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

Luiz Eduardo Martins Spotti

A ESTRUTURA E O FUNCIONAMENTO DA INTERNET E SUAS CONSEQUÊNCIAS GEOPOLÍTICAS PARA OS ESTADOS

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 ESTRUTURA E O FUNCIONAMENTO DA INTERNET E SUAS CONSEQUÊNCIAS GEOPOLÍTICAS PARA OS ESTADOS
AUTOR: LUIZ EDUARDO MARTINS SPOTTI

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, 01 de julho de 2020.

_____

Cad Luiz Eduardo Martins Spotti

Luiz Eduardo Martins Spotti

A ESTRUTURA E O FUNCIONAMENTO DA INTERNET E SUAS CONSEQUÊNCIAS GEOPOLÍTICAS PARA OS ESTADOS

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

Luiz Eduardo Martins Spotti

A ESTRUTURA E O FUNCIONAMENTO DA INTERNET E SUAS CONSEQUÊNCIAS GEOPOLÍTICAS PARA OS ESTADOS

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

_____
Marcos de Mendonça Silva, Major
Avaliador 1

_____
André Köhler Damião, Major
Avaliador 2

Resende
2020

Dedico este trabalho principalmente a Deus, por estar sempre a meu lado, dando-me forças para continuar nesta caminhada, assim como também o dedico a minha família, em especial a minha mãe e irmã que, sem elas não seria possível que eu estivesse lutando em busca dos meus sonhos.

AGRADECIMENTOS

Agradeço a todos aqueles que me deram forças e me ajudaram na confecção deste trabalho, seja diretamente ou indiretamente. Agradeço a minha família, base para todos os passos que já tenha dado até os dias de hoje, assim como a minha namorada que, mesmo deixada de lado alguns momentos, sempre me ajudou e percebeu a importância do trabalho em minha vida.

Destaco um agradecimento especial ao meu orientador que, sempre apaixonado pelo conteúdo que leciona, nunca deixou de prestar a devida orientação aos seus alunos.

RESUMO

A ESTRUTURA E O FUNCIONAMENTO DA INTERNET E SUAS CONSEQUÊNCIAS GEOPOLÍTICAS PARA OS ESTADOS

AUTOR: Cadete Luiz Eduardo Martins Spotti
ORIENTADOR: Major Walfredo Bento Ferreira Neto

O crescimento do ciberespaço, materializado especialmente pela internet, principal vetor deste meio, está cada dia mais interligado às estruturas dos Estados. Isto se faz presente tanto através dos meios privados como dos governamentais, e torna de elevada importância estudar as formas como este meio interfere no mundo físico das nações, assim como compreender se há um monopólio em seu controle e as consequências geopolíticas destes fatos. Como forma de responder a estes questionamentos, foram observados os principais aspectos do funcionamento da internet e sua estrutura, assim como os conceitos e projeções geopolíticas que podem ser desenvolvidos no meio cibernético. Foram levantados dados que relacionam o pioneirismo norte-americano na criação das estruturas bases da Internet, através do projeto ARPAnet, com o controle que atualmente exercem nas decisões que são tomadas no domínio cibernético e no fluxo de informações que o percorrem. Desta forma, foi possível compreender o grau de projeção que as estratégias geopolíticas de um país dominante na área cibernética podem influenciar sobre países menos desenvolvidos nos setores tecnológicos e de telecomunicações. Muitos destes refletem em domínios que já são comumente conhecidos dos estudos geopolíticos, como o domínio aéreo, terrestre, naval e espacial. Em paralelo a isto, foi possível reconhecer a importância do desenvolvimento de novas tecnologias e de estratégias para que os estados subdesenvolvidos no domínio cibernético possam se defender da influência das fronteiras demarcadas por Estados predominantes neste meio.

Palavras-chave: Internet. Ciberespaço. Consequências Geopolíticas.

ABSTRACT

THE STRUCTURE AND FUNCTIONING OF THE INTERNET AND ITS GEOPOLITICAL CONSEQUENCES FOR THE STATES

AUTHOR: Luiz Eduardo Martins Spotti
ADVISOR: Major Walfredo Bento Ferreira Neto

The growth of cyberspace, materialized especially by the Internet, the main vector of this medium, is each day more interconnected the structures of states. This is present both through private and governmental means, and makes it of high importance to study the ways in which this medium interferes with the physical world of nations, as well as to understand if there is a monopoly in its control and the geopolitical consequences of these facts. As a way of answering these questions, the main aspects of the functioning of the Internet and its structure, as well as the concepts and geopolitical projections that can be developed in the cyberspace have been observed. Data were collected that relate the American pioneer in the creation of the basic structures of the Internet, through the ARPAnet project, with the control that they currently exert in the decisions that are made in the cyber domain and in the flow of information that travels through it. In this way, it was possible to understand the degree of projection that the geopolitical strategies of a dominant country in the cyberspace area can influence on less developed countries in the technological and telecommunications sectors. Many of these reflect on domains that are already commonly known in geopolitical studies such as the air, land, naval and space domains. At the same time, it has been possible to recognize the importance of developing new technologies and strategies so that underdeveloped states in the cyber domain can defend themselves from the influence of the boundaries demarcated by states predominating in this environment.

Keywords: Internet. Cyberspace. Geopolitical consequences.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA	*Advanced Research Projects Agency* (Agência de Projetos e Pesquisa Avançada)
ARPAnet	*Advanced Research Projects Agency Network* (Rede da Agência de Projetos e Pesquisa Avançada)
GCHQ	*Government Communications Headquarters* (Sede de Comunicações do Governo)
TCP/IP	*Transmission Control Protocol/Internet Protocol* (Protocolo de Controle de Transmissão/Protocolo de Internet)
WAN	*Wide Area Networks* (redes de longa distância)
IANA	*Internet Assigned Numbers Authority* (Autoridade para Atribuição de Números de Internet)
ICANN	*Internet Corporation for Assigned Names and Numbers* (Corporação da Internet para Atribuição de Nomes e Números)
DNS	*Domain Name System* (Sistema de Nomes de Domínio)
CRI's	*Crítical Internet Resources* (Recursos Críticos da Internet)
NSA	*National Security Agency* (Agencia nacional de segurança)
FBI	*Federal Bureau of Investigation* (Departamento Federal de Investigação)

SUMÁRIO

1 INTRODUÇÃO

O ser humano vive em um “mundo do futuro”. Desde o surgimento dos primeiros aparatos tecnológicos até os dias de hoje, vimos nossa sociedade passar por uma constante evolução da tecnologia. A praticidade e o conforto que esta nos proporciona, assim como as oportunidades que nos são oferecidas através da mesma nos tornou, senão por completo, mas em boa parte, dependentes das nossas próprias criações. Hoje, boa parte das informações que buscamos e que circulam sobre nós mesmos estão dentro de uma rede de máquinas conectadas entre si.

A rede mundial de computadores (Internet) é um dos maiores acumuladores de informações da atualidade, que vai desde o individual até o coletivo, contendo informações, tanto de uma pessoa e seu cotidiano como de países ou organizações internacionais e suas atividades. Este campo, conhecido como campo cibernético (o qual envolve redes de computadores como a Internet) se faz tão importante atualmente que chega a ser considerada como uma nova dimensão do estudo geopolítico e da projeção de poder das nações.

Frente a este novo cenário da nossa sociedade, paira sobre nós, então, inúmeras dúvidas sobre esta nova dimensão do mundo moderno, e uma delas é sobre o controle deste espaço/território desconhecido. Seria ele dividido por fronteiras, assim como as outras dimensões espaciais que já conhecemos, onde cada país, através de tratados e influências, exerce seu poder? Ou seria um lugar livre e sem questões que envolvam a unipolaridade, bipolaridade ou multipolaridade de poder, onde qualquer um possa exercer sua influência? E caso mais esta espécie de monopólio exista, qual são suas consequências para outros Estados e atores do sistema internacional? Para chegar a alguma conclusão considerável, primeiro precisamos entender melhor como funciona a rede mundial de computadores, onde se faz presente, como é seu gerenciamento e quais as consequências que o conteúdo que está contido nela pode influenciar no mundo físico que conhecemos, assim como a ligação deste novo domínio às estratégias geopolíticas dos Estados.

Esta pesquisa tem como objetivo entender e levantar estas conclusões de forma coerente e que demonstre qual é a importância que deve ser dada a esta nova dimensão do nosso mundo, considerando quais as consequências para aqueles países que não se fazem presentes neste novo território geopolítico – pelo menos não na forma de controladores. Tudo isso através de um pensamento crítico, que visa entender a existência, ou não, de um órgão, nação ou organização

internacional que exerça influência, controle ou regule de forma a fazer valer seus anseios neste novo ambiente geopolítico.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Entender a estrutura e o funcionamento da internet, se há forma de exercer controle sobre esse recurso e, caso positivo, quais as consequências geopolíticas.

1.1.2 Objetivos específicos

Entender a estrutura e o funcionamento da internet, assim como sua dinâmica espacial/territorial;

Identificar o(s) ator(es) que detém(êm) um possível controle da internet;

Compreender consequências geopolíticas a partir de um possível monopólio ou outra forma de controle da internet para os Estados.

2 REFERENCIAL TEÓRICO

2.1 O CONCEITO DE GEOPOLÍTICA

Geopolítica é uma área da Ciência Política criada pelo professor e cientista político Rudolf Kjellén que estuda a influência das condições geográficas na política adotada pelos Estados (AMAN, 2019). Kjellén via os Estados como fenômenos de espaço e que estão organicamente ligados ao solo o qual se encontram (AMAN, 2019). Partindo deste ponto de vista, surgiram inúmeros conceitos e formas de estudo geopolítico. Muitos destes conceitos criados foram estudados pelos Estados e motivaram, assim como justificaram, as ações dos mesmos.

Com o crescimento da importância do estudo geopolítico, surgiram teorias que separavam e estudavam de forma mais profunda os aspectos geográficos que influenciavam os Estados. Teorias como a do poder marítimo, do norte-americano Alfred Thayer Mahan, a do poder terrestre, do inglês Halford J. Mackinder, e a do poder aéreo, do italiano Giulio Douhet e do russo Alexsander Seversky, dividiram as áreas de estudo e provaram que os Estados que dominavam certas regiões estavam sempre a frente das outras nações.

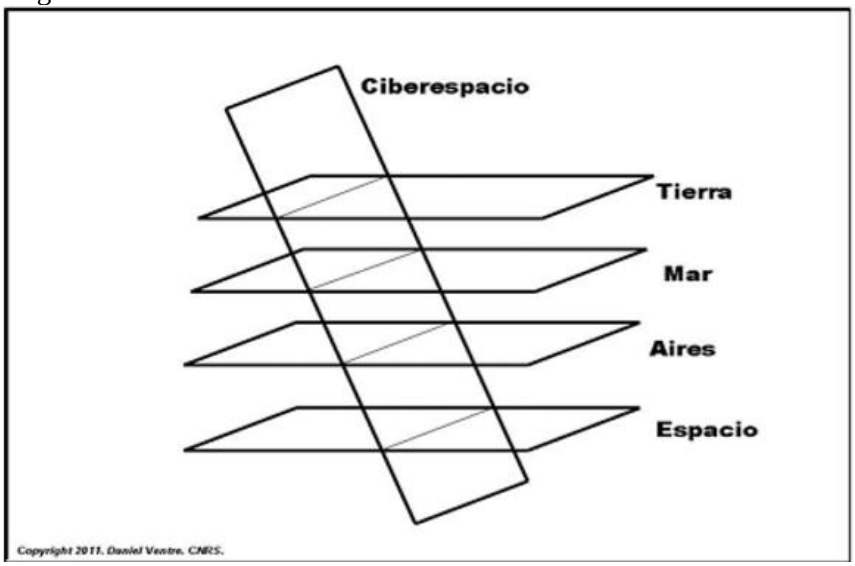
Diversas outras teorias surgiram com o desenvolvimento do tema geopolítica. Todas elas tinham em comum a consequência para os estados do domínio ou influência sobre uma determinada região ou área, sempre levando em consideração a relação entre espaço e poder. Em contrapartida, com o desenvolvimento tecnológico e das sociedades, começaram a surgir inúmeras outras variáveis na “Equação do Poder” para os Estados (AMAN, 2019). O que antes tratava-se somente da geografia física dos territórios, passou a considerar outros aspectos que se assemelham a geografia dos territórios e que possuem equivalente importância.

Novas áreas de estudo surgiram com o desenvolvimento da sociedade, como o do espaço cibernético, o qual agregou importância a computação e as redes de computadores, da mesma forma que a população e a economia dos Estados começaram a ser levadas em consideração de forma equivalente. Com isso, o geógrafo e antropólogo inglês Thomas Griffith Taylor apresenta uma definição indicativa destas novas tendências do estudo geopolítico para as nações, a qual afirma que: “Geopolítica é o estudo dos mais relevantes aspectos da situação e dos recursos de um país, com vistas à determinação de sua posição relativa na política mundial” (AMAN, 2019).

2.1.1 A Geopolítica e o Ciberespaço: Uma nova dimensão de extrema relevância

Hoje o ciberespaço está em toda parte, em todo lugar em que encontramos um computador, um processador, ou um cabo de ligação (FERREIRA NETO, 2014). Desta forma, quando falamos de ciberespaço, consequentemente pensamos na Internet, pois ela é a materialização do ciberespaço em escala global, e que hoje está vinculada na vida de cada um dos indivíduos, empresas e órgãos da sociedade, seja direta ou indiretamente. Ela se faz real quando observamos o tamanho do poder de transversalidade que a internet possui, permitindo a projeção de poder e seus reflexos nos demais domínios espaciais.

Figura 1 – Transversalidade do domínio cibernético



Fonte: VENTRE, (2011) *apud* FERREIRA NETO (2014).

Um ator que controle o ciberespaço, pode influenciar, ainda que indiretamente, todos os outros domínios que já conhecemos. A possibilidade de interromper serviços essenciais à população ou então no ataque a estruturas estratégicas de um estado como o de distribuição de energia elétrica, fornecimento de água, etc., deve ser levado em consideração, afinal, grande parte destes recursos está conectado entre si e possuem saídas e entradas para a rede mundial de computadores. O alcance da internet também é algo que assume proporções globais. O número de usuários que recebem uma informação em questão de minutos é algo jamais visto anteriormente na história da humanidade. Consequentemente, a força para influenciar as decisões de um ou mais grupos de pessoas é considerável, isto que é fortalecido pela credibilidade que a Internet vem obtendo nas novas gerações que já nasceram integradas ao ciberespaço.

Frente a esta projeção, é de interesse dos Estados demonstrar influência no ciberespaço e proteger seus interesses. Alinhar os planos de defesa e traçar metas que envolvam este novo domínio já se faz presente nas condutas adotadas pelos países. Celso Amorim, Ministro de Estado da Defesa do Brasil, em 2012, afirmou:

> O próprio conceito de realidade foi expandido pelo espaço digital. A cibernética emergiu como um novo domínio para a Defesa, e veio somar-se ao mar, à terra, ao ar e ao espaço. Aberto à ação humana, o domínio cibernético abre-se também ao conflito (*apud* FERREIRA NETO, 2014, p. 10).

É com este intuito que uma das ferramentas mais antigas de demonstração de controle e domínio, a fronteira, é usada pelos Estados para influenciarem este ambiente. No espaço cibernético, as fronteiras também se fazem presentes, entretanto, assumem outras formas. Elas devem ser vistas como formas de ponto, seja ele um "nó" de uma infovia ou uma estrutura estratégica selecionada por um Estado (FERREIRA NETO, 2014). Entretanto, a dificuldade de reconhecer uma fronteira neste domínio é imensa. Diferente das fronteiras físicas, o ciberespaço obedece a outras regras, e não considera o território mero substrato físico. Ele é artificial, produto do homem e fruto do nível tecnológico atual (FERREIRA NETO, 2014).

Podemos desta forma, analisar este fator como o que acontece com alguns governos fechados que buscam controlar de forma mais severa a interferência do ciberespaço dentro de seus territórios, com algo que se assemelha a formação de uma "fronteira fechada" ao acesso do ciberespaço pela sua população. Nasce então um embate entre a governança da Internet com a geopolítica regional (PINTO, 2015).

> A China permite que seus habitantes acessem a Internet, porém controla o conteúdo disponível através de filtros de conteúdo na sua arquitetura de governança da Internet local. O acesso ao aplicativo de geolocalização da empresa Google, o Google Maps, não é permitido na China, portanto o governo local redireciona cada tentativa de acesso ao site para um site do governo. O caso da Coreia do Norte é mais extremo, pois a infraestrutura local de acesso à Internet é permitida apenas a poucos funcionários do estado que recebem o conteúdo da Internet pré-selecionado por censores (PINTO, 2015, p.48)

2.2 A INTERNET: ESTRUTURA E FUNCIONAMENTO

Durante o período da Guerra Fria, no qual as informações representavam objetivos de alto valor e a corrida pelo melhor desenvolvimento tecnológico era acirrada, os EUA, buscando

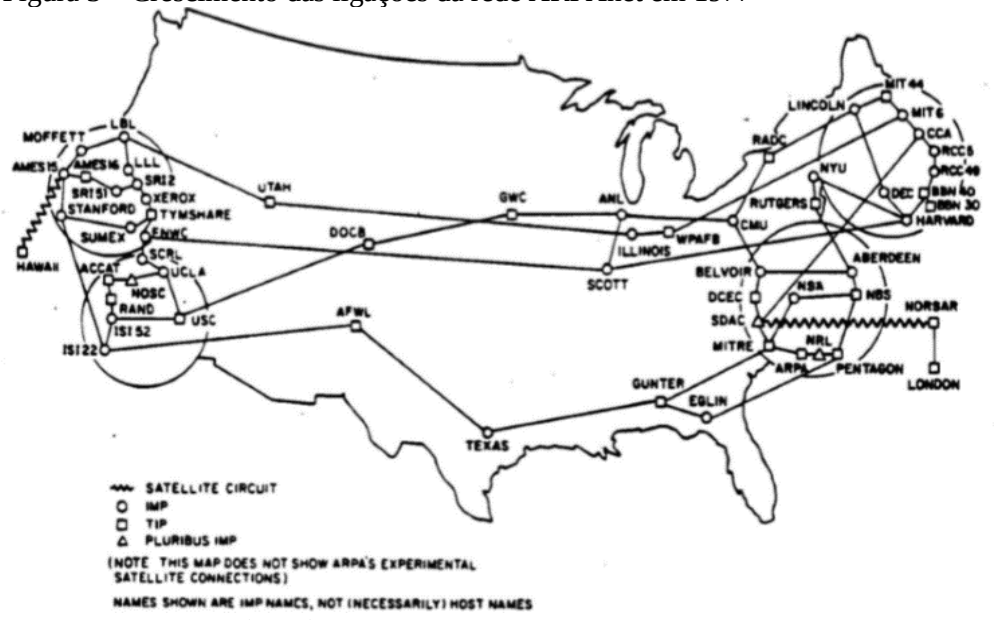
uma rápida troca de informações entre seus grandes centros de pesquisa e a proteção dos seus canais de comunicação, desenvolveu o projeto ARPAnet. Este projeto norte-americano proporcionava que duas redes locais de computadores, distantes uma da outra, conseguissem trocar informações entre si formando uma rede ainda maior chamada WAN, berço do que futuramente se tornaria a internet.

Abaixo podemos observar duas figuras que mostram o crescimento das ligações entre as redes da ARPAnet, do ano de 1969 até 1977:

Figura 2 – Crescimento das ligações da rede ARPAnet em 1969

Fonte: TANCMAN (2008)

Figura 3 – Crescimento das ligações da rede ARPAnet em 1977



Fonte: TANCMAN (2008)

Neste período a ARPA (órgão responsável pelo projeto ARPAnet) operava 3 redes distintas que utilizavam meios distintos (satelital, rádio e cabo). O desafio de interligar estas três redes com características distintas era chamado de Internet e tinha o desafio de criar protocolos (convenções ou padrão que possibilita uma rede reconhecer o conteúdo de outra) e gateways (caminhos padrões para comunicação entre redes) que fossem simultâneas as 3 redes. Esse projeto perdurou por toda a década de 70, culminando na criação do protocolo TCP/IP, este que universalizou as comunicações entre redes e tornou-se algo fundamental para o funcionamento da internet (CARDOSO JUNIOR, 2008).

Com o sucesso deste projeto, e a necessidade e benefícios que a rede poderia oferecer para o meio acadêmico junto com a necessidade de manutenção técnica, os militares norte-americanos dividiram a "internet" em duas partes. Uma das partes recebeu o nome de MILNET, contando com diversas organizações militares em sua composição. A outra parte perpetuou o nome ARPAnet, contando com 45 instituições civis (CARDOSO JUNIOR, 2008). Esta separação criou uma rede exclusiva para o meio civil, o que permitiu maior liberdade neste meio e fomentou o aperfeiçoamento das técnicas usadas para a troca de informações, nascendo consigo inúmeras aplicações comerciais para este novo meio de comunicação.

O surgimento de ferramentas como os provedores de serviços abriu as portas para que os usuários comuns conseguissem fazer parte da grande rede já existente. Os *backbones* (espinha dorsal em tradução direta) surgiram como sendo a grande estrutura que liga grandes redes entre si. É através deles que boa parte da informação que trafega pela internet passa. São os *backbones* que ligam a sua rede local, seja ela do seu bairro ou sua cidade, a uma outra rede local, pertencente a outro país ou continente. Eles utilizam cabos de fibra ótica e possibilitam conexões com velocidades muito altas entre longas distâncias. Desta forma, com a multiplicação dos meios técnicos implementados na rede e com o surgimento de novas redes semelhantes a ARPAnet, que a internet e seu funcionamento, inicialmente algo complexo e de conhecimento de poucos, começou a se simplificar, agregando cada vez mais usuários para o sistema. E assim a rede de computadores, antes local e voltada para a segurança, tornou-se a grande conurbação de redes chamada de internet, hoje utilizada tanto para o lazer quanto para a guerra.

> a Internet não é entidade única, mas uma coleção de redes locais, nacionais, regionais e globais que operam de modo relativamente descentralizado, porém conectados entre si. (LUCERO, 2011, p.35).

As características da internet e oportunidades que ela proporciona tornaram-na um dos maiores meios de globalização do mundo moderno.

> Com a disseminação da Internet em escala universal, é possível acessar e gerar informações a partir do continente Europeu, e armazenar esta mesma informação em tempo real em qualquer ponto do planeta. (PINTO, 2015, p.26)

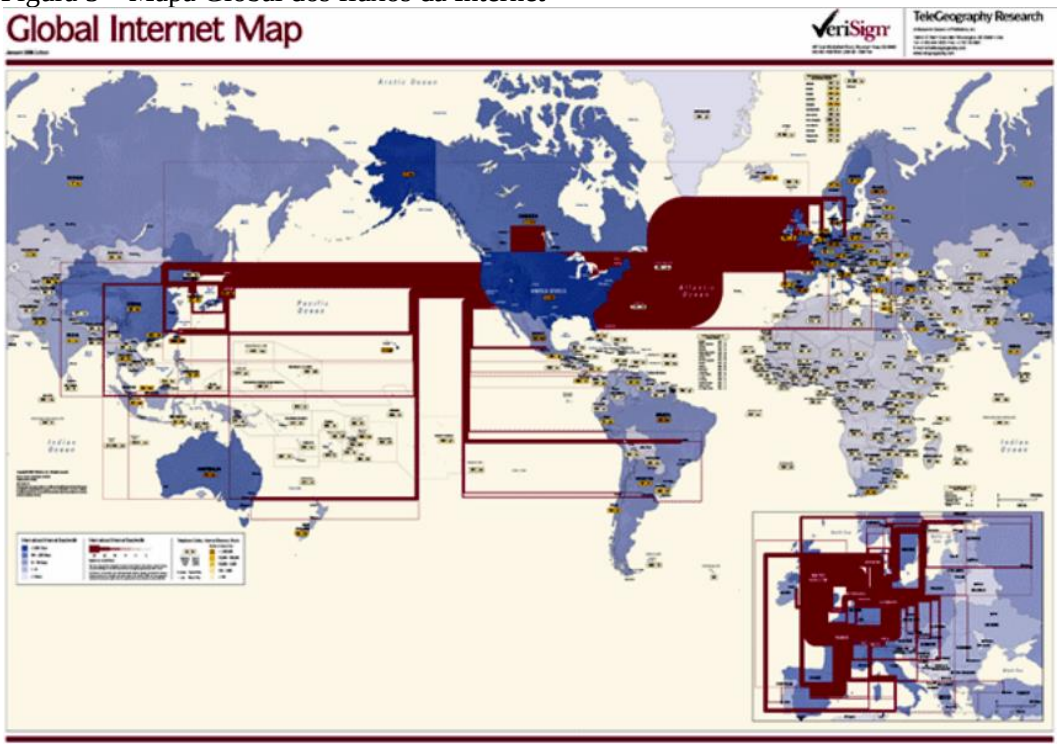
Um usuário comum, para ter acesso a uma informação de seu interesse, precisa somente enviar a solicitação através da sua rede local, chegando ao seu *provedor de acesso* à internet, o qual decide o melhor caminho a ser percorrido para acessar o conteúdo buscado. E, assim, os dados são extraídos do servidor e retornam ao usuário que os solicitou. É isso que acontece a todo momento quando acessamos um site. Enviamos o pedido ao servidor onde os arquivos que compõem o *site* estão armazenados (cores, textos, imagens) e ele nos devolve os arquivos solicitados, apresentando na forma de uma página online. Algo semelhante acontece com nossos dados. Quando cadastramos alguma informação particular ou realizamos ações em determinados sites da internet (*Facebook*, por exemplo, com a ação de curtir, comentar e postar conteúdo), tudo é enviado ao servidor daquela entidade que armazena nossos dados. É desta forma que praticamente todos os passos que realizamos na internet ficam registradas de alguma maneira.

2.3 A GEOGRAFIA DE UM SISTEMA GLOBAL

O acesso a qualquer tipo de informação na internet sempre possui um destino final a ser alcançado. Na maioria dos casos, o nosso destino é um servidor de armazenamento pertencente a um órgão estatal, privado ou internacional, localizado em algum outro país ou continente, assim como vimos anteriormente. São estes servidores que compõem a grande fonte de informações contidas na internet e são objeto de grande parte do valor que ela possui. Em outros casos, o nosso destino pode ser algum computador ou dispositivo específico que desejamos acessar ou então enviar informações. O que realmente importa para nossa observação é que, mesmo que nosso destino seja um servidor ou um dispositivo específico, há um trajeto a ser percorrido, o qual, inevitavelmente, passa por pontos específicos em seu percurso. Como já é de nosso conhecimento, a estrutura responsável por proporcionar este trajeto é nomeada de *backbone*. É ela que é responsável pelo acesso de longas distâncias (entre países e entre continentes) e pelo transporte do maior volume de informações.

É esta vasta estrutura que diminui a separação entre a origem e o destino da informação que deveria tornar a internet um sistema pulverizado globalmente, o que de fato é. Entretanto, analisando o fluxo das informações, vemos que, mesmo tendo a possibilidade de acessar praticamente qualquer lugar do mundo, grande parte do trafego da internet converge para um único local, os EUA. Observando o mapa global dos fluxos da internet do ano de 2007 (figura 5), nos deparamos com a magnitude desta convergência de informações para um único ponto, onde as ligações em vermelho representam os pontos conectados entre países e continentes, assim como o volume de informações trocadas entre as localidades.

Figura 5 – Mapa Global dos fluxos da Internet



Fonte: CARDOSO JUNIOR (2008)

Um dos aspectos que nos leva a entender melhor este evento, é a centralização dos meios de maior valor para a rede. Os maiores e mais importantes servidores da internet, responsáveis por disponibilizar que qualquer usuário digite um domínio de um site e seja redirecionado para o servidor do endereço procurado são os *root zone file*. Eles são constituídos por diversos servidores menores, espalhados globalmente e que juntos formam um grupo de servidores de armazenamento os quais estão sob o controle de um único servidor principal. Esta dispersão global de parte dos servidores não representa sua totalidade. Boa parte deles, assim como os de maior importância, localizam-se centralizados em território norte-americano.

Figura 4 – Localização dos principais servidores raiz da internet

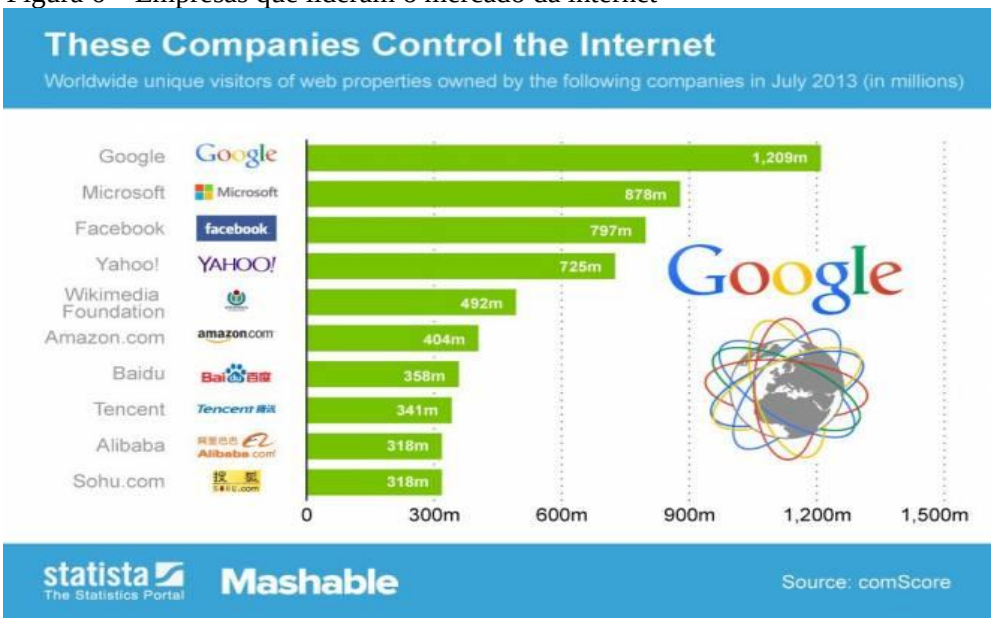
Fonte: TANCMAN (2008)

> Estes servidores centrais são chamados de root zone file (arquivo da zona raiz), eles são administrados pela IANA, instituição controlada pelo ICANN. Esta instituição terceirizou para 12 servidores nos Estados Unidos a tarefa de hospedar estes arquivos, os servidores ficam em instituições norte-americanas. (PINTO, 2015, p. 55).

Esta centralização geográfica com a qual nos deparamos é decorrente dos primórdios do surgimento da internet. Por ter surgido em solo americano, houve um grande pioneirismo por parte deles no desenvolvimento das tecnologias que formaram suas bases, assim como com os órgãos que surgiram para regulamentar o espaço cibernético. A corrida por maior segurança e desenvolvimento tecnológico desencadeada pela Guerra Fria, fez com que o Exército Americano, em cooperação com o setor privado aperfeiçoassem e desenvolvessem novas tecnologias que deram origem as bases do que conhecemos hoje como internet. O protocolo TCP/IP, maior e mais utilizado conjunto de regras que a internet já possuiu e que é utilizado até hoje, foi concebido e aperfeiçoado em solo americano.

Outro aspecto que molda a geografia do espaço cibernético como o conhecemos é que grande parte das maiores empresas de telecomunicações e serviços de internet que lideraram o mercado durante anos, sendo que algumas ainda lideram, surgiram nos EUA. Empresas como Google, Microsoft e Facebook dominam o número de acessos no mundo todo, como podemos observar na imagem abaixo a qual demonstra a quantidade de acessos no ano de 2013.

Figura 6 – Empresas que lideram o mercado da internet



Fonte: STATISTA (2013)

Seis das dez empresas que lideram este gráfico são americanas, sendo que todas elas estão no topo da lista, seguidas por empresas chinesas. Não podemos deixar de observar empresas como a Apple, que com o lançamento de seus computadores, principalmente em 1977 com o Apple II, "cambiaram os princípios de operação de um computador de um ambiente voltado à programação para um voltado ao uso de software, o que passou a permitir que mesmo usuários sem muita especialidade técnica conseguissem fazer uso deles" (RUNDLE, 2014 *apud* DATYSGELD, 2017, p. 38).

2.4 GERENCIAMENTO E REGULAMENTAÇÃO DO ESPAÇO CIBERNÉTICO

2.4.1 ICANN (*Internet Corporation for Assigned Names and Numbers*)

Por ser uma entidade global que se estende a praticamente todos os países, estes que possuem políticas econômicas e sociais das mais diversas, surge a necessidade de organizar e regulamentar todos os assuntos referentes a internet. Assim, foi criando um dos principais organismos responsáveis pelo gerenciamento da internet, chamado de ICANN (*Internet Corporation for Assigned Names and Numbers*). Conforme Michéle Tancman afirma, a ICANN, basicamente, é a instituição que faz a internet funcionar, possuindo uma estrutura baseada e controlada por grandes empresas que a financiam (SILVA, 2008).

> A ICANN (Corporação da Internet para Atribuição de Nomes e Números) é responsável pelo gerenciamento e pela coordenação do DNS (Sistema de Nomes de Domínio) a fim de garantir que cada endereço seja único e que todos os usuários da Internet possam encontrar todos os endereços válidos. Para isso, a ICANN supervisiona a distribuição de endereços IP e nomes de domínio exclusivos. Ela também garante que cada nome de domínio seja associado ao endereço IP correto. A ICANN também é responsável por credenciar registradores de nomes de domínio. (ICANN, 2020)

Ela busca um papel global, agindo como um guardião das livres ações na internet. Para isso, ela tira sua força por ser a única instituição capaz de realizar este controle, além de ter sido apoiada pelo projeto progenitor da internet, a ARPAnet, e pelos Estados Unidos, a maior economia e política do mundo, a qual possuía grande influência sobre ela através do seu Departamento de Comércio (DATYSGELD, 2017). O principal fator que ressalta o poder presente no ICANN é o controle que ele possui sob alguns dos alicerces da internet, os CRI's (*Crítical Internet Resources*), que nada mais são que recursos essenciais para o funcionamento da internet (PINTO, 2015). Para que um usuário consiga acessar a internet, ele depende da alocação e consumo destes recursos essenciais. (PINTO, 2015). Desta forma, a ICANN possui o poder necessário para vetar a existência de algo que considere ilícito na internet.

2.4.2 O setor privado e sua influência

O setor privado, mesmo que sob a fiscalização de órgãos internacionais, possui maior participação na internet. Boa parte dos conteúdos acessados estão hospedados em serviços disponibilizados por empresas privadas, além de que o acesso dos usuários à rede também é provido pelo mesmo. "A governança no espaço digital possui uma estrutura operacional mista, pautada por instituições de caráter privado, orientadas e parcialmente financiadas por instituições públicas" (PINTO, 2015, p.28)."São empresas que providenciam a infraestrutura necessária para uma pessoa acessar a Internet em sua casa, são empresas que hospedam conteúdo na Internet, e são empresas que operam a transmissão de divisas pela Internet" (PINTO, 2015, p.46).

Em posse de todo este poder, o setor privado não fica restrito somente a disponibilização de serviços e monitoramento de ações no meio cibernético. Elas participam ativamente da governança da internet, seja em prol de seus objetivos, seja de objetivos de governos ou Estados. Na maioria dos casos, participam de eventos políticos e econômicos e acabam por serem peças chaves para as ações executadas neste ambiente (PINTO, 2015). Associado a este controle que

se encontra centralizado no setor, elas possuem a liberdade de diferente dos órgãos internacionais, não estarem totalmente sujeitas às regras internacionais. Um grande exemplo foi a empresa *Amazon Web Services*:

> Corporações privadas cortaram serviços do WikiLeaks depois de eles divulgarem informações sensíveis sobre a diplomacia internacional. A Amazon Web Services, empresa responsável pelo armazenamento de conteúdo na Internet, retirou do ar o site do WikiLeaks alegando que eles haviam descumprido seus termos de serviço. (PINTO, 2015, p. 46).

Mesmo que haja regras para controlar este setor quanto as suas ações, privacidade da informação dos usuários e o seu uso indevido, ficamos dependentes da ética aplicada pelas empresas quanto ao gerenciamento da informação de seus usuários. É uma forma não muito confortável de dependência que, infelizmente, o usuário comum precisa se submeter para conseguir o acesso a rede de internet.

2.5 A PROJEÇÃO DE PODER ATRAVÉS DA INTERNET

A internet, diferente da geografia dos territórios formada a partir de espaços geográficos naturais, não possui fronteiras bem delimitadas, eis que é artificial e na forma de um espaço-rede, o que lhe proporciona capilaridade que se estende por praticamente todo o mundo, assim como vimos anteriormente. Desta forma, diversos Estados veem este instrumento como um meio de aumentar sua influência global, muitas vezes interferindo diretamente em outros países sem se fazerem presentes fisicamente. Essa influência é facilitada aos Estados que possuem maior controle sobre os mecanismos da internet, os quais utilizam de meios, muitas vezes ilícitos, para influenciar outras sociedades. A influência projetada no mundo virtual, cibernético, culmina em resultados reais que afetam o mundo físico, assim como Denardis explica:

> a arquitetura técnica da Internet abarca decisões de projeto que moldam a estrutura social e econômica, de liberdades individuais a políticas públicas de inovação. Sobre o controle através dos artefatos (DENARDIS, 2014, p. 7 *apud* PINTO, 2015, p. 45)

Muitos meios são utilizados para exercer esta influência de forma a aumentar as fronteiras de poder dos estados neste mundo cibernético. Em sua maioria, são controlados pelo setor privado, este que, apesar de ser independente em muitos aspectos e um dos maiores meios

influenciadores, sucede-se a manipulações dos Estados. Muitos governos, para regular a internet sem se submeter ao processo burocrático, utilizam dos intermediários privados o que lhes concede novas formas de exercitar o seu poder sobre o fluxo da informação, na maioria dos casos, sem precisar exercer a devida transparência ou prestação de contas à sociedade (DENARDIS, 2014, p.7, *apud* PINTO, 2015).

É desta forma que as barreiras físicas que anteriormente eram decisivas nas ações de um estado, acabam por perderem sua força. Dados fisiográficos, psicossociais, políticos, econômicos, militares, científicos e tecnológicos podem ser descobertos e até mesmo alterados ou influenciados em questões de minutos interferindo na equação do poder de determinado Estado. Tudo isso pode ser feito de um simples escritório localizado a quilômetros de distância do local onde os dados estão contidos, sem movimentar grandes grupos de pessoas ou qualquer tipo de suspeita.

2.5.1 Snowden e o governo americano

No ano de 2013 o mundo pode mensurar o tamanho da influência que um país pioneiro nas tecnologias de telecomunicações pode exercer. Edward Snowden, antigo membro da NSA, órgão americano responsável pelo levantamento de informações nas áreas de telecomunicações, cibernética e sinais, divulgou diversos documentos sigilosos das ações dos Estado Unidos em conjunto com a Inglaterra na área de espionagem. Através de grandes jornais europeus e americanos, ele trouxe à tona o modo como alguns dos programas de vigilância são usados pelos Estados Unidos para espionar alvos, utilizando servidores de empresas privadas como o Google, Apple e Facebook, além de outros meios (ESPIONAGEM CIBERNÉTICA, 2014).

> Em conjunto com o GCHQ, a NSA tinha ligado secretamente interceptadores de dados aos cabos de fibra ótica submarinos que circundam o globo. Isso permitiu que os EUA e o Reino Unido tivessem acesso à maior parte das comunicações mundiais. Tribunais secretos convenciam empresas de telecomunicações a entregar seus dados. Mais que isso: praticamente todo o Vale do Silício estava envolvido com a NSA, disse Snowden. Google, Microsoft, Facebook, até mesmo a Apple, de Steve Jobs. A NSA alegava ter "acesso direto" aos servidores das gigantes da tecnologia. (HARDING, 2014, p. 9)

A comunidade de inteligência dos Estados Unidos escondia a verdade sobre suas atividades enquanto violava a constituição do EUA, assim como o direito à privacidade dos indivíduos. Haviam colocado até mesmo *backdoors* secretas em *softwares* de criptografia *on-line* – usados para garantir a segurança de transações bancárias –, enfraquecendo o sistema para

todos e abrindo brechas para possíveis coletas de informações a seu favor (HARDING, 2014, p. 9). Seu poder de acesso à informação era tão grande que se projetava de forma muito precisa ao redor de todo o mundo, assim como cita o trecho do livro de Luke Harding:

> A NSA pode interceptar fotos e mensagens de voz. Pode hackear Facebook, Google Earth e Yahoo Messenger. Particularmente úteis são os dados de geolocalização, que apontam onde um alvo esteve e quando. A agência recolhe bilhões de registros diariamente mostrando a localização de usuários de telefonia móvel em todo o mundo. (HARDING, 2014, p. 103)

Os alvos da espionagem da NSA iam muito além de seus inimigos mais comuns, como a Al-Qaeda ou outros grupos terroristas. Sua vigilância se estendia entre seus supostos aliados (França, Alemanha) e também monitoravam as comunicações de milhões de cidadãos norte-americanos (HARDING, 2014, p. 6). Figuras políticas e órgãos estatais de ao menos oito países foram alvo da espionagem, entre eles o Brasil. E-mails da então presidente Dilma Russeff destinados a seus assessores foram interceptados usando servidores de e-mail da empresa Google. Ministérios como o de Minas e Energia e a Petrobras também foram alvos de planos da NSA (ESPIONAGEM CIBERNÉTICA, 2014).

Em sua defesa, o governo americano afirmou que as informações coletadas foram somente os *metadados*, algo como hora, remetente e destinatário das mensagens, e não o conteúdo propriamente dito. Afirmaram também que o único objetivo para o controle destas informações é a prevenção de ataques terroristas como o ocorrido em onze de setembro de 2001, entretanto, ainda assim se caracteriza como quebra do sigilo de informações pessoais (PILATI; OLIVO, 2014).

2.5.2 Rússia e as eleições americanas

Durante as eleições de 2016 nos Estados Unidos, ano da candidatura do atual presidente americano Donald Trump, um dos acontecimentos que mais movimentou o cenário político da época foi o vazamento de *e-mails* confidenciais da campanha de Hillary Clinton, principal opositora de Donald Trump. As informações coletadas foram a público através de *sites* como o WikiLeaks, comumente utilizado para postagens de informações vazadas sobre governos ou órgãos internacionais. O FBI, junto com o Departamento de Segurança Interna americano, acusou o governo russo de trabalhar ao lado de Donald Trump para derrubar a popularidade da candidata Hillary Clinton, sua principal opositora, através da divulgação de informações sigilosas sobre sua campanha (GAZETA DO POVO, 2016).

Supostamente os ataques de *hackers* sob o comando do governo russo, teriam como objetivo roubar contas de usuários do partido democrata usando técnicas que simulam as áreas de login de aplicativos e sites usados pelas vítimas. Desta forma, o *hacker*, após obter a senha e login do atacado, poderia acessar livremente o seu conteúdo pessoal. Supostamente, foi desta forma que o governo russo, em apoio ao então candidato à presidência Donald Trump, levaram a público informações sigilosas sobre a campanha da principal concorrente de Trump, diminuindo sua popularidade entre os eleitores e prejudicando sua campanha.

As reais intenções dos ataques, assim como o envolvimento do presidente russo Vladmir Putin, ainda não foram comprovadas. Entretanto os ataques ocorreram e acabaram por influenciar, direta ou indiretamente, no resultado das eleições presidências do ano de 2016 nos EUA (GAZETA DO POVO, 2016). Observando através da ótica geopolítica deste caso, temos claramente não só o levantamento de informações do fator político do país, mas sim uma direta interferência no mesmo.

2.5.3 Notpetya: Rússia e Ucrânia

Em 2017, um mês após um dos ataques cibernéticos mais notáveis realizado por um *ransonware* conhecido como *WannaCry* (vontade de chorar, em tradução direta), este que afetou diversos países no mundo, chegou a vez da Ucrânia ser o alvo. *NotPetya*, como ficou conhecido, foi um *ransonware* que afetou diversos computadores, comprometendo o sistema financeiro da Ucrânia consideravelmente. O governo americano, através da CIA, atribuiu o ataque realizado aos *hackers* militares da Rússia com o objetivo de enfraquecer a guerra contra os separatistas. "A CIA atribuiu aos hackers militares russos um ataque cibernético que paralisou computadores na Ucrânia no ano passado, um esforço para interromper o sistema financeiro daquele país em meio à guerra em andamento com separatistas leais ao Kremlin[1]" (NAKASHIMA, 2018).

A principal técnica usada para propagar o vírus foi a infecção de *sites* comumente usados pelos alvos, no caso em questão a população da Ucrânia. A máquina, uma vez infectada, tinha todo o seu disco rígido criptografado impedindo o acesso a qualquer tipo de informação contida nele. Logo após criptografar o sistema, o vírus solicitava um pagamento semelhante a um resgate, o qual prometia liberar os dados criptografados após o pagamento. Um tempo depois

[1] *The CIA has attributed to Russian military hackers a cyberattack that crippled computers in Ukraine last year, an effort to disrupt that country's financial system amid its ongoing war with separatists loyal to the Kremlin* (NAKASHIMA, 2018).

do ataque estar em andamento, técnicos especialistas em segurança de redes descobriram que a promessa de resgate era falsa e o único objetivo do vírus era destruir completamente as informações contidas nos dispositivos infectados (NAKASHIMA, 2018). A infecção pelo vírus foi reconhecida em computadores de países como Estados Unidos, Índia e Dinamarca, causa provável devido à rápida propagação de um *ransonware*, entretanto o país mais afetado foi a Ucrânia. Estima-se que os danos causados pelo vírus chegam a aproximadamente 10 milhões de dólares e o setor mais afetado foi o farmacêutico.

3 REFERENCIAL METODOLÓGICO

3.1 TIPO DE PESQUISA

Foi realizada uma pesquisa bibliográfica buscando coletar informações pertinentes ao assunto para descobrir se há um domínio unilateral da internet por parte de algum Estado ou organização, dando ênfase nas consequências geopolíticas deste domínio para a comunidade global. Desta forma, diversos fatos, temas e conceitos teóricos foram abordados para facilitar ao leitor o entendimento da dinâmica do espaço cibernético, assim como dos conceitos geopolíticos envolvidos.

3.2 MÉTODOS

3.2.1 Levantamento de dados

Foram levantados dados para entender a estrutura da internet, assim como os organismos que a administram, sempre buscando compreender uma possível unilateralidade em seu sistema de administração e controle de seus recursos, assim com as consequências destas afirmações. 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 RESULTADOS E DISCUSSÃO

Apesar da internet ser um sistema global e que pode ser utilizado por todos, ainda assim vemos resquícios consideráveis de unilateralidade em seu controle e gerenciamento. Remontado dos primórdios de sua criação, a internet ainda carrega muitos traços do controle do EUA em sua estrutura, o qual vem sido acompanhado sequencialmente pelo grande crescimento da CHINA neste cenário. Seu desenvolvimento foi dado em paralelo aos mecanismos que a fazem funcionar, movimentando o mercado americano para a área, assim como a pesquisa e desenvolvimento tecnológico na mesma. Rapidamente a internet se espalhou por todo o mundo, dando o acesso de milhões de usuários a rede, entretanto, assim como as raízes de uma árvore que se dispersam ao solo, sempre há um ponto de partida que acaba por se tornar mais forte. Foi isso que aconteceu com o estado norte-americano, tendo como ponto de partida o projeto ARPAnet.

O desenvolvimento do mecanismo que é a internet foi ocorrendo, de certa forma desordenado no aspecto de planejamento de longo prazo, principalmente em países menos desenvolvidos tecnologicamente. Este rápido crescimento foi se embasando em estruturas preestabelecidas que estavam e ainda estão sobre o controle majoritário dos EUA. O crescimento e controle das empresas sobre as informações dos usuários cresceu de forma exponencial, sem que boa parte da grande massa utilizadora da internet notasse. Desta forma, mesmo sem o conhecimento por parte dos usuários sobre o trajeto que suas informações desenvolvem, assim como onde são armazenadas, grande parte dos dados acabam por convergir para terras norte-americanas ou para entidades as quais estão sobre sua influência.

Empresas privadas dos EUA representam, hoje, grandes reguladores da internet e, apesar da China possuir uma considerável participação no setor privado base da internet, os EUA ainda estão na liderança. As maiores empresas que hoje são líderes no setor surgiram em suas terras. São estas empresas que armazenam e gerenciam o maior tesouro que a internet possui. São milhões de *terabytes* em informações de inúmeros lugares, pessoas, empresas e órgãos do mundo todo concentrados sob o alcance de poucas empresas subordinadas a um único Estado. Empresas estas, que podem, assim como já foram em tempos anteriores, vinculadas e usadas como ferramentas governamentais para se obter um resultado geopolítico para o país.

Quando quebrado os preceitos éticos do sigilo das informações de seus usuários, as grandes empresas, em posse deste vasto número de informações, podem desencadear ações que rastreiam, monitoram, reconhecem lugares e indivíduos de formas que nem mesmo as mentes mais criativas conseguiriam imaginar. Tudo isso, realizado de forma passiva e com a própria

iniciativa do usuário que, muitas vezes, opta por aceitar as condições impostas pelas grandes corporações em troca de seus serviços.

A submissão e vulnerabilidade dos países que carecem do setor tecnológico, assim como a dos usuários desinformados é uma realidade global. Semelhante a visão geopolítica mais clássica, onde países maiores tendiam a se expandir e subjugar países menores, o expansionismo de um Estado no domínio cibernético torna nações menores suscetíveis as estratégias geopolíticas dos estados dominantes, as quais, historicamente, objetivam o crescimento e o expansionismo de suas nações. Os Estados Unidos como principal ator do espaço cibernético, possui a capacidade de influenciar nos domínios do ar, da terra, do mar e até mesmo no espacial de outros estados, resultado do grande expansionismo das suas fronteiras cibernéticas ao longo dos anos. Hoje, um ataque cibernético realizado por uma pequena força tarefa de *hackers* pode simplesmente destruir setores como o da saúde ou bancário de uma país sem deixar rastros, colocar as vidas de quem ataca em risco ou até mesmo ser identificado, retardando o crescimento e deixando reflexos profundos na estrutura do seu alvo.

5 CONSIDERAÇÕES FINAIS

O controle unilateral americano é um fato que não temos como contestar. Apesar da China representar um forte oponente ao estado norte-americano, ainda assim o país é o grande centro do desenvolvimento tecnológico e estrutural da internet. O poder que está sob suas mãos é algo que deve ser considerado sensivelmente e precisa ser dissolvido perante a um meio global e multilateral como a internet. Cabe aos países com menor expressão no teatro internacional prepararem-se de formas que descentralizem o poder que está sob o controle dos EUA, diminuindo a volatilidade presente neste meio e igualando as forças que controlam o espaço cibernético.

Investimentos em cibersegurança, assim como em tecnologias avançadas e preparo de pessoal, tanto no setor privado, quanto no setor estatal, para enfrentar os problemas do mundo cibernético são a chave para que não tenhamos uma rede monopolizada. É preciso interromper o ciclo que gera essa dependência entre os usuários, tornando pequenos Estados mais autossuficientes e preparando-os para enfrentar os futuros problemas que um mundo cibernético incerto proporcionam. Com o maior entendimento por parte dos Estados e, principalmente, dos indivíduos sobre as mudanças do mundo em que estão inseridos é que serão atingidos os verdadeiros níveis de globalização. Não somente a globalização do acesso à informação, a cultura e aos territórios, mas também ao processo decisório de grandes atividades que influenciam a todos.

É através de formas bem simples que ensinamos os usuários a protegerem suas informações, começando no ensino básico, chegando até ao desenvolvimento de projetos de governo que objetivem maior influência neste ambiente. Somente desta forma, a unipolaridade resultante da dependência de um único vetor de tecnologia será amenizada, fazendo assim com que países menores não estejam vulneráveis as estratégias geopolíticas de um único Estado. É compreendendo e aceitando este espaço de estudo que se faz presente no mundo atual, que conseguiremos atuar cada vez melhor nas estratégias de defesa e segurança, enfrentando os novos obstáculos que um mundo tecnológico e cibernético apresenta, mantendo a soberania de nossas terras e de nosso povo, através de vitorias neste novo campo de batalha que nos é apresentado.

REFERÊNCIAS

BBC BRASIL. **Por que os serviços de inteligência dos EUA acham que a Rússia interferiu na eleição de Trump.** 2017. Disponível em: <https://www.bbc.com/portuguese/internacional-38525951>. Acesso em: 28 fev. 2020

CARDOSO JUNIOR, Amadeu. **A dimensão geográfica da Internet no Brasil e no Mundo.** 2008. 255 f. Dissertação (Mestrado) - Curso de Pós- Graduação em Geografia Humana, Departamento de Geografia da Faculdade de Filosofia, Universidade de São Paulo, São Paulo, 2008.

DATYSGELD, Mark William. **O papel da Governança da Internet dentro da Governança Global: Um estudo de caso da ICANN.** 2017. 156 f. Dissertação (Mestrado) - Curso de Pós-graduação em Relações Internacionais, Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo, 2017.

EM DISCUSSÃO**, Espionagem Cibernética: Rede Vulnerável.** Brasília: SEEP, n. 21, jul. 2014.

FELIX RICHTER. **These Companies Control the Internet.** 2013. Disponível em: https://www.statista.com/chart/1573/top-10-web-properties/. Acesso em: 03 mar. 2020.

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.

GATTO, Raquel Fortes. **O impacto da Governança da Internet sob o prisma da Soberania.** 2008. 139 f. Dissertação (Mestrado) - Curso de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2008.

GAZETA DO POVO. **Como a Rússia influenciou o resultado das eleições americanas, segundo os EUA.** 2016. Disponível em: <https://www.gazetadopovo.com.br/mundo/como-a-russia-influenciou-o-resultado-das-eleicoes-americanas-segundo-os-eua-bzgv5aa32wypd2czs1rzcvj5s/>. Acesso em: 28 fev. 2020.

HARDING, Luke. **Os Arquivos Snowden: A história secreta do homem mais procurado do mundo.** 246. ed. Rio de Janeiro: LeYa, 2014.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. **Sobre a ICANN** 2020. Disponível em: <http://icannlac.org/PO/sobre-ICANN>. Acesso em: 28 fev. 2020.

LEITE, Olga Fernandes de Moura. **Os limites do Direito de Privacidade na Sociedade de Informação no Âmbito Contratual.** 2018. 206 f. Dissertação (Mestrado) - Curso de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2018.

LUCERO, Everton. **Governança da Internet**: Aspectos da formação de um Regime Global e Oportunidades para a Ação Diplomática. Brasília: Fundação Alexandre de Gusmão, 2011, ISBN 978.85.7631.300-7.

MAZZEO, Luzia Maria. **Evolução da Internet no Brasil e no Mundo.** Rio de Janeiro: Editora da Faeterj-rio, 2000. Disponível em: https://www.faeterj-rio.edu.br/downloads/bbv/0032.pdf. Acesso em: 03 mar. 20202.

MELO, Paulo Roberto de Sousa; GUTIERREZ, Regina Maria Vinhais. **A Internet e os Provedores de Acesso**. Bnds Setorial. Rio de Janeiro, p. 115-172. set. 1999. Disponível em: <https://www.bndes.gov.br/SiteBNDES/bndes/bndes_pt/Galerias/Convivencia/Publicacoes/Consulta_Expressa/Setor/Complexo_Eletronico/199910_4.html>. Acesso em: 28 fev. 2020.

MORAIS, Carlos Tadeu Queiroz de; LIMA, José Valdeni de; FRANCO, Sérgio R. K.. **Conceitos sobre Internet e Web.** 2012. 112 f. Curso de Série Educação A Distância, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2012, ISBN 978-85-386-0159-3

NAKASHIMA, E. National Security. **Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes**, Washington, 12 janeiro 2018.

OLIVEIRA, Maria Engel de. **ORKUT: O Impacto da Realidade da Infidelidade Virtual.** 2007. 103 f. Dissertação (Mestrado) - Curso de Pós-graduação de Psicologia, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

PILATI, José Isaac; OLIVO, Mikhail Vieira Cancelier de. Um novo olhar sobre o Direito à privacidade: Caso Snowden e Pós-modernidade jurídica. **Seqüência**: Estudos Jurídicos e Políticos, [s.l.], v. 35, n. 69, p.281-300, 17 dez. 2014. Universidade Federal de Santa Catarina (UFSC). http://dx.doi.org/10.5007/2177-7055.2014v35n69p281

PINTO, Marcel Arins. **A estrutura da liderança norte-americana no espaço digital e na internet.** 2015. 102 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação em Relações Internacionais, Universidade Federal de Santa Catarina, Florianópolis, 2015.

PORTELA, Lucas Soares. Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle. **Revista Brasileira de Estudos de Defesa**, [s.l.], v. 5, n. 1, p.141-165, 2 abr. 2019. Associacao Brasileira de Estudos de Defesa - ABED. http://dx.doi.org/10.26792/rbed.v5n1.2018.75081.

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

ROBERTO FRANCISCATTO. **Redes de Computadores.** Santa Maria: Editora da UFSM, 2014. 116p.

SANTOS, Lucas Vicente Romero Rodrigues Frias dos. **RESPONSABILIDADE CIVIL DOS PROVEDORES DE INTERNET PELO CONTEÚDO GERADO POR TERCEIRO.** 2015. 183 f. Dissertação (Mestrado) - Curso de Direito Civil, Pontifícia Universidade Católica de São Paulo, São Paulo, 2015.

SILVA, Michéle Tancman Candido da. **A GEOPOLÍTICA DA REDE E GOVERNANÇA GLOBAL DA INTERNET A PARTIR DA CÚPULA MUNDIAL SOBRE A SOCIEDADE DA INFORMAÇÃO.** 2008. 307 f. Tese (Doutorado) - Curso de Filosofia, Universidade de São Paulo, São Paulo, 2008.

GLOSSÁRIO

Backbone – Ligações centrais de um sistema de rede de larga escala. Constitui a rede central onde a maioria do tráfego de internet circula entre países e continentes.

***Backdoors* –** Pequenas brechas quase imperceptíveis deixadas nas configurações de um dispositivo ou deu um sistema com o intuito de burlar alguma espécie de monitoramento ou de segurança**.**

***Cluster* -** Arquitetura de sistema capaz combinar vários computadores para trabalharem em conjunto.

Divisas – São cheques, ordens de pagamento, moedas de origem estrangeira.

Espaço Cibernético – Remete a um espaço virtual composto por dispositivos eletrônicos que possuem acesso a uma rede comum entre eles.

Hacker – Indivíduo com grande conhecimento em Tecnologia da Informação e Cibernética que se dedica ao conhecimento de aspectos internos de dispositivos, *softwares* e redes, normalmente com grande conhecimento em violação de sistemas e dispositivos.

Provedor de Acesso – Organização que oferece o acesso, utilização ou participação no sistema de internet.

Rede - Computadores interligados por um único meio de transmissão, que é compartilhado por todos, normalmente um cabo.

***Ransomware* -** *Software* malicioso (vírus) que, quando instalado no computador ou dispositivo, bloqueia os dados através de criptografia. Normalmente é cobrado um valor ao proprietário do dispositivo para que seus arquivos sejam recuperados.

Servidor - Computadores de grande porte que armazenam arquivos, informações e disponibilizam serviços de internet.

Software - Conjunto de componentes lógicos de um computador ou sistema de processamento de dados.

Terabytes – Unidade de medidas usada para contabilizar a quantidade de informação virtual armazenada em um dispositivo físico. Em sua contagem, um *terabyte* representa 1.024 *giabytes*, representando uma grande quantidade de espaço de armazenamento de informações.