pois suas ações são pautadas por atos dos centros ou movimentos centrais.

Da mesma forma que ocorre com os movimentos centrais e alternativos, os movimentos reacionários podem ser caracterizados por grupos de Estados centrais e raios. Em virtude disso, encontramos alguns movimentos reacionários compostos por Estados raios e Estados centrais, em uma heterogeneidade. Da mesma forma, encontramos movimentos reacionários homogêneos, em que somente há presença de Estados raios. Entretanto, nos movimentos subjacentes, de uma forma geral, não encontramos homogeneidade de Estados Centrais.

Em virtude dessas colocações, a proposta da Alemanha e Brasil sobre privacidade na ONU pode ser considerado um movimento reacionário. Essa proposta foi feita à ONU em 2013, pouco tempo após as revelações de Snowden sobre as atividades de espionagem da NSA. Naquele período, tanto o Brasil quanto a Alemanha tiveram conhecimento de que seus líderes estavam sendo constantemente monitorados pelos Estados Unidos, por meio de vigilância no espaço cibernético.

Embora essa proposta tenha sido apresentada à ONU em 2013, durante a 68ª Assembleia Geral, ela somente virou uma resolução em 2014, durante a 69ª Assembleia Geral. Durante a fase de apresentação, a proposta foi aprovada para ser incluída na pauta com o consenso. Ademais, ela também foi aprovada com unanimidade dentro do comitê de Direitos Humanos, mas sem uma votação no plenário dos 193 países, conforme apontado por reportagem de O Globo (2014).

Apesar dessa proposta ter sido aprovada pelos 65 países do Conselho de Direitos Humanos, cinco países se abstiveram da votação (O GLOBO, 2014). Esses cinco países são: os Estados Unidos, Austrália, Canadá, Reino Unido e Nova Zelândia, conforme O Globo (2014). Assim, como essa resolução é um movimento reacionário Alemanha-Brasil contra as ações de espionagem dos Estados Unidos, o movimento central dos *"Five Eyes Group"* não apresentou apoio à proposta.

O desapoio desse movimento central não se deu somente por ser uma proposta advinda de um movimento reacionário, mas devido ao conteúdo do documento em si. Isso porque o texto da proposta faz menção às ações que eram realizadas pela NSA, mesmo sem citar diretamente os nomes dos Estados Unidos ou dessa agência, conforme observamos na própria resolução (ONU, 2014a).

A resolução 69/166 da ONU consiste em condenar algumas formas de vigilância, salientar os limites dela e afirmar os princípios sobre privacidade no espaço cibernético. Ela enfatiza que a vigilância não pode ser realizada em larga escala, deve respeitar os direitos civis e políticos dos indivíduos e respeitar a privacidade (ONU, 2014a). Ademais, o documento enfatiza a necessidade dos Estados em respeitar as obrigações internacionais de direitos humanos (ONU, 2014a).

Em virtude disso, a resolução se demonstra preocupada com a forma em que a interceptação de comunicações digitais pode ocorrer. Isso porque a vigilância e interceptação de dados extraterritoriais e recolhimento de dados pessoais em larga escala pode gerar impactos negativos na sociedade. Conforme a resolução, esses impactos não se dão apenas em relação aos indivíduos, mas também engloba as empresas e Estados.

Além disso, a resolução enumera três princípios: direito à privacidade, universalização da Internet e a paridade. Este último reconhece que os mesmo direitos que um indivíduo dispõe fora do espaço cibernético, devem ser aplicados também dentro dele. Ademais, o documento faz algumas considerações aos Estados, conforme quadro abaixo:

Quadro 4.1 – Exortações da Resolução 69/166 da ONU aos Estados

Exortação		Descrição
1	*Proteção do Direito à Privacidade*	A respeitar e proteger o direito à privacidade, inclusive no contexto da comunicação digital;
2	*Prevenir violações de Privacidade*	Tomar medidas para pôr fim às violações desses direitos e para criar condições para prevenir tais violações,
3	*Pertinência da Legislação Nacional*	Assegurar uma legislação nacional relevante, que esteja em conformidade com as obrigações decorrentes do direito internacional dos direitos humanos;
4	*Revisão de Procedimentos de Vigilância de Comunicação*	Rever os seus procedimentos, práticas e legislação relativa à vigilância de comunicações, a intercepção e a recolha de dados pessoal, incluindo a vigilância em grande escala.
5	*Manter Transparência sobre a Vigilância de Comunicação*	Estabelecer ou manter mecanismos existentes, independentes e eficazes, com recursos adequados e imparciais judiciais, administrativos e / ou parlamentares nacionais de fiscalização capazes de garantir a transparência e prestação de contas para a vigilância de comunicações.
6	*Assistência às Vítimas*	Oferecer às pessoas cujo direito à privacidade foi violado por vigilância ilegal ou arbitrária assistência consistente com as obrigações internacionais de direitos humanos;

Fonte: Elaboração própria com base em ONU (2014a).

Como visto anteriormente e por meio dessas exortações, compreendemos que a resolução 69/166 foi possível devido a um movimento reacionário da Alemanha-Brasil. Esse movimento é assim caracterizado, porque engloba um centro do espaço cibernético, a Alemanha, que visa reagir ao *Five Years Group*, um movimento central do qual não participa e que pode prejudicar seu poder. Dessa forma, notamos que um mesmo ator pode participar de movimentos diferentes, pois a Alemanha participa de movimentos alternativos dentro da Europa, com normas próprias para transferência de dados dentro e fora da União Europeia, e de movimentos reacionários com o Brasil, em face da espionagem da NSA.

4.3.2 Buracos Negros do Espaço Cibernético

Como vimos anteriormente, o grupo do BRIC foi criado após um estudo abrangendo esses Estados. Antes mesmo de ser oficialmente um grupo, o BRIC já vinha sendo observado como um grupo. Se um conjunto de países diversificados como os BRIC podem ser observados como um grupo, quiçá países que apresentam características e comportamentos semelhantes, mesmo sem um movimento oficial. Assim, países com objetivos, posições e posturas semelhantes podem ser considerados como um movimento espontâneo, mesmo sem de fato serem.

Um exemplo de um conjunto de países que seguem essas características são os chamados Buracos Negros do Espaço Cibernético. Embora não constituam um grupo oficial,

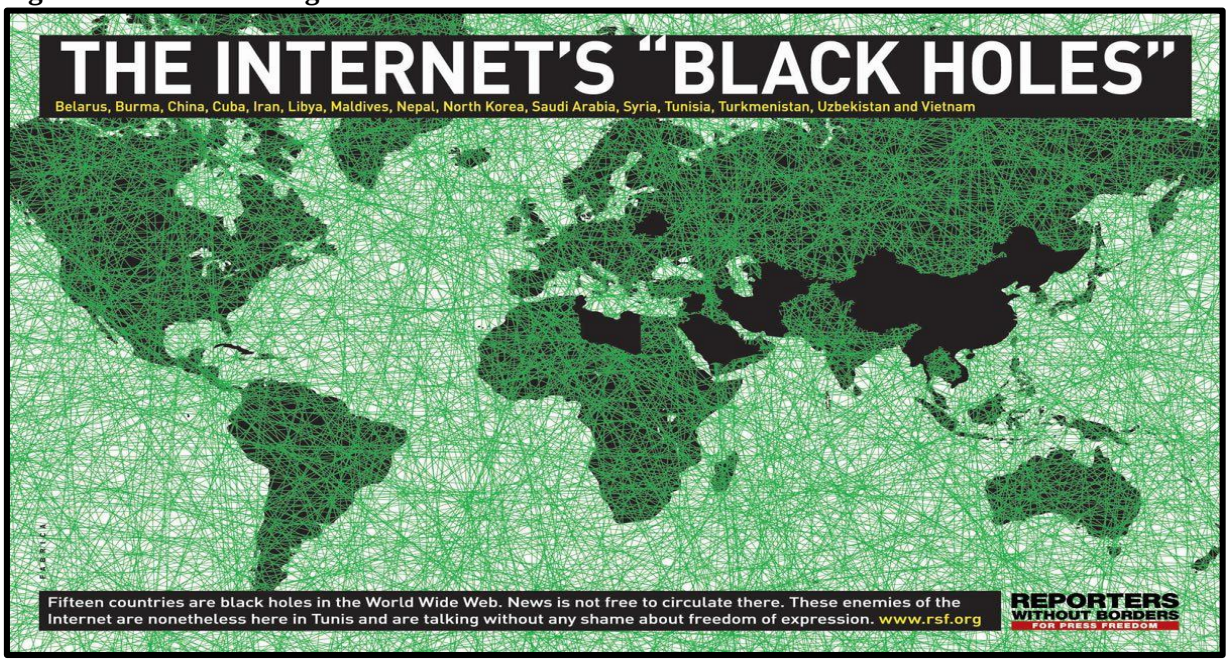
sua importância para os estudos sobre relações internacionais do espaço cibernético é tamanha, que deixar de abordar esse tema pode trazer prejuízos a qualquer pesquisa sobre o assunto. Se observarmos o contexto no espaço cibernético desses Estados chamados Buracos Negros como um possível grupo, a qualificação mais apropriada seria de um movimento reacionário.

O termo Buraco Negro aplicado ao espaço cibernético pode vislumbrar três significados diferentes. O primeiro significado faz referência aos problemas da rede no envio e recepção de pacotes de dados, em que informações são constantemente perdidas (BASSETT *et al*, 2008). Esse termo também pode ser utilizado para falar sobre os riscos que a Internet pode causar aos conceitos históricos, conforme apontado por Vint Cerf (COOKSON, 2015).

O terceiro significado, de interesse para nosso estudo, diz respeito à pesquisa realizada pelos Repórteres sem Fronteiras (RSF) sobre o que eles chamaram de "os inimigos da internet". Os RSF é uma ONG com posição de consultoria juntamente à ONU. De acordo com eles, no contexto do espaço cibernético, os Buracos Negros são países que suprimem a liberdade de expressão on-line (RSF, 2007).

Para controlar a liberdade de expressão, esses países se utilizam de filtros que bloqueiam termos em suas redes nacionais. Por impedir os nacionais de acessarem certos conteúdos de fora dos países e não transmitir uma transparência de sua realidade, esses Estados são chamados de Buracos Negros. De acordo com a RSF (2007), existem no mundo 12 buracos negros, conforme demonstrado pela figura abaixo:

Figura 4.2 – Buracos Negros da Internet



Fonte: RSF (2007).

A listagem criada pelos RFS (2007) vislumbra tanto os filtros que censuram a Internet como também as prisões ou represarias a usuários que divulgaram opiniões contra o governo de seus países. Cabe ressaltar que embora a imagem apresente 15 países como buracos negros, os RFS retiraram da lista três países, restando apenas 12 atores. Eles retiraram a Líbia, Maldiva e Nepal, pois estes países apresentaram, posteriormente, uma melhora nas políticas de liberdade de imprensa, conforme os RFS (2007).

Os buracos negros da Internet são considerados aqui como um movimento reacionário, porque parte dos filtros e restrições impostas pelos países servem para manter os nacionais sob o controle do governo, como notado pela RFS (2007). Em vista da estrutura de mundo atual, em que os organismos internacionais estão constantemente requerendo dos países o compromisso com direitos humanos e liberdade, os chamados Buracos Negros não respondem a esse projeto. Dessa forma, enxergamos o não pareamento desses países com o projeto de um espaço cibernético liberalizado como uma reação aos movimentos que buscam essa liberdade.

Assim, compreendemos que os movimentos reacionários reagem não somente aos centros, mas também a alguns movimentos alternativos. Como os buracos negros reagem à liberalização do espaço cibernético, ele também vai de encontro com a proposta de uma *FreeNet* ou uma *Deep Web*. Ademais, notamos ainda que os movimentos reacionários também podem ser compostos pelo conjunto de Estados centrais e Estados raios, pois dentre os Buracos Negros citados encontramos a presença chinesa, por exemplo.

4.3.3 Casos Wikileaks e Edward Snowden

No mundo da era da conexão, em que a globalização e a interdependência tornam as relações internacionais complexas, pensar em movimentos centrais e subjacentes sem interação com atores não estatais seria errôneo. Essa constatação fica mais evidente quando observamos esses movimentos dentro do espaço cibernético. Mesmo assim, no decorrer desse capítulo, percebemos que parte dos movimentos é constituída principalmente pelos Estados, sejam eles centrais ou raios.

Isso ocorre, em parte, porque os atores não estatais não teriam recursos suficientes de poder, como um Estado tem, para atuar no espaço cibernético, conforme evidenciado por Nye Jr (2012). Entretanto, ainda de acordo com ele, esse fato não exclui a possibilidade dos atores não estatais influírem significativamente nas relações internacionais no espaço

cibernético. Os atores não estatais que são classificados como movimentos reacionários são aqueles que criticam a estrutura vigente ou seu uso pelos movimentos centrais.

Nesse tópico analisaremos dois atores que poderiam ser classificado dentro dos movimentos reacionários, caso viessem a participar de algum: Wikileaks e Edward Snowden. O Wikileaks é uma organização transnacional sem fins lucrativos sediada na Suécia. Essa organização foi criada em 2006 e tinha autorização para armazenamento de documentos oficiais da Secretária de Estado estadunidense e outras secretárias desse país, conforme apontado por Celso Lafer (2011).

Em 2010, entretanto, essa organização começou a publicar uma série de telegramas sensíveis de cunho secreto na rede. Parte dessas publicações exaltaram alguns atores, como os Estados Unidos, contra as ações do Wikileaks, pois comprometiam as atividades desses países (CASTELLS, 2010). Naquele ano, o Wikileaks passou a ter como objetivo o "combate, pela publicidade, de más condutas governamentais e não governamentais, de variável gravidade, da hipocrisia a crimes de guerra" (LAFER, 2011, p. 11).

A publicação de documentos secretos revelou a dimensão do processo de negociação dos Estados. De acordo com Lafer (2011), a publicidade e transparência são princípios necessários a qualquer democracia, para que os cidadãos possam acompanhar o processo político e participar dele. Entretanto, esse autor explica que esses princípios devem ser aplicados somente após o resultado final de uma negociação, pois o segredo do processo de negociação é importante para garantir o canal de diálogo entre as partes.

Em virtude disso, o sigilo de certas informações é necessário para garantir a segurança da sociedade e dos Estados (LAFER, 2011). Esse sigilo compõe o poder invisível e, em certa medida, a razão de Estado. Dessa forma, ao publicar os documentos que revelavam esse processo, o Wikileaks divulgou não somente como os Estados realizavam seus processos informacionais, como também suas opiniões sobre alguns pontos de certas negociações.

Ao demonstrar como os países agiam e pensavam em suas negociações, o Wikileaks utilizou de documentos oficiais. Dessa forma, ele evidenciou atividades legais dos Estados, mas que estavam sendo realizadas sem pudor e respeitos aos demais atores. No caso de Edward Snowden, por outro lado, as suas revelações demonstraram o lado obscuro das coletas de informações por parte dos Estados centrais.

De acordo com Luke Harding (2014), Snowden revelou os acessos clandestinos às informações eletrônicas de outros Estados. As principais revelações dadas por Snowden diz

respeito, principalmente, aos países do *"Five Eyes Group"* e o sistema de vigilância mantido por eles, o ECHELON (HARDIND, 2014). Além dos acessos a informações não autorizadas, outras características que chamaram a atenção do mundo sobre a espionagem estadunidense e de aliados sobre o mundo era a quantidade de informação monitorada, incluindo de pessoas insuspeitas.

Tanto as publicações do Wikileaks quanto as revelações de Edward Snowden são considerados reacionários, devido ao *modus operandi* utilizado. De acordo com Lafer (2011), a diplomacia contemporânea varia conforme os fins e meios utilizados, podendo ser classificada em categorias, como por exemplo, diplomacia parlamentar, de cúpula, presidencial, de combate. Esta última categoria de diplomacia, a de combate, é classificada por Lafer (2011) como:

> Na vida internacional contemporânea há muito da diplomacia pública na diplomacia parlamentar que é parte da diplomacia que se dá em organizações internacionais, na diplomacia de cúpula de reuniões presidenciais e de ministros das Relações Exteriores. Também é uma das características da diplomacia contemporânea, com um forte componente de diplomacia pública, o que Calvet de Magalhães qualifica como diplomacia de combate, com seus ingredientes de batalha ideológica, de conquista da opinião pública e de deslegitimação de atores do sistema internacional. Ela foi uma das notas da Guerra Fria no confronto bipolar entre os Estados Unidos e a então URSS. Ela é uma das características da diplomacia de Hugo Chávez da Venezuela no seu combate ideológico aos EUA e de muitos países árabes, e do Irã, voltado para deslegitimar a presença de Israel no sistema internacional. (LAFER, 2011, p. 15).

De acordo com a passagem acima, a diplomacia de combate é utilizada para desacreditar e desestruturar ações de outros Estados. Aqui podemos incluir também como uma forma de reagir aos movimentos centrais. Cabe ressaltar que no espaço cibernético, em que os canais de acesso são facilitados, a diplomacia não é exclusividade dos agentes da Secretaria de Estado, podendo ser exercidas sob a forma da paradiplomacia. Ademais, cabe ressaltar que, embora o Wikileaks e o Edward Snowden sejam uma organização e um indivíduo, respectivamente, ambos ganham adeptos para suas ações, como o jornalista Luke Harding e o Governo Russo.

CONSIDERAÇÕES FINAIS

O espaço cibernético não é um conceito comum aos pesquisadores, pois ele apresenta diversidade quanto aos elementos que o englobam. A revisão bibliográfica realizada sobre as diversas definições desse espaço cibergeográfico, chamou nossa atenção para uma conceituação que abrangesse duas visões, a de Richard Clarke e a de Daniel Ventre. Assim, o espaço cibernético seria toda a rede de equipamentos do mundo, que produza ou manipule informações, e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles, seja na Internet ou fora dela.

Embora esse espaço seja um produto humano e territorializado desde seu princípio, as pessoas que o utilizam não devem ser englobadas em sua definição. De acordo com essa dissertação, os usuários do espaço cibernético constitui um recurso humano (*peopleware*). Dessa forma, enquanto os usuários do espaço terrestre não constituem a terra, no espaço cibernético, os usuários não constituem a cibergeografia, mas são agentes de sua territorialização, ou seja, seus operadores.

Além disso, observamos no decorrer da bibliografia consultada, o tratamento do conceito de espaço cibernético e de Internet como sinônimos. Entretanto, para abordagens mais profundas e específicas, a distinção entre esses dois conceitos deve ser evidenciada. Isso porque o espaço cibernético também engloba todos os aparelhos e recursos produtores e manipuladores de informações que não estão conectadas à Internet ou que compõe apenas uma internet particular.

Essa composição complexa de pontos de acesso do espaço cibernético permite que ele seja de fácil exploração, porém de complexa segurança e defesa. Isso porque o espaço cibernético permite o anonimato e também o disfarce de informações e localizações dos seus usuários. Em virtude disso, alguns autores analisados consideram sinônimos os termos Guerra Cibernética e Guerra Invisível.

Essas mesmas características que tornam a guerra cibernética uma guerra invisível, também são motivadoras de conflitos entre soberanias nesse espaço cibergeográfico. Embora, os registros de domínios e utilização da rede de um país por estrangeiros respeitam uma regulamentação nacional, a insuficiência tecnológica facilita a propagação de crimes e ataques cibernéticos, tanto aos nacionais do próprio Estado quanto a terceiros no estrangeiro. Diante disso, a paz no espaço cibernético carece de uma soberania responsável, em que o Estado deve responder as demandas tanto dos nacionais como da comunidade internacional.

Nesse sentido, a observação da soberania responsável no espaço cibernético pelos Estados também previne litígios nos demais espaços. Isso porque os espaços terrestre, marítimo, aéreo e extra-atmosférico são interconectados pelo espaço cibernético. Essa premissa nos ensina que qualquer dispositivo conectado ao espaço cibernético, seja na terra, água ou ar, pode gerar consequências reais, pois há uma integração entre as fronteiras dos demais espaços e as fronteiras cibernéticas.

Essa dissertação reconheceu especificidades nas fronteiras do espaço cibernético, compreendendo sua composição em fronteiras materiais e imateriais. As fronteiras materiais dizem respeito às maquinas, cabos submarinos e torres de transmissão, enquanto as fronteiras imateriais são os pacotes de dados, divisões geográficas e de responsabilidades. Assim, compreendemos o espaço cibernético delimitado por fronteiras multifacetárias.

Entretanto, o espaço cibernético não deve ser observado apenas como algo tangível e físico, pois ele também é um espaço conectivo. Os usuários desse espaço se mantêm conectados continuamente e em diversos lugares, por meio de computadores, celulares, televisores, carros e até mesmo refrigeradores. Em virtude disso, podemos identificar o período atual como a "Era da Conectividade".

Cabe ressaltar que o espaço cibernético não elimina as identidades reais ou as relações sociais. Pelo contrário, o aumento da conectividade dos indivíduos aflora suas redes sociais e aprofunda suas identidades. Ademais, embora as características do espaço cibernético permitam ao indivíduo transitar no mundo como se não houvesse fronteiras, sua ligação com o território permanece devido aos sentimentos topofílicos e terrafílicos.

Essa liberdade de navegação gera um sentimento de ausência de controle no espaço cibernético. Entretanto, a territorialização do espaço cibernético gerou regras e organizações responsáveis pela manutenção desse espaço. Embora existam essas organizações, não existe um regime internacional do espaço cibernético.

A ausência de um regime internacional sobre o espaço cibernético pode ser justificada por três premissas. A primeira diz respeito ao ineditismo deste espaço, que começa a ser veementemente um assunto de questões soberanas neste século XXI. A segunda é sobre a nacionalidade das atuas organizações responsáveis pela gestão desse espaço, pois a maioria delas está sediada nos Estados Unidos. A terceira premissa tem ligação com a segunda, ela diz respeito ao desinteresse dos Estados Unidos em perder a predileção sobre esse espaço.

Um regime internacional para o espaço cibernético poderia limitar o poderio dos Estados Unidos nesse território, impedindo-o de ser o principal centro nesse tabuleiro. Cabe ressaltar que mesmo com tal poderio, os Estados Unidos não é o único centro do espaço

cibernético. Juntamente com ele, podemos citar como principais centros do espaço cibernético a Alemanha; a China; a França; o Japão; o Reino Unido e a Rússia.

Esses países apresentam alta penetração da Internet em suas sociedades, parte considerável dos controladores do espaço cibernético e os principais produtores de conhecimento dessa temática. Entretanto, cabe ressaltar que embora esses países apresentem essas características, a estrutura do espaço cibernético é suportada por organizações estadunidenses. Sobre os recursos de poder *peopleware*, a centralidade do mundo é dividida entre Estados Unidos e China, sendo que apenas os Estados Unidos apresenta projeção global.

A percepção de um mundo formado por centro e raios surge dentro da política externa estadunidense no início da década de 1950. Por meio da percepção dessa política externa, essa dissertação entendeu que Estados centrais são caracterizados como *global players* do sistema internacional vigente, com poder para moldar as predileções de outros atores e defender seus interesses nacionais. Ademais, em um sistema centro-raios perfeito, esses Estados são constantemente consultados sobre todos os temas e discussões, mesmo aquelas que não lhe dizem respeito diretamente.

Por sua vez, os Estados raios são aqueles que estão sob a influência de algum Estado central e não constituem poder para serem classificados como *global players*. Além do mais, em um sistema centro-raios perfeito, todos os seus assuntos e negociações com outros países devem considerar também o posicionamento do Estado central. Entretanto, em um sistema imperfeito, a relação entre raios-raios também é possível, chegando mais próximo da realidade que presenciamos.

Quando essas categorias de Estado negociam e tentam projetar um interesse conjunto no cenário internacional, elas constituem movimentos. Estes podem ser classificados quanto aos seus objetivos em movimentos centrais ou subjacentes. Os movimentos centrais são aqueles que pretendem manter a estrutura internacional e os atores centrais, enquanto os movimentos subjacentes divergem da estrutura vigente e dos *global players*.

Os movimentos subjacentes ainda podem ser divididos em subcategorias, movimentos alternativos e movimentos reacionários. Os movimentos alternativos visam à manutenção da estrutura internacional, porém, eles desejam a mudança dos *global players*, Por sua vez, os movimentos reacionários visam à alteração tanto da estrutura internacional quanto dos Estados centrais.

Cabe ressaltar que os movimentos centrais e subjacentes não são estadocentricos, pois em um século marcado pela difusão de poder gerada pelos avanços tecnológicos, a atuação de atores não estatais está cada vez mais evidenciada. Entretanto, os custos para

coordenar um movimento central e alternativo é demasiadamente caro, o que limita a participação desses atores como apêndices. Em virtude disso, nota-se uma maior participação desses atores nos movimentos reacionários, devido à facilidade de se opor aos centros com pequenas ações e em pequenos grupos.

O ensejo para essa atuação se dá devido às características do poder cibernético. Enquanto para se construir um avião é necessário ao agente dispor de recursos elevados, no caso das armas cibernéticas, poucos investimentos podem ser suficientes para grandes danos. Assim, atores não estatais conseguem lançar ataques cibernéticos aos Estados.

Outra particularidade do poder cibernético é que ele pode ser divido em factual e especulativo. O poder cibernético factual é aquele que utiliza recursos tangíveis para moldar comportamentos, tais como satélites, servidores, *hackers*, estratégias, dentre outros. O poder cibernético especulativo, por sua vez, está associado aos recursos intangíveis de um Estado, que são revelados pelo discurso e não podemos ter certeza da sua existência, mas que gera dissuasão e constrangimentos aos demais atores.

O jogo da relações internacionais em torno do poder cibernético resulta na existência de movimentos centrais e subjacentes, que após mapeados e analisados, podem ser sintetizados pelo quadro abaixo:

Quadro 4.2 – Movimentos Centrais e Subjacentes do Espaço Cibernético

Categorias	Movimentos	Característica	Atores	Formalidade
Centrais	Five Eyes Group	Heterogêneo	Estatais	Negociado
	Safe Harbor	Homogêneo	Misto	Negociado
Alternativos	BRICS Cable	Heterogêneo	Estatais	Negociado
	Estônia; Irlanda e Microsoft	Homogêneo	Misto	Espontâneo
	Deep Web	Heterogêneo	Não Estatais	Espontâneo
Subjacentes	Alemanha-Brasil	Heterogêneo	Estatais	Negociado
	Buracos Negros	Heterogêneo	Estatais	Espontâneo

Fonte: Elaboração própria com base em O Globo (2014); Ciancaglini et al (2015); The Economist (2015); Altieres Rohr (2014); Gill Lopes (2013); James Cox (2012); Connolly (2009).

Para a manutenção de seu poder, os Estados Unidos, o principal centro do espaço cibernético, participam e empreendem alguns movimentos centrais. Dos movimentos que ele participa, analisamos dois emblemáticos: o acordo *Safe Harbor* e o *Five Years Group.* O primeiro movimento apresenta participação exclusiva de Estados centrais, enquanto o segundo apresenta também participação de Estados raios.

O acordo *Safe Harbor* apresenta participação principal dos Estados Unidos, Reino Unido, França e Alemanha. O principal objetivo desse acordo é estabelecer canais de

transferência de dados diferenciados entre os Estados Unidos e os centros europeus. Esse exemplo nos demonstrou também que um movimento central pode ser agredido por Estados raios e por atores não estatais, como a Irlanda e os irlandeses envolvidos, respectivamente.

Sobre o *Five Years Group*, ele é um acordo voltado às questões de inteligência. O objetivo desse grupo é criar uma rede cooperação na temática de inteligência entre Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia. Essa cooperação envolveria não somente o compartilhamento de cursos e técnicas, como também o intercâmbio de informações sobre os demais países do mundo.

Ele apresenta participação de Estados raios, mesmo sendo um projeto conduzido pelos Estados Unidos e pelo Reino Unido. Isso nos mostra que um movimento central pode buscar apoio de raios, quando percebem benefício na cooperação. Percebemos também que as decisões adotadas nos movimentos centrais, de forma geral, sempre apresentam impactos aos demais Estados não participantes.

Cabe ressaltar, ainda sobre os movimentos centrais, que a dissertação não vislumbrou nenhum exemplo constituído unicamente ou com prerrogativa de atores não estatais. Entretanto, com o exemplo abordado da inserção da Google na China, compreendemos que a ausência de movimentos com essa característica ocorre devido ao poder necessário para manter um movimento central. Isso porque embora as relações internacionais no espaço cibernético apresente abertura facilitada para todos os atores, somente os Estados apresentam recursos para uma projeção global.

Além disso, os Estados centrais não constituem apenas movimentos centrais, eles também estão inseridos em movimentos alternativos e reacionários. Um exemplo de movimentos alternativos com a participação de Estados centrais foi encontrado nos BRICS. Os principais centros do espaço cibernético que compõe esse grupo é a Rússia e a China.

Os BRICS foram caracterizados como movimentos alternativos, porque não visam à reestruturação do espaço cibernético, mas apenas a criação de uma rede de domínio de seus Estados membros. Assim, eles pretendem criar uma rede para uso em que os Estados Unidos não tenham a prerrogativa. Entretanto o projeto criado para isso, o *BRICS Cable*, ainda não conseguiu investimentos suficientes, como também outros colaboradores.

Embora a iniciativa dos BRICS não tenha recebido ainda o apoio esperado, ela é considerada aqui como um projeto tangível, pois não evidenciamos outros movimentos alternativos significativos. O que foi percebido no mapeamento desses movimentos no espaço cibernético são ensaios individuais, como no caso da Estônia e Irlanda. A abordagem dos casos em que um único país adota medidas alternativas aos movimentos centrais foi

considerada na dissertação, pois pode gerar movimentos alternativos espontâneos posteriores, caso comprovados os benefícios advindos desses atos.

Os casos da Estônia e Irlanda demonstraram também que atores não governamentais sediados nos Estados centros podem apoiar movimentos alternativos contra seu próprio país. Isso foi notado pelo apoio que a empresa estadunidense Microsoft forneceu à Estônia e Irlanda. Mais evidente ainda foi a participação dessa empresa juntamente com a Irlanda em uma disputa jurídica contra o acesso de dados no estrangeiro pelos Estados Unidos.

Além da relação entre Estados e atores não estatais nos movimentos alternativos, podemos considerar a atuação conjunta dos atores não estatais como um movimento próprio. Isso porque esses atores apresentam, algumas vezes, objetivos em comum, o que gera uma impressão de ações conjuntas em um movimento unificado e espontâneo. No caso do espaço cibernético, esse fenômeno pode ser vislumbrado pela manutenção de iniciativas como a *Deep Net*, que visa à manutenção da liberdade e privacidade na rede.

Embora os movimentos subjacentes que são compostos por atores não estatais aparentam ser, em sua maioria, mais reacionários do que alternativo, devemos tomar cuidado quanto à classificação. Isso porque partes desses movimentos não agem em reposta às ações especificas dos centros, mas são movimentos espontâneos. Assim, os exemplos observados da *Deep Web* e do navegador Mozilla nos ensinou que a linha entre os movimentos alternativos e os movimentos reacionários é bem tênue, sejam eles movimentos compostos somente por Estados ou aqueles com participação de atores não estatais.

Sobre os movimentos reacionários, a dissertação analisou a proposta da ONU sobre privacidade *on-line*. Essa proposta foi resultado do movimento Alemanha-Brasil, que foi configurado como reacionário, pois pretendia responder a um movimento central vigente, o *Five Years Group*. Cabe ressaltar que este movimento pode ser configurado como heterogêneo, pois vislumbrou a participação de um Estado central, a Alemanha, e de um Estado raio, o Brasil.

Além do mais, esse exemplo nos permitiu compreender que um ator estatal pode compor diferentes movimentos. Dessa forma, encontramos a Alemanha que participa de um movimento alternativo – a União Europeia e a norma europeia sobre privacidade de dados –, mas que também compõe um movimento reacionário com o Brasil. Este por sua vez, além do movimento com a Alemanha, compõe um movimento alternativo com os demais membros dos BRICS.

Cabe ressaltar ainda, que os movimentos reacionários podem reagir também aos movimentos alternativos. Isso ficou claro quando abordamos os exemplos dos chamados Buracos Negros da Internet. O grupo de Estados que compõe esse movimento reacionário aplicam filtros no espaço cibernético para controlar certos dados. Por aderirem a essa filtragem, os Buracos Negros reagem à liberdade e privacidade do espaço cibernético, que é defendida por alguns movimentos alternativos, como a *DeepWeb* e a *FreeNet.*

Sobre a participação dos Estados no espaço cibernético, a dissertação não observou uma hierarquia entre aqueles movimentos compostos somente de centros e aqueles formados apenas por raios. Dessa forma, um movimento formado unicamente de raios pode ser mais forte do que um movimento formado por centros. Igualmente, observamos que certos atores não estatais, como Wikileaks e Edward Snowden, podem constranger movimentos centrais e subjacentes formados por Estados, mesmo não participando de movimentos.

Por fim, o espaço cibernético foi criado em território dos Estados Unidos, sendo esse o Estado com maior domínio e autonomia sobre ele. Para restringir este domínio ou garantir o exercício da soberania, os demais Estados formam movimentos subjacentes (alternativos e reacionários). Estes movimentos não se limitam somente aos atores estatais, também sendo observado nos demais atores. Desta forma, existe uma correlação entre os movimentos centrais dos Estados Unidos e movimentos subjacentes, sejam eles alternativos ou reacionários.

REFERÊNCIAS

Ações da Opera Software decolam e valor da empresa pode chegar a US$ 1 bi. **TI Inside Online.** São Paulo, mai. 2012. Disponível em <http://convergecom.com.br/tiinside/29/05/2012/acoes-da-opera-software-decolam-e-valor-da-empresa-pode-chegar-a-us-1-bi/>. Acesso em: 19 jul. 2015

AGOSTINHO, Santo. **Confissões**. Coleção Os Pensadores, São Paulo: Nova Cultural, 1996

AMARAL, Roberto. Política de Defesa de um País Emergente. In: MONTEIRO, Álvaro A. D; WINAND, Érica C. A; GOLDONI, Luiz R. F. **Defesa da Amazônia**. VII Encontro Nacional da Associação Brasileira de Estudos de Defesa. Sergipe: Ed. UFS, 2014.

ANDRADE, Regis de Castro. "Kant: a liberdade, o indivíduo e a república". In: WEFFORT, Francisco C. (org.). **Os clássicos da política**. Volume 2. São Paulo: Ática, 1998.

ARON, Raymond. **Paz e Guerra entre as Nações**. Brasília: Editora Universidade de Brasília, 1979.

AS MAIORES EMPRESAS do mundo em valor de mercado. **Exame**. São Paulo, mai. 2014. Seção de Mercados. Disponível em <http://exame.abril.com.br/mercados/noticias/as-maiores-empresas-do-mundo-em-valor-de-mercado/lista>. Acesso em: 19 jul. 2015.

ASH, Timothy Garton. As threats multiply and power fragments, the coming decade cries out for realistic idealism. **The Guardian,** Reino Unido, dez. 2009. Seção World News. Disponível em <http://www.theguardian.com/commentisfree/2009/dec/30/threats-multiply-power-fragments-realistic-idealism>. Acesso em: 08 jul. 2015.

BARROS, Otávio Santana Rêgo (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretária de Assunto Estratégicos da Presidência da República, 2011.

BASSETT, Ethan K; MADHYASTHA, Harsha V; JOHN, John P; KRISHNAMURTHY, Arvind; WATHERALL, David; ANDERSON, Thomas. **Studying black hole in the Internet with Hublle**. USENIX Symposium. California: USENIX Association Berkeley, 2008.

BAUMAN, Zygmunt. **Globalização:** as consequências humanas. Tradução Marcus Penchel. Rio de Janeiro: Jorge Zahar Editor, 1999.

BISSIO, Beatriz**.** De Bandung aos BRICS: dois estilos, um objetivo. **Diálogos do Sul.** Rio de Janeiro, jun. 2015. Disponível em <http://www.dialogosdosul.org.br/de-bandung-aos-brics-dois-estilos-um-objetivo/19062015>. Acesso em 07 dez. 2015.

BOBBIO, Norberto. **Dicionário de política**. 6 ed. Brasília: Editora Universidade de Brasília, 1994.

BODIN, Jean. **Os seis livros da República**: Livro Primeiro. São Paulo: Editora Ícone, 2011.

BOOZ ALLEN HAMILTON. **Cyber Power Index.** Estados Unidos: Economist Intelligence Unit, 2011.

BUAINAIN, Antonio Márcio *et al*. Propriedade intelectual e inovação tecnológica: algumas questões para o debate atual. *In*: OLIVEIRA, D. H. de (Org.). **O futuro da indústria: cadeias produtivas.** V. 1, p. 11-38. Brasília: MDIC/STI, 2005.

BURNS, Edward Macnall. **História da Civilização Ocidental.** Vol. 1. Rio de Janeiro: Ed. Globo, 1948.

BUZAN, Barry. WÆVER, Ole. **Regions and Powers:** The Structure of International Security. Reino Unido: Cambridge University Press, 2003.

CARROLL, William K.. **Hegemony, counter-hegemony, anti-hegemony.** Socialist Studies 2(2), 9-43. Canada: University of Victoria, 2006.

CARVALHO, Paulo Sergio Melo de. Conferência de Abertura: o setor cibernético nas forças armadas brasileira. In: BARROS, Otávio Santana Rêgo (Org.). **Desafios estratégicos para segurança e defesa cibernética.** Brasília: Secretária de Assunto Estratégicos da Presidência da República, 2011.

CASELLA. Paulo Borba (Org.). **Manual de Direito Internacional Público.** 20ª Ed. São Paulo: Saraiva, 2012.

CASTELLS, Manuel. **A Galáxia da Internet:** reflexões sobre a internet, os negócios e a sociedade. Tradução Maria Luiza Borges. Rio de Janeiro: Jorge Zahar Editor, 2003.

_____. A ciberguerra do Wikileaks. **Observatório da Imprensa**. São Paulo, dez. 2010. Seção Imprensa em Questão. Disponível em <http://observatoriodaimprensa.com.br/imprensa-em-questao/a-ciberguerra-do-wikileaks/> Acesso em 24 ago. 2015.

CERVO, Amado. **Inserção Internacional:** formação dos conceito brasileiros. São Paulo: Ed. Saraiva, 2008.

CHA, Victor. **Powerplay:** The Origins of the U. S. Alliance System in East Asia. International Security, 34. United States: Harvard, 2001.

CHINN, Menzie D; FAIRLIE, Robert W. **The determinants of the global digital divide:** a cross-country analysis of computer and internet penetration. Oxford Economic Papers. United King: Oxford, 2006.

CIANCAGLINI, Vincenzo; BALDUZZI, Marco; MCARDLE, Robert; RÖSLER, Martin. **Below the Surface:** Exploring the Deep Web. TrendLab Research Paper. Tóquio: Trend Micro, 2015.

CIANCAGLINI, Vincenzo; BALDUZZI, Marco; MCARDLE, Robert; GONCHAROV, Max. **Deepweb and Cybercrime:** It's Not All About TOR. Trend Micro Research Paper. Tóquio: TrendMicro, 2013.

CHACOS, Brad. Como navegar anônimo na Internet. **PCWorld.** Estados Unidos, 30 nov. 2012. Disponível em: <http://pcworld.com.br/dicas/2012/11/30/como-navegar-anonimo-na-internet> Acesso em: 10 fev. 2015.

CLARKE, Richard A. **Cyber War:** the next threat to national security and what to do about it. New York: HarperCollins Publishers, 2012.

CLAUSEWITZ, Carl Von. **On War**. Reino Unido: Penguin Books Limited, 1982.

CONNOLLY, Chris. **The US Safe Harbor:** Fact or Fiction. Australia: Galexia, 2008.

COOKSON, Clive. Web pioneer Vicent Cerf warns of internet history 'black hole'. **Financial Times.** California, fev. 2015. Disponível em <http://www.ft.com/intl/cms/s/0/095e2af2-b328-11e4-b0d2-00144feab7de.html#axzz3jC4dq955> Acesso em 18 ago. 2015.

CORRÊA, Alessandra. Banco dos BRICS tem potencial de virar o jogo, diz economista dos EUA. **BBC Brasil**. Brasil, jul. 2014. Disponível em <http://www.bbc.com/portuguese/noticias/2014/07/140710_banco_brics_lk> Acesso em 17 ago. 2015.

COX, James. **Canada and The Five Eyes Intelligence Community.** Strategic Studies Working Group Papers. Canada: CIC, 2012.

COX, Robert. **Social Forces, States and World Orders:** Beyond International Relations Theory. Millennium Journal of International Studies. United States: SAGE, 1981.

CRUZ JR, Samuel César da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual.** Texto para Discussão 1850. Brasília: IPEA, 2013.

CUNHA, Ciro. **Terrorismo Internacional e a Política Externa Brasileira após o 11 de Setembro.** Dissertação [Mestrado em Diplomacia]. Brasília: IRBr, 2010.

DLA PIPER. **Data Protection Laws of the World.** United King: DLA Piper Global Law Firm, 2015. Disponível em <www.dlapiperdataprotection.com/#handbook/world-map-section> Acesso em 08 ago. 2015.

DUPAS, Gilberto. **Atores e Poderes na Nova Ordem Global:** assimetrias, instabilidades e imperativos de legitimação. São Paulo: Ed. UNESP, 2005.

FARREL, Henry. Negotiating Privacy across Arenas: The EU-US 'Safe Harbor' Discussions. In: HÉRITIER, Adrienne. **Common Goods:** Reinventing European and International Governance. Maryland: Rowman and Littlefield, 2002.

FAUSTO, Boris. **História do Brasil.** 13ª ed. São Paulo: Ed. USP, 2009

FERREIRA NETO, Walfredo B. Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso do poder. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONZALES, Selma Lúcia de Moura (Org.) **Segurança e Defesa Cibernética**: da fronteira física aos muros virtuais. Coleção I - Defesa e Fronteiras Cibernética Pernambuco: Editora UFPE, 2014.

FIANI, Ronaldo. **Teoria dos Jogos**: com aplicação e Economia, Administração e Ciências Sociais. 2ª ed. rev. e atual - Rio de Janeiro: Elsevier, 2006.

FINKLEA, Kristin M. **The Interplay of Borders, Turf, Cyberspace, and Jurisdiction**: issues confronting U.S. Law Enforcement. CRS Report for Congress Washington: Congressional Research Service, 2013.

FONSECA FILHO, Cléuzio. **História da Computação:** O caminho do Pensamento e da Tecnologia. Porto Alegre: EDIPUCRS, 2007.

FOUCHER, Michel. **Obsessão por fronteiras**. São Paulo: Radical Livros, 2009

FRANCHI, Tássio. **Igualdades e diferenças no discurso do Exército Zapatista de Libertação Nacional**: construção e estratégias do discurso zapatista (1994-1996). Dissertação [mestrado]. São Paulo: UNESP, Brasil. 2004.

FURTADO, Celso. **Formação Econômica do Brasil.** São Paulo: Companhia das Letras, 2007.

GAMA NETO, Ricardo Borges; LOPES, Gills Vilar. Armas Cibernéticas e Segurança Internacional. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONZALES, Selma Lúcia de Moura (Org.) **Segurança e Defesa Cibernética**: da fronteira física aos muros virtuais. Coleção I - Defesa e Fronteiras Cibernética Pernambuco: Editora UFPE, 2014.

GOMES, Ulisses. FREITAS, Whitney. (Org.) **Desafios Estratégicos para a Segurança e Defesa Cibernética.** Brasília: SAE, 2011.

GONÇALVES, Ana Teresa M. **Romanos e Partos:** atividades bélicas na república e no principado. Saeculum, v. 13. Pernambuco: UFPB, 2005.

HARDING, Luke; LEIGH, David; PILKINGTON, Ed. **Wikileaks:** a Guerra de Julian Assange contra os Segredos de Estado. Rio de Janeiro: Ed. Verus, 2011.

_____. **Estrutura de Segurança, Estabilidade e Resiliência**. California: ICANN, 2013. Disponível em <https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-pt.pdf> Acesso em 19 ago. 2015.

HARE, Forrest. **Borders in Cyberspace**: Can Sovereignty Adapt to the Challenges of Cyber Security? In CZOSSECK, Christian; GEERS, Kenneth. The Virtual Battlefield: Perspectives on Cyber Warfare. Cryptology and Information Security Series, Vol. 3. Estonia: CCDCOE, 2009.

HEMMER, Christopher; KATZENSTEIN, Peter J. **Why is there No Nato in Asia?** Collective Identity, Regionalism, and the Origins of Multilateralism. International Organization 56, No 3. Massachusetts: MIT, 2002.

HOBBES, Thomas. **Leviatã ou Matéria, Forma e Poder de um República Eclesiástica e Civil**. São Paulo: Martins Fontes, 2003.

HOBSBAWM, Eric J. **A Era das Revoluções:** 1789-1848. 33ª ed. Rio de Janeiro: Ed. Paz e Terra, 2014.

HOSANG, Alexandre**. Política Nacional de Segurança Cibernética:** uma necessidade para o Brasil. Rio de Janeiro: ESG, 2011.

HOW to back up a country. **The Economist**. Estados Unidos, mar. 2015. Seção Internet Security. Disponível em <http://www.economist.com/news/technology-quarterly/21645505-protect-itself-attack-estonia-finding-ways-back-up-its-data-how> Acesso em 24 ago. 2015.

HUSEK, Calor Roberto. **Curso de Direito Internacional Público.** 3a ed. São Paulo: LTr, 2000.

IKENBERRY, John G; MASTANDUNO, Michael; WOHLFORT, William C. International **Relations Theory and the consequence of Unipolarity.** United King: Cambridge University Press, 2011.

JOHNSON, David R.; POST, David G. **Law and Borders: The Rise of Law in Cyberspace**. Stanford Law Review 1367. California: Stanford University, 1996.

JSTOR. Browse by Publisher**. Banco de dados de Revistas Cientificas.** Nova York: Ithaca Harbors, 2015. Disponível em: <http://www.jstor.org/action/showJournals?contentType=allcontents&browseType=publisherInstance&publisherLetter=U>. Acesso em: 15 jul. 2015.

KANT, Immanuel. **A paz perpétua**. Tradução de Marcos Zingano. Porto Alegre: L&PM, 2008.

KAPLAN, Robert D. **A Vingança da Geografia:** A construção do mundo geopolítico a partir da perspectiva geográfica. Rio de Janeiro: Elsevier, 2013.

KIISKI, Sampsa; POHJOLA, Matti. **Cross-country diffusion of the Internet.** Information Economics and Policy, Vol. 14, Issue 2. Filand: Elsevier, 2002.

KNIGHT, Peter T. **A Internet no Brasil:** Origens, Estratégia, Desenvolvimento e Governança.

LAFER, Celso. **Vazamentos, sigilo, diplomacia:** a propósito do significado do Wikileaks. Revista Política Externa, Vol. 19, Nº 4. São Paulo: HMG Editora, 2011.

LEMOS, André. Cibercultura e mobilidade: a era da conexão. In: LEÃO, Lucia [Org]. **Derivas:** cartografias do Ciberespaço. São Paulo: Annablume, 2004.

LESAME, Zandi. **Technology Transfer and Business Partnerships in BRICS:** Development, Integration and Industrialisation. Mediterranean Journal of Social Sciences, Vol. 05 No 7. Rome: MCSER Publishing, 2014.

LIST Of the 13 Internet Enemies. **RSF.** Paris, ago. 2007. Disponível em <http://en.rsf.org/list-of-the-13-internet-enemies-07-11-2006,19603> Acesso em 19 ago. 2015.

LJUNGGREN, David; HOSENBALL, Mark. Canada Intelligence-Sharing on Suspects Curbed by Court Ruling. **Reuters**. United States, out. 2014. Seção World. Disponível em <http://www.reuters.com/article/2014/10/25/us-canada-attacks-intelligence-idUSKCN0IE0T320141025> Acesso em: 12 ago. 2015.

LOCKE, John. **Segundo Tratado sobre o Governo Civil e Outros Escritos**: Ensaio sobre a Origem, os Limites e os Fins Verdadeiros do Governo Civil. Petrópolis: Vozes, 1994.

LOPES, Gills. **BRICS Cable:** levando a cabo uma resposta brasileira à espionagem internacional. Boletim Mundorama. Brasília: UnB, 2013. Disponível em <http://mundorama.net/2013/09/28/brics-cable-levando-a-cabo-uma-resposta-brasileira-a-espionagem-internacional-por-gills-lopes/> Acesso em 17 ago. 2015.

MANDARINO JR, Raphael. **Segurança e Defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010.

MAQUIAVEL, Nicolau. **Discursi:** comentários sobre a primeira década de Tito Lívio. Brasília: Ed. Universidade de Brasília, 1994.

_____. **O Príncipe.** Porto Alegre: L&PM, 2010.

MATSU, Carla. No Brasil, jornalista James Bamford. **Terra IDGNow.** São Paulo, jul. 2015. Seção de Internet. Disponível em <http://idgnow.com.br/internet/2015/07/03/no-brasil-jornalista-james-bamford-discute-privacidade-em-tempos-de-nsa/> Acesso em: 12 ago. 2015.

MATTOS, Carlos de Meira. **Geopolítica e Teoria de Fronteiras:** Fronteiras do Brasil. Rio de Janeiro: Biblioteca do Exército, 1990.

MATTOS, Adherbal Meira. Os novos limites dos espaços marítimos nos trinta anos da Convenção das Nações Unidas sobre o Direito do Mar**.** *In.:* BEIRÃO, André P; PEREIRA, Antônio Celso A. (Org.). **Reflexões sobre a Convenção do Direito do Mar.** Brasília: FUNAG, 2014.

MAZZUOLI, Valerio de Oliveira. **Curso de Direito Internacional Público.** 5ª ed. São Paulo: Editora Revista dos Tribunais, 2011.

MCGREGOR, Richard; DYER, Geoff. US Split over whether allies' spying fury is genuine. **Financial Times**. Estados Unidos, out. 2014. Seção US Politics & Policy. Disponível em <http://www.ft.com/intl/cms/s/0/b9fc90ae-3ff4-11e3-a890-00144feabdc0.html#axzz3idT9sPUb> Acesso em 12 ago. 2015.

MCGUIRE, Mike. DOWLING, Samantha. **Cyber crime:** a review of the evidence**.** Home Office Research Report 75. Reino Unido: Londres, 2013.

MEDEIROS FILHO, Oscar. Em busca de ordem cibernética internacional. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONZALES, Selma Lúcia de Moura (Org.) **Segurança e Defesa Cibernética:** da fronteira física aos muros virtuais. Coleção I - Defesa e Fronteiras Cibernética Pernambuco: Editora UFPE, 2014.

MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius. **As dobras semióticas do ciberespaço**: da web visível à invisível. Transinformação, No 25. Campinas: PUC, 2013.

MONTESQUIEU, Barão de. **O Espírito das Leis.** São Paulo: Martins Fontes, 1996.

MUNIZ, Rafael. **A nacionalidade do Navio à luz da Convenção das Nações Unidas sobre o Direito do Mar de 1982**: o vínculo efetivo entre o Estado e o Navio. Dissertação de Mestrado [Ciência Jurídica]. Santa Catarina: UNIVALI, 2009.

NAÍM, Moisés. **Ilícito:** o ataque da pirataria, da lavagem de dinheiro e o do tráfico à economia global. Rio de Janeiro: Ed. Jorge Zahar, 2006.

NCPC. **Cybercrimes.** National Crime Prevetion Council. EUA: Departamento de Justiça dos Estados Unidos, 2012.

NIELSEN, Wayne. **Submarine Telecoms Industry Report.** Issue 3. Submarine Telecoms Forum. Estados Unidos: Terabit Consulting, 2014.

NYE JR, Joseph S. **O Paradoxo do Poder Americano:** Por que a única superpotência do mundo não pode prosseguir isolada. São Paulo: Ed. UNESP, 2002.

_____. **O futuro do poder**. São Paulo: Benvirá, 2012.

NYST, Carly; CROWE, Anna. **Unmasking the Five Eyes' global surveillance practices.** Global Information Society Watch: Communications surveillance in the digital age. South Africa: GISWatch, 2014.

O'NEILL, Jim. **Building Better Global Economics BRICs**. Global Economics Paper No 66. New York: Goldman Sachs, 2001.

OBAMA diz entender preocupações do Brasil sobre espionagem. **Terra Notícias**. São Paulo, set. 2013. Seção de Política. Disponível em <http://noticias.terra.com.br/brasil/politica/obama-diz-entender-preocupacoes-do-brasil-sobre-espionagem,8e48489e9a3f0410VgnCLD2000000dc6eb0aRCRD.html>. Acesso em: 10 jul. 2015.

OLIVEIRA, João Roberto de. Sistema de Segurança e Defesa Cibernética Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional. In*:* BARROS, Otávio Santana Rêgo (Org.). **Desafios estratégicos para segurança e defesa cibernética.** Brasília: Secretária de Assunto Estratégicos da Presidência da República, 2011.

ONU. **Convenção das Nações Unidas sobre Direito do Mar.** Jamaica: ONU, 1982.

_____. **Resolution 69/166**: the right to privacy in the digital age. 69a General Assembly. New York: General Assembly, 2014a.

ONU aprova resolução proposta por Brasil e Alemanha sobre privacidade on-line. **O Globo.** Rio de Janeiro, nov. 2014. Disponível em

<http://oglobo.globo.com/sociedade/tecnologia/onu-aprova-resolucao-proposta-por-brasil-alemanha-sobre-privacidade-on-line-14678862> Acesso em 22 ago. 2015.

OOKLA. Value Index by Country. **Net Index.** Washington: Ookla, 2015. Disponível em <http://www.netindex.com/value/allcountries/> Acesso em: 17 jul. 2015.

_____. Global Download Speed. **Net Index.** Washington: Ookla, 2015a. Disponível em <http://www.netindex.com/download/map> Acesso em: 17 jul. 2015.

OPPERMANN, Daniel. **A nova abordagem do Google na China:** um furo no grande *Firewall?* Meridiano 47, n. 115. Brasília: IBRI, 2010.

PNUD. **Relatório do Desenvolvimento Humano**: Ascensão do Sul. Portugal: Camões Instituto da Cooperação e da Língua, 2013.

_____. **Human Development Report 2000.** New York: Oxford University Press, 2000.

PUTNAM, Robert D. **Diplomacy and Domestic Politics:** The Logic of Two-Level Games. International Organization, Vol. 42, No. 3. Massachusetts: MIT Press, 1988.

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

REALE, Miguel. **Filosofia do Direito**. 19ª ed. São Paulo: Ed. Saraiva, 2002.

REZEK, José Francisco. **Direito Internacional Público:** curso elementar. 13a Ed. rev. São Paulo: Saraiva, 2011.

RIBEIRO, Sérgio Luís. Estratégia de Proteção da Infraestrutura Crítica de Informação e Defesa Cibernética Nacional. In: BARROS, Otávio Santana Rêgo (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretária de Assunto Estratégicos da Presidência da República, 2011.

RICUPERO, Rubens. **A Revolução Russa e o Sistema Internacional.** Revista Lua Nova, nº 75. São Paulo: CEDEC, 2008.

ROCA, Z.; OLIVEIRA, J.A.; LEITÃO, N. **Desenvolvimento territorial entre a topofilia e a terrafilia:** das palavras aos actos. Lisboa: TERCUD, 2006.

ROHR, Altieres. Governo da Irlanda apoia Microsoft contra ceder dados de e-mail aos EUA. **G1**. São Paulo, dez. 2014. Seção Tecnologia e Games. Disponível em <http://g1.globo.com/tecnologia/noticia/2014/12/governo-da-irlanda-apoia-microsoft-contra-ceder-dados-de-e-mail-aos-eua.html> Acesso em 19 ago. 2015.

ROUSSEAU, Jean-Jacques. **O Contrato Social.** São Paulo: Martins Fontes, 1996

RSF. List of The 13 Internet Enemies. **Reporters Without Borders.** França, 07 nov. 2006. Disponível em: <http://en.rsf.org/list-of-the-13-internet-enemies-07-11-2006,19603> Acesso em: 16 jul. 2015.

SACK, Robert. **Human Territoriality:** its theory and history. Cambridge: Cambridge University Press, 1986.

SAINT-EXUPÉRY, Antoine de. **O Pequeno Príncipe.** Rio de Janeiro: Ed. Agir, 1999.

SANTOS, Milton. **Por uma Geografia Nova**. 3a ed. São Paulo: Ed. Hucitec, 1986.

SCHECHNER, Sam; POP, Valentina. Personal Data Gets Day in Court. **The Wall Street Journal.** Estados Unidos, mar. 2015. Seção Tech. Disponível em <http://www.wsj.com/articles/court-hears-challenge-to-safe-harbor-data-deal-1427206554> Acesso em 13 ago. 2015.

SIMPSONS, Aaron P. The Future of Safe Harbor. In: JAY, Rosemary P. **Data Protection & Privacy**. Estados Unidos: Hunton & Williams, 2015.

SJR. **Jornal Search:** cyber. Espanha: SCImago, 2015. Disponível em: <http://www.scimagojr.com/journalsearch.php?q=cyber&tip=jou>. Acesso em 23 jul. 2015.

SOBREIRA, Paulo Henrique Azevedo. **Cosmografia Geográfica: a Astronomia no Ensino de Geografia.** Tese [Doutorado em Geografia Física]. São Paulo: USP, 2005.

SOFAER, Abraham D. GOODMAN, Seymour E. **The Transnational Dimension of Cyber Crime and Terrorism.** Hoover Institute. California: Universidade de Stanford, 2001.

STATISTA. **Leading social networks worldwide as of March 2015, ranked by number of active users (in millions).** New York: Statista Inc, 2015. Disponível: <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>. Acesso em: 20 jul. 2015.

STRANGE, Suzan. **The Retreat of the State:** the diffusion of power in the World Economy. Reino Unido: University Press, 1996.

TOCQUEVILLE, Alexis de. **A democracia na América:** leis e costumes de certas leis e certos costumes políticos que foram naturalmente sugeridos aos americanos por seu estado social democrático. São Paulo: Martins Fontes, 2005.

VARELLA, Marcelo D. **Direito Internacional Público**. 4a Ed. São Paulo: Ed. Saraiva, 2012.

VENTRE, Daniel. Ciberguerra**.** In: ACADEMIA GENERAL MILITAR. **Seguridad global y potências emergentes em um mundo multipolar.** XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza, 2011.

VIDAL, Lívia Ferreira; SANTOS, Rafael Teixeira. **DEEP WEB:** como acessar e porque não acessar. Anais da II Simpósio de Pesquisa e de Práticas Pedagógicos. Nova Iguaçu: UGB, 2014.

W3COUNTER. **Web Browser Market Share Trends.** Pennsylvania: Awio Web Service, 2015. Disponível em: <http://www.w3counter.com/trends>. Acesso em: 19 jul. 2015.

_____. **Global Market Share.** Pennsylvania: Awio Web Service, 2015a. Disponível em: <http://www.w3counter.com/globalstats.php>. Acesso em: 20 jul. 2015.

Wikileaks: US 'spied on Japan government and companies'. **BBC News**. United King, jul. 2015. Seção Asia. Disponível em <http://www.bbc.com/news/world-asia-33730758> Acesso em: 12 ago. 2015.

WORLD BANK. Internet users (per 100 people)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015. Disponível em: <http://data.worldbank.org/indicator/IT.NET.USER.P2>. Acesso em: 15 jul. 2015.

_____. Total Population (in number of people)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015a. Disponível em: <http://data.worldbank.org/indicator/SP.POP.TOTL>. Acesso em: 15 jul. 2015.

_____. GDP per capita (current US$)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015b. Disponível em: <http://data.worldbank.org/indicator/NY.GDP.PCAP.CD?order=wbapi_data_value_2013+wbapi_data_value&sort=asc>. Acesso em: 16 jul. 2015.

_____. Charges for the use of intellectual property, payments (BoP, current US$)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015c. Disponível em: < http://data.worldbank.org/indicator/BM.GSR.ROYL.CD/countries>. Acesso em: 21 jul. 2015.

_____. Charges for the use of intellectual property, receipts (BoP, current US$)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015d. Disponível em: <http://data.worldbank.org/indicator/BX.GSR.ROYL.CD/countries>. Acesso em: 21 jul. 2015.

_____. Research and development expenditure (% of GDP)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015e. Disponível em: <http://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS/countries>. Acesso em: 21 jul. 2015.

_____. High-technology exports (% of manufactured exports)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015f. Disponível em: <http://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS/countries>. Acesso em: 21 jul. 2015.

_____. GDP (current US$)**. Banco de dados dos Indicadores de Desenvolvimento Mundial.** Washington: World Bank, 2015g. Disponível em: <http://data.worldbank.org/indicator/NY.GDP.MKTP.CD?page=3>. Acesso em: 31 jul. 2015.

YOUNG, Oran R. **Regime Dynamics:** the Rise and Fall of International Regimes. International Organization, Vol. 36, No. 2. Massachusetts: MIT Press, 1982.

ZAKARIA, Fareed. **O mundo pós-americano.** São Paulo: Companhia das Letras, 2008.

ZUCCARO, Paulo Martino. Tendência Global em Segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. In: BARROS, Otávio Santana Rêgo (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretária de Assunto Estratégicos da Presidência da República, 2011.