ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES

Felipe Hansen Polesi

A EXISTÊNCIA DAS FRONTEIRAS CIBERNÉTICAS E SUA SEGURANÇA NO ÂMBITO NACIONAL

Resende
2020

A EXISTÊNCIA DAS FRONTEIRAS CIBERNÉTICAS E SUA SEGURANÇA NO ÂMBITO NACIONAL

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Orientador: Major Walfredo Bento Ferreira Neto

Resende
2020

	APÊNDICE III (TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL) AO ANEXO B (NITCC) ÀS DIRETRIZES PARA A GOVERNANÇA DA PESQUISA ACADÊMICA E DA DOUTRINA NA AMAN	**AMAN 2020**

TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL

TÍTULO DO TRABALHO: A EXISTÊNCIA DAS FRONTEIRAS CIBERNÉTICAS E SUA SEGURANÇA NO ÂMBITO NACIONAL
AUTOR: FELIPE HANSEN POLESI

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

Autorizo a Academia Militar das Agulhas Negras - AMAN a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como a divulgá-lo por publicação em revista técnica da Escola ou outro veículo de comunicação do Exército. A Academia Militar das Agulhas Negras poderá fornecer cópia do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos dos mesmos, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com a autorização do autor ou da Direção de Ensino da Academia Militar das Agulhas Negras

Resende, 26 de Outubro de 2020.

_____

Cad Felipe Hansen Polesi

Felipe Hansen Polesi

A EXISTÊNCIA DAS FRONTEIRAS CIBERNÉTICAS E SUA SEGURANÇA NO ÂMBITO NACIONAL

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Aprovado em____de_____de 2020

Banca examinadora:

_____
Walfredo Bento Ferreira Neto, Major
orientador

_____
Claudio Magni Rodrigues, Cel PTTC

_____
Antônio Fernando Pires Patury Júnior, TC

Resende
2020

Dedico este trabalho a Deus, por ter me dado forças e a capacidade necessária para que pudesse realizar meus sonhos e assim continuar conquistando mais do que posso almejar; ao meu falecido pai, por ter me apoiado desde sempre e ter me instigado a conhecer e me interessar pelo assunto relacionado a cibernética, assim como eu ele era fascinado pelos horizontes e ilimitáveis expansões que a cibernética pode alcançar; à minha mãe e irmãos que me ajudaram na difícil situação da maior perda de nossas vidas e seguem me apoiando nas minhas difíceis decisões ao longo de minha carreira; e à minha esposa que sempre me apoiou em minhas decisões me acompanhando desde a época de cursinho e hoje é minha companheira para vida toda.

AGRADECIMENTOS

Agradeço a todos que me apoiaram e me auxiliaram na confecção deste trabalho, ainda que não o tenham feito diretamente, porém sempre me mostrando que tudo era possível na medida em que as coisas se encaixam e se completam. Agradeço em especial minha esposa que no tocante apoio não deixou faltar nada, como também na moral, fazendo com que eu não desanimasse de fazer todo dia um pouco do trabalho, e também mostrando o quanto esse trabalho era importante para minha carreira como futuro oficial da arma de comunicações do Exército Brasileiro.

Destaco também um agradecimento especial ao meu orientador que esteve sempre cobrando retornos sobre o trabalho, assim como sempre animado com os assuntos de seus alunos orientados, mostrando sempre entusiasmo e extrema capacidade intelectual para auxiliar e guiar-me para o sucesso, cabe ressaltar que muitas de suas obras foram essenciais para o êxito do término deste trabalho.

RESUMO

A EXISTÊNCIA DAS FRONTEIRAS CIBERNÉTICAS E SUA SEGURANÇA NO ÂMBITO NACIONAL

AUTOR: Cadete Felipe Hansen Polesi
ORIENTADOR: Major Walfredo Bento Ferreira Neto

As fronteiras cada vez mais interligadas através de avanços tecnológicos e de meios de comunicações implicam em uma maior preocupação com sua segurança de utilização. A geopolítica está intrinsecamente relacionada com a cibernética, com suas fronteiras ciberespaciais, o ciberespaço é físico sim e não está apenas no mundo virtual ou no mundo intangível que muitos pensam ser. A internet vem ganhando espaço no mundo atual e com isso suas fronteiras estão cada vez maiores e até por vezes pensamos em uma espécie de sobreposição do ciberespaço sobre os demais domínios já existentes no contemporâneo, assim como sua utilização para o meio militar, como também muito utilizado no meio civil. A importância de conhecermos nossas conexões do Brasil com o resto do mundo, fisicamente falando, através de seus *backbones*, espinha dorsal dos fluxos de informações que transcorrem e interligam os diversos Estados, por meio de cabos de fibra ótica submarinos que partem do Brasil e rumam ao exterior, assim como conhecer os fluxos de informações que trafegam no território nacional e seu gerenciamento, através de ferramentas do governo. As principais dificuldades na história brasileira de inserção nesse mundo virtual, com muitos obstáculos encontrados pelo caminho e sua necessidade de maiores investimentos para o desenvolvimento das tecnologias de comunicações e o novo conceito da cibernética. Assim reconhecer a existência das fronteiras cibernéticas, apresentando o aparecimento de falhas e vulnerabilidades ao longo dos tempos com seu constante desenvolvimento, através da utilização maldosa de alguns usuários, que aproveitaram desse "nascimento" de uma nova era da informação, em que, vários países ainda estavam "engatinhando" rumo ao seu desenvolvimento. Dessa forma esses *hackers* usufruíram da internet como meio de se beneficiarem, ou até mesmo por simples prazer de aterrorizar a vida de outros usuários comuns, e com isso extraindo e furtando dados importantíssimos para algumas pessoas e solicitando preços altíssimos pelo resgate de seus ativos. Entretanto com seu constante desenvolvimento e suas inúmeras falhas encontradas, acabou por gerar nos Estados um sentimento de necessidade de uma infraestrutura cibernética bem protegida, com o objetivo de mitigar ou até mesmo anular as tentativas de ataques e invasões. Temos com isso a ativa participação de nossas Forças Armadas para contenção desses cibercriminosos, dando ênfase no Exército Brasileiro, principal responsável pela Defesa e Proteção Cibernética da Nação.

Palavras-chave: Fronteiras. Ciberespaço. Vulnerabilidades. Defesa. Proteção Cibernética.

ABSTRACT

THE EXISTENCE OF CYBER BORDERS AND THEIR SECUITY AT THE NATIONAL LEVEL

AUTHOR: Cadete Felipe Hansen Polesi
ADVISOR: Major Walfredo Bento Ferreira Neto

Borders which are increasingly interlinked through technological advances and communications media imply an increased concern for their security of use. Geopolitics is intrinsically related to cybernetics, to its cyberspace borders, cyberspace is physical yes and it is not only in the virtual world or the intangible world that many think it is. The Internet has been gaining space in today's world and with that its frontiers are getting bigger and bigger and sometimes we even think about a kind of overlapping of cyberspace over the other domains already existing in the contemporary, as well as its use for the military, as well as widely used in the civil environment. The importance of knowing our connections between Brazil and the rest of the world, physically speaking, through its backbones, the backbone of the flows of information that flow and interconnect the various states, through submarine fiber optic cables that depart from Brazil and head abroad, as well as knowing the flows of information that travel in the national territory and its management, through government tools. The main difficulties in the Brazilian history of insertion in this virtual world, with many obstacles encountered along the way and its need for greater investments for the development of communications technologies and the new concept of cybernetics. Thus, recognizing the existence of cybernetic borders, presenting the appearance of flaws and vulnerabilities over time with its constant development, through the malicious use of some users, who took advantage of this "birth" of a new era of information, in which several countries were still "crawling" towards its development. In this way, these Hackers enjoyed the Internet as a means of benefiting themselves, or even for the simple pleasure of terrorizing the lives of other common users, and with this extracting and stealing very important data for some people and asking very high prices for the rescue of their assets. However, with its constant development and its countless failures, it has ended up generating in the states a feeling of need for a well-protected cyber infrastructure, with the objective of mitigating or even nullifying the attempts of attacks and invasions. We have with this the active participation of our Armed Forces to contain these cybercriminals, with emphasis on the Brazilian Army, which is mainly responsible for the Cyber Defense and Protection of the Nation.

Keywords: Borders. Cyberspace. Vulnerabilities. Defense. Cyber Protection.

LISTA DE TABELAS

Tabela 1 - Espaço cibernético - "capas" e respectiva composição.....15
Tabela 2 - Enquadramento dos pleitos de FDT pela aplicação (1987 a 1994).....26
Tabela 3 - Fronteiras jurídicas e Fronteiras metafísicas.....29
Tabela 4 - Ações cibernéticas nos níveis de decisão.....34

LISTA DE GRÁFICOS

Gráficos 1 – Curva de incidentes reportados em valor absoluto (1999 – 2017).....33
Gráficos 2 – Curva de incidentes com origem no Brasil em valor absoluto (2004 – 2017).....33

LISTA DE FIGURAS

Figura 1 – Transversalidade do domínio cibernético.....16
Figura 2 – Pares de ligações backbones no Brasil – 2008.....17
Figura 3 – Mapa do backbone internacional que interliga o Brasil a vários países.....18
Figura 4 – Cabos submarinos de fibra ótica.....22
Figura 5 – Mapa global de Tráfego de informações.....23
Figura 6 – Estrutura do Portfólio do Exército Brasileiro.....34

LISTA DE ABREVIATURAS E SIGLAS

GERN	Grupo Europeu de Pesquisa de Normas
SDH	Hierarquia Digital Síncrona
Gbps	Gigabits por segundo
Tbps	Terabits por segundo
DWDM	Multiplexação Densa por Divisão de comprimento de onda
SAC	South American Crossing
TI	Tecnologia da Informação
FDT	Fluxo de Dados Transfronteiriços
CAPRE	Comissão de Coordenação das Atividades de Processamento de Dados
SEI	Secretaria Especial de Informática
CDCiber	Centro de Defesa Cibernética
ICI	Infraestrutura Crítica da Informação
ICN	Infraestrutura Críticas Nacionais
END	Estratégia Nacional de Defesa
MD	Ministério da Defesa
FIFA	Federação Internacional de Futebol Associação
CERT.br	Centro de Estudos, Respostas e tratamento de incidentes de Segurança no Brasil
DdoS	Negaçao Distribuida de Serviço
ICANN	*Internet Corporation for Assigned Names and Numbers* (Corporação da Internet para Atribuição de Nomes e Números)

SUMÁRIO

1 INTRODUÇÃO.....12
1.1 OBJETIVOS.....13
1.1.1 Objetivo geral.....13
1.1.2 Objetivos específicos.....13
1.2 GUIA AO DOCUMENTO.....13
2 REFERENCIAL TEÓRICO.....14
2.1 O CIBERESPAÇO COMO ESPAÇO DA GEOPOLÍTICA.....14
2.2 TOPOLOGIA DOS BACKBONES DE INTERNET NO BRASIL.....16
2.2.1 Americas II.....19
2.2.2 Atlantis 2.....19
2.2.3 Emergia - SAM 1.....19
2.2.4 *Global Crossing* – SAC.....20
2.2.5 Globenet/360 *Network*.....20
2.2.6 Unisur.....20
2.3 CONEXÕES MUNDIAIS.....21
2.4 TRATAMENTO DO FLUXO DE DADOS DAS FRONTEIRAS BRASILEIRAS.....24
2.4.1 Desafios enfrentados.....26
2.5 AS FRONTEIRAS CIBERNÉTICAS.....27
2.6 OS AVANÇOS DA CIBERNÉTICA.....29
2.7 PROTEGENDO NOSSAS FRONTEIRAS.....30
2.8 A ATUAÇÃO DO EXÉRCITO BRASILEIRO NA DEFESA CIBERNÉTICA.....32
3 REFERENCIAL METODOLÓGICO.....35
3.1 TIPO DE PESQUISA.....35
3.2 MÉTODOS.....35
3.2.1 Levantamento de dados.....35
3.2.2 Análise de dados.....35
4 CONSIDERAÇÕES FINAIS.....36
REFERÊNCIAS.....38
GLOSSÁRIO.....40

1 INTRODUÇÃO

Até onde podemos delimitar a internet? Poderíamos utilizar a internet sem nos preocuparmos com ataques e invasões? Existe um meio de navegação e comunicação 100% seguro? São dúvidas constantes que a cibernética e a tecnologia buscam responder.

Os conflitos na atualidade dos exércitos não mais ocorrem apenas no ambiente terrestre, mas também no ciberespaço, onde podemos observar que através das constantes evoluções tecnológicas e dos avanços informacionais crescem um aumento significativo das precauções e dos cuidados com a utilização deste meio. Meio este que revolucionou as comunicações por todo o mundo, em razão de sua facilidade de acesso e velocidade de trâmite de informações. Entretanto a medida em que se desenvolvem e modificam as capacidades de transmissão de dados como a inovação de sistemas computacionais altamente velozes, o aumento da velocidade em que os dados trafegam pela rede, e o alargamento de bandas de transmissão, há o surgimento constante de vulnerabilidades e falhas que muitas vezes passam despercebidos pelos usuários.

Essas vulnerabilidades consistem em “brechas” ou “aberturas” na rede de dados, podendo ser uma simples falha no seu código-fonte, ou até mesmo erros de configuração. São pontos de riscos críticos para a segurança de empresas ou até mesmo hospitais, que utilizam de softwares e hardwares para gerenciar seu banco de documentos e registros de importantes pacientes. Com isso cresce a necessidade dessas empresas utilizarem medidas de segurança para evitar ou combater ataques de cibercriminosos, que buscam informações de alto valores para se beneficiarem através da solicitação de resgate por documentos criptografados ou até mesmo a venda dessas informações para o mercado negro.

A fronteira cibernética diferentemente da fronteira física, vai além das dimensões territoriais de cada país. Através da internet podemos acessar servidores que muitas vezes estarão a quilômetros de distância, até mesmo em outro continente. Devido a esta expansão no ciberespaço, as fronteiras de cada país estão cada vez mais interligadas e com isso se dá a preocupação com a segurança e delimitação de suas fronteiras ciberespaciais, buscando cada vez mais redes restritas e com o máximo de segurança possível.

Assim busca-se ao final deste estudo, responder às perguntas evidenciadas acima com o intuito de obter conhecimento acerca de nossas fronteiras cibernéticas, através de pesquisas, fatos e importantes informações que mapearão e iluminarão a ainda obscura compreensão sobre o assunto.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Buscar a compreensão sobre a existência das fronteiras cibernéticas, assim como os fluxos de informações que tramitam ao redor do globo. E conhecer algumas estratégias que vêm sendo tomadas para que se busque alcançar um sistema de proteção cibernética com eficiência, visando sua segurança no âmbito nacional.

1.1.2 Objetivos específicos

Analisar e compreender o ciberespaço inserido atualmente como meio de estudo para a Geopolítica.

Mapear as principais redes e conexões que dão acesso e interligam o Brasil com o restante do mundo espectro cibernético.

Apresentar o fluxo de dados e informações que transcorrem por todo o globo e as conexões mundiais.

Tratar e compreender o fluxo de dados em nossas fronteiras e apresentar as dificuldades encontradas.

Compreender a existência das fronteiras cibernéticas e apresentar os meios de defesa empregados, assim como os principais atores participantes.

1.2 GUIA AO DOCUMENTO

Este trabalho está dividido em 4 capítulos, que estão organizados conforme apresentado: O segundo capítulo apresenta o referencial teórico, que aborda assuntos relacionados ao ciberespaço como espaço da Geopolítica, estrutura física da internet e conhecimentos sobre a utilização e segurança cibernética, assim como a atuação do Exército Brasileiro no sistema de Defesa Cibernética.

O terceiro capítulo recai sobre o referencial metodológico, explicando o tipo de pesquisa, os métodos utilizados e análise de dados sobre a pesquisa.

O quarto capítulo refere-se às considerações finais, onde encerro as ideias contidas no trabalho e dessa forma atingindo uma conclusão coerente com o tema abordado.

2 REFERENCIAL TEÓRICO

2.1 O CIBERESPAÇO COMO ESPAÇO DA GEOPOLÍTICA

Através do vertiginoso crescimento e expansão da internet por todo o mundo houve a necessidade da criação de um novo espaço: o ciberespaço. O qual diariamente vem se expandindo cada vez mais, com a inserção de novos usuários em razão da facilidade e da disponibilidade que esses usuários possuem, com a agregação de novas tecnologias, como a internet das coisas, assim como a digitalização de serviços e a geração de dados em volumes impensáveis, conhecido como Big Data (MALAGUTTI, 2017).

O ciberespaço trouxe uma percepção de liberdade e proximidade espacial e temporal anteriormente não experimentados. Com a utilização de um simples computador conectado à rede da internet podemos deslumbrar de locais que por vezes jamais poderíamos visitar, como museus, bibliotecas internacionais, igrejas históricas, até mesmo locais de difícil acesso. Assim como sua utilização possibilita realizar compras de eletrônicos de lugares demasiadamente distantes, como um relógio chinês ou um celular japonês (MALAGUTTI, 2017).

O ciberespaço corresponde a um espaço de comunicação aberto pela interconexão de computadores e das memórias dos computadores, incluindo os sistemas de comunicação tanto por meio de ondas *hertz* quanto pela telefonia clássica, a partir do momento em que essas participarem do processo de transmissão de informações digitalizadas (LÉVY, 1999 *apud* FERREIRA NETO, 2014). Desta forma o ciberespaço não se trata de algo impossível de se compreender e nem de algo em que as pessoas não consigam estar em constante participação.

Segundo as declarações da independência do Ciberespaço (BERLOW, 1996):

> O ciberespaço consiste em transações, relacionamentos e o próprio pensamento, dispostos como uma onda permanente na rede de nossas comunicações. O nosso é um mundo que está em toda parte e em lugar nenhum, mas não é onde os corpos vivem.
> Estamos criando um mundo no qual todos possam entrar sem privilégios ou preconceitos concedidos por raça, poder econômico, força militar ou estação de nascimento.
> Estamos criando um mundo onde qualquer pessoa, em qualquer lugar, possa expressar suas crenças, não importa quão singular, sem medo de ser coagida ao silêncio ou à conformidade. (BERLOW, 1996)

De forma geral o ciberespaço não somente se trata da parte lógica e intangível do meio, mas também é compreendido pelas pessoas que a utilizam, as empresas e todos equipamentos que estejam conectadas a rede e que de alguma forma sejam agentes ativos dentro do tráfego de informações (MANDARINO JÚNIOR, 2011 *apud* FERREIRA NETO, 2014). Hoje o ciberespaço está em toda parte, em todo lugar em que encontramos um computador, um processador, ou um cabo de ligação (CLARKE; KNAKE, 2010 *apud* FERREIRA NETO, 2014).

> Quando se fala em ciberespaço é comum pensar em algo que não nos é palpável, imaterial, um lugar distante de nossa realidade, onde relações sociais, culturais, econômicas ao se estabelecerem se fazem no imaginário, "algo de outro mundo", um ambiente futurístico, um divertido desenho animado dos Jetsons. Essa é uma visão idealista do tempo e do espaço. Algumas tentativas de explicar o ciberespaço esbarram numa postura idealista, com todos os seus matizes, ou seja, procuram negar a realidade objetiva do espaço como forma de existência da matéria. (DA SILVA; TANCMAN, 2009, p. 57)

A abrangência do ciberespaço possibilita uma comparação das redes e máquinas como partes do hardware; informações, como dados e mídia; o cognitivo, como o processo mental das pessoas; e o virtual, no qual as pessoas se conectam socialmente (REVERON, 2012 *apud* FERREIRA NETO, 2014).

Tabela 1 – Espaço cibernético – "capas" e respectiva composição

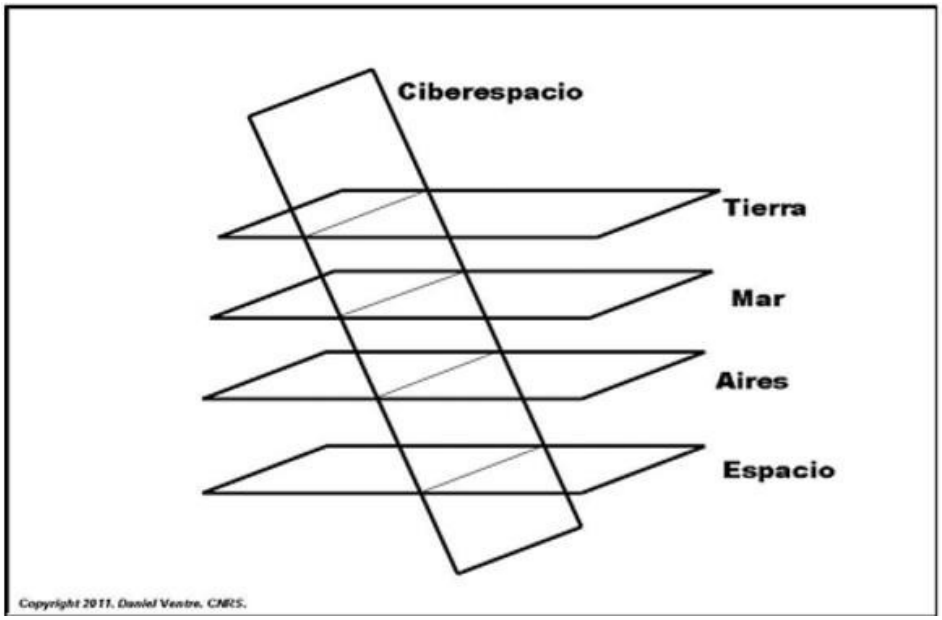
"CAPA"	COMPONENTES
Inferior	- física, material, condizente com a infraestrutura (hardware, redes,...)
Intermediária	- softwares de aplicações
Superior	- cognitiva

Fonte: VENTRE, (2012) apud FERREIRA NETO, (2014)

A figura acima mostra que segundo a visão de alguns especialistas e de Daniel Ventre, pesquisador do Centro de Investigações Científicas e secretário geral do Grupo Europeu de Pesquisa de Normas (GERN), divide o ciberespaço em três partes simples de serem compreendidas, o *Hardware* como parte física ou rígida do sistema; o *Software* como parte aplicável, a programação propriamente dita; e o *peopleware* como a parte cognitiva das pessoas que estão inseridas nesse meio.

Um conceito muito abrangido pelos pesquisadores se trata da transversalidade do ciberespaço, que se trata da projeção de poder que o ciberespaço incide sobre os outros domínios.

Figura 1 – Transversalidade do domínio cibernético



Fonte: VENTRE, (2012) *apud* FERREIRA NETO, (2014)

Através da figura podemos notar o imenso impacto que esse espaço vem tomando conta, e se apresentando cada vez mais efetivo para diferentes ações. Dessa forma o ciberespaço é constantemente utilizado em atividades militares e até mesmo atividades civis em que necessitam do controle de tráfegos aéreos e também terrestre. Hoje "ciber" constitui-se um quinto domínio operacional militar, depois de terra, mar, ar e espaço (US JCS, 2013 *apud* MALAGUTTI, 2017).

2.2 TOPOLOGIA DOS BACKBONES DE INTERNET NO BRASIL

A realidade da internet não somente está atrelada ao fato de conseguirmos nos comunicar com pessoas há vários quilômetros de distância e nos usarmos do anonimato nas redes sociais, pensando estarmos totalmente imersos em um mundo virtual que seria impossível de ser alcançado.

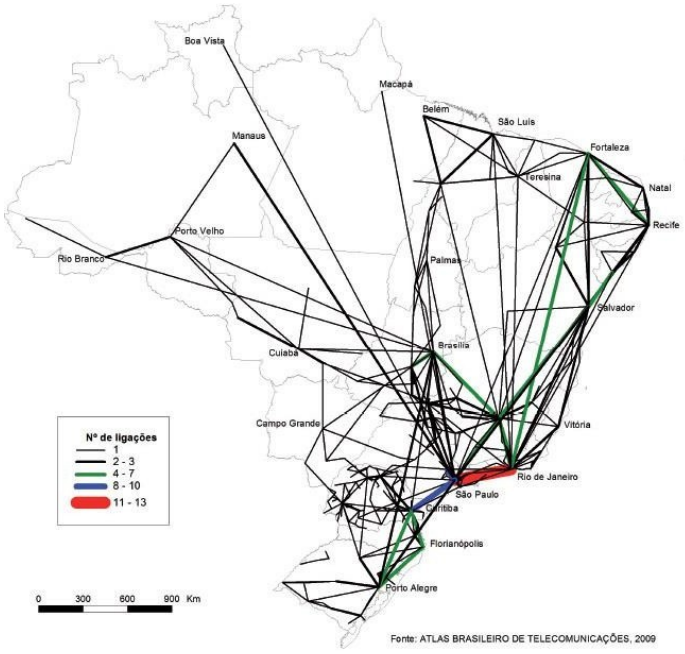
> A Internet, à primeira vista, não parece ser um caso de estudo para o geógrafo. O chamado ciberespaço, noção que é frequentemente tomada como sinônimo da própria internet, é um campo puramente imaterial, na realidade uma metáfora do próprio espaço. (MOTTA, 2012)

Quando perguntamos para alguém se ela é capaz de identificar e entender por onde e como a internet chega em suas casas, no trabalho ou até mesmo no celular, a maioria das

respostas é de que vem pelo roteador de sua casa ou pelo sinal de celular, porém nem todos sabem ou conhecem os *backbones* e o tráfego de dados que circulam pelo mundo através de cabos de fibra ótica e linhas de alta capacidades que interligam a internet mundial à rede urbana brasileira.

Os *backbones* são a espinha dorsal da internet, como seu próprio nome sugere, ou seja, ela subdivide a internet em várias outras redes menores, para que essas redes locais possam se comunicar com servidores externos. Com isso podemos identificar que se não fosse pelos *backbones* muitas pessoas talvez não iriam conseguir ter acesso a servidores externos e serviços como sites que estão presentes apenas em outros países. Logo, quando enviamos uma mensagem através de uma rede, utilizando um serviço local, essas informações são encaminhadas às centrais telefônicas ou a qual fornece o serviço de dados de internet para seus clientes, assim encaminhadas à altas velocidades pelos *backbones* chegando ao seu destino final. Dessa forma é notável entender como a internet possui fronteiras e como o ciberespaço é mais físico do que imaginávamos (BERTOLOTO, 2012).

Figura 2 – Pares de ligações backbones no Brasil – 2008



Fonte: ATLAS BRASILEIRO DE TELECOMUNICAÇÕES, 2009 *apud* MOTTA (2012)

A figura nos mostra o caminho em que estão inseridos os *backbones* nacionais brasileiros, e sua concentração em regiões que apresentam maior densidade demográfica, assim

como regiões que possuem maior condições financeiras de prover os meios necessários para que se efetive suas conexões.

Podemos observar também que essas conexões se espalham pelo Brasil e buscam alcançar os extremos do país, mais especificamente próximos do litoral e mais ao Sul nas principais fronteiras terrestres, restando algumas ao Norte que ainda estão em projetos de expansão. Essas linhas de conexões compõe os *backbones* de internet brasileiros, que resumidamente são cabos de fibras óticas que por sua vez serão responsáveis por comunicar o país com o restante do mundo.

As principais conexões de fibra ótica do Brasil se ligam com a Argentina. Desta forma possibilitando acessar os dados de servidores na Europa ou dos EUA, a maior parte dos cabos que partem do Brasil passam pela região do Caribe. Há também uma rede que interliga o Brasil à África, cabos que partem da região do estado do Rio Grande do Norte com destino às ilhas de Cabo Verde, que por sua vez se liga com Senegal e por fim de Senegal para Portugal (BERTOLOTO, 2012).

Abaixo podemos observar as conexões que partem do Brasil e rumam ao exterior:

Figura 3 – Mapa do backbone internacional que interliga o Brasil a vários países.

Fonte:http://www.portaladsl.com.br/modules.php?name=Forums&file=viewtopic&t=9535 (*apud* BERTOLOTO, 2012)

Com isso confirmamos que o Brasil está conectado com o restante do mundo através de redes de fibra ótica, que reafirmam o fato de nossas conexões serem físicas e dessa forma os limites das fronteiras cibernéticas. Podemos também elencar os principais ramos que partem do Brasil para o exterior e explanar sucintamente sobre cada um:

2.2.1 Americas II

De acordo com Bertoloto (2012), o AMERICAS II Liga o Brasil aos Estados Unidos, sendo produto de um consórcio formado por várias empresas de telecomunicações internacionais, como: Embratel, WorldCom, Sprint, CANTV e outras. Trabalhando com uma tecnologia SDH (Hierarquia Digital Síncrona), permitindo que o sinal seja enviado e recebido com sincronia. Sua extensão atinge os 9.000 Km de extensão, sua utilização de quatro pares de fibras óticas lhe dá uma capacidade de 80 Gbps. Possuindo também uma capacidade de transmitir aproximadamente 151.200 ligações ao mesmo tempo (BERTOLOTO, 2012).

2.2.2 Atlantis 2

Com cerca de 12.000 Km de extensão tem por finalidade conectar o Brasil à Europa, África e países da América do Sul. Com uma demanda de aproximadamente US$ 370 milhões com setenta por cento de empreendimento feito pelas seguintes operadoras: Embratel, Deutsche Telecom, Telecom Itália, *STET-France* Telecom e Telefônica de Espanha. Sua capacidade de transmissão podendo variar de 20 Gbps até aproximadamente 40 Gbps (BERTOLOTO, 2012).

> Através do cabo submarino *Atlantis 2*, o Brasil, até a presente pesquisa, participa da rede digital que conecta os cinco continentes e que será composta pela interligação de
> 73 grandes sistemas de cabos de fibras óticas, totalizando uma extensão de aproximadamente 385 mil quilômetros de cabos ópticos do sistema mundial de comunicações. (BERTOLOTO, 2012)

2.2.3 Emergia - SAM 1

Entrando em operação em fevereiro de 2001 e instalado pela Telefônica S.A (Empresa Espanhola de Telecomunicações) este tronco submarino possui aproximadamente seus 25 mil quilômetros de extensão, possuindo quatro pares de fibras óticas e 48 portadoras em cada par de fibras, com isso lhe garantindo uma capacidade de transmissão de aproximadamente 1,92 Tbps, ligando todo o continente Americano (BERTOLOTO, 2012).

Bertoloto (2012) afirma também que o SAM 1 é um anel óptico que circunda as Américas através do Atlântico e do Pacífico, sendo assim o SAM 1 é auto restaurável, dando-lhe maior qualidade e segurança das informações entre os países conectados. E devido a sua utilização da tecnologia DWDM (*Dense Wavelength Division Multiplexer*), pode restaurar o circuito sempre que haja alguma interrupção, fazendo com o que a informação percorra o caminho contrário e consiga chegar em seu destino. Dessa forma ele basicamente consegue reagir a possíveis falhas em menos de 300 milissegundos, sem perder sua transmissão (BERTOLOTO, 2012).

2.2.4 *Global Crossing* – SAC

Sendo um anel óptico auto restaurável assim como o SAM 1, este tronco concede ao sistema um serviço de alta velocidade com qualidade e segurança, custando aproximadamente 2 bilhões de dólares e possuindo cerca de 15 mil quilômetros de extensão, interliga Brasil, Argentina, Chile, Peru, Panamá e Estados Unidos. Possuindo uma capacidade de transmissão final de 1,28 Tbps (BERTOLOTO, 2012).

2.2.5 Globenet/360 Network

Possuindo cerca de 22,5 mil quilômetros de extensão e 303 estações repetidoras o anel óptico da *Globenet* diferentemente do SAM 1 e do *Global Crossing*, circunda o Atlântico, com isso interconectando Estados Unidos, às Ilhas Bermudas, à Venezuela e ao Brasil. Sua capacidade final de transmissão será de 1,36 Tbps (BERTOLOTO, 2012).

2.2.6 Unisur

Este tronco tem por finalidade interligar os países do Mercosul: Argentina (*La Plata)*, o Brasil (Florianópolis) e o Uruguai (*Maldonado)*, constituído de um cabo de aproximadamente 1.741 quilômetros extensão, 10 estações repetidoras e 15.120 canais para seu tráfego (BERTOLOTO, 2012).

2.3 CONEXÕES MUNDIAIS

O Mundo está em constante evolução ao que se refere as comunicações e o intenso tráfego de informações que transcorre por todo o globo. O Brasil não ficou para trás e também buscou com seus meios de telecomunicações e com o auxílio de algumas empresas de telefonia participar deste imenso e vasto fluxo de dados.

Pudemos observar anteriormente como o Brasil está intrinsicamente ligado ao mundo através de seus troncos de fibras óticas, os *backbones*, de forma que crescentemente o país vem se desenvolvendo e se inserindo cada vez mais no *cyberspace*, termo cunhado por Willian Gibson (1984) em sua obra literária *Neuromancer*.

> Em 1995 mais de 95% do fluxo da internet no Brasil era internacional (usuários brasileiros se conectando com endereços estrangeiros), enquanto em 1997 mais de 40% do tráfico era doméstico, à medida que mais sites locais se tornaram disponíveis. (TIGRE, 1999, p. 88)

Segundo Tigre (1999), os países periféricos por possuírem uma infraestrutura física e social mais precária, se limitam no que se refere a difusão da internet pelo globo, com isso acabam ocupando o papel de simples importadores de serviços e dados informacionais. Tigre destaca dentre os periféricos, o Brasil por possuir elevada capacitação na informática adquirida anteriormente em meados dos anos 70 até os dias atuais (TIGRE, 1999).

De acordo com Afonso em sua obra, Internet no Brasil – alguns dos desafios a enfrentar, 2002, p. 170, os meios e caminhos para a Sociedade da informação são incertos, com isso cada país possui seu próprio caminho para se alcançar seu objetivo, porém a maior parte dos países sequer possuem condições básicas econômicas para chegar a definir um.

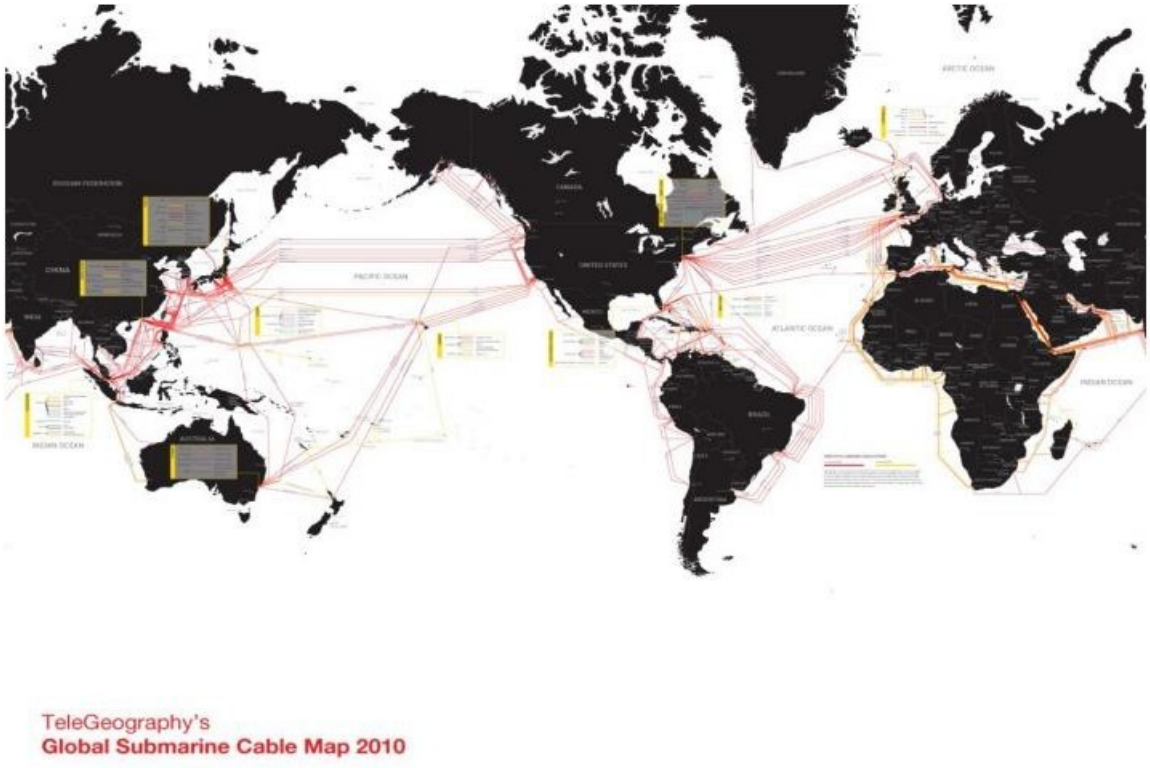
Dessa forma podemos compreender que os países mais desenvolvidos possuem elevada capacidade de oferecer melhores serviços e possuem melhores estruturas para proverem bandas com altas velocidades e de excelentes qualidades.

> ...as implicações do novo modelo de infra- estrutura estão apenas começando a serem entendidas na primeira década do século 21. Ao invés de estar isolada em casas e escritórios, a conectividade espalhou-se por árvores, parques, cafés e outros espaços urbanos, públicos de mediação digital recentes. Ao invés de trazer o usuário para a rede, pela primeira vez a rede está sendo levada ao usuário. (TOWNSEND, 2003 *apud* LEMOS, 2014)

De acordo com Afonso (2002), o esquema atual de endereçamento de internet, que permite um computador qualquer conectado à rede estabelecer um *link* com outro computador conectado à mesma rede através dos respectivos nomes de domínio, não permite realizar a troca

de dados e informações sem que antes faça contato com os servidores-raiz (atualmente controlados pela ICANN localizados nos Estados Unidos) (AFONSO, 2002).

Figura 4 - Cabos submarinos de fibra ótica



Fonte: TeleGeography's (*apud* BERTOLOTO, 2012)

O mapa (figura 4) acima nos mostra os *backbones* que estão espalhados pelo globo e suas respectivas interconexões com outros países, interligando continentes e com isso aumentando cada vez mais o tráfego e o fluxo de informações. Notamos uma certa concentração das conexões no hemisfério Norte, tendo como principal ator os Estados Unidos. Podemos observar também as principais ligações em que o Brasil participa dentro desta vasta e imensa malha de conexões.

Segundo os autores Bezerra (2014) e Waltz (2014), mesmo que a rede não possua sua centralidade bem definida, não caracteriza uma dispersão dos fluxos, visto que a maior parte do tráfego de dados da América Latina passa pelos Estados Unidos, o qual concentra grande parte da estrutura global de telecomunicações.

> Não estamos na era da informação. Não estamos na era da Internet. Nós estamos na era das conexões. Ser conectado está no cerne da nossa democracia e nossa economia. Quanto maior e melhor forem essas conexões, mais forte serão nossos governos, negócios, ciência, cultura, educação... (WEINBERGER, 2003 *apud* LEMOS, 2004)

A conectividade global nos proporciona uma rapidez e uma flexibilidade demasiadamente prática em nossas vidas. Com ela podemos nos comunicar com pessoas ou empresas que estão a quilômetros de distância, dessa forma a internet e seu vultuoso trâmite de informações facilitou a vida de muitas pessoas. Entretanto precisamos entender que junto dessas facilidades existem os riscos de sua utilização.

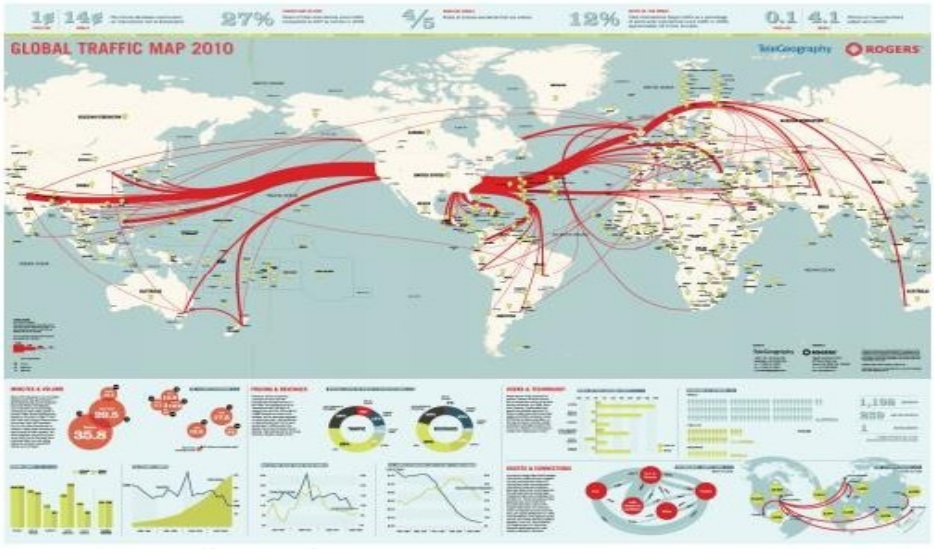
> Foi assim com a invenção da máquina a vapor, das ferrovias, dos automóveis, dos aviões e do telefone. E acontece, agora, com um novo meio de "transporte": a internet. Que acarreta não o transporte físico de pessoas, mas o livre fluxo de ideias e de informações numa velocidade assustadora. E que criou uma nova riqueza: o conhecimento. (VIEIRA, 2003, p. 205)

De acordo com Bertoloto (2012), no Brasil o principal nó das rotas internacionais do trâmite de informações fica em Brasília, ligando o extremo oriente da Ásia às rotas europeias e o Brasil ao tronco América Central. Afirma também que a extensão do *backbone* brasileiro alcança 150 mil quilômetros, sendo que 16 mil quilômetros deles pertencentes a *Eletronet*, empresa que veio a falir em 2003.

> A demanda por transmissão de *stream* de vídeo cresce exponencialmente com o sucesso de sites de compartilhamento de vídeos como o *Youtube.com* e redes sociais como *Twitter* e *Facebook*, o país precisa exportar essas informações para outros continentes e a largura de banda se faz absolutamente necessária para que o escoamento desses dados ocorra. (BERTOLOTO, 2012)

A seguir analisaremos outro mapa da *TeleGeography,* sediada em Washington-DC e especializada em dados da internet, divulgou no mapa (Figura 6) abaixo o tráfego mundial de informações que transitam por todo o globo e seus maiores troncos (BERTOLOTO, 2012).

Figura 5 - Mapa global de Tráfego de informações



Fonte: TeleGeography's (*apud* BERTOLOTO, 2012)

Ao analisarmos o mapa (Figura 5) global do tráfego de informações e realizarmos uma comparação com o mapa (Figura 4) anteriormente visto, notaremos certa semelhança entre eles, porém se formos analisar mais a fundo, notaremos que no mapa de cabos submarinos de fibra ótica (Figura 4) nos retomamos a estrutura física das redes de comunicações pelo globo, já o mapa de tráfego de informações (Figura 5) utiliza das estruturas físicas para disseminar informações por todo o mundo. Ratificando a quantidade demasiadamente vultuosa de dados que partem dos Estados Unidos, como sendo um dos principais países participantes desse mundo ciberespacial, e também um dos maiores fornecedores de serviços pela internet.

De acordo com Paul Saffo (1997), do *Future Institute* (*apud* Tigre, 1999), conclui que aproximadamente 60% dos serviços comerciais dos Estados Unidos, serão realizados via internet já na primeira década do século. Afirma também que os programas nacionais dos Estados Unidos e Canadá tiveram extrema importância em sua elaboração para que se estimulasse a oferta e demanda de TI, com o intuito de globalizar o uso da internet, com o foco principal em pequenas empresas e populações que não possuem uma condição mínima de acesso à internet (TIGRE, 1999).

2.4 TRATAMENTO DO FLUXO DE DADOS DAS FRONTEIRAS BRASILEIRAS

Compreendemos por fluxo de dados transfronteiriços (FDT), como sendo uma parte da política de controle voltada a segurança de um país e sua regulamentação quanto ao fluxo de dados que entram e saem para o exterior (LINS, 2002). Segundo Lins (2002), Consultor Legislativo da Câmara dos Deputados, fluxo de dados transfronteiriços podem ser entendidos também como um *link* estabelecido entre dois países onde são transmitidas as informações entre si e o processamento ou armazenamento em um dos lados, podendo por vezes ser feito em ambas as pontas.

Dessa forma seria viável que países em desenvolvimento adotassem a política de limitação do fluxo de dados transfronteiriços (FDT), a fim de garantir que os países processassem seus próprios dados no país. Essa política de limitação não somente assegura o mercado local para os profissionais da computação, mas também fomenta o consumo de equipamentos e *softwares* locais (LINS, 2002). Tendo em vista a estratégia desenvolvimentista brasileira à época, o Estado utilizou-a como medida de controlar os serviços de informática que eram importados pelo país e assim estimular os serviços informáticos internos (LINS, 2002).

> Até meados da década de cinquenta, o Brasil vivia uma fase embrionária das telecomunicações, quando uma série de ações, de diferentes governos federais, deram

> início ao desenvolvimento desse setor. O Plano de Metas do governo de Juscelino Kubitschek (de 1956 a 1961) revelou a necessidade de um sistema nacional de telecomunicações que facilitasse e agilizasse a difusão de informações, com o objetivo de atingir a esperada "integração nacional". (CARVALHO, 2006, P. 51)

Podemos notar que essa política de controle de dados pode ser muito benéfica para um país, partindo do pressuposto que ela fomenta e estimula as indústrias nacionais a cada vez mais desenvolverem seus equipamentos eletrônicos e computacionais, desenvolvendo também a tecnologia aplicada nas máquinas. Não somente o desenvolvimento na parte de *hardwares*, mas também os *softwares* ou serviços nacionais, que usualmente não são muito utilizados. A exemplo disso podemos levantar uma breve análise rápida de ser respondida, qual o serviço de busca mais utilizado no mundo? Se você respondeu o Google você está certo disso, entretanto nós também possuímos serviços de busca nacionais como o Yahoo!, o Aonde.com, e até mesmo o Cadê? antigo buscador que foi muito utilizado por muitos brasileiros. De uma maneira geral os desenvolvimentos consequentes dessa política estão voltados todos para a área da informática nacional, área extremamente importante tanto para os profissionais da computação quanto para o desenvolvimento cultural da população.

> ...a informática deve ser ressaltada, virá a ter implicações, profundas implicações na organização geral da sociedade, nos métodos educacionais, na ordem econômica e social e poderá até influir no conceito de soberania de um país, pois a mobilidade do fluxo de informações, que já atinge graus elevadíssimos, podendo percorrer sem dificuldades o mundo, de computador a computador, desafia qualquer fiscalização e a própria noção jurídica de territoriedade. (PION, 1985, p. 280)

Segundo Pion (1985) da Secretaria Especial de Informática, a indústria de base de dados pode ser vista da seguinte forma: os acervos de dados são estruturados, a informação é organizada e estruturada, cria-se o banco de dados que posteriormente serão utilizados para acesso através da prestação de serviços de consulta às bases de dados. A autora afirma também que as consequências do uso da política do fluxo de dados transfronteiriços permitem um desenvolvimento econômico e cultural, a partir do qual a própria população irá se modificar através do acesso às informações e culturas estrangeiras. Teremos uma predominância científica e tecnológica, através das consultas às informações de tecnologias exteriores, com isso garantindo sua soberania e poder político envolvido (PION, 1985).

> A internet democratizou o acesso à informação, permitindo que os países adotassem metodologias e tecnologias similares, independentemente de seu estágio de desenvolvimento. Os países em desenvolvimento foram e serão os maiores beneficiados com a publicação eletrônica, que permitiu superar barreiras de visibilidade e acesso à literatura que publicam, antes praticamente inacessível no cenário internacional. (CASTRO, 2006)

2.4.1 Desafios enfrentados

De acordo com Lins (2002), no Brasil não houve uma legislação para o fluxo de dados transfronteiriços (FDT), sua regulação proveio da resolução nº 1/78 da Comissão de Coordenação das Atividades de Processamento de Dados (CAPRE), responsável pela política de informática. A resolução exigia um consentimento do governo para que fosse permitido que uma empresa ou usuário estabelecesse uma conexão com o exterior para o intercâmbio de dados, um FDT. A Embratel era quem estabelecia as ligações, sendo que, antes mesmo de fechar contrato com seus clientes, necessitava da aprovação da CAPRE (LINS, 2002).

Após a extinção da CAPRE em 1979, houve o surgimento da Secretaria Especial de Informática (SEI), órgão que assumiu controle sobre as responsabilidades da FDT e manteve as restrições para a atividade, sua concessão para que fosse concretizada uma ligação com o exterior era a exigência de um certificado que permitisse a aplicação a ser executada (LINS, 2002).

Tabela 2 - Enquadramento dos pleitos de FDT pela aplicação (1987 a 1994)

Denominação	Descrição	Aprovação	Prazo de validade
FDT Administrativo	Ligação intracorporativa ou intercorporativa que não cause "dependência crítica do exterior"	Aprovado sempre que solicitado	3 anos, renovável
FDT Informativo	Ligação para recebimento de "tickers" de câmbio e cotações de bolsas internacionais, processadas no País	Reservado a empresas nacionais	1 ano, renovável, sujeito a aprovação de projeto
FDT Redes de Computadores	Ligação a serviços de rede setoriais, transcorporativos (SITA, SWIFT, BitNet, etc.)	Aprovado sempre que solicitado	3 anos, renovável
FDT Serviços e Processos	Utilizado para processamento no exterior de aplicações técnicas e de controle de processos, ou outras aplicações que criem "dependência crítica"	Aprovado somente em casos especiais	1 a 3 anos, renovável
FDT Bases de Dados	Destinado ao acesso a bases de dados bibliográficas, documentais ou estatísticas	Aprovado em rito simplificado	3 anos, renovável
FDT Temporário	Ligação destinada a feiras, demonstrações comerciais e eventos	Aprovação imediata e sumária	30 dias, não renovável

Fonte: LINS (2002)

O quadro acima (Figura 7) nos mostra como foram distribuídas as prioridades de aplicação das FDT nas diferentes situações e as diversas necessidades que surgiram a partir

delas. Podemos notar também as medidas restritivas que a comissão especial, criada pela SEI em 1986, apresentou em sua proposta de resolução (LINS, 2002).

De acordo com Jacobus (2014), na história da indústria de TI brasileira, a política adotada em meados dos anos 70 e 80, condenada por muitos pesquisadores, é argumentada que as reservas de mercado foram a razão do país ter entrado no mercado global tardiamente, mercado esse que obtinha um padrão tecnológico com qualidade superior àquela oferecida no Brasil. Afirmando também que o foco brasileiro no mercado interno por anos, com o objetivo de desenvolvimento e proteção à indústria nacional, foi um dos motivos do Brasil ter dificuldade em suplantar o mercado doméstico e alcançar projeção como exportador de produtos e serviços em TI (JACOBUS, 2014).

> Em países como o Brasil, a maneira de estender à maioria da população o acesso à internet não pode seguir o modelo comercial dos países desenvolvidos, baseado na aquisição individual de um eletrodoméstico caro (o computador) e no pagamento mensal de serviços comerciais de acesso. (AFONSO, 2002, p. 170)

Nota-se que o Brasil ao longo de seu desenvolvimento e avanço nas áreas de TI, na tentativa de inserir-se no espaço global interconectado por redes de internet espalhadas pelo mundo, encontrou várias dificuldades ao longo do caminho, seja na criação de uma malha física capaz de suportar tais avanços tecnológicos, como também no baixo investimento de políticas de incentivos ou no excesso de regularização por parte delas. Com isso dificultando os fluxos de informações que circulam pelo mundo.

2.5 AS FRONTEIRAS CIBERNÉTICAS

Até aqui pudemos observar como a estrutura de rede de internet possui suas infraestruturas físicas, os caminhos transcorridos pelos cabos submarinos, assim como os servidores nacionais e as empresas de telefonia que participaram intrinsicamente de maneira insubstituível. Pois sem essa estrutura que está em constante desenvolvimento desde a descoberta da nova era da informação, não seria possível nos conectar com o mundo e compartilharmos informações para diversas necessidades, sejam elas por lazeres ou trabalho.

O ciberespaço desafia conceitos tradicionais, entre eles as fronteiras geopolíticas ou mesmo os organizacionais, um novo ambiente que ainda necessita ser desbravado pelos bandeirantes do século XXI (PINHEIRO, 2013). Para Côrtes (2002), Embaixador de Carreira aposentado, as diversas definições sobre o estudo das fronteiras nacionais podem ser resumidas

na concepção de fronteiras jurídicas, sendo como o limite legal entre as jurisdições soberanas de dois Estados (CÔRTES, 2002).

Quando falamos de fronteira, pensamos em algo físico, como uma divisa entre dois países fortemente armados e prontos para intervirem e interromperem qualquer tentativa de invasão por parte do outro Estado sobre o seu, porém quando falamos de internet não pensamos da mesma maneira, visualizamos como algo que corre livremente pelos diversos Estados e que não possui qualquer medida restritiva ou regulamentar para seu uso.

Entretanto segundo Ventre (2019), em meados dos anos 70 e 80 os Estados instituíram seu arcabouço jurídico nacional, que cuidava das legislações sobre tratamento de dados de caráter pessoal, ataques à sistemas de informações e de sancionar alguns casos de criminalidade informática, constituindo dessa forma a base de uma corte territorial dessa rede planetária. Dessa forma os Estados projetavam nas redes, no ciberespaço, uma arquitetura estatal do sistema internacional (VENTRE, 2019).

> Foram as considerações securitárias que levaram a pensar no corte territorial do ciberespaço. Sua própria arquitetura (a primeira camada, física) presta-se facilmente a um fatiamento da rede bem próximo do corte do planeta em Estados: os cabos chegam e saem de pontos – instalações que conectam os cabos entre si entram e saem do território, criando uma relação entre a rede interna e o resto do mundo – que poderiam ser os "pontos-fronteiras", equivalentes aos portos marítimos, aos aeroportos internacionais. (VENTRE, 2019, p. 78)

Para Oliveira (2011), a evolução do ambiente eletrônico provocou nos liberais uma visualização nova do ciberespaço, passaram a considerá-lo em duas perspectivas: a primeira que trata a internet como pública, e a segunda tratando como o espaço das trocas econômicas e comerciais. Com isso levando os liberais a seguinte conclusão: de que a internet era privada e não pública, de que o fato de vetar acesso à certos conteúdos, demonstra que a internet tem, sim, fronteiras e que o espaço cibernético não é algo que se constrói separado da realidade, tendo em vista que muitos problemas gerados no mundo virtual impactam no mundo real (OLIVEIRA, 2011).

> O Território Virtual ou *Ciberespaço* assinala o rejeite irrestrito infligido pelas fronteiras físicas e políticas esquivando-se da realidade conceitual costumeira de território, pertinente a uma ideia nova, de rede, fundamentada pela localização da informação como elemento identificador do território no ciberespaço e instituindo uma nova modalidade de fronteira transnacional. (WESLEY, 2013, p. 6)

A imprecisão das fronteiras cibernéticas faz com que os Estados fiquem mais fragilizados, pois não possuem condições de delimitar sua soberania nesse espaço cibernético. Sem essas referências tradicionais que definem um território nacional, os Estados ficam

impedidos de exercerem seus plenos poderes e ativar suas defesas (VENTRE, 2019). Para Ventre, a fronteira virtual é definida pelo conjunto de capacidades e poderes de fiscalização, filtragem, bloqueio e vigilância dos fluxos nos extremos terrestres que definem e delimitam o território nacional entre seu interior e exterior.

Tabela 3 - Fronteiras jurídicas e Fronteiras metafísicas

Fronteiras jurídicas:	Fronteiras metafísicas:
Regidas por normas do Direito Internacional Público, Atos Internacionais, acordos e tratados bilaterais.	Não sujeitas a normas internacionais específicas.
Visíveis (ainda que por convenção).	Invisíveis, de detecção difícil ou até impossível.
Ações detectáveis, às vezes antes mesmo de efetivar-se a violação.	O "agressor" age de forma sigilosa ou sub-reptícia.
Violações fisicamente perceptíveis.	O "agredido" não percebe a violação ou só a discerne após o fato consumado.

Fonte: CORTÊS (2006)

Para o Embaixador Marcos Henrique Camillo Côrtes, as fronteiras cibernéticas definidas em sua obra como sendo uma fronteira metafísica, não somente são invisíveis, mas também como de difícil detecção. Afirmando também que as normas do Direito Internacional, que regem as fronteiras na concepção jurídica, não são aplicadas (CÔRTES, 2006).

Com isso cresce a importância dos Estados se capacitarem e se habilitarem na nova "linguagem moderna" global, a cibernética, conceito esse que vem exponencialmente se desenvolvendo e ganhando espaço no nosso cotidiano, em seus avanços tecnológicos e informacionais.

2.6 OS AVANÇOS DA CIBERNÉTICA

O avanço da internet pelo mundo, possibilitou pessoas se comunicarem há miliares de quilômetros de distância, facilitando a vida de todos seus usuários como, agilizar pagamentos, buscar informações importantes em sites de pesquisa, aproximar pessoas que ficaram anos sem se encontrarem, entre outros miliares de benefícios que a internet e seu uso como principal meio de ferramenta nos proporcionou.

Dessa maneira a utilização da internet como meio de comunicação e sistema de organização, por meio de seu avanço exponencial nas últimas décadas, fez com que várias atividades econômicas, políticas e socias fossem realizadas pela internet (CASTELLS, 2003 *apud* TERROSO; ARGIMON, 2016).

> O traço marcante da sociedade contemporânea é a alta tecnologia, introdutora de nova dimensão à comunicação. Não se trata apenas, de uma evolução da realidade física, material, concreta dos objetos, a utilizar os recursos da natureza, mas de uma realidade criada, de impulsos eletrônicos, codificada e simbólica em outra dimensão do tempo- espaço. O físico e o virtual passam a coexistir na cumplicidade e complexidade da configuração cibernética, cujos comandos codificados produzem ondas imateriais. (VIEIRA, 2006)

Entretanto com sua constante evolução e seu desenvolvimento, vieram as vulnerabilidades e ameaças presentes nas redes. O ciberespaço possibilitou que usuários com más intenções, pudessem invadir um computador ou qualquer dispositivo móvel conectado a uma rede de internet. Acessando arquivos pessoais e extraindo o máximo de informações ou ativos.

Dessa forma não podemos deixar de lado a necessidade de um sistema de defesa em nossas fronteiras, afim de mitigar os ataques e invasões pelos *hackers*, termo orginalmente definido como sendo, um programador de computador talentoso que resolveria qualquer problema muito rapidamente, utilizando meios incomuns (SILVEIRA, 2010, p. 34).

> A ausência de registro na História de um país potente sem Forças Armadas adequadas corrobora o quanto o rompimento do limite entre defesa (ação) e segurança (sensação) causado pelas novas ameaças transacionais, impõe a análise da integração das Forças Armadas conectadas com as agências da Segurança e Defesa Nacional. (WESLEY, 2013)

2.7 PROTEGENDO NOSSAS FRONTEIRAS

Para Ventre (2019) as conexões livres das redes acarretaram um conjunto de violências que os Estados não têm condições de impedir antes que produzam seus efeitos no território nacional. Para ele o ciberespaço gera dúvidas no Estado em sua capacidade de garantir a segurança em seus territórios, com isso os Estados estão buscando recuperar tal capacidade (VENTRE, 2019).

> Enquanto potência emergente, o Brasil está mais preocupado que seus vizinhos com as ameaças de guerra e terrorismo cibernéticos, que são ações politicamente motivadas visando penetrar nas redes e sistemas de computadores de uma nação a fim de infligir dano e destruição às infraestruturas nacionais. (MUGGAH; DINIZ, 2013, p. 11)

A exemplo de um país com bons perímetros de fronteira cibernética é a rede de ciberguerra da China, reconhecida em 2015 pelo governo. Sua gigantesca rede corporativa composta por inúmeras sub - redes e redes virtuais, é capaz de se desconectar efetivamente da internet em caso de ataques cibernéticos contra a nação. O país possui também efetividade de detectar os ataques externos, porém escolhe não os prevenir ou detê-los (ORLOFF, 2017 *apud* VENTRE, 2019).

Segundo Ventre (2019), foi observado que nos últimos anos, houveram várias interrupções da internet em vários países, ativando as fronteiras que passaram de filtro para se tornarem barreiras, bloqueando qualquer dado de entrar ou sair. Podendo ser seletiva, cortando apenas alguns aplicativos específicos, como as mídias sociais, que regularmente são alvos de tais bloqueios.

Quando falamos em defesa nacional nos retomamos às Forças Armadas que são responsáveis por tal tarefa. Dessa forma o principal responsável pela segurança e Defesa Cibernética do nosso país foi incumbido ao Exército Brasileiro. Os exércitos desenvolvem capacidades defensivas e ofensivas, dotando-se de unidades dedicadas à "ciberguerra" (o *Cyber Command* americano e o CDCiber brasileiro, por exemplo) (VENTRE, 2019). O Centro de Defesa Cibernética (CDCiber) em 2012 recebeu fundos iniciais de aproximadamente R$ 120 milhões do governo federal, visando futuras projeções que irão aumentar exponencialmente os investimentos na área de segurança e Defesa Cibernética, afirmam Muggah e Diniz (2013), em seu artigo estratégico.

> Centrando o foco nos avanços tecnológicos avultam as atividades cibernéticas como principal ameaça à Soberania e a Segurança Nacional de grandes potências mundiais através da emergência da *guerra cibernética* e práticas terroristas que sob o manto da invisibilidade das fronteiras cibernéticas constituem a grande ameaça contemporânea. (WESLEY, 2013, p. 5)

Sendo assim, podemos observar que a partir do momento em que nos conectamos à rede mundial de computadores, a internet, estamos totalmente expostos e sujeitos à receber tentativas de ataques e invasões de pessoas que utilizam de tal meio para promover o caos e até mesmo ganhar dinheiro, através de chantagens abusivas causadas pelo atacante, que logo após invadir uma máquina e extrair documentos pessoais como por exemplo, contas bancárias ou trabalhos importantes, criptografam seus documentos, cobrando preços absurdos de serem pagos.

De acordo com Carvalho (2010), General de Brigada do Exército Brasileiro, no que diz respeito às infraestruturas críticas nacionais, afirma que com a crescente dependência de sistemas de informação no controle de computadores e aplicativos expostos à internet, torna

como principal foco das ações de Segurança e Defesa Cibernética, a proteção das ICI que controlam a operação das ICN (CARVALHO, 2010).

2.8 A ATUAÇÃO DO EXÉRCITO BRASILEIRO NA DEFESA CIBERNÉTICA

A Estratégia Nacional de Defesa (END), de 2008, definiu os três setores considerados de importância estratégica para a defesa nacional, quais sejam: o nuclear, o espacial e o cibernético (CARVALHO, 2010, p. 1). O Ministério da Defesa, atribuiu a coordenação do setor cibernético a cargo do Exército Brasileiro, conforme a Diretriz Ministerial do MD nº 14/2009 (BRASIL, 2012, p. 68 *apud* RAMOS; GOLDONI, 2016, p. 165).

Consequentemente, o Exército Brasileiro criou, em 2010, o Centro de Defesa Cibernética (CDCiber) para coordenar os planejamentos da Defesa Cibernética, iniciando assim sua capacitação de recursos humanos para atuar nesse setor (RAMOS; GOLDONI, 2016, p. 165).

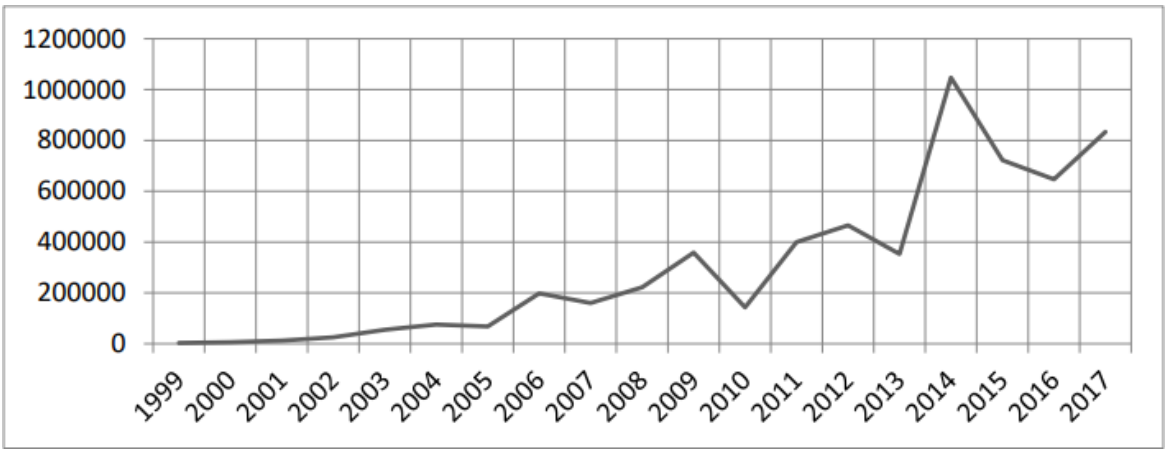
> O Exército Brasileiro, como Força coordenadora e integradora na condução do processo de estabelecimento das estruturas de Defesa Cibernética no âmbito da Defesa, antecipou ações no seu campo interno e emitiu, em junho de 2010, a Diretriz para a Implementação do Setor Cibernético no Exército, e já em agosto do mesmo ano foram assinadas as portarias criando o Centro de Defesa Cibernética do Exército (CDCiber) e ativando o seu Núcleo (Nu CDCiber), que já se encontra operativo, sendo a referência no âmbito das Forças Armadas. (BARROS; GOMES e FREITAS, 2011, p. 210)

Quando falamos de cibercriminalidade não podemos nos prender apenas a ataques externos. No ano de 2014 o Brasil foi alvo de inúmeros incidentes e ataques cibernéticos, ano esse em que o Brasil foi responsável por sediar a Copa do Mundo FIFA – 2014, entretanto de acordo com levantamentos feitos pelo Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, CERT.br, apresentou que a maioria dos ataques foram originados a partir do próprio Brasil (VENTRE, 2019).

> Os eventos ocorridos durante a Copa do Mundo FIFA – 2014, quando vários órgãos sofreram interferências por ataques cibernéticos, com potenciais prejuízos para o desenvolvimento de suas atividades e até com o comprometimento da instituição ou da imagem do país no exterior, mostram a importância e a necessidade de um eficiente sistema de defesa cibernética no país. (FREIRE, 2015)

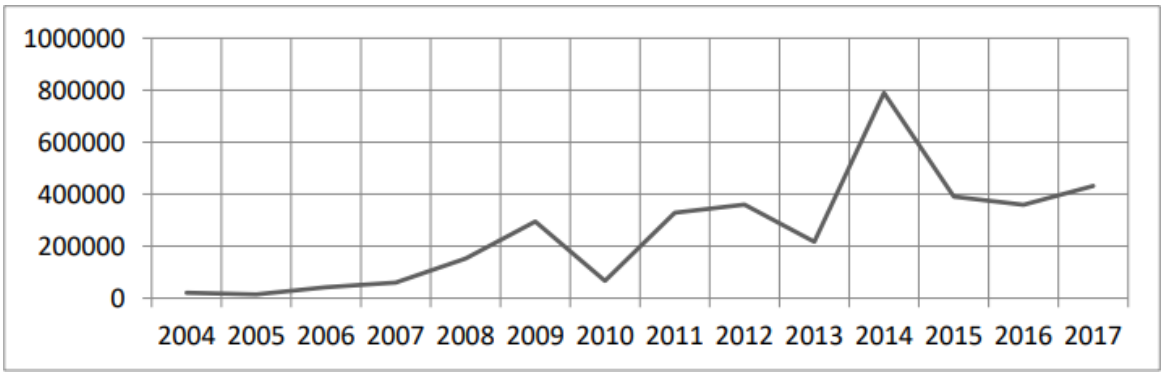
Podemos comparar as curvas de incidentes absolutos, ou seja, a somatória de ataques recebidos provenientes de qualquer origem geográfica e a curva de incidentes originadas no Brasil:

Gráficos 1 - Curva de incidentes reportados em valor absoluto (1999 - 2017)



Fonte: CERT.br (*apud* VENTRE, 2019)

Gráficos 2 - Curva de incidentes com origem no Brasil em valor absoluto (2004 – 2017)



Fonte: CERT.br (*apud* VENTRE, 2019)

Como podemos observar, os ataques cibernéticos nem sempre preveniram de agentes externos, mostrando o quanto o Brasil é vulnerável à sua própria cibercriminalidade. A média é de 52% entre os anos de 2004 a 2017 e de 65% entre 2008 e 2017, apresentando picos de até 82 % (VENTRE, 2019). No Brasil diversos especialistas alertam quanto aos ataques ininterruptos coordenados de Negação de Serviço Distribuído (DDoS), desde 2011 por *hackers* brasileiros participantes do grupo *Lulz Security*, vinculado ao grupo que atacou sites do Senado americano e da CIA (WESLEY, 2013).

Segundo os autores, Muggah e Diniz (2013), os crimes cibernéticos custam aproximadamente R$16 bilhões anuais, ou 7% do custo global para a economia do país. O Brasil é considerado como um dos maiores usuários de *malwares* na América, tanto como alvo quanto como origem de ataques (MUGGAH; DINIZ, 2013).

As ações cibernéticas, para fim de Defesa Nacional, enquadram-se nos chamados níveis de decisão previstos na Estrutura Militar de Defesa (CARVALHO, 2010).

Podemos observar os níveis no quadro abaixo:

Tabela 4 - Ações cibernéticas nos níveis de decisão

NÍVEL	DENOMINAÇÃO	ÓRGÃO DE COORDENAÇÃO
Político	Segurança da Informação e Comunicações (SIC) Segurança Cibernética	Gabinete de Segurança Institucional da Presidência da República (GSI-PR)
Estratégico	Defesa Cibernética	Ministério da Defesa
Operacional	Guerra Cibernética	Forças Armadas
Tático		

Fonte: (CARVALHO, 2010)

O Programa de Defesa Cibernética, criado pelo Exército Brasileiro, enquadra-se no chamado Subportfólio Defesa da Sociedade, reunindo todos os Programas que atingem diretamente a capacidade operacional da Força Terrestre (COELHO, 2018).

Abaixo podemos observar a gama de Programas que o Exército Brasileiro apresenta em seu Portfólio Estratégico do Exército:

Figura 6 - Estrutura do Portfólio do Exército Brasileiro

Fonte: COELHO, (2018)

O Projeto Gestão de Talentos na Defesa Cibernética, tema da obra abordada por Coelho (2018), tem por finalidade a correta gestão dos recursos humanos em se empregar no Setor Cibernético pessoas vocacionadas, assim aumentando sua eficiência. Não se pretende capacitar pessoas medianas e torná-las boas, mas sim encontrar as pessoas que são naturalmente boas e torna-las excepcionais. O projeto pretende alocar os talentos em funções que possam alcançar seu máximo potencial (COELHO, 2018).

3 REFERENCIAL METODOLÓGICO

3.1 TIPO DE PESQUISA

Foi realizada uma pesquisa bibliográfica com o objetivo de formar um conceito sobre o que são as fronteiras cibernéticas e suas estruturas físicas que promovem a conectividade do Brasil e do mundo. A pesquisa também norteou os conhecimentos e conceitos sobre esse imenso espaço da cibernética. Com isso, diversos conceitos teóricos foram implementados para melhor compreensão do leitor no entendimento da infraestrutura espacial cibernética, assim como dos conceitos geopolíticos envolvidos.

3.2 MÉTODOS

3.2.1 Levantamento de dados

Foram levantados dados para compreensão da estrutura de rede mundial e também brasileira, com o intuito de explorar mais sobre o tráfego de informações que transcorrem pelas redes físicas ou virtuais, nos quais foram tratados. Assim como conhecer o desenvolvimento da cibernética e no que suas vulnerabilidades podem causar, tanto nos setores de gerenciamento de dados como também no Setor de Defesa Cibernética. Para isso, todos os dados serão retirados de pesquisas, sites, livros e artigos de estudiosos da área de tecnologia e afins, assim como sites de notícias e informações de grande relevância, sempre buscando as fontes mais atuais e confiáveis disponíveis.

3.2.2 Análise de dados

De posse das informações disponíveis sobre o tema, foi feita uma análise dos conhecimentos adquiridos buscando uma conclusão satisfatória que comprove o questionamento levantado pelo tema e que esteja embasada em fontes de conhecimento de grande relevância e confiança.

4 CONSIDERAÇÕES FINAIS

Por meio das diversas fontes de pesquisa, podemos concluir que o Brasil possui sim fronteiras cibernéticas, sejam elas físicas ou virtuais. Provando dessa forma que ao falarmos de cibernética podemos rapidamente vincular seu escopo com a Geopolítica. Enfatizando o termo cibernético, observamos a necessidade de um novo tipo e forma de fronteira: a "fronteira-ponto" (FERREIRA NETO, 2018), cuja teoria abordará sobre a exigência de novos limites político– jurídicos. Fronteiras essas que estão crescentemente em expansão e carecem de desenvolvimentos em Tecnologia de Informação e Comunicação, com o intuito de proteger ativos confidenciais de muitos dos usuários, que comumente utilizam a internet para transferir documentos pessoais e até mesmo dados bancários. A imputabilidade jurídica em razão das fronteiras virtuais não possuírem com clareza uma área de abrangência, sendo assim dificultando os Estados de rastrearem ataques e invasões causadas por usuários maliciosos, apresentando fatos que demandam por profundos investimentos nessas áreas de atuação.

Pudemos acompanhar uma parcela da história da construção dos *backbones* brasileiros que são imprescindíveis para a interligação do Brasil com o resto do mundo. A topologia de *backbones* brasileiros abordados nos primeiros capítulos, nos mostra a realidade física em que a internet está infra estruturada em nossa nação por meio dos cabos de fibra ótica que permitem a entrada e saída do fluxo de informações no Brasil, apresentando sucintamente algumas descrições como, distâncias máximas em que cada um percorre, data de criação, principais atores e desenvolvedores do arcabouço tecnológico envolvido e países interligados, ainda acerca dos mesmos, notamos que o Brasil sofreu dificuldades no gerenciamento dessas redes físicas, seja por parte do governo como por imperícia de seus usuários, portanto cabe ressaltar a importância e a necessidade de uma melhoria de métodos e projetos para o seu gerenciamento e monitoramento.

A malha de conexões da internet é assustadoramente grande, com milhares de internautas conectados a esse imenso e vasto mundo digital, onde as pessoas conseguem em uma fração de segundos enviar uma mensagem e logo em seguida já serem respondidas, quase que instantaneamente. Foi possível concluir que os Estados Unidos estão em primeiro lugar quando o assunto é trâmite de informações, de forma que elas acabam se centralizando ao redor do país e por conseguinte se espalhando para outras nações, basta voltarmos e analisarmos a Figura 5 ilustrado na página 22.

Observamos como os avanços e o desenvolvimento da internet causaram muita disparidade entre os países, enquanto países que possuíam melhores condições de oferecer redes

de altíssimas velocidades de transmissão estavam no topo da “pirâmide” na área da cibernética, países subdesenvolvidos ainda nem imaginavam o que seria uma estrutura tão elaborada como era a internet. Com isso houveram muitas falhas durante o processo de tentativa de acompanhamento com o restante do mundo que já havia se inserido no ciberespaço, abrindo assim várias portas de entrada para atuação de *hackers* usufruírem das vulnerabilidades criadas ao longo do tempo. Crescendo de importância o constante investimento nas tecnologias da informação e sua Defesa Cibernética. Enfatizando a existência das fronteiras cibernéticas e sua constante exploração.

Acerca dos avanços cibernéticos e suas vulnerabilidades, o Brasil se fez presente no Setor Cibernético e na Defesa Cibernética. Através de uma Diretriz Ministerial do MD nº 14/2009, incumbindo responsabilidade ao Exército Brasileiro para fazer frente à tais ameaças, dessa forma a Defesa Cibernética brasileira vem cumprindo com efetividade sua função. Pudemos observar os inúmeros ataques e tentativas de invasões durante eventos importantes como por exemplo a Copa Do Mundo, fato este que levantou dados importantes para análise de incidentes feito pelo CERT.br, que observou que mais de 70% dos ataques proviam do próprio Brasil. Cabendo ressaltar a necessidade de continuarmos investindo cada vez mais no Setor Cibernético, assim como Exército Brasileiro está fazendo, através da criação de vários Programas e projetos relacionados com a defesa de nossas fronteiras, tanto seu emprego no meio terrestre como também no ciberespaço.

Como pudemos observar, através da busca e pesquisa das diversas fontes de consulta, podemos responder com clareza às perguntas iniciais do trabalho. A internet não é algo que se possa delimitar com facilidade, temos vários pesquisadores que incessantemente buscam respostas por haver algum tipo de linha imaginária que pudesse ser vista e usada como delimitadora das fronteiras cibernéticas. Até o presente momento os limites cibernéticos são impostos de acordo com o potencial cibernético dos Estados em se defenderem e gerenciarem o fluxo de dados que transcorrem no seu interior, sendo assim países com alto potencial acabam construindo seus próprios limites no ciberespaço e obtendo uma certa “liberdade” de ação pela rede mundial, entrando e saindo de outros Estados como bem quiserem. Assim como a internet está em exponencial evolução, seria possível afirmar que enquanto os sistemas de TIC estão se desenvolvendo, sempre haverá uma outra versão mais atualizada com menores vulnerabilidades e portas de entrada para atacantes e invasores, resumindo-se a uma “queda de braço” sem fim, em que sempre que se desenvolve um sistema de defesa altamente poderoso e eficaz de um lado, do outro lado *hackers* de todo o mundo inovam e melhoram seus métodos de ataques e invasões. Não havendo atualmente meio de comunicação em que se possa confiar 100%.

REFERÊNCIAS

AFONSO, Carlos A. Internet no Brasil–alguns dos desafios a enfrentar. **Informática Pública**, v. 4, n. 2, p. 169-184, 2002.

BARLOW, John Perry. Declaração de independência do ciberespaço. 1996.

BARROS, Otávio S. R.; GOMES, Ulisses M. G.; FREITAS, Whitney L. de. (Org.). Desafios Estratégicos para a Segurança e Defesa Cibernética. Brasília: Secretaria de Assuntos Estratégicos, 2011. pp. 105-128.

BEZERRA, Arthur Coellho; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil. Revista de Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura, Florianópolis, v.16, n.2, p.157-171, maio/ago. 2014.

BERTOLOTO, Danilo Costa *et al.* **Redes de fibra óptica**: conexões locais em dimensões globais no Brasil. 2012.

CASTRO, Regina C. Figueiredo. Impacto da Internet no fluxo da comunicação científica em saúde. **Revista de Saúde Pública**, v. 40, n. SPE, p. 57-63, 2006.

CARVALHO, Paulo Sérgio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. **Coleção Meira Mattos-Revista das Ciências Militares**, 2011

CARVALHO, M. S. R. M. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança. **Unpublished Estudos de Ciência e Tecnologia no Brasil, Universidade Federal do Rio de Janeiro, Rio de Janeiro**, 2006.

COELHO, Cláudio Borges. Projeto gestão de talentos na defesa cibernética. 2018.

CÔRTES, Marcos Henrique Camillo. As Violações 'Invisíveis' das Fronteiras. **Rio de Janeiro: Revista Ideias em Destaque**, n. 20, 2006.

DA SILVA, Carlos Alberto F.; TANCMAN, Michéle. A dimensão Sociespacial do Ciberespaço: uma nota. **GEOgraphia**, v. 1, n. 2, p. 55-66, 2009.

DA SILVEIRA, Sérgio Amadeu. Ciberativismo, cultura hacker e o individualismo colaborativo. **Revista Usp**, n. 86, p. 28-39, 2010.

WESLEY, Maria Helena de Amorim. CIBERNÉTICA E CULTURA: TRANSIÇÃO E CONFLITOS NA SEGURANÇA E NA SOBERANIA.

FERREIRA NETO, Walfredo Bento. Territorializando o "Novo" e (Re)territorializando os Tradicionais: a Cibernética como Espaço e Recurso de Poder. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 8, n. 31, p.07-18, fev. 2014.Quadrimestral. Disponível em: <http://ebrevistas.eb.mil.br/index.php/RMM/issue/archive>. Acesso em: 28 fev. 2020.

FERREIRA NETO, Walfredo Bento Ferreira. Territorializando o "novo" e (re) territorializando os tradicionais: a cibernética como espaço e recurso de poder. **REVISTA BRASILEIRA DE ESTUDOS ESTRATÉGICOS**, n. 4, 2018.

FREIRE, Volber. Os projetos estratégicos do Exército Brasileiro e seus reflexos para a política externa brasileira: a importância do incremento do poder militar para a projeção de poder do Brasil em sua área de interesse estratégico. 2015.

GIBSON, William. **Neuromancer**. Aleph, 2015.

JACOBUS, Artur Eugênio. Empreendedorismo institucional: o papel de empresas e suas variações na evolução da indústria de software e serviços no Brasil. 2014.

LEMOS, André. Cibercultura e mobilidade: a era da conexão. **Razon y palabra**, v. 41, 2004.

LINS, Bernardo FE. O tratamento do fluxo de dados transfronteiras no Brasil. **Cadernos ASLEGIS**, v. 6, n. 16, p. 88-101, 2002.

MALAGUTTI, M. Ciberespaço: Instrumento Geopolítico com Implicações para o Brasil. **Anais do 6o Encontro da Associação Brasileira de Relações Internacionais. Anais... Belo Horizonte: ABRI**, v. 25, 2017.

MANDARINO JÚNIOR, Raphael. Reflexões sobre Segurança e Defesa Cibernética.

MOTTA, Marcelo Paiva da. Topologia dos backbones de internet no Brasil. **Sociedade & Natureza**, v. 24, n. 1, p. 21-35, 2012.

MUGGAH, Robert; DINIZ, Gustavo. Protegendo as Fronteiras.

OLIVEIRA, Luis Henrique Almeida de. Cyberwar: novas fronteiras da guerra. 2011. 69 f. Monografia (Especialização em Relações Internacionais) – Universidade de Brasília, Brasília, 2011.

PINHEIRO, Fábio Ponte. A Cibernética como arma de combate. **Rio de Janeiro**, 2013.

PION, M. Política de base de dados brasileiros. **Revista de biblioteconomia de Brasília**, v. 13, n. 2, p. 279-283, 1985.

RAMOS, Wagner Medeiros; GOLDONI, Luiz Rogério Franco. Os Projetos do Exército Brasileiro e o alinhamento com as diretrizes da Estratégia Nacional de Defesa. **Revista Política Hoje**, [S.l.], v. 25, n. 1, p. 153-175, mar. 2016. ISSN 0104-7094. Disponível em: <https://periodicos.ufpe.br/revistas/politicahoje/article/view/3714/3016>. Acesso em: 07 jun. 2020.

RIO DE JANEIRO. ACADEMIA MILITAR DAS AGULHAS NEGRAS. **Introdução ao Estudo da Geopolítica.** Resende: Editora Acadêmica, 2019. p.57

SILVEIRA, S. Ciberativismo, cultura hacker e o individualismo colaborativo. **Revista USP**, n. 86, p. 28-39, 1 ago. 2010.

TIGRE, Paulo Bastos. Comércio eletrônico e globalização: desafios para o Brasil. **Informação e globalização na era do conhecimento**, p. 84, 1999.

TERROSO, Lauren Bulcão; DE LIMA ARGIMON, Irani Iracema. Dependência de internet e habilidades sociais em adolescentes. **Estudos e pesquisas em psicologia**, v. 16, n. 1, p. 200-219, 2016.

VENTRE, Daniel. Ciberguerra. In: Seguridad Global y Potencias Emergentes em un Mundo Multipolar, XIX Curso Internacional de Defensa, 2011. Zaragoza: Imprenta Ministerio de Defensa, 2012. pp. 32-45.

VENTRE, Daniel. (2019). O dilema da fronteira virtual: Quando os Estados se tornam construtores de ciberfronteiras. *Dilemas - Revista de Estudos de Conflito e Controle Social, 0*, 75-96. Recuperado de https://revistas.ufrj.br/index.php/dilemas/article/view/23117/14951

VIEIRA, Eduardo. **Os bastidores da Internet no Brasil**. Editora Manole Ltda, 2003.

VIEIRA, Eurípedes Falcão. A sociedade cibernética. **Cadernos Ebape. BR**, v. 4, n. 2, p. 01-10, 2006.

GLOSSÁRIO

Backbone – "Espinha dorsal" dos fluxos de informações, é uma rede principal por onde os dados dos clientes da internet trafegam. Ele controla o esquema de ligações centrais de um sistema mais abrangente com elevado desempenho.

Hackers – usuários com intenções maliciosas, que utilizam de meios para tiraram proveito de outros usuários, com intuito de extrair informações confidenciais.

Rede – malha de conexões entre vários nódulos, como uma espécie de "teia", porém que interliga computadores de diversos locais do mundo.

***Peopleware* –** são pessoas que trabalham diretamente, ou indiretamente, com a área de tecnologia da informação, ou mesmo com Sistema de informação.

Ciberguerra – A ciberguerra ou guerra cibernética é uma modalidade de guerra em que a conflitualidade não ocorre com armas físicas, mas via eletrônicos e informáticos no chamado ciberespaço.

Cibercriminalidade – é o nome dado aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na rede.

Ativos – pode ser simplesmente entendido como algo que tem algum valor comercial: um bem que pode ser negociado entre dois agentes.

Malwares – é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou até mesmo vulnerabilidades para futuros ataques.

Portfólio – é uma coleção de trabalhos já realizados de uma empresa ou de um profissional.