UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

BERNARDO LOBO VINHAS

O CIBERESPAÇO E A DINÂMICA INTERNACIONAL: A INSERÇÃO BRASILEIRA E SEUS OBSTÁCULOS

Porto Alegre
2014

BERNARDO LOBO VINHAS

O CIBERESPAÇO E A DINÂMICA INTERNACIONAL: A INSERÇÃO BRASILEIRA E SEUS OBSTÁCULOS

Trabalho de Conclusão submetido ao Curso de Graduação em Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.

Orientador: Prof. Dr. Carlos Schmidt Arturi

Porto Alegre

2014

BERNARDO LOBO VINHAS

O CIBERESPAÇO E A DINÂMICA INTERNACIONAL: A INSERÇÃO BRASILEIRA E SEUS OBSTÁCULOS

Trabalho de conclusão submetido ao Curso de Graduação Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.

Aprovada em: Porto Alegre, 18 de dezembro de 2014.

BANCA EXAMINADORA:

Prof. Dr. Carlos Schmidt Arturi – Orientador
UFRGS

Prof. Dr. Marco Aurélio Chaves Cepik - Examinador
UFRGS

Prof. Dr. Érico Esteves Duarte - Examinador
UFRGS

AGRADECIMENTOS

Agradeço aqui aos meus pais, por me terem proporcionado todas as ferramentas para aproveitar as oportunidades que na vida surgem. Aos meus irmãos, Otávio e Isabela, por transformarem o processo de realização deste trabalho em algo mais agradável e descontraído.

Ao professor Carlos Arturi, pela grande atenção, disponibilidade e paciência no acompanhamento do trabalho, sempre com as recomendações mais sábias e proveitosas. À Universidade Federal do Rio Grande do Sul e seus professores, sem os quais eu não teria formação de tamanha qualidade, além de não conhecer pessoas que hoje são tão importantes para mim.

Aos meus amigos de colégio, pelo apoio e camaradagem, pois os que perduram são os que realmente valem a pena. Aos que perduram da faculdade também: Bruno, Txai, Luíza, Eduardo, Laura e Matheus. Ao Pedro, pela amizade inestimável e pelas inúmeras sugestões que tornaram compreensíveis coisas que não passariam adiante do esboço desse trabalho. À Giovanna, à Mariana e à Isadora, pela assistência e companheirismo ao longo da feitura de nossas pesquisas e leituras. Enfim, a todos aqueles envolvidos em minha formação acadêmica e pessoal nos últimos anos, dos quais levo, de cada um, um pedaço nas linhas aqui escritas.

[…] *Distant ARPA spurred us in our quest*
And for our part we worked and put to test
New thoughts and theories of computing art;

We deemed it science not, but made a start.
Each time a new machine was built and sold,
We'd add it to our list of needs and told
Our source of funds "Alas! Our knowledge loom
Will halt 'til it's in our computer room."

Even ARPA with its vast resources
Could not buy us all new teams of horses
Every year with which to run the race.
Not even ARPA could keep up that pace!

But, could these new resources not be shared?
Let links be built; machines and men be paired!
Let distance be no barrier! They set
That goal: design and built the ARPANET! […]

- "Requiem for the ARPANET", Vinton G. Cerf

RESUMO

O Brasil, baseado em uma política externa soberana e ativa, tornou-se um ator muito importante no debate político atual sobre o ciberespaço. Nesses termos, medidas de securitização interna mostram-se necessárias e importantes para a ascensão internacional do país de maneira sólida e duradoura. Assim, pontualmente, este trabalho visa analisar como se dá o debate e a promoção dos interesses brasileiros acerca, principalmente, da Internet no cenário internacional e o sincrônico investimento na construção de capacidades cibernéticas e de segurança de suas infraestruturas críticas. Assim, este trabalho objetiva examinar o crescimento do Brasil como ator internacional relevante acerca do tema da segurança no ciberespaço e na Internet, concomitantemente com o desenvolvimento de capacidades cibernéticas para a cibersegurança em âmbito nacional. A compreensão das dinâmicas de ciberpoder se mostra importante para o entendimento das disputas globais e da relação entre a política externa brasileira assertiva e as ações concretas para embasamento de uma escalada contínua do país no cenário internacional. Metodologicamente, o trabalho é realizado por meio da análise de documentos oficiais, discursos e notícias relacionadas ao tema, além da revisão bibliográfica selecionada.

Palavras-chave: Brasil. Ciberespaço. Cibersegurança. Política Externa. Internet.

ABSTRACT

Brazil, based on a sovereign and active foreign policy, has become a very important player in the current political debate about cyberspace. Regarding to this, internal securitization measures appear to be necessary and important for the rise of the country in a solid and lasting way. Thus, particularly, this study aims to analyze in which way occurs the debate and promotion of Brazilian interests, mainly about the Internet, in the international arena and simultaneously the investment in the construction of cyber capabilities and security of their critical infrastructure. In that sense, this study aims to examine the growth of Brazil as an important international actor on the subject of safety in cyberspace and the Internet, concurrently with the development of cyber capabilities for cyber security at the national level. Therefore, considering the dynamics of cyber power is important to the understanding of global disputes and the relationship between the assertive Brazilian foreign policy and concrete actions to the support of a continued escalation in the international arena. Methodologically, the work is carried out through the analysis of official documents, speeches and news related to the subject, in addition to selected literature review.

Keywords: Brazil. Cyberspace. Cybersecurity. Foreign Policy. Internet.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

APF	– Administração Pública Federal
ARPA	– *Advanced Research Projects Agency*
ARPANET	– *Advanced Research Projects Agency Network*
BBC	– *British Broadcasting Corporation*
BRICS	– Brasil, Rússia, China e África do Sul
CDCiber	– Centro de Defesa Cibernética
CDN	– Conselho de Defesa Nacional
CGI	– Comitê Gestor da Internet
DDN	– *Defense Data Network*
DDoS	– *Distributed Denial of Service*
DNS	– *Domain Name System*
DoD	– *Departament of Defense*
EB	– Exército Brasileiro
END	– Estratégia Nacional de Defesa
EUA	– Estados Unidos da América
EY Brasil	– Ernest & Young Brasil
FTP	– *File Transfer Protocol*
FY	– *Federal Year (Budget)*
GAC	– *Governmental Advisory Committee*
GSI/PR	– Gabinete de Segurança Institucional da Presidência da República
HTTP	– *Transfer Protocol*
IANA	– *Internet Assigned Numbers Authority*
ICANN	– *Internet Corporation for Assigned Numbers and Names*
IGF	– Fórum de Governança da Internet
IISS	– *International Institute for Strategic Studies*
IP	– *Internet Protocol*
IPTO	– *Information Processing Techniques Office*
ISOC	– *Internet Society*
ISP	– *Internet Service Providers*
LAN	– *Local Area Network*
LOA	– Lei Orçamentária Anual
MD	– Ministério da Defesa

MILNET – *Military Network*
NASA – *National Aeronautics and Space Administration*
NFA – *National Futures Association*
NSA – *National Security Agency*
NSFNET – *National Science Foundation Network*
NTIA – *National Telecomunications and Information Agency*
NU CDCiber – Núcleo do Centro de Defesa Cibernética
ONU – Organização das Nações Unidas
P&D – Pesquisa e Desenvolvimento
PLOA – Projeto de Lei Orçamentária Anual
PND – Política Nacional de Defesa
PTT – Ponto de Troca de Tráfego
SCADA – *Supervisory Control and Data Acquisition*
SMTP – *Simple Mail Transfer Protocol*
TCP – *Transmission Control Protocol*
TCP/IP – *Transmission Control Protocol*/*Internet Protocol*
TI – Tecnologia da Informação
TIC – Tecnologia da Informação e Comunicação
TIP – *Terminal Interface Processor*
UIT – União Internacional de Telecomunicações
UNESCO – *United Nations Educational, Scientific and Cultural Organization*
USCyberComm – *United States Cyber Command*
VLAN – *Virtual Local Area Network*
WWW – *World Wide Web*

SUMÁRIO

1. INTRODUÇÃO

O trabalho atenta para três elementos observáveis em relação à inserção internacional dos países no século XXI, com destaque ao caso brasileiro. Primeiro, a tendência de reconfiguração do sistema internacional, por meio da superação da ideia de unipolaridade dos Estados Unidos e da percepção da emergência de um cenário multipolar que ganha complexidade com a entrada de novos atores. Segundo, o desenvolvimento da Era Digital, o advento do ciberespaço e o surgimento da Internet como plataforma de comunicação mundial. Por fim, a ascensão do Brasil no que toca à nova agenda de cibersegurança e sua inserção com anseios de se constituir como ator determinante na ordem internacional.

O surgimento do ciberespaço, como ambiente e conceito, suscita diversos debates justamente acerca da sua delimitação espacial e terminológica. Concomitantemente, o tema da cibersegurança começa a receber grande atenção, principalmente com a consolidação da Doutrina Bush após os atentados de 11 de setembro de 2001, que direcionou os objetivos estratégicos dos Estados Unidos para os problemas de segurança, englobando também o domínio cibernético. Mais recentemente, o Governo Obama trouxe transformações em relação à questão da segurança no ciberespaço e da governança da Internet, levantando interesses não condizentes com as aspirações brasileiras no assunto. Apesar de as diretrizes gerais não serem alteradas, a crescente imposição regional do Brasil e a institucionalização de alternativas ao declinante regime norte-americanos na Internet manifestam uma política externa brasileira adaptada particularmente para a questão cibernética e às disputas globais nesse âmbito.

Nesse trabalho, a compreensão das dinâmicas de ciberpoder se mostra importante para o entendimento dessas disputas globais. Acerca disso, a inserção de diferentes atores e de novos atores estatais nesse tipo de interação implica uma valorização do tema no sentido da interpretação dos acontecimentos internacionais cibernéticos. Acredita-se que poucos são ainda os países detentores de ciberpoder, no entanto a governança da Internet, por exemplo, manifesta-se como palco para as discussões e instrumento para uma desconcentração de poder a favor de uma maior participação de Estados menores ou menos desenvolvidos – fato este que privilegia a ascensão brasileira.

Desse modo, a percepção das mudanças que ocorreram no cenário internacional, somadas às transformações de cunho econômico e social, bem como à consolidação do ciberespaço e suas particularidades, são elementos importantes para se possam compreender as intenções da política externa brasileira atual. De fato, a reconfiguração estrutural rumo à multipolaridade é uma tendência real, em particular, no âmbito da Internet. Tendo em vista

essa realidade, o Brasil passou a assumir uma postura ativa nas dinâmicas de poder internacionais, promovendo o diálogo e demonstrando vocação para a defesa dos seus interesses e de outros países em desenvolvimento frente aos desafios no ciberespaço (AMORIM, 2013).

Essa ênfase na multipolaridade impacta obrigatoriamente os objetivos Estados Unidos. O Brasil articula um forte discurso crítico e uma mobilização internacional na condenação das práticas agressivas no espaço cibernético (a se citar o caso Snowden, de julho de 2013). Essa atuação pode ser vista pela ótica da inserção internacional do Brasil nos últimos anos, através do papel protagonista que o país assumiu no fortalecimento da multipolaridade na Internet.

Nesse sentido, o presente trabalho tem como objetivo avaliar de que forma a política externa brasileira sustenta a promoção da multipolaridade no ciberespaço. Ao responder a pergunta de como, no país, o desenvolvimento da cibersegurança acompanha o crescimento da imagem e da posição brasileira no sistema internacional em relação à promoção dos interesses dos Estados menos favorecidos, o trabalho analisará a incorporação do tema cibersegurança e do desenvolvimento de capacidades na área como elemento essencial para o sucesso do país. Procuraremos mostrar, portanto, que o aumento das ameaças cibernéticas em nível mundial, bem como o fato do Brasil ser alvo desse tipo de prática, valorizaram o escopo da cibersegurança para o país, tanto interna, quanto externamente. Desse modo, se concebe a política externa como ferramenta de projeção do Brasil dentro do escopo da segurança e governança dos ativos de informação, que implica o desenvolvimento das cibercapacidades e da cibersegurança para o sustento de uma ascensão duradoura nesse cenário.

Neste trabalho, abordam-se dois principais eixos: a atuação multilateral do Brasil com organizações internacionais na promoção de uma maior igualdade de direitos e participação no domínio cibernético; e os investimentos e esforços do país em busca de melhores condições de segurança de sua infraestrutura referente à cibernética. Sustenta-se que houve uma incorporação do tema cibersegurança de uma maneira mais enfática no discurso e na ação externa brasileira, como elemento capaz de agregar às pretensões do Brasil a firmar-se como uma potência dotada de influência na ordem internacional. Por outro lado, acredita-se que os esforços de modernização, desenvolvimento e segurança do aparato cibernético nacional ainda não é suficiente, o que constitui uma limitação do país em sua trajetória crescente de influência em nível global. Verificou-se, com efeito, a existência de um "*gap*" de desenvolvimento entre a política externa altiva do Brasil e os dispêndios internos para a securitização das infraestruturas críticas do país e da rede.

Primeiramente, para o entendimento de todas essas dinâmicas, faz-se necessária a clarificação dos debates e fixações dos conceitos que se travam nessa nova discussão. Assim, o primeiro capítulo tratará da evolução do ciberespaço no cenário mundial e sua delimitação, enfatizando a Internet e as dinâmicas de ciberpoder propulsionadas com o seu surgimento. No segundo capítulo, o crescimento da Internet é enfatizado e, com isso, o debate acerca da governança da Internet aparece como aspecto relevante. Nesse mesmo âmbito, os Estados Unidos, como grande ator no ciberespaço e na Internet, e sua declinante influência vai ao encontro do afloramento das diretrizes da política externa brasileira para o assunto. Por fim, na conclusão são retomados os principais aspectos essenciais ao entendimento do ciberespaço, a escalada do fenômeno da Internet e principalmente as interações do Brasil a respeito destes temas no cenário internacional.

2 O ADVENTO DO CIBERESPAÇO, O CRESCIMENTO DA INTERNET E AS TENTATIVAS DE CONCEITUAÇÃO

Atualmente, o denominado "ciberespaço" afeta praticamente a todos, por meio da disponibilização de uma plataforma para inovação e de meios para melhorar o bem-estar geral dos indivíduos ao redor do planeta. Entretanto, uma infraestrutura digital precariamente regulada, traz grandes riscos e ameaçam nações, empresas públicas e privadas e os próprios direitos individuais. O governo tem a responsabilidade de lidar com essas vulnerabilidades estratégicas para garantir que seus cidadãos possam realizar todo o potencial da revolução da tecnologia da informação.

2.1 Definindo o Ciberespaço

Para o entendimento do ciberespaço, parte-se das noções mais amplas da cibernética, a qual pode ser entendida como o estudo da interação homem-máquina, guiado pelo princípio em que numerosos tipos diferentes de sistemas podem ser estudados de acordo com as concepções de *feedback*, controle e comunicações. Norbert Wiener foi o fundador do campo[1], inspirando uma geração de cientistas a ponderar sobre a tecnologia de computadores como um meio de expandir as capacidades humanas.

Ainda hoje, a nomenclatura "ciber" pode ser definida de muitas maneiras. De acordo com Richard Kramer (2009), há pelo menos 28 definições de ciberespaço com diferentes enfoques. Desse modo, a conceituação referente a tudo que seria "cibernético", em seus tempos mais antigos, deriva do grego *kybernetes* ou, traduzindo-se para o português, "timoneiro", o responsável pela navegação.[2] Essa "navegação" e a própria ideia de movimento é justamente o cerne da singularidade do ciberespaço, diferenciando-o, por exemplo, do espaço aéreo ou sideral. O uso do espectro eletromagnético como meio de "movimento" dentro do domínio, e esta clara distinção de outros ambientes físicos podem ser cruciais para o seu desenvolvimento futuro dentro das estruturas de segurança nacional, em uma conceituação possivelmente de um quinto domínio.[3]

---

[1] Cf. WIENER (1948).
[2] Cf. PRIBERAM (2013).
[3] "A *Estratégia de segurança nacional* dos Estados Unidos, por exemplo, apresenta o ciberespaço como um quinto domínio operacional para as forças armadas do país, ao lado da terra, da água, do ar e do espaço sideral" (UNITED STATES, 2010 *apud* CEPIK; CANABARRO; BORNE, 2014, p.171)

O termo referente ao ciberespaço, apesar de ter sua criação datada de 1984 com William Gibson (e sua ideia de *dataspace* em seu livro de ficção científica "Neuromancer")[4], apresenta com Daniel T. Kuehl (2009) a definição mais adequada ao trabalho aqui proposto e à atual dinâmica do espaço cibernético. O autor, em sua tentativa de conceituação, concilia elementos de classificação antes considerados, com grande aproximação aos esforços do Estado-Maior Conjunto dos Estados Unidos, em 2006, para o desenvolvimento da Estratégia Nacional Militar de Operações no Ciberespaço. Assim, Kuehl (2009) afirma:

> Ciberespaço é um domínio global dentro do ambiente da informação cujo único e distinto caráter é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar a informação através de redes interdependentes e interligadas usando tecnologias de informação e comunicação. (KUEHL, 2009, p.04, tradução nossa)[5]

Desse modo, pode-se inferir que todo e qualquer aparato capaz de gerar campos eletromagnéticos, ou seja, executar movimento e troca de elétrons, é considerado como parte constituinte do ciberespaço. Nesse aspecto, é possível dividi-lo em três subdomínios[6]: o domínio dos sistemas, compreendendo a base técnica, infraestrutura (*hardware* e *software*) e arquitetura do ciberespaço; o domínio de conteúdo e aplicação, contendo a base de informação do ciberespaço e os mecanismos de acesso e processamento de informações; e o domínio social, englobando a interação entre pessoas e informações (consumidores, empresas, campanhas políticas, por exemplo, estão nesse domínio).[7] Ainda, pode-se considerar um quarto aspecto no ciberespaço: a governança, que sobrepõe todos os outros aspectos do ciberespaço, enfatizando-se a governança da Internet (ZIMET; SKOUDIS, 2009; EISENBERG; CEPIK, 2002).

[4] Cf. GIBSON (2003).
[5] "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies" (KUEHL, 2009, p.04).
[6] No entanto, com aplicações sobrepostas umas as outras, a Internet, em particular, pode ser concebida em várias camadas (BLUMENTHAL; CLARK, 2009)
[7] Libicki distingue três camadas: física, sintática e semântica (LIBICKI, 2009).

Quadro 1 - Domínios do Ciberespaço

Domínio da Governança		
Domínio dos Sistemas	**Domínio de Conteúdo/Aplicação**	**Domínio das Pessoas/Social**

Fonte: Elaboração própria. Baseado em Zimet e Skoudis (2009)

De maneira abrangente, o próprio uso e a natureza do ciberespaço, de acordo com Kuehl (2009), advêm da concepção de "um ambiente projetado, criado com a intenção específica de facilitar a utilização e exploração da informação, a interação humana e a intercomunicação" (KUEHL, 2009, p.01), ainda que as características físicas do ciberespaço sejam delineadas e venham de forças e fenômenos que existem e ocorrem no mundo natural.

Portanto, deriva-se daí que o ciberespaço pode ser entendido como a rede interdependente de infraestruturas de tecnologia da informação, que inclui a Internet, redes de telecomunicações, sistemas de computadores, processadores embutidos e controladores em indústrias críticas, além de englobar também o ambiente virtual de informações e interações entre as pessoas.

Nesse aspecto, percebe-se que há, hodiernamente, um uso incorreto de termos como "ciberespaço", "Internet" e "Web", comprometendo a pesquisa no campo, além de criar grandes dificuldades na adoção de políticas públicas em relação ao ciberespaço e à própria Internet (CANABARRO; BORNE, 2013). Canabarro, Cepik e Borne (2014) salientam que o ciberespaço e a Internet não se referem à mesma coisa:

> O primeiro precede o desenvolvimento do segundo em décadas. [...] Neste sentido, as redes de telégrafo, radioamador, telefonia fixa e/ou móvel e televisão via satélite configuravam o ciberespaço muito antes do advento da Internet. (CEPIK; CANABARRO; BORNE, 2014, p. 162)

De fato, é interessante se ressaltar que redes de comunicação já existiam muito antes do surgimento dos computadores. Redes de telefone, por exemplo, já haviam crescido massivamente por aproximadamente 60 anos quando o primeiro computador começou a ser desenvolvido, por volta de 1940. Logo, tal sinonímia é, na verdade, inexistente e o que existe na realidade é uma relação de confinamento, na qual a Internet, assim como a telefonia, insere-se dentro do ciberespaço como uma de suas redes e ferramentas de integração.

2.2 A Internet: história, protocolos e a ARPANET

A evolução do ciberespaço parece estar aumentando em velocidade. Muito do ciberespaço foi criado na década de 1970, quando computadores foram interligados e sistemas de e-mail primitivos foram estabelecidos. É nesse contexto que, na década de 1990 surge a Internet na forma como é conhecida, uma das soluções desenvolvidas com a intenção de interligar computadores, mas que, graças às suas especificidades intrínsecas - padrões abertos, governança técnica participativa, neutralidade - (CANABARRO; BORNE, 2013), acabou se tornando a rede de maior adesão internacional.

O grande impulso de crescimento e de popularização da rede coincidiu com o final da Guerra Fria e a derrocada da União Soviética, quando os norte-americanos resolveram abrir do que ainda viria a ser a Internet para o público e explorá-la comercialmente, seguindo a consolidação da divisão da ARPANET (*Advanced Research Projects Agency Network*) em NSFNET (*National Science Foundation Network*) e MILNET (*Military Network*) - a primeira para uso acadêmico e a segunda para fins militares. O crescimento da NSFNet é de fato notável e, apesar de a comercialização da Internet ter começado oficialmente em 1995, no ano de 1992 já havia mais de um milhão de hosts[8] na Internet, graças a Tim Berners-Lee[9] que, em 1991, criou a conhecida "*World Wide Web*", ou seja, o popular "*www*"[10], até hoje utilizado (MAZONI, 2009).[11]

Assim, como a relação entre ciberespaço e Internet, o termo "*www*" é muitas vezes usado equivocadamente como sinônimo da própria Internet, mas a *Web* é , na realidade, um serviço que opera através da Internet. Sendo assim, a *World Wide Web* é um conjunto interligado de documentos e arquivos vinculados entre si por *hiperlinks*[12] (MÖLLER, 2007).

De qualquer maneira, a Internet não seria o que é hoje se não fosse pelo advento do mecanismo de "*packet switching*", ou "comutação de pacotes", de modo a, mais tarde, utilizar um padronizado IP (*Internet Protocol*).[13] Assim, a chamada comutação de pacotes, desenvolvida por Paul Baran em meados da década de 1960, tornou muito mais fácil a troca

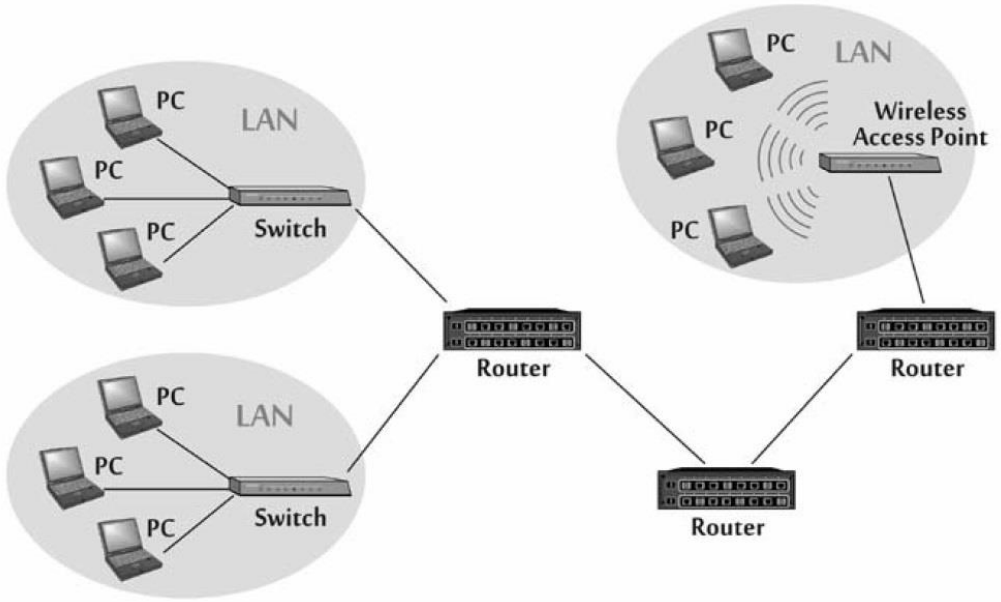
[8] Um *host*, na linguagem da informática, diz respeito a um hospedeiro, que seria computador ou máquina com conexão a uma rede, podendo oferecer informações e serviços por meio de aplicações aos usuários.
[9] Cf. BERNERS-LEE (2000).
[10] Ou simplesmente *Web*.
[11] É ainda nessa mesma época que foi concebido também o protocolo HTTP – o qual viabilizou a existência da Web -, possibilitando o envio de dados criptografados para operações de dados comerciais pela Internet.
[12] Signos como palavras ou imagens que, quando clicados, acessam novos endereços na rede.
[13] "The Internet is the publicly accessible worldwide system of interconnected computer networks that transmit data by packet switching using a standardized Internet Protocol (IP) and many other protocols". (MÖLLER, 2007, p.31)

de informações de maneira segura, por meio do fracionamento da informação digital em pequenos pedaços (“pacotes”) que, quando chegam ao seu destino, são (re)montados e então passíveis de serem interpretados.

> O desenvolvimento da tecnologia de “comutação de pacotes” que organizava essa interconexão foi percebido como habilitador da criação de uma rede descentralizada que pudesse conectar, ao mesmo tempo, inúmeros centros de comando e controle do Departamento de Defesa, em substituição a um nodo central de comando de ações militares, aumentado, com isso, sua resiliência em caso de ataques externos (BING, 2009 apud CANABARRO, 2012, p.04).

Ao mesmo tempo, o protocolo TCP/IP (*Transmission Control Protocol*/*Internet Protocol*) possibilitou, desde a década de 1970 (com sua criação por Vincent Cerf e Bob Kahn), uma universalização por meio da padronização entre computadores e redes distintos. Desse modo a Internet torna possível a prestação de serviços em tempo real, como rádio on-line - e até mesmo TV (IPTV) - que podem ser acessados de qualquer lugar o mundo, desde que exista o acesso à Internet com a devida velocidade. A Figura 1, a seguir, representa de forma simplificada o funcionamento estrutural da Internet: várias redes locais que anteriormente se encontravam isoladas de um nível maior, mundial, as LANs (Local Area Networks), com a Internet e especialmente o protocolo TCP/IP (que padroniza a forma como essas redes se comunicarão), passam a integrar uma rede muito maior, sendo seu fluxo de informações mediado por roteadores, responsáveis por redirecionar a mensagem enviada ao destinatário.

Figura 1 - Internetworking Local Area Networks via Routers and Point-to-Point Links



Fonte: Zimet e Skoudis (2009).

2.2.1 As Origens na ARPANET

Atentando à origem da rede, a criação da ARPA (*Advanced Research Projects Agency*), em 1957, está particularmente ligada à reação do governo estadunidense ao lançamento pela União Soviética do Sputnik 1, o primeiro satélite artificial da Terra, em 4 de outubro do mesmo ano. O primeiro projeto da ARPA era justamente o desenvolvimento de um satélite próprio para os Estados Unidos, a fim de equilibrar a corrida espacial com os soviéticos. Com o prosseguimento da Guerra Fria na década de 1960, a probabilidade de uma guerra nuclear e a necessidade de se manter as comunicações marcaram o começo do envolvimento da ARPA com a computação (MAZONI, 2009). Assim, "a ARPANET nasceu de uma inspiração e uma necessidade" (ABBATE, 1999, p.54). Nesses termos, a inspiração foi provavelmente originada de Joseph C. R. Licklider, o primeiro diretor de Gabinete de Técnicas de Processamento de Informação (IPTO) da ARPA, o qual demonstrava uma visão bastante interessante sobre o futuro e a convergência das redes:

> O conjunto de pessoas, hardware e software - o computador de acesso múltiplo juntamente com a sua comunidade local de usuários - vai se tornar um nó em uma rede de computadores distribuídos geograficamente. Suponhamos, por um momento, que essa rede foi formada (LICKLIDER; TAYLOR, 1968, p.32 tradução nossa).[14]

Em março de 1970, a ARPANET teve seu primeiro nó na costa leste dos Estados Unidos. Em setembro de 1971, o primeiro TIP (*Terminal Interface Processor*) foi implantado, permitindo a terminais de computadores individuais discarem diretamente para a ARPANET, aumentando a facilidade de conexões de rede e levando a um crescimento significativo. Até o final de 1973, havia 37 sites na ARPANET, incluindo o DoD (Departamento de Defesa dos Estados Unidos), a NFA (*National Futures Association*), a NASA (*National Aeronautics and Space Administration*) e o Sistema de Reserva Federal dos Estados Unidos, além das primeira conexões internacionais com o Reino Unido e Noruega.

Em 1983, uma rede militar única não classificada chamada MILNET (*Military Network*) separou-se da ARPANET, permanecendo apenas ligada a um pequeno número de gateways para a troca de correio eletrônico, que poderia ser facilmente desconectada por motivos de segurança, se necessário. A MILNET, mais tarde, passou a fazer parte da Rede de Informação de Defesa do DoD (DDN). Em meados da década de 1980, havia *gateways* da

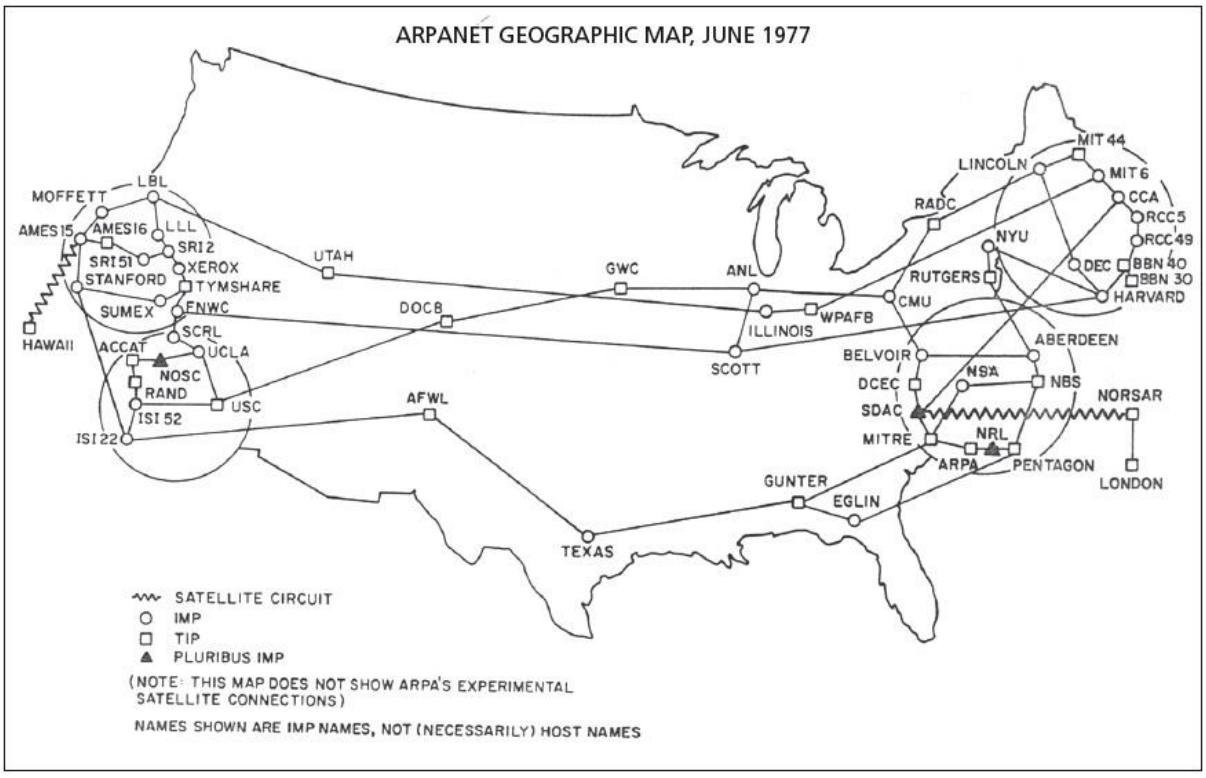
[14] "The collection of people, hardware, and software -- the multiaccess computer together with its local community of users -- will become a node in a geographically distributed computer network. Let us assume for a moment that such a network has been formed". (LICKLIDER; TAYLOR, 1968, p.32)

ARPANET para redes externas em toda a América do Norte, Europa e Austrália: a Internet se encontrava a âmbito mundial (HAUBEN, 1997).[15]

> Entre os anos 1960 e 1980, a tecnologia de computação passou por uma transformação dramática: o computador, originalmente concebido como um dispositivo de cálculo isolado, renasceu como um meio de comunicação (ABBATE, 1999, p.12).[16]

Logo, o desenvolvimento da ARPANET advém da própria necessidade de criação de uma rede de área ampla com a finalidade de conectar sites do governo, militares e universitários, a fim de permitir que pesquisadores compartilhassem fontes e resultados mais fluentemente (KLEINWÄCHTER, 2007).

Figura 2 - Mapa Geográfico da ARPANET em junho de 1977



Fonte: Dodge e Kitchin (2001).

Na década de 1990, a Internet finalmente absorveu a antiga ARPANET - que expirou em 1989 - e a disseminação dos protocolos de comunicação para diferentes aplicações especializadas da Internet (e-mail: *Simple Mail Transfer Protocol* – SMTP; troca de arquivos:

[15] Cf. HAUBEN (1997).

[16] "Between the 1960s and the 1980s, computing technology underwent a dramatic transformation: the computer, originally conceived as an isolated calculating device, was reborn as a means of communication". (ABBATE, 1999, p.12)

File Transfer Protocol – FTP; acesso a sítios virtuais graficamente constituídos: *Hypertext Transfer Protocol* – HTTP; entre outros) contribuiu para a popularização da nova ferramenta (CEPIK; CANABARRO; BORNE, 2014). No início dos anos 2000, motores de busca e *e-commerce* aparecem. Muitos dos aplicativos mais populares e comunidades on-line são ainda mais recentes, como *blogs, wikis* e aplicações de realidade virtual.

2.2.2 Os Protocolos da Rede

Para o entendimento dos protocolos é de extrema importância a sua relação com as camadas da Internet. De modo grosseiro, assim como no ciberespaço (mas, claro, em um escopo mais específico, como já explicado), a Internet pode ser pensada em três grandes camadas: inferior, intermediária e superior. A camada inferior, engloba o nível físico e, desse modo, linhas telefônicas, cabos de conexão e infraestruturas físicas de suporte ao fluxo e armazenamento de dados.

Na camada intermediária pode-se situar os níveis de rede e transporte, responsáveis pela transformação da informação de padrões codificados, computacionais, para padrões "humanos", compreensíveis, e vice-versa. É nessa camada que se estabelece grande parte da interação TCP/IP, por exemplo. O nível de transporte (TCP) seria o responsável por dividir a mensagem em segmentos de tamanho compatível com as especificações de transporte, além de anexar o endereço destinatário para, então, enviar o pacote ao nível de rede. O nível de rede (IP), por sua vez, responsabiliza-se por assegurar a conectividade da Internet, estabelecendo a interconexão de diversas redes. O nível de enlace cumpriria o papel da ligação de dados, ou seja, detecta e, opcionalmente, corrige erros que possam acontecer na camada física, além de regular o fluxo de dados e estabelecer a comunicação entre sistemas diretamente conectados.

A camada superior, também considerada a camada da informação, corresponde basicamente ao nível de aplicação, com o papel de oferecer aos softwares do usuário o acesso à Internet, com protocolos e serviços padronizados de comunicação para as tarefas mais comuns na rede, como o correio eletrônico (SMTP), a conexão remota (Telnet) e a transferência de arquivo (FTP), entre outros. Autores como Eisenberg e Cepik (2002) ou Canabarro e Borne (2013) ainda consideram uma quarta camada, advinda da interação entre a informação e diferentes usuários, formando redes sociais, econômicas e políticas.

Quadro 2 - Camadas da Internet

CAMADA SUPERIOR – informação	**Nível de Aplicação** (Telnet, FTP, SMTP)
CAMADA INTERMEDIÁRIA - transporte e conexão	**Nível de Transporte** (TCP)
	Nível de Rede (IP)
	Nível de Enlace (Ethernet, Wifi, VLAN)
CAMADA INFERIOR - infraestrutura física	**Nível Físico** (cabos de conexão, linhas telefônicas)

Fonte: Elaboração própria (com base em Zimet e Skoudis, 2009).

Sendo assim, de acordo com Skoudis (2009), o futuro do ciberespaço vai gradativamente convergindo na incorporação da Internet em diversos objetos cotidianos, incluindo sistemas de posicionamento global, de aviões e de armas, por exemplo. Logo, a importância da Internet surge da finalidade para a qual foi concebida:

> A Internet foi projetada para não apoiar uma aplicação específica, mas com o objetivo de generalidade. Em contraste com a rede de telefonia, por exemplo, que foi inicialmente projetada especificamente para realizar chamadas telefônicas, a Internet foi projetada para suportar uma ampla gama de aplicações, mesmo aquelas ainda não pensadas (BLUMENTHAL; CLARK, 2009, p.02, tradução nossa).[17]

Tal caráter inclusivo que acompanha o conceito e finalidade da Internet está intrinsecamente conectado com as ideias de *ubiquidade* e *convergência digital*. A ubiquidade estaria relacionada justamente com a propriedade de onipresença da rede e a possibilidade de inúmeros dispositivos compatibilizarem suas plataformas e se integrarem nesse espaço. Ao mesmo tempo, a convergência digital diz respeito a "um fenômeno social complexo de integração de mídias distintas em um único canal de transmissão" (CEPIK; CANABARRO; BORNE, 2014, p.165), transformando assim a Internet, ao final do século passado, na "rede das redes" (CANABARRO; BORNE, 2013). Essa onipresença e compatibilidade da rede é a principal responsável pela alavancagem das interações entre indivíduos e Estados em uma velocidade nunca antes vista. As relações de Poder e influência, assim, se moldam de maneira a se manifestarem de forma diferente em função de um novo ambiente de intercâmbio, dando espaço para o que seriam, então, relações de ciberpoder.

[17] "The Internet was designed not to support a specific application, but with the goal of generality. In contrast to the telephone network, for example, which was initially designed specifically to carry telephone calls, the Internet was designed to support a wide range of applications, even those not yet thought of". (BLUMENTHAL & CLARK, 2009, p.02)

2.3 Os Desafios de Conceituação do Ciberpoder

Como já discorrido, a Era Digital apresentou, principalmente após a difusão da Internet, um crescente uso em processos políticos da informação digitalizada, caracterizada pela forte presença nas diferentes esferas sociais e que representa fonte de poder para os atores que dela usufruem. Nesse âmbito, como afirmam Cepik e Arturi (2011), os processos de inserção internacional dos países no pós-Guerra Fria (convergindo com a abertura comercial da Internet) demonstram que o "[...] desenvolvimento e o aprimoramento do uso das Tecnologias de Informação e Comunicação (TIC) têm potencial para ampliar a capacidade de resposta dos Estados frente a tais desafios" (CEPIK; ARTURI, 2011, p.651-652), germinados nas disputas de poder no cenário global. Nesse sentido, faz-se essencial entender o papel do ciberespaço e da Internet para a disputa de poder internacional e a importância dos Estados Unidos – como berço da Internet e de diversas tecnologias de informação – nesse escopo.

Por ser uma área ainda de recente exploração nos estudos cibernéticos e de segurança, os debates acerca do campo do ciberpoder continuam em aberto. Por isso, uma inicial aproximação aos primeiros conceitos de Poder se faz pertinente.

2.3.1 A Teoria de Poder e seus Debates

Essencialmente, Poder designa a capacidade ou a possibilidade de agir, de produzir efeitos (STOPPINO, 1998, p.943; RUSSELL, 1938, p.50). Partindo-se de Max Weber (1947) pode-se considerar uma compreensão instrumental do poder:

> Poder é a probabilidade de que um ator, dentro de uma relação social, estará em uma posição para executar sua própria vontade, mesmo em face de resistência, independentemente da base em que essa probabilidade se apoia. (WEBER, 1947, p.152)[18]

Dessa maneira, entende-se que o próprio poder seria um meio, uma ferramenta para a realização de um determinado fim, sendo a instrumentalização de uma vontade individual, havendo sanções para o seu não cumprimento . Por não existir uma base exata e comum para comparação no que tange o poder de atores com grupos de objetivos distintos, Robert Dahl

[18] "Power (Macht) is the probability that an actor within a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests." (WEBER, 1947, p.152)

(2012) explicita suas ressalvas e a ideia de que a delimitação de Poder ainda só é possível, na atual realidade, em termos qualitativos.

> Um limite drástico ao rigor de conceitos como o poder e a influência também é estabelecido pelo fato infeliz de que ainda não foi criada nenhuma medida quantitativa de poder ou influência. Consequentemente, a distribuição do poder nos sistemas reais pode ser descrita apenas em termos qualitativos. (DAHL, 2012, p.433)

Na mesma lógica, Joseph Nye Jr. (2010), em uma análise do conceito, já chama a atenção para a dificuldade de mensuração existente, entretanto não descarta, em nenhum momento, a importância do estudo e da delimitação do conteúdo.[19] Portanto, pode-se, de modo sumário, considerar que, para B ter poder sobre A, basta que, ao impor ou ameaçar impor sanções a A, B é capaz de afetar as ações de A de maneira que os interesses de B preponderem, ao tempo que A não dispõe dessa capacidade em relação a B (BOWLES; GINTIS, 1992).[20] Tal análise se daria, assim, de maneira mais qualitativa e a ameaça de imposição de sanções verifica esse caráter, uma vez se mostrando uma manifestação que exige uma maior subjetividade para o seu entendimento.

Para fins deste trabalho, utiliza-se uma acepção de poder interpessoal, ou seja, que caracteriza uma relação entre pessoas, e não uma qualidade de um indivíduo solitário. Em segundo lugar, o exercício do poder envolve a ameaça e uso de sanções. De fato, teóricos da ciência política como Lasswell e Kaplan (1950) consideram sanções como atributos definidores da relação de poder e afirmam uso (ou a ameaça do mesmo) de "sanções severas" como caráter integrante no sustento de uma política contra uma oposição – assinalando, assim, uma *decisão*.[21]

Stoppino (1998) compartilha quase que do mesmo preceito e sustenta que Poder "é uma relação entre pessoas" (STOPPINO, 1998, p.944), isto é, não existe Poder se, perante ao indivíduo que o exerce, não há outro que seja induzido à vontade do primeiro. Nye Jr. (2010), em uma tentativa de simplificação, define Poder de uma maneira abrangente e chega a fazer alguma alusão ao conceito de influência, presente nas ideias de Lasswell e Kaplan:

---

[19] "Para um conceito que é tão amplamente utilizado, 'poder' é surpreendentemente elusivo e difícil de medir. Mas esses problemas não fazem com que um conceito perca seu sentido". (NYE JR, 2010, p.06 tradução nossa)

[20] "The following sufficient condition for the exercise of power captures these four desiderata: For B to have power over A, it sufficient that, by imposing or threatening to impose sanctions on A, B is capable of affecting A's actions in ways that further B's interests, while A lacks this capacity with respect to B." (BOWLES; GINTIS, 1992, p.08)

[21] "Decisão é uma política que inclua sanções graves (privações)" (LASSWELL; KAPLAN, 1950, p.75); "Política é um programa projetado de metas e práticas" (LASSWELL; KAPLAN, 1950, p.71).

> Poder é a capacidade de afetar outras pessoas para obter os resultados que se quer. Algumas pessoas chamam isso de influência, e distinguem poder de influência, mas isso é confuso, pois o dicionário define os dois termos indistintamente. (NYE JR, 2010, p.02, tradução nossa)[22]

Para o trabalho aqui proposto, a distinção citada por Nye Jr. (2010) se faz ainda interessante. Sendo assim, a diferença entre Poder e influência estaria relacionada à ameaça do uso de sanções e, organizando-se hierarquicamente, Poder se configuraria como uma forma particular de exercício da influência. Logo, de acordo com Lasswell e Kaplan (1950), o que se entende por influência teria um escopo mais amplo e abrangente, implicando na ocupação *value-position* e *value-potential*[23] para se afetar as políticas de outros atores.

Ainda, aspecto de grande importância a ser destacado é a determinação da esfera de atividade à qual o Poder se refere – ou a *esfera de Poder*. Logo, não basta especificar o indivíduo ou grupo que detém o Poder e o indivíduo ou que a ele está sujeito (STOPPINO, 1998) sem se especificar Poder "para quê" (NYE JR, 2010). E é exatamente nessa particularidade que se expressa a própria construção do que seria o Poder no contexto do ciberespaço:

> É preciso especificar quem está envolvido na relação de poder (o alcance do poder), bem como os tópicos que estão envolvidos (o domínio do poder). As declarações sobre o Poder sempre dependem do contexto, e o ciberespaço é um novo e importante domínio de Poder. (NYE JR, 2010, p.02, tradução nossa)[24]

2.3.2 O Ciberpoder e as Heranças da Teoria de Poder

Assim como Poder depende de contexto, o ciberpoder irá depender dos recursos que caracterizam o domínio do ciberespaço. Logo, em uma articulação com os conceitos primeiros de Poder, trata-se o ciberpoder, visto a sua inserção e seu ambiente, como uma medida da capacidade de utilizar esse espaço[25].

---

[22] "Power is the ability to affect other people to get the outcomes one wants. Some people call this influence, and distinguish power from influence, but that is confusing because the dictionary defines the two terms interchangeably". (NYE JR, 2010, p.02)

[23] "*Value-position*" seria a posição ocupada por um grupo ou por um indivíduo e "v*alue potential*" seria o "value position" provável de ser ocupado. Desse modo, Influência seria a combinação resultante, sendo plausível a ocorrência de um grupo ou indivíduo com influência crescente, mesmo que com um *value-position* constante, caso o *value-potential* aumente.

[24] "One must specify who is involved in the power relationship (the scope of power) as well as what topics are involved (the domain of power.) Statements about power always depend on context, and cyberspace is a new and important domain of power". (NYE JR, 2010 p.02)

[25] "While cyberspace as an environment simply 'is', cyberpower is always a measure of the ability to use that environment". (KUEHL, 2009:12)

> Ciberpoder é a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais e através dos instrumentos de poder. (KUEHL, 2009, p.01, tradução nossa).[26]

Prontamente, a crescente importância do ciberpoder e da construção de seu entendimento advém da sua particularidade, essa qual ainda está no curso de ser totalmente absorvida pelos Estados, que se encontram dividindo palco com novos atores internacionais e com mais dificuldades no controle de suas fronteiras dentro do ciberespaço.

Alguns intelectuais acabaram por interpretar tal tendência de maiores dificuldades como apontadoras do declínio dos Estados soberanos, considerados instituições globais dominantes desde a Paz de Vestfália, em 1648. No entanto, o Estado continuará a ser o ator dominante no cenário internacional por, ao menos, um longo tempo (NYE JR., 2010). Nesses termos, é justificável que o foco desse trabalho resida nas dinâmicas do Estado nesse novo espaço de interação.

Novamente, é importante ressaltar que o ciberespaço não vai substituir o espaço geográfico e tampouco abolir a soberania do Estado; todavia não se descarta que a difusão de poder no ciberespaço tenda a complicar o seu exercício nesse e em outros campos. Logo, uma dependência do ciberespaço ao espaço geográfico pode ser notada, uma vez que sua infraestrutura física, aquela referente ao primeiro domínio descrito por Zimet e Skoudis (2009), permanece vinculada à localização geográfica dentro do território soberano dos países, caracterizando a localização ainda como recurso de poder para o ciberespaço (NYE JR., 2009).

> A geografia do ciberespaço é muito mais mutável do que outros ambientes. Montanhas e oceanos são difíceis de mover, mas partes do ciberespaço podem ser ligadas e desligadas com o simples clique de um botão. [...] Entretanto, o ciberespaço não é infinitamente maleável: limites sobre o ritmo e o alcance da mudança são regidos por leis físicas, propriedades lógicas de código, e as capacidades das organizações e das pessoas. (RATTRAY, 2009, p.03, tradução nossa)[27]

De maneira geral, pode-se falar de atores no ciberespaço em três categorias: governos, organizações e indivíduos[28]. Com Richard Kramer (2009), há uma breve alusão a esses atores:

---

[26] "Cyberpower is the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power". (KUEHL 2009:12)

[27] "The geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch. [...] Cyberspace is not, however, infinitely malleable: limits on the pace and scope of change are governed by physical laws, logical properties of code, and the capacities of organizations and people." (RATTRAY, 2009, p.03)

[28] Obviamente, dentro das devidas proporções, consideram-se governos e organizações detentores de redes altamente estruturadas, ao passo que os indivíduos dispõem de redes levemente estruturadas.

> O ciber é tanto um elemento de, quanto um suporte para Poder - para as nações, para os indivíduos e para outras entidades, incluindo empresas, organizações sem fins lucrativos e criminosos e terroristas. (KRAMER 2009, p.08, tradução nossa)[29]

O baixo custo de engajamento, o anonimato e a persistente vulnerabilidade reduzem alguns dos diferenciais de poder entre os atores, resultando em uma maior capacidade dos competidores menores para exercer poder no "domínio" cibernético quando comparado com outros domínios tradicionais[30], havendo, assim, uma grande parte da população dentro dos países com acesso ao Poder advindo da informação.

Nye Jr. (2010), em sua aproximação do conceito, como tradição, aborda-o a partir dos comportamentos de *hard* (que diz respeito à coerção) e *soft power* (refere-se a enquadramento agendas, atração ou persuasão). No entanto tal divisão, especificamente, não se mostra totalmente necessária para a construção desse trabalho.[31] De modo abrangente e de grande utilidade para esse trabalho, é a definição de ciberpoder de Dan Kuehl e Richard Kramer (2009), mencionada anteriormente, caracterizando o conceito como a capacidade de obter resultados desejados por meio do uso dos recursos de informação eletronicamente interligados de domínio cibernético, de modo a cumprir objetivos dentro do ciberespaço, ou a até mesmo transcende-lo.[32] Ainda, tal qualidade de transcendência refere-se às chamadas intra e extra dimensões do poder cibernético, de acordo com o alcance dos resultados desejados.

Jeffrey Hunker (2010) já aborda a própria ameaça do uso de ciberataques em sua definição[33]. Em relação a isso, o autor faz grande alusão aos entraves inerentes à ameaça do "uso da força" no ciberespaço, em função da dificuldade de credibilidade de um ataque desse tipo perante seu alvo ou à comunidade internacional:

> Ameaçar o 'uso da força' no ciberespaço pode ser problemático. Pode haver um número limitado de circunstâncias em que uma ameaça de lançar ataques

---

[29] "Cyber is both an element of, and a support for power - for nations, for individuals, and for other entities including businesses, nonprofit organizations, and criminals and terrorists". (KRAMER, 2009, p.08)

[30] "As barreiras à entrada no domínio cibernético são tão baixas que os atores não-estatais e pequenos Estados podem desempenhar papéis importantes com baixos níveis de custo. Em contraste com o mar, ar e espaço, as ações cibernéticas dividem três características com a guerra terrestre - embora em dimensões ainda maiores: o número de jogadores, a facilidade de entrada, e a oportunidade de encobrimento." (NYE JR, 2010, p.04 tradução nossa)

[31] Mais adiante, considera-se a tentativa de ponderação do que seria a influência cibernética, fixando assim maior relação com os conceitos anteriores de Poder e Influência, principalmente nos entendimentos de Lasswell e Kaplan (1950).

[32] "Ciberpoder é a capacidade de obter resultados preferidos por meio do uso dos recursos de informação electrônica interligados do domínio cibernético. […] Ciberpoder pode ser usado para produzir resultados preferidos dentro do ciberespaço ou […] em outros domínios fora do ciberespaço". (NYE JR., 2010, p.04 tradução nossa)

[33] "Ciberpoder é o uso, uso ameaçado, ou efeito pelo conhecimento de seu uso potencial, de capacidades de ataque cibernético disruptivos por um Estado." (HUNKER, 2010, p.04 tradução nossa)

> cibernéticos irruptivos será considerada crível pelo Estado-alvo ou pela comunidade das nações. (HUNKER, 2010, p.07, tradução nossa)[34]

Tal prerrogativa se aplica particular e principalmente à dinâmica da Internet. Em função de não ter sido projetada com atenção à segurança, a rede não apresenta um mecanismo de todo confiável para o rastreamento da fonte de uma mensagem, por exemplo. "Elétrons não comportam marcas nacionais" (HUNKER, 2010, p.05), logo a responsabilização de atores é em muito dificultada.

A possibilidade de que a cibersegurança cause interrupção ou danos à infraestrutura física em larga escala torna difícil precisar quais seriam as potencialidades e os efeitos colaterais de um ataque deste tipo. Ainda, devido ao "problema da atribuição" - a dificuldade de identificação de potenciais agressores (já citada anteriormente), inerente do espaço em discussão -, o entendimento de dissuasão (ou *deterrence*)[35] no ciberespaço não se mostra aplicável de maneira consensual ao ciberpoder (HUNKER, 2010; KUGLER, 2009). Ainda, uma possível comparação com a dissuasão em termos do modelo nuclear se torna de fato desgastada, visto que as característica punitivas de longe não mostram a mesma equivalência nos dois campos.

> Ataques cibernéticos não possuem as dimensões catastróficas de ataques com armas nucleares, e a atribuição é mais difícil, mas a dissuasão interestatal ainda existe. (NYE JR., 2010, p.16 tradução nossa)[36]

Em Pimentel (2014), encontra-se a mesma ideia acerca das dimensões dos ataques cibernéticos, além de levantar o ponto sobre a reação aos ataques de forma mais contundente, uma vez que seria difícil delimitar as potencialidades e efeitos colaterais de um ataque do tipo, ao passo que "é difícil prever qual seria a reação das audiências frente a um ataque cibernético" (PIMENTEL, 2014, p.07).

Enfim, para um melhor entendimento e relacionamento do ciberpoder com as anteriores conceituações de Poder, pode-se conciliar as ideias de Kuehl e Kramer (2009) com as de Nye Jr. (2010) e Hunker (2010), valendo-se majoritariamente de uma interpretação de

---

[34] "Threatening 'the use of force' in cyberspace can be problematic. There may be a limited range of circumstances in which a threat to launch disruptive cyber attack will be regarded as credible by either the target state or the community of nations." (HUNKER, 2010, p.07)

[35] Dissuasão refere-se, de modo simplificado, à situação em que "os indivíduos são dissuadidos de fazer alguma coisa pelo temor das conseqüências possíveis, das punições previstas ou da execução de uma ameaça" (ARON, 2002:509). "Dois elementos básicos sustentam o princípio da dissuasão: retaliação e negação ('*denial*'). A retaliação é o elemento direto que prevê uma punição frente a uma agressão. Já a negação é a resistência pela força a ataques vindos de outrem". (PIMENTEL, 2014, p.07)

[36] "Cyber attacks lack the catastrophic dimensions of nuclear weapons attacks, and attribution is more difficult, but inter-state deterrence still exists". (NYE JR., 2010, p.16)

Lasswell e Kaplan (1950). Desse modo, agregando as características de Poder e Influência, compreende-se ciberpoder como a capacidade de uso, ou ameaça de uso, do ciberespaço para criar vantagens e afetar outros atores e eventos em todos os ambientes operacionais e por meio dos instrumentos desse ambiente obter os resultados pretendidos. Contudo, merece destaque um problema herdado dos debates da anterior teoria de Poder: o desafio da mensuração citado por Dahl (2012). Assim, apesar de o IISS (2014), em uma tentativa de aproximação, organizar uma ainda incompleta avaliação do que seriam as capacidades cibernéticas, em relação ao ciberpoder tal questão perdura.

Outro debate que fica em aberto é sobre a capacidade de dissuasão e principalmente a influência cibernética que, como já explicado, ainda apresentam grande dificuldade de delimitação. Talvez, em uma tentativa de *stretching* conceitual, fosse possível uma relação desses conceitos, que estariam inclusos na "estratégia cibernética" de um país, descrita por Stuart H. Starr (2009):

> Uma das questões-chave associadas com a estratégia cibernética lida com o desafio de conceber dissuasão adaptada a afetar o comportamento das entidades-chave empoderadas pela evolução do ciberespaço. (STARR, 2009, p.4-5, tradução nossa)[37]

Entretanto, ainda perduram as discussões sobre o que exatamente a estratégia cibernética de um país poderia ser (IISS, 2014) e uma acomodação desses conceitos continua se mostrando incompleta. O próprio *International Institute for Strategic Studies* (IISS) relaciona muito a estratégia cibernética dos Estados como suas doutrinas militares para o ciberespaço. Logo, o aumento de preocupação com a questão cibernética evidencia a securitização do espaço em questão, uma vez este que representou um desafio e uma ameaça que requer atenção nacional urgente. Nesse encadeamento é suscitada a ideia da cibersegurança na tentativa de se resumir todos os anseios e necessidades de proteção do Estado em relação aos seus ativos, com ênfase nas infraestruturas críticas da informação, debate este a ser abordado a seguir.

2.4 Cibersegurança: uma aproximação conceitual

A arquitetura de infraestrutura digital de uma nação, baseada em grande parte na Internet, não é segura ou resiliente. Durante o próprio desenvolvimento da Internet (ainda

[37] "Thus, one of the key issues associated with cyber strategy deals with the challenge of devising tailored deterrence to affect the behavior of the key entities empowered by developments in cyberspace". (STARR, 2009, p.4-5)

ARPANET, em seus primórdios), a segurança não havia sido uma grande preocupação para os pesquisadores. Estes estavam mais interessados no uso da tecnologia e suas vantagens do que em protegê-la. Sobre isso, Myriam Dunn Cavelty (2012) atenta para a falta do caráter securitário ao longo do crescimento do ciberespaço e do que viria a ser a Internet:

> O ambiente de informação em rede - ou ciberespaço - é genericamente inseguro, porque nunca foi construído visando à segurança. A globalização dinâmica de serviços de informação, aliada à inovação tecnológica, levou a um aumento constante de conectividade e complexidade. Quanto mais complexo um sistema de TI é, mais problemas que ele apresenta e sua segurança se torna mais difícil de controlar ou gerenciar. (CAVELTY, 2012, p.106 tradução nossa)[38]

Richard Kramer (2009) também destaca as vulnerabilidades as quais o mundo cibernético estaria suscetível. Cada nível do "ciber" – desde a infraestrutura física até as pessoas, passando pelo espectro do software e da informação *per se* – estaria sujeito a quebras de segurança, seja por meios de ataque, infiltração ou até mesmo por acidentes.

Nesse contexto, o surgimento do conceito de cibersegurança coincide com a agenda do pós-Guerra Fria, como uma reação às mudanças nas condições geopolíticas na época[39] e o advento de novas tecnologias. Em seu início, na década de 1990, o termo fora usado para se referir a uma série de inseguranças de computadores ligados em rede, entretanto evoluiu de uma mera concepção técnica no momento em que foi percebida a existência de consequências político-sociais extremamente destrutivas (HANSEN; NISSENBAUM, 2009). Desse modo, primordialmente, de maneira mais simples, pode-se definir o problema da cibersegurança de acordo com o que Pimentel (2014) propõe:

> "a (in)segurança produzida pelas novas tecnologias da informação, referindo-se tanto aos problemas de natureza técnica (pautados pela engenharia e pela ciência da computação) como pelos problemas de natureza política (sobretudo, as relações de poder, os desafios estratégicos e os dilemas ético-políticos engendrados pela tecnologia)." (PIMENTEL, 2014, p.03)

Assim, junto com o termo, "emerge uma forte retórica sobre a ideia de ciberguerra" (PIMENTEL, 2014, p.03), além de outros "conceitos adjacentes" a serem aplicados sob essa mesma tendência, como "*netwar*" e "*network security*", "segurança informacional" e "guerra informacional" (HANSEN; NISSENBAUM, 2009). Basicamente, o termo ciberguerra se

[38] "The networked information environment – or cyberspace – is pervasively insecure, because it was never built with security in mind. The dynamic globalization of information services in connection with technological innovation led to a steady increase of connectivity and complexity. The more complex an IT system is, the more problems it contains and the harder it is to control or manage its security." (CAVELTY, 2012, p.106)

[39] Estas condições estariam muito ligadas com a ideia da perda dos inimigos declarados e pontuais, principalmente em relação aos Estados Unidos, que perdem o foco em um só alvo estatal com a descensão soviética.

refere ao "uso de computadores para interromper as atividades de um país inimigo, especialmente [com] ataques deliberados a sistemas de comunicação" (CAVELTY, 2012, p.118, tradução nossa),[40] contudo, recebe de maneira indiscriminada alusões a todos os tipos de atividades maliciosas no ciberespaço (FARIVAR, 2009), fazendo assim com que o termo "guerra" perca seu valor conceitual e seja menosprezado, mais em função de um alarde midiático do que uma real avaliação das proporções que representaria.

Um exemplo disso seria a ideia do cenário de "Pearl Harbor Digital"[41], mas que não se verifica até hoje, mesmo em meio a um já longo histórico de agressões no campo cibernético (LEWIS 2006; 2010). Os casos da Estônia em 2007 e do Irã (mais incisivo ainda, com o *Stuxnet*, em 2010), poderiam ser exemplos da "ciberguerra" (CAVELTY, 2012), dada a especificidade (principalmente em 2010) dos ataques direcionados, mas as evidências ainda não são suficientes e, mais uma vez, volta-se ao problema da atribuição. Em resumo, a guerra cibernética estratégica permanece altamente improvável num futuro próximo (CAVELTY, 2012), principalmente devido aos resultados incertos trazidos e à possibilidade de encobrimento. Nesse ponto, a influência de atores não-estatais é condicionante para o barramento do desenvolvimento da guerra cibernética entre Estados[42], porquanto, ao mesmo tempo que atacam a infraestrutura de um país, confundem a real identidade do agressor ou da origem do ataque. Assim surge o cibercrime, como forma de agressão irregular no que tange a autores e possivelmente onerosa a ponto de demandar a securitização de determinados aspectos no ciberespaço.

Logo, uma vez que o conceito de ciberespaço é notadamente mais amplo que o de Internet, não é surpresa a existência de "cibercriminosos" datada de muito tempo. Desse modo, um ataque cibernético organizado que explore as várias vulnerabilidades dos sistemas de um país tem grandes chances de colocar em risco a segurança das infraestruturas críticas da nação, além de outras consequências advindas de roubo de informações, principalmente.

> As vulnerabilidades que mais ameaçam o ciberespaço ocorrem nos ativos de informação de empresas de infraestrutura crítica e suas estruturas de apoio externos, tais como os mecanismos da Internet. [...] Vulnerabilidades resultam de deficiências

[40] "Cyber war: The use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems". (CAVELTY, 2012, p.118)

[41] Tal termo surge em meados de 1990, prevendo um cenário em que *hackers* mergulhariam cidades na escuridão, cortariam o abastecimento de água e fariam com que aviões colidissem uns com os outros (LEWIS, 2006).

[42] Entretanto, reforça-se a ideia de que os Estados continuam desempenhando o papel de ator mais importante nessa interação e o trabalho proposto tem o intuito de focar-se nesse aspecto.

> na tecnologia e, devido à aplicação e fiscalização inadequada de produtos tecnológicos. (KRAMER, 2009, p.03 tradução livre)[43]

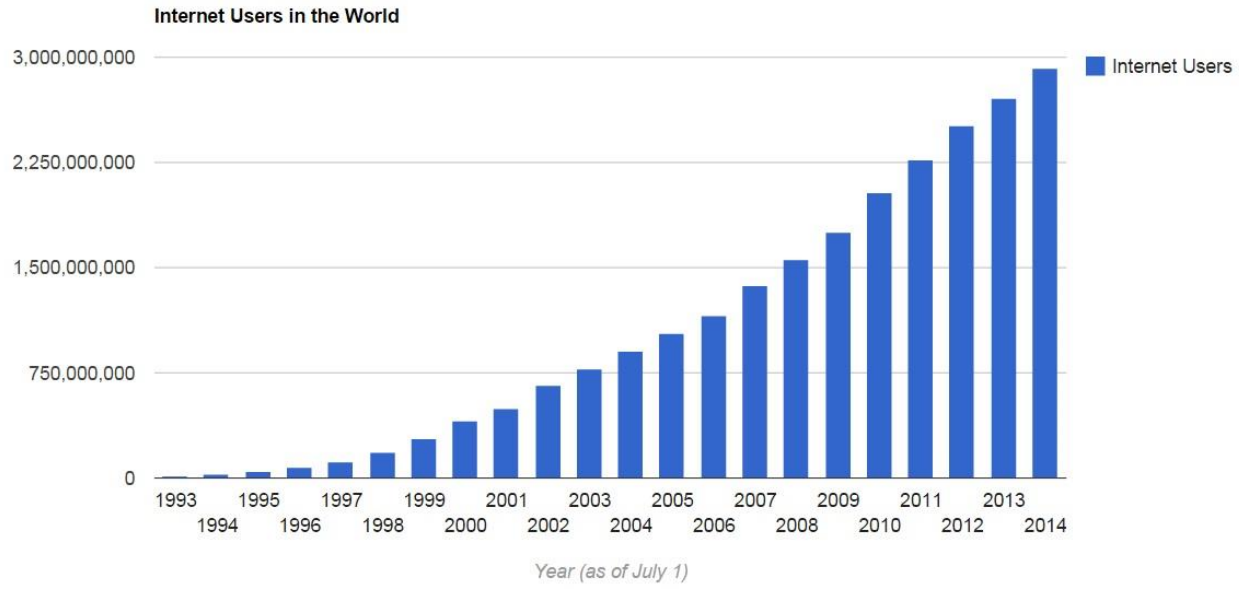
Depreende-se, então, que cibersegurança refere-se à proteção e garantia de utilização de infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) responsáveis pelo controle das infraestruturas críticas nacionais (CRUZ JÚNIOR, 2013). A dinâmica de ciberpoder (principalmente na sua face que tange à parte física do ciberespaço, as cibercapacidades) e cibersegurança, então, mostra-se em muito conectada com a proteção desses ativos físicos de grande interesse aos Estados.

[43] "The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet. [...] Vulnerabilities result from weaknesses in technology and because of improper implementation and oversight of technological products". (KRAMER, 2009, p.03)

3. A SECURITIZAÇÃO DO CIBERESPAÇO, A GOVERNANÇA DA INTERNET E A POSIÇÃO BRASILEIRA NA DINÂMICA INTERNACIONAL

O próprio caráter multifacetado da Internet demonstra que ela constitui uma ferramenta de incrível versatilidade, ao tempo que sua característica da convergência de diversas interações catalisa as relações de Poder e do próprio ciberpoder na esfera do ciberespaço. Assim, o crescimento da Internet demonstra cada vez mais necessidade de atenção a ser despendida com o assunto em escala mundial. O número de indivíduos conectados à rede chega a cerca de 40% da população mundial hoje. Na época da "abertura" comercial da Internet, a proporção era inferior a 1% (INTERNET LIVE STATS, 2014).[44]

Gráfico 1 - Usuários de Internet no Mundo



* Estimativa para 1º de julho de 2014

Fonte: Internet Live Stats (2014) - elaboração de dados pela União Internacional de Telecomunicações (UIT) e da Divisão de População das Nações Unidas.

Nesses termos, a populosa China figura como país com a maior parcela da população mundial da Internet, com 641.601.070 usuários (21,9%), seguida dos Estados Unidos, que possui 279.834.232 internautas (9,58%). O Brasil ocupa somente a quinta posição nesse ranking, apresentando 3,69% (107.822.831) dos indivíduos conectados no planeta, mas com

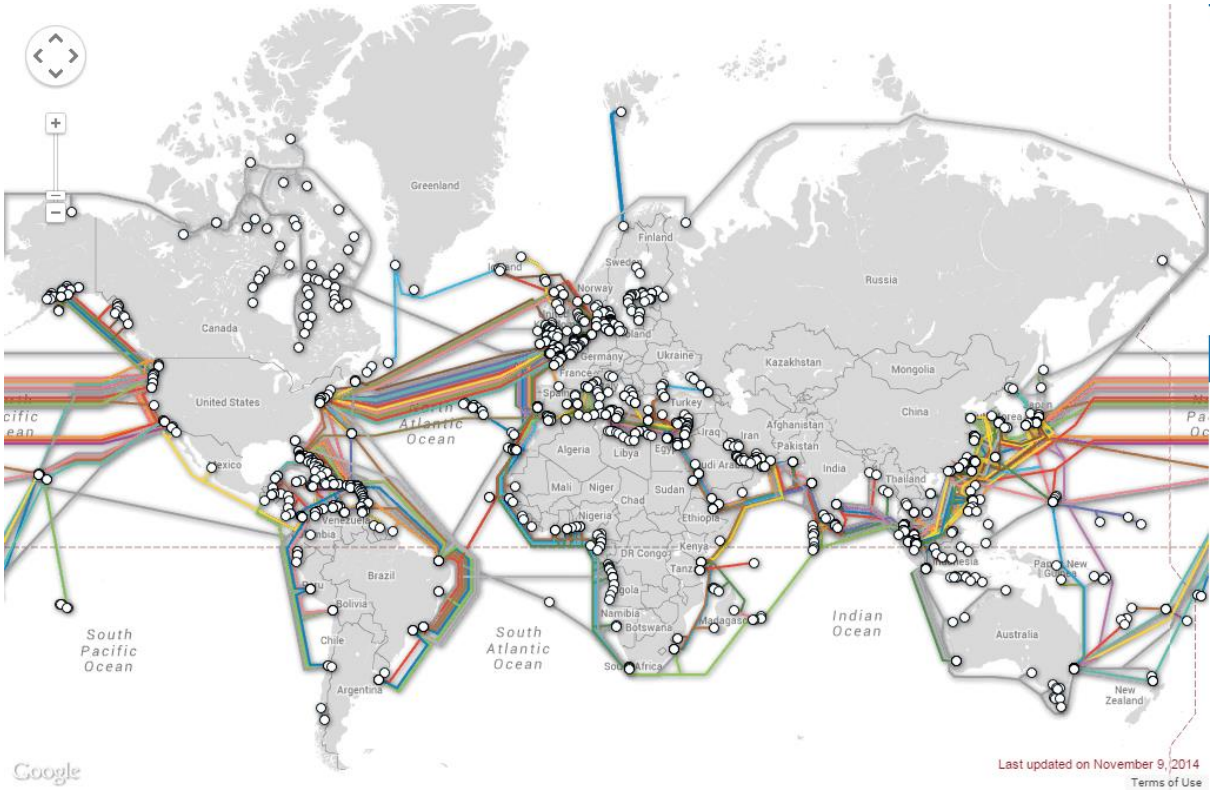
[44] Em 2005, foi atingido o primeiro bilhão; o segundo em 2010; e o terceiro bilhão se completa em 2014 (INTERNET LIVE STATS, 2014).

uma baixa penetração[45]: algo em torno de 53,37% (107.822.831 usuários). Por exemplo, os Estados Unidos possuem uma das maiores penetrações entre os países, com 86,75% (INTERNET LIVE STATS, 2014), mais um sinal da dependência, importância e atenção que a rede recebe nesse país, uma vez que as necessidades e interações da população (e do próprio governo) se dão por meio da rede, originando *inputs*[46] ao governo em relação a tal área.

3.1 O Pioneirismo Estadunidense e a Inserção Brasileira

O grande alcance dos Estados Unidos na camada física que envolve a Internet e o ciberespaço, combinado com a posição de potência militar com pretensões hegemônicas no sistema internacional torna notório o reconhecimento de grande capacidade relativa americana, em termos tecnológicos, de acompanhar a expansão da *net* e fazer uso e vantagem de suas lacunas, principalmente em termos securitários.

Figura 3 - Mapa Mundial de Cabos Submarinos



Fonte: TeleGeography (2014)

[45] *Penetração* diz respeito à porcentagem ou parcela da população do país com conexão à Internet.
[46] *Inputs* são demandas de uma população ao governo em relação a determinada questão.

Logo, como se pode observar (Figura 3), no que tange à primeira camada do ciberespaço, uma centralidade estadunidense é visível, uma vez que a grande maioria do cabeamento submarino parte dos Estados Unidos, além de muitos deles serem os primeiros a existirem no mundo. De Canabarro (2014), em sua descrição, pode-se inferir o predomínio americano, principalmente de caráter físico cibernético:

> A espinha dorsal da Internet é formada pela interconexão pareada de redes de provedores de serviços de telecomunicação e pouco mais de uma dezena de empresas opera nesse nível de interconectividade total. Um levantamento do ano de 2012 computou apenas doze delas: sete são sediadas nos EUA. A raiz da Internet é formada por treze servidores espalhados no mundo, controlados por entidades públicas e privadas, com e sem fins lucrativos. A gestão e o controle da raiz estão a cargo da Internet Corporation for Assigned Names and Numbers (ICANN), supervisionada pelo Departamento de Comércio dos Estados Unidos. Dez daqueles servidores encontram-se nos Estados Unidos, um na Suécia, um na Holanda e outro no Japão. (CANABARRO, 2014, p.47)

Em contraponto, Kramer e Wentz (2009) afirmam que os americanos vêm perdendo influência no campo cibernético a nível mundial. Os Estados Unidos apresentariam, de fato, uma enorme capacidade cibernética, contudo sua influência não se traduziria de forma proporcional.

> O status dos Estados Unidos como uma superpotência informacional não se traduziu para a influência internacional. Tanto a pesquisa da Pew publicado em meados de 2006, e a pesquisa da BBC publicada em janeiro de 2007 ressaltam a percepção internacional em declínio dos Estados Unidos. (KRAMER; WENTZ, 2009, p.08, tradução nossa)[47]

Apesar de uma série de esforços para melhorar a sua imagem com o uso regular da Internet e de outros meios de comunicação para promover sua figura, os Estados Unidos têm atualmente o entrave da influência, que se mostra decrescente. Logo, por mais que a governança da Internet tenha caráter multidimensional e pluriparticipativo, onde os direitos e deveres dos atores conectados a rede são determinados, assim como qualquer tecnologia, a rede não é um campo "unidimensional, estático e neutro", sendo este um espaço para interações políticas e com uma perceptível vantagem inicial dos Estados Unidos, hoje em gradual declínio.

Nesses termos, o debate acerca da governança da Internet surge como um tema de vital importância, com urgência a ser abordado, a fim de que se atinja uma melhor e mais democrática gestão da rede. A interpretação da "governança da Internet" baseia-se no conceito de "governança sem governos" (KLEINWÄCHTER, 2007) e alude à gerência técnica da rede.

---

[47] "U.S. status as an information superpower has not translated to international influence. Both the Pew poll published in mid-2006 and the BBC poll published in January 2007 underscore the declining international perception of the United States." (KRAMER; WENTZ, 2009, p.8)

Dentre as principais instituições ligadas ao controle da rede, principalmente à sua governança, podemos citar com destaque a ICANN (*Internet Corporation for Assigned Numbers and Names*). Criada pelo governo dos Estados Unidos em 18 de setembro de 1998, é uma corporação sem fins lucrativos composta amplamente por membros da ISOC (*Internet Society*)[48] e com funções como a coordenação da gestão dos elementos técnicos do DNS (*Domain Name System*) para que seja possível achar os vários endereços válidos da Internet por meio da resolução dos *Domain Names*[49], ou nomes de domínio (ICANN, 2012).

DNS é um sistema gerenciamento hierárquico e distribuído, que armazena informações sobre nomes de *host* e nomes de domínio, sendo assim responsável pela tradução (ou a chamada resolução) de endereços numéricos (endereços IP) para o formato alfabético, facilitando a localização de *websites* para os usuários.

> Cada servidor tem um endereço IP único, que é apenas um conjunto de números, como 194.8.63.155. [...] No entanto, porque é difícil lembrar números, um endereço de IP pode ser associado a um nome de domínio. (MÖLLER, 2007, p.33 tradução nossa)[50]

Funções como a coordenação citada anteriormente e uma série de tarefas relacionadas à Internet são herdadas e assumidas da IANA (*Internet Assigned Numbers Authority*)[51], que realizava tais papéis em nome do governo dos Estados Unidos (MÖLLER, 2007). Assim, a ICANN marca uma maior distributividade (ainda que longe de suficiente) de poder sobre a Internet criando um GAC (Comitê Governamental de Aconselhamento)[52] como meio de exercício de influência dos países membros da ONU nas decisões do órgão (apesar de não incluir votos) e reforçando um caráter internacional da instituição. Suas raízes, entretanto,

---

[48] A *Internet Society* (ISOC), fundada em 1992 por Vint Cerf e Bob Kahn, também é uma organização sem fins lucrativos, com o foco na transparência no sustento da evolução técnica da Internet como uma plataforma para invoção, desenvolvimento econômico e progresso social ao redor do globo. Sediada na cidade de Reston (Virgínia, EUA) e com mais de 28.000 membros, é financiada pela *Corporation for National Research Initiatives*, um grupo do governo americano (ISOC, 2014).

[49] "Um nome de domínio é o nome de um computador na Internet que o distingue de outros sistemas na rede. Nomes de domínio são, por vezes, coloquialmente conhecidos como endereços da Web." (MÖLLER, 2007, p.33)

[50] "Each server has a unique IP address which is just a set of numbers, such as 194.8.63.155. […] However, because it is difficult to remember numbers, an IP address can be associated with a domain name." (MÖLLER, 2007, p.33)

[51] Empresa regulada pelas leis da Califórnia e que também substituiu uma primeira autoridade numeradora sediada em Stanford (CANABARRO, 2012).

[52] "a. O Comitê Consultivo Governamental deve considerar e aconselhar sobre as atividades da ICANN relacionadas aos assuntos governamentais, principalmente aqueles que podem ter uma interação com as políticas da ICANN e várias leis e acordos internacionais ou que podem afetar políticas públicas.

b. A afiliação ao Comitê Consultivo Governamental deve estar aberta a todos os governos nacionais. A afiliação também deve estar aberta a economias distintas, conforme reconhecidas em fóruns internacionais e organizações governamentais multinacionais e organizações de tratados no convite do Comitê Consultivo Governamental por meio de seu Presidente". (ICANN, 2012)

ainda representam a enorme capacidade e potencialidade americana para a manipulação do espaço da rede, em vista de sua criação ter partido de uma "iniciativa" estadunidense e de seu Departamento de Comércio.

Dessa forma, depois da abertura comercial da rede, a governança multissetorial passou a ganhar maior ênfase na gestão da Internet a nível mundial. Atores estatais e não estatais instituem, a partir de então, relações de conflito e cooperação para tentar regular e "governar" a Internet.

> Governos que não o governo dos EUA se deram conta de quão pouco podiam controlar o que acontece dentro e ao redor da Internet. À medida que a Internet cresceu como mecanismo poderoso de crescimento econômico e discurso político, as questões da Internet tomaram significância que não possuíam alguns anos atrás. O que certa vez foram consideradas questões técnicas a serem relegadas a cientistas e engenheiros passaram a ser questões de políticas públicas que interessam enormemente uma série de pessoas que reivindicam participação nas decisões. (KWALWASSER, 2009, p.01)[53]

O papel do Brasil, nesse aspecto, adentra o tema de maneira essencial. Aliado a alguns parceiros (como Alemanha, Argentina, Bolívia, Equador, países do BRICS[54], entre outros)[55], o país faz forte crítica ao controle americano da Internet e fomenta a participação dos governos com igualdade para com a rede. A aprovação do Marco Civil da Internet - lei que prevê princípios, garantias, direitos e deveres na regulamentação do uso da Internet no Brasil e determina critérios para a atuação da União, dos Estados, do Distrito Federal e dos Municípios relativa ao assunto (BRASIL, 2014d) -, se mostra, nesse contexto, como uma articulação das forças políticas nacionais para garantir uma resposta à sociedade. Tal elemento impacta na política doméstica e também na externa, pois se reflete na inserção do Brasil e na promoção de sua imagem internacionalmente.

Logo, o Marco Civil da Internet representa o avanço dos anseios brasileiros na busca de uma horizontalidade de competências, deveres e poderes sobre a Internet que, quase ao mesmo tempo, é seguido por uma iniciativa internacional. Isso verifica a necessidade de uma sustentação interna do Brasil a respeito do tema da cibersegurança e, especificamente, da

---

[53] "Governments other than that of the United States have realized how little they can control what happens in and around the Internet. As it has grown into a powerful engine of economic growth and political speech, Internet issues have taken on a significance they did not have just a few years ago. What were once considered technical questions to be left to scientists and engineers have become matters of public policy that greatly interest large numbers of people who claim a stake in the decisions". (KWALWASSER, 2009, p.01)

[54] Rússia, China e África do Sul, além do próprio Brasil.

[55] O Brasil vem aproveitando a visita de chefes de Estado e seus representantes e as viagens de seus diplomatas para emitir comunicados a favor da regulamentação da Internet e contra atitudes invasivas no ciberespaço, bem como acordos de cooperação na área de cibersegurança. Até maio de 2014, o Itamaraty relatou a assinatura de documentos com França, Espanha, Alemanha, China e Índia, que afirmava a adoção do Marco Civil brasileiro como modelo internacional de governança da internet (ITAMARATY, 2014).

segurança da informação, para assim promover uma política externa com moldes em iniciativas nacionais, demonstrando o engajamento brasileiro para com a questão e uma independência em relação ao assunto (a política externa "ativa e altiva").

Desse modo, nasce a ideia de sediar o NETmundial[56], evento sobre a governança da Internet, que partiu da presidente Dilma Rousseff durante seu discurso na abertura da Assembleia Geral da ONU em 2013, devido às denuncias de espionagem em massa realizada pelos Estados Unidos (KELION, 2014). É nítida, no discurso da presidente, a afirmação da importância da ONU para o funcionamento do Sistema Internacional e a cobrança de uma maior ação do organismo nesse sentido. É justamente nesse ponto que o discurso de Dilma na ONU parece antecipar o que viria a ser a mobilização do Brasil em termos multilaterais na discussão da cibersegurança e da governança da Internet em âmbito global. Ao condenar o uso do meio cibernético para fins de guerra, Dilma afirma a necessidade de uma regulamentação dos temas relacionados ao ciberespaço:

> A ONU deve desempenhar um papel de liderança no esforço de regular o comportamento dos Estados frente a essas tecnologias e a importância da internet, dessa rede social, para construção da democracia no mundo. Por essa razão, o Brasil apresentará propostas para o estabelecimento de um marco civil multilateral para a governança e uso da internet e de medidas que garantam uma efetiva proteção dos dados que por ela trafegam. (ROUSSEFF, 2013)

Em seu discurso na NETmundial, Dilma Rousseff relembrou a importância da convergência diplomática entre Brasil e Alemanha na ONU e reiterou a importância do Marco Civil brasileiro como modelo de gestão da internet a ser adotado internacionalmente, além de reforçar o papel da discussão multilateral acerca do tema:

> Esse esforço requer, ainda, o fortalecimento do Fórum de Governança da Internet como instância de diálogo apta a produzir resultados e recomendações; uma ampla revisão dos 10 anos da Cúpula Mundial da Sociedade da Informação; e o aprofundamento das discussões sobre ética e privacidade na UNESCO. O Brasil tem a sua parte de contribuição a dar, a partir do amplo processo interno de discussão, de debate, de contribuições que resultou na lei do Marco Civil da Internet, aprovada ontem pelo Congresso Nacional e que eu tive a honra de sancionar, aqui, há pouco. (ROUSSEFF, 2014)

Ainda, em depoimento ao Senado, anterior ao evento, o Ministro Figueiredo enfatizou que a NETmundial foi um exemplo da disposição do Brasil "em liderar um movimento a

[56] Encontro Multissetorial Global Sobre o Futuro da Governança da Internet organizado em uma parceria do Comitê Gestor da Internet no Brasil (CGI.br), que aconteceu nos dias 23 e 24 de abril de 2014 em São Paulo. Teve como foco a elaboração de princípios de governança da Internet e a proposta de um roteiro para a evolução futura da rede em termos da multipolaridade e multissetorialidade (NETMUNDIAL, 2014), a qual sofre várias críticas em função do poder de controle americano.

favor do aprofundamento da cooperação internacional voltada para a construção de uma governança da internet" (ITAMARATY, 2014).

Hodiernamente, na Declaração Multissetorial de São Paulo (declaração da NETmundial sobre a Governança Multissetorial, 2014) encontram-se grandes indícios dessa escalada à uma maior distributividade de competências sobre a rede. Atentando ao respeito aos direitos humanos, diversidade cultural, segurança, resiliência e ao caráter distributivo da Internet, as recomendações do documento apresentam com grande relevância a questão da extensão do IGF (Fórum de Governança da Internet) para além dos seus cinco anos de mandato (seu primeiro mandato acabou em 2010 e o último encontro do segundo está previsto para novembro de 2015 no Brasil, em João Pessoa) (BADII, 2014) e, principalmente, demonstram a debatida intenção estadunidense de fazer a transição da administração de funções da IANA/ICANN, demonstrada desde 14 de março de 2014 (NTIA, 2014).

> 5. No seguimento do recente e bem-vindo anúncio do governo dos Estados Unidos em relação a sua intenção de fazer a transição da administração de funções da IANA, a discussão sobre mecanismos para garantir a transparência e a prestação de contas dessas funções após o término do papel do Governo dos EUA deve ter acontecer por meio de um processo aberto, com a participação de todos os interessados que se estendem para além da comunidade da ICANN; [...] Qualquer mecanismo adotado deve proteger a natureza progressista, aberta e participativa dos processos de desenvolvimento de políticas e assegurar a estabilidade e resiliência da Internet; [...] Esta transição deve ser conduzida [...] reforçando o princípio da igualdade de participação entre todos os grupos das partes interessadas e que se esforçando no sentido de uma transição a ser concluída até Setembro de 2015. (NETmundial, 2014 tradução nossa)[57]

Até os dias de hoje, o controle da ICANN permanece sendo exercido pela NTIA (*National Telecomunications and Information Agency*), agência americana com o papel de aconselhamento presidencial para assuntos de telecomunicações e informação. O atual contrato expira em 30 de setembro de 2015, mas são notáveis os entraves impostos pelos Estados Unidos no tema da própria neutralidade da rede (GROSSMANN, 2014). Os Estados Unidos reforçam a necessidade de se atender às expectativas dos clientes e parceiros globais dos serviços de Internet e, veemente, negam um controle multilateral, posição defendida por

[57] "5. In the follow up to the recent and welcomed announcement of US Government with regard to its intent to transition the stewardship of IANA functions, the discussion about mechanisms for guaranteeing the transparency and accountability of those functions after the US Government role ends, has to take place through an open process with the participation of all stakeholders extending beyond the ICANN community; Any adopted mechanism should protect the bottom up, open and participatory nature of those policy development processes and ensure the stability and resilience of the Internet; This transition should be conducted […] maintaining the security and stability of the Internet, empowering the principle of equal participation among all stakeholder groups and striving towards a completed transition by September 2015". (NETMUNDIAL, 2014)

Dilma Rousseff. A justificativa é que um processo multilateral coibiria a participação de atores não governamentais que hoje estariam presentes no âmbito da governança da Internet.

Apesar do grande debate pela frente, os esforços brasileiros (como, por exemplo, a declaração oficial do NETmundial com uma menção à neutralidade de rede e ao reforço, de leve, a crítica à vigilância em massa) apontam com isso a uma governança multissetorial, e o Fórum de Governança da Internet, como instância indicada para o espaço de discussão, contribui para identificar os possíveis caminhos da governança de como endereçá-los (PRESCOTT, 2014).

De fato, os EUA possuem certa vantagem para manobras por ter influência desde os primórdios da criação das ferramentas virtuais - por exemplo, da *World Wide Web* (em 89, com Berners-Lee) - até o momento (ou além) da abertura comercial da Internet. Desse modo, é inegável que os Estados Unidos, até os dias de hoje, constituem um modelo a ser seguido em matéria de gestão de instituições vitais ao funcionamento da Internet e, por consequência, do ciberespaço.

Porém, mais uma vez, poder-se-ia entender um nível alto dos EUA em termos de ciberpoder, vistas suas óbvias capacidades tangíveis do ciberespaço. Contudo, como já abordado no capítulo anterior, a conceituação de ciberpoder herda certos debates e problemas da sua antecessora teoria de Poder. Um desses grandes entraves é a ainda não definida mensurabilidade do ciberpoder, uma vez que o conceito é novo e, além disso, o próprio ambiente em que se desenvolve - o ciberespaço - é relativamente de recente importância. Ainda, ataques cibernéticos, como DDoS (*Distributed Denial of Service*)[58], inserção de *malwares* e rupturas de SCADA[59] (*Supervisory Control and Data Acquisition*), apresentam o já mencionado problema da atribuição, uma vez que estão presentes diversos atores, de diversas naturezas, no ciberespaço (governos, organizações e indivíduos)[60], dificultando a delegação de responsabilidades entre os Estados (e, assim, influindo na dinâmica de ciberpoder). Além disso, no campo cibernético, danos causados a estruturas de um Estado

[58] Ataques executados principalmente por meio de *botnets* - redes de 'computadores-robôs' que permitem o controle remoto seus sistemas através pelo criador da *botnet*, o *botmaster* - para criar vasta quantidade de tráfego e direcioná-lo a um sistema a fim de que este se sobrecarregue e não funcione corretamente, efetivamente negando acesso ao serviço oferecido. (ZIOLKOWSKI, 2014, p.38). Os ataques possuem tipicamente como alvo sites ou servidores de bancos, gateways de pagamento de cartão de crédito ou até mesmo servidores de nomes de raiz.

[59] SCADA, ou "Sistemas de Supervisão e Aquisição de Dados", são sistemas que dispõem de software para monitoramento, supervisão e controle das variáveis e dos dispositivos de sistemas industriais, majoritariamente.

[60] "Na prática, os governos e as jurisdições geográficas desempenham um papel importante, mas o domínio também é marcada pelo difusão de poder". (NYE JR, 2010, p.03 tradução livre)

podem ser de difícil observação, a menos que a informação flua de volta a partir do sistema atacado ou que mesmo um Estado divulgue o incidente sofrido (IISS, 2014, p.14).

Para uma aproximação do tema em relação específica aos atores estatais, pode-se utilizar como parâmetro inicial – para, no futuro, se analisar o ciberpoder de fato - o exame do que seriam as capacidades cibernéticas, as quais o *International Institute for Strategic Studies* (IISS, 2011) faz menção, entretanto com as mesmas ressalvas.[61] Nesses termos, é proposta uma série de possíveis indicadores pelo mesmo IISS, em 2014, para tal medição, visto que é evidente a grande dificuldade ainda de atribuição de um caráter quantitativo aplicável ao conceito. Indicadores como sistema político, estabilidade social e número de estudantes de pós-graduação (entre outros), caracterizam uma sugestão demasiadamente ampla para a mensuração das capacidades dos países – várias são pertinentes também, mas às vezes pecam por uma não uniformidade para sua análise.[62]

Nye Jr. (2010) sugere que governos podem tomar medidas visando subsidiar a infraestrutura, educação em computação e proteção da propriedade intelectual, os quais incentivarão (ou desencorajarão) o desenvolvimento de capacidades dentro das suas fronteiras. "A provisão de bens públicos, incluindo um ambiente legal e regulado, pode estimular o crescimento comercial das capacidades cibernéticas" (NYE JR, 2010:9 tradução livre).[63]

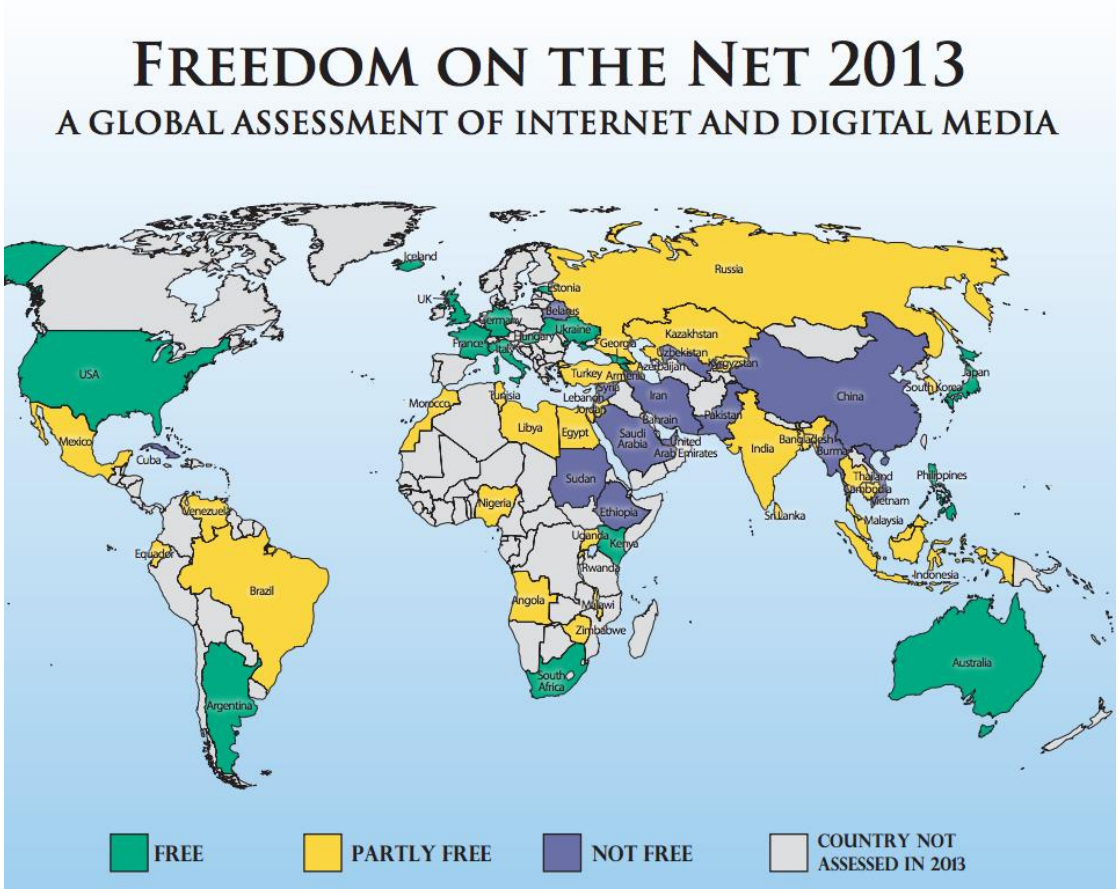
Portanto, propõe-se uma análise (mesmo que também ampla) das capacidades cibernéticas como ponto inicial para a avaliação de ciberpoder de algum país, com um viés um tanto mais qualitativo. Consideram-se importantes (principalmente para o foco na segurança) variáveis como posição internacional, ações regulatórias e liberdade na rede, doutrina de ciberestratégia, infraestrutura, investimentos, números de ISPs (*Internet Service Providers*), velocidade de acesso e conhecimento acumulado ou penetração da Internet para, desse modo, tornar mais fácil a abordagem no âmbito nacional brasileiro a ser feita mais adiante.

Aproveitando o exemplo dos Estados Unidos, sua posição internacional é evidentemente uma das melhores; possui até hoje grande influência sobre as principais (em especial a ICANN) instituições administradoras da Internet e é considerado um país com alto nível de liberdade na Internet (vide Figura 4); as políticas e doutrina de ciberestratégia

[61] "É importante que o *Military Balance* comece a incluir análises dos componentes militares do ciberpoder, contudo o problema está na definição do que se analisar" (IISS, 2011, p.20).
[62] Para a tabela completa de indicadores, ver: IISS (2014, p.15).
[63] "The provision of public goods, including a legal and regulatory environment, can stimulate commercial growth of cyber capabilities". (NYE JR., 2010, p.09)

americanas, de 2008/2009 (UNITED STATES, 2008), são as primeiras a nível mundial; a infraestrutura e o cabeamento são os mais completos também no mundo e, hoje em dia, apresentam o maior número de nodos de rede e origem de cabos submarinos (vide o mapa da Figura 3). Sobre o investimento, este é talvez o mais claro indicador do poder americano nessa esfera: os gastos dos EUA em segurança cibernética para FY2014 (planejamento orçamentário) está programado para saltar para US$ 4,7 bilhões, um aumento de 20% sobre os US $ 3,9 bilhões do FY2013, apesar de o Pentágono planejar cortar despesas (IISS, 2014); possuem 3603 ISPs (YAHOO, 2014); e a oitava maior média de velocidade de conexão (AKAMAI, 2013), com uma penetração entre as três maiores no mundo (INTERNET LIVE STATS, 2014).

Figura 4 - Liberdade na Internet



Fonte: Freedom House (2013)

3.2 O Brasil e os Esforços para o Desenvolvimento no Ciberespaço

A Era Digital, ao expandir o leque de informações disponíveis aos tomadores de decisão, também trouxe a necessidade de que fossem tomadas medidas para proteger essas

informações. Acontecimentos recentes, como os já mencionados ataques cibernéticos na Estônia em 2007, a guerra da Ossétia do Sul em 2008, a utilização do vírus *Stuxnet* (ataque de ruptura SCADA) no programa nuclear iraniano e o Wikileaks em 2010, demonstram que o ciberespaço tornou-se um dos níveis onde os Estados procuram maximizar sua segurança, competindo com diversos atores de outras naturezas. Visto o recente aumento de ameaças , o tema da cibersegurança no Brasil merece grande atenção, e o desenvolvimento de capacidades e meios para a proteção dos ativos do país se mostra essencial no médio prazo.

Logo, apesar de o termo "ciber" figurar pela primeira vez em algum documento oficial na Segunda Política Nacional de Defesa (BRASIL, 2005), no país, essa preocupação é evidente a partir da Estratégia Nacional de Defesa (aprovada pelo Decreto número 6.703, de 18 de dezembro de 2008), a qual define o setor cibernético entre os três setores estratégicos e essenciais para a defesa nacional - ao lado do espacial e do nuclear - (BRASIL, 2008) e prevê o desenvolvimento de uma organização com foco no desenvolvimento da área contemplada:

> As capacitações cibernéticas [...] incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. [...] No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. (BRASIL, 2008, p.33)

Além disso, o Livro Branco (2012) destaca a importância dos investimentos em segurança cibernética, atentando para as vulnerabilidades que a ameaça cibernética trouxe como preocupação, uma vez que colocariam "em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (BRASIL, 2012a, p.69). Ademais, dentro das provisões para a área cibernética, recebe boa atenção a questão do aperfeiçoamento de dispositivos e procedimentos de segurança para a redução das vulnerabilidades dos sistemas ligados à Defesa Nacional contra ataques cibernéticos (BRASIL, 2008, p.66). Nesse sentido, Celso Amorim (2013) também atribui grande importância e ênfase aos setores de Defesa, Segurança e Política Externa:

> Os armamentos cibernéticos podem ser usados para multiplicar a destrutividade de armamentos convencionais ou para facilitar o seu uso durante um conflito. A infraestrutura crítica de um país pode ser afetada de muitas formas pelos ataques cibernéticos, desde áreas sensíveis da soberania nacional até áreas que podem desorganizar a vida da sociedade, como os sistemas bancário, meteorológico, elétrico ou hospitalar. Embora seja uma ameaça cronologicamente nova, a guerra cibernética parece incorporar-se com rapidez à antiga lógica do sistema de Estados. (AMORIM, 2013, p.290)

Assim, as mencionadas infraestruturas sensíveis são então interpretadas como "infraestruturas críticas da informação" (CANONGIA; MANDARINO JUNIOR, 2009, p.07). Além desse conceito, o Brasil, ao nível do governo federal, adota também o conceito de "ativos de informação", lado a lado às "infraestruturas críticas", consideradas os subconjuntos de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e que, "se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade" (CDN, 2009).

> Art. 2º Para fins desta Portaria consideram-se Infraestruturas Críticas da Informação o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.
> Parágrafo único. Consideram-se ativos de informação os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. (CDN, Portaria 34, de cinco de agosto de 2009)

James A. Lewis (2006) explicita a importância da segurança das "Infraestruturas Críticas", uma vez que uma infraestrutura é considerada "crítica" em função de ela atender algum padrão de importância para o interesse nacional em que os bens ou serviços que presta são essenciais para a segurança nacional, a vitalidade econômica e modo de vida[64]. Para atender a essa norma, há uma suposição implícita de que o rompimento das infraestruturas reduziria o fluxo de bens e serviços essenciais e criaria dificuldades ou impedimentos ao governo e às operações econômicas (LEWIS, 2006). Os próprios Estados Unidos, após os ataques de 11 de setembro de 2001, com a administração Bush, redefiniram a infraestrutura de Internet como uma "infraestrutura crítica" para a segurança e economia americana e convocou uma nova abordagem para a Governança da Internet, mais orientada em termos securitários (KLEINWÄCHTER, 2007, p.56). Assim, Nye Jr. (2010) reforça a ideia da importância do caráter geográfico e de sua proteção, uma vez que "a camada de informação cibernética repousa sobre uma infraestrutura física que é vulnerável a ataque militar direto" (NYE JR., 2010, p.07 tradução livre)[65] ou de atores não estatais, como terroristas e criminosos.

Ainda, na percepção de que a construção das capacidades cibernéticas é indispensável, entende-se que a proliferação de tecnologias intrusivas reforça a assimetria internacional, beneficiando a atuação das grandes potências na disputa por poder global e prejudicando os

[64] "An infrastructure is judged to be critical because it meets some standard of importance for the national interest—in that the goods or services it provides are essential to national security, economic vitality and way of life. To meet this standard, there is an implicit assumption that the disruption of the infrastructures would reduce the flow of essential goods or services and create hardship or impede important government or economic operations." (LEWIS, 2006:04)

[65] "The cyber information layer rests upon a physical infrastructure that is vulnerable to direct military attack or sabotage both by governments and non-state actors such as terrorists or criminals". (NYE JR, 2010:7)

direitos dos cidadãos em prol da segurança nacional (AMORIM, 2013). A declaração do Ministro Figueiredo à Comissão de Relações Exteriores e Defesa Nacional do Senado indica o ganho de importância da questão cibernética:

> Ainda nesse campo da nova agenda, eu gostaria de dizer uma palavra especial sobre as questões relativas ao direito à privacidade na era digital, à governança da internet e à segurança da questão cibernética. Esses temas ganharam particular relevância para nós na sequência de notícias divulgadas, a partir de junho do ano passado, de interceptação não autorizada de comunicações e dados de cidadãos brasileiros, empresas, membros do Governo e a própria Presidenta da República. (ITAMARATY, 2014)

O que se percebe, portanto, principalmente a partir das revelações acerca das atividades conduzidas pela NSA, em 2013, é a incorporação da cibersegurança na agenda de promoção do multilateralismo e de defesa da multipolaridade do Brasil. Rapidamente, as revelações do Wikileaks, de junho de 2013[66], mostravam que a Agência de Segurança Nacional (NSA) estadunidense utilizava de um aparato considerável de espionagem eletrônica e monitoramento de dados de cidadãos norte-americanos, estrangeiros, empresas e Chefes de Estado de todo o mundo, evidenciando as consequências da estratégia de inserção norte-americana posterior a 2001. As denúncias envolviam a utilização de um dos programas da NSA, o Prism[67], consistindo em capturar dados privados de cidadãos que não eram suspeitos de qualquer ligação com terrorismo ou qualquer irregularidade - com a colaboração de empresas de tecnologia (as datas em que aparentemente começaram a cooperar foram divulgadas com o programa).[68] Apesar de os números não serem precisos, estima-se que em janeiro de 2013, o Brasil teve 2,3 bilhões de telefonemas e mensagens espionados, ficando atrás apenas dos próprios Estados Unidos (GREENWALD; KAZ; CASADO, 2013).

Em consequência desse contexto, o Brasil vem adaptando suas políticas públicas à questão cibernética. Especificamente, a Estratégia Nacional de Defesa (2008) já enfatizava a busca por cooperação com outros países como necessária para avanços nas tecnologias, as quais possam ser compatibilizadas com o objetivo de servirem à segurança nacional. Tal aspiração de cooperação se mostra compatível com a ideia de que Estados menos desenvolvidos, embora possam compreender o potencial militar do ciberespaço, poderiam efetivamente ser privados dos meios de exercer controle sobre o domínio cibernético em

[66] O especialista em computação e ex-funcionário da NSA, Edward Snowden, foi o responsável pelo vazamento de centenas de milhares de documentos que detalham os procedimentos secretos da agência americana.

[67] PRISM é uma ferramenta utilizada pela Agência de Segurança Nacional dos EUA para coletar dados eletrônicos particulares pertencentes aos usuários dos principais serviços da Internet, como Gmail, Facebook, Outlook e outros (GREENWALD, 2013). Considerando a evolução dos esforços de vigilância eletrônica do governo dos EUA pós-11/9, começou sob o mandato do presidente Bush com o *Patriot Act*.

[68] Cf. GREENWALD (2013).

função de uma falta de capacidade tecnológica e de inovação. O IISS (2014) explicita a dificuldade de se desenvolver capacidade cibernética eficazmente, sem um histórico bem sucedido de inovação em TI, manufatura e educação, ou em tradições militares e de segurança bem estabelecidas.

> No entanto, os países com infraestrutura de tecnologia pouco desenvolvida podem começar a aumentar sua força formulando capacidades específicas e estabelecendo alianças estratégicas. (IISS, 2014: 13-14 tradução nossa)[69]

É nesse sentido que o estudo do âmbito cibernético e o desenvolvimento de uma estratégia no campo importam para o futuro do próprio Brasil, tomando amplamente como base o argumento de Amorim (2013) sobre a proximidade da política de defesa e da política externa no contexto brasileiro atual:

> Hoje, é possível reunir essas diretrizes na ideia de uma *grande estratégia* brasileira, que combina política externa e política de defesa como objetivo de prover a paz. Do ponto de vista da política externa – e aqui falo naturalmente de minha experiência –, prover a paz significa acompanhar, promover e, quando possível, contribuir para o equacionamento pacífico de controvérsias (AMORIM, 2013, p.304).

A respeito do desenvolvimento de uma estratégia cibernética, poucos Estados as têm publicizado, e menos ainda detalharam em público as suas capacidades cibernéticas militares (IISS, 2014:12). Enquanto alguns consideram a necessidade de criar novas organizações dedicadas à cibersegurança e defesa, outros talvez ainda não vejam o setor cibernético como demandante de novas estruturas ou doutrinas, podendo colocá-lo dentro de disciplinas militares já existentes.

Em maio de 2011, os Estados Unidos anunciaram o lançamento da Estratégia Internacional Norte-americana para o Espaço Cibernético (UNITED STATES, 2011), sendo este um marco para o ambiente cibernético mundial, pois, "além de ser o primeiro nesse sentido, torna pública a posição estratégica e operacional do maior ator mundial no ambiente virtual" (CRUZ JÚNIOR 2013, p.16). No caso brasileiro, a doutrina militar ao lado da estratégia no campo cibernética é vista como um importante condicionante para a tradução de interesses estratégicos em objetos bem sucedidos, por meio de capacidades operacionais, atualmente com foco na cibersegurança[70].

---

[69] "Nonetheless, countries with poorly developed technology infrastructure can begin to grow capacity by formulating niche capabilities and establishing strategic alliances". (IISS, 2014, p.13-14)

[70] A respeito disso, Samuel César da Cruz Júnior (2013) afirma uma complementaridade do conceito de cibersegurança com o que se entende por defesa cibernética. De fato, por vezes, as definições se confundem, uma vez que defesa diz respeito "às ações de proteção do Estado brasileiro frente a ameaças que possam colocar em risco a soberania nacional" (CRUZ JÚNIOR, 2013, p.11).

O Brasil ainda não dispõe de uma doutrina ou documento que delimite as diretrizes próprias de uma estratégia nacional de defesa e segurança cibernética (CRUZ JÚNIOR, 2013), mas um bom ponto de partida para a análise do incremento dessas aspirações brasileiras é detalhando os desenvolvimentos organizacionais importantes no âmbito, como forma de indicar a mobilização da nação em resposta às ameaças cibernéticas. Nesses termos, a criação do CDCiber o Centro de Defesa Cibernética (equivalente ao *USCyberComm* nos EUA, situando-se dentro da NSA), se mostra balizador principalmente a partir de 2012 (SÁ, 2012) - quando a aproximação dos Grandes Eventos no país se mostraram requerentes de uma maior garantia de proteção cibernética. Antes mesmo do caso Snowden, o Ministério da Defesa e o Gabinete de Segurança Institucional (GSI/PR) já haviam declarado que o Brasil apresentava grandes espaços passíveis de intrusão através de meios eletrônicos. O lento processo de assimilação dessa necessidade foi a iniciativa de criação, em 2010, por meio das Portarias número 666 e 667 (EB, 2010), do CDCiber pelo exército, com sua consolidação prevista no Livro Branco (BRASIL, 2012a).

Nessas portarias, ficou estabelecida a criação do Núcleo do Centro de Defesa Cibernética (NU CDCiber), subordinado ao Departamento de Ciência e Tecnologia, responsável pela implantação do Centro de Defesa Cibernética do Exército. Em 2012, com a adoção do Livro Branco[71], a consolidação plena do CDCiber foi prevista até 2015, devendo ser formalmente criado por meio de decreto presidencial (CANABARRO, BORNE, 2013). O Centro de Defesa Cibernética teve um orçamento aprovado e previsto para quatro anos (2012 a 2015) de R$ 400 milhões[72] "a serem liberados em quatro partes iguais a cada ano" (CRUZ JÚNIOR, 2013, p.33).

Nesse aspecto, reside um problema: o orçamento previsto para o quadriênio não corresponde àquilo que foi dispendido. Apesar de um aumento de 20% em 2012 (quando o CDCiber entra em atividade), em função da Rio+20 (CRUZ JÚNIOR, 2013), o orçamento para defesa cibernética, previsto no Projeto de Lei Orçamentária Anual (Ploa), foi reduzido em R$ 20 milhões para o ano de 2014. "Apenas R$ 70 milhões foram destinados à ação 'Implantação do Sistema de Defesa Cibernética', valor que representa 78% dos R$ 90 milhões previstos no Ploa 2013" (CONTAS ABERTAS, 2013). Além disso, dos R$ 90 milhões

[71] Ações de curto prazo são previstas no Livro Branco (2012), como a implementação de uma escola de defesa cibernética, a construção da sede permanente do CDCiber, a aquisição de infraestrutura de apoio e formação de recursos humanos, além de aquisição de soluções de hardware e software para defesa cibernética, visando aumentar a capacidade do país na resposta de ameaças nacionais e internacionais (BRASIL, 2012a, p.198 apud CANABARRO; BORNE, 2013).

[72] No entanto, o general José Carlos dos Santos, chefe do Centro de Defesa Cibernética do Exército, afirma que seriam necessários pelo menos R$ 800 milhões (SENADO, 2013).

autorizados em 2013, somente R$ 15,7 milhões foram empenhados (reservados em orçamento para pagamento posterior) de fato. Ainda, o chefe do Centro de Defesa Cibernética do Exército, general José Carlos dos Santos, admitiu as dificuldades orçamentárias no setor:

> Para fazermos progredir alguns programas que acelerem a implantação da defesa cibernética no âmbito do ministério, nós teríamos que dobrar o orçamento inicialmente previsto. Os recursos para implantação do setor cibernético no Exército foram de R$ 400 milhões. Em 2012, dos R$ 81,5 milhões iniciais, foram alocados R$ 61 milhões. Em 2013, estavam previstos R$ 110 milhões, que acabaram reduzidos para R$ 90 milhões. (EM DISCUSSÃO, 2013)

Mais especificamente, a Lei Orçamentária Anual de 2013 mostra uma despesa para "implantação do Sistema de Defesa Cibernética" avaliado em R$ 67.520.000,00 (BRASIL, 2014e, p.388), ao passo que a Loa de 2012 demonstra um valor de R$ 83.678.780,00 (BRASIL, 2012, p.148): um decréscimo de 19,32% (R$ 16.158.780,00), pontualmente. Para 2014 o montante previsto para "Implantação do Sistema de Defesa Cibernética" é R$ 70.000.000,00 Comando do Exército (BRASIL, 2014f, p.129).

Além do mais, ações como a projeção do Projeto de Defesa Cibernética de investimento de R$ 840 milhões até 2031 (CANABARRO; BORNE, 2013) se mostram muito distantes no curto prazo para concretizarem avanços necessários em termos de segurança no campo. Entretanto, atualmente o CDCiber busca solidificar parcerias e com centros acadêmicos e de pesquisa e com a própria iniciativa privada (CRUZ JÚNIOR, 2013). Logo resta saber quanto tempo essas aproximações hão de levar para se concretizarem.

Ainda, um aspecto organizacional se mostra também um entrave para a proteção nacional no ciberespaço. "No Brasil, fez-se a opção por segregar a direção das ações de segurança da informação e defesa cibernética em dois órgãos distintos e independentes entre si, respectivamente: GSI/PR[73] e CDCiber/EB/MD" (CRUZ JÚNIOR, 2013, p.28). Essa descentralização acaba por ser desvantajosa, uma vez que depende da afinidade, integração e colaboração dos dirigentes das instituições e, assim, o nível de colaboração passa a ser relativizado conforme a conveniência do momento.

Nos dias de hoje, aproximadamente de 35 a 40 empresas de desenvolvimento de soluções em segurança cibernéticas se localizam no Brasil. Entretanto, a quantidade de empresas nacionais se mostra muito reduzida, principalmente levando-se em consideração o contexto futuro. "O setor público jamais conseguirá atingir níveis desejados de segurança ou

[73] O GSI é o Gabinete de Segurança Institucional da Presidência da República e cumpre o papel de coordenador, no âmbito da Administração Pública Federal (APF), englobando assuntos estratégicos como segurança das infraestruturas críticas nacionais; segurança da informação e comunicação; e segurança cibernética (CRUZ JÚNIOR, 2013, p.25).

defesa sem parcerias com o setor privado e vice-versa" (CRUZ JÚNIOR, 2013, p.28). Nesse aspecto, o Livro Verde (2010) atenta para os obstáculos do Brasil em termos da segurança cibernética, abrangendo aspectos econômicos, sociais e político-institucionais, "como a criação de estímulos para a indústria de TI nacional e da adaptação do quadro legal em torno das TIC no setor público" (CANABARRO; BORNE, 2013, p.07). Assim, Amorim (2013) afirma que "hoje o desenvolvimento de capacidades autônomas na indústria de defesa é um objetivo fundamental de nossa política" (AMORIM, 2013:308), expressando a consolidação e a expansão da base industrial de defesa como uma das prioridades do governo Dilma e citando a criação, em março de 2012, dos conceitos de Produto Estratégico de Defesa e Empresa Estratégica de Defesa pela Lei 12.598 (BRASIL, 2012b).

Visto isso, para a construção de capacidade militar cibernética eficaz, é imperativo um setor de TI civil e comercial frutífero. O nível de tecnologia avançada disponível e um alto padrão de pesquisa e desenvolvimento (P&D) em cibersegurança, aliado a um alto grau de penetração da Internet aumenta o potencial de inovação e criatividade do país, consequentemente alavancando o crescimento no campo cibernético (IISS, 2014, p.12). Caso contrário, com uma dependência de utilização, por parte do Brasil, de sistemas de computadores de fabricação estrangeira, outros Estados rivais podem ganhar uma vantagem estratégica: se eles têm uma forte produção de TIC para o mercado brasileiro, uma vantagem de defesa sobre o país comprador é quase que óbvia.

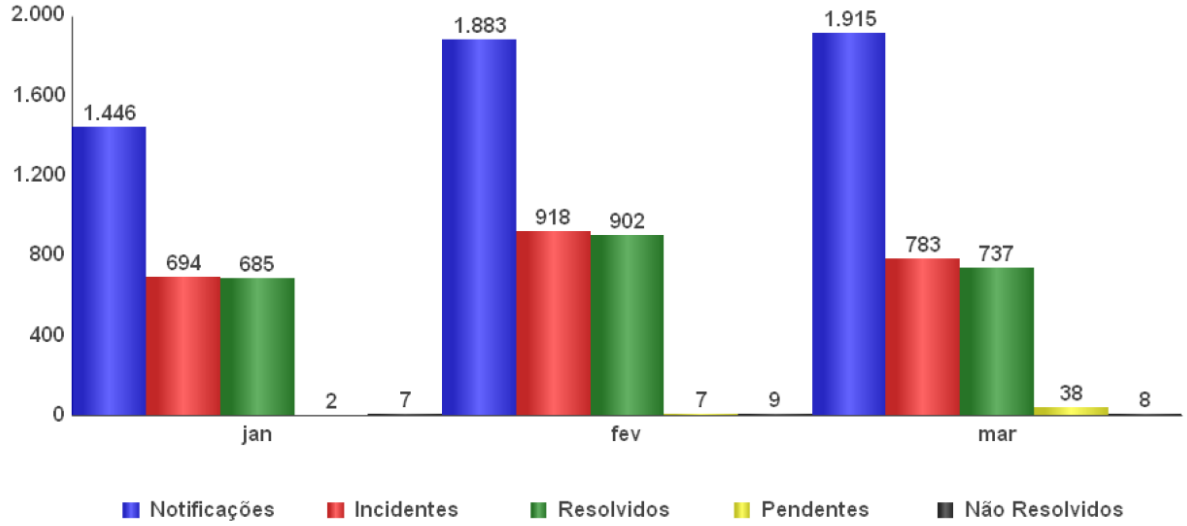
Entretanto, mais uma vez, uma ressalva a ser feita é a crescente de ataques aos ativos de informação no âmbito privado também. A EY Brasil (antiga Ernst & Young) divulgou resultados de sua 16ª Pesquisa Anual Global sobre Segurança Cibernética e constatou que para 54,2% dos empresários brasileiros os riscos de ataques cibernéticos aumentaram no ano de 2013 e 62,2% das empresas declararam a ampliação de seus investimentos em segurança da informação (CANALTECH, 2014). Tais indicativos denotam a preocupação dos empresários brasileiros e, com isso, as empresas estão também demandando da máquina pública infraestrutura, em função do aumento dos investimentos na securitização de seus ativos no ciberespaço. Por ano, estima-se que o Brasil gaste, empatado com a Índia, US$ 8 bilhões (CAMPI, 2013), que são desviados com o cibercrime.

Ainda, em função do destaque brasileiro adquirido por uma ascensão econômica notável e a própria inserção que vem sendo adquirida pelo país, muita atenção vem sendo voltada para o governo em termos de ameaças cibernéticas. A nível de América Latina, o Brasil figura na primeira posição "em todos os critérios de vulnerabilidade" (CRUZ JÚNIOR, 2013) e, atualmente, são notificados cerca de 2.700 incidentes de segurança cibernética por

mês nas redes da Administração Pública Federal, provenientes de países como Estados Unidos, Brasil, Alemanha, França (os dois últimos com expressivo aumento), entre outros (BRASIL g, 2014). Os dados mais atuais seriam referentes ao mês de junho e teriam uma parcela de origem decorrente da Copa do Mundo FIFA 2014, entretanto, nos últimos anos, o Brasil sedia diversos grandes eventos passíveis de comparação com este em questão.

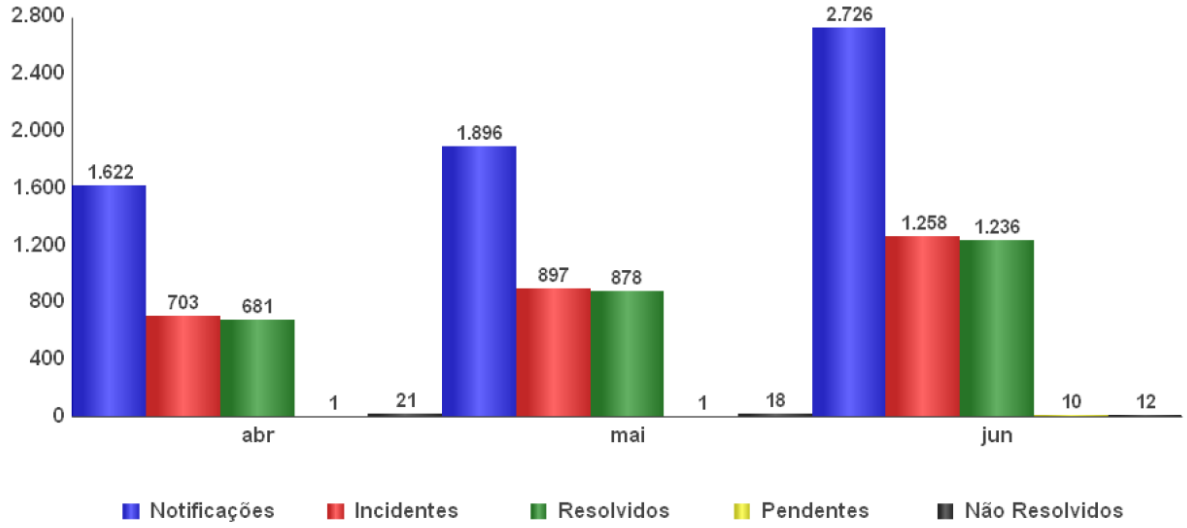
Contrapondo-se os primeiros três semestres do ano de 2013 para 2014, pode-se perceber claro aumento no número de ataques à APF e, diversas vezes, um número menor de incidentes resolvidos.

Gráfico 2 - Número de notificações e incidentes à APF – primeiro trimestre de 2014



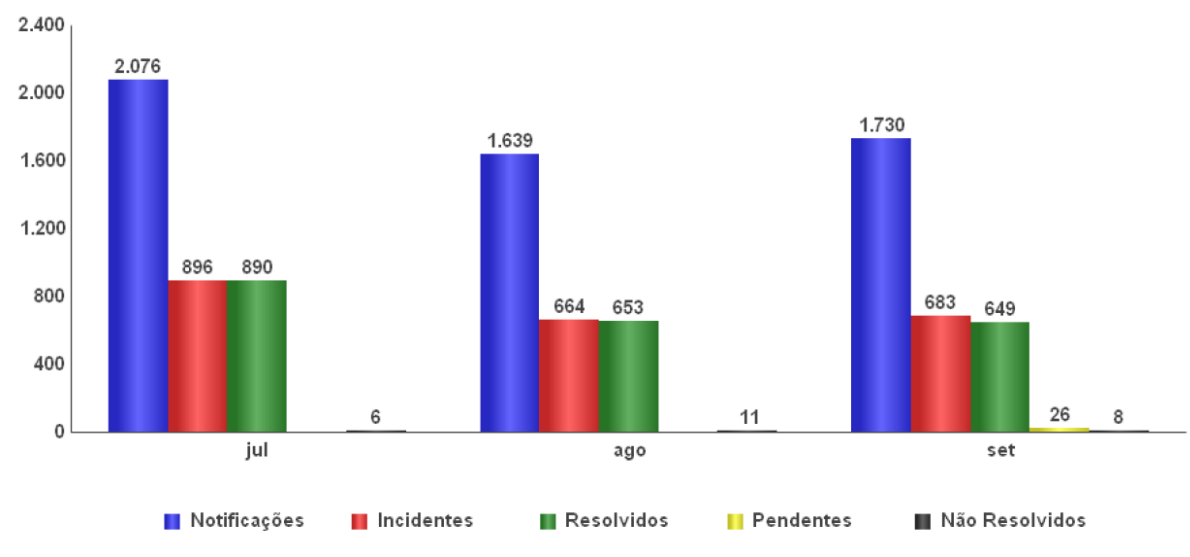
Fonte: BRASIL (2014a).

Gráfico 3 - Número de notificações e incidentes à APF – segundo trimestre de 2014



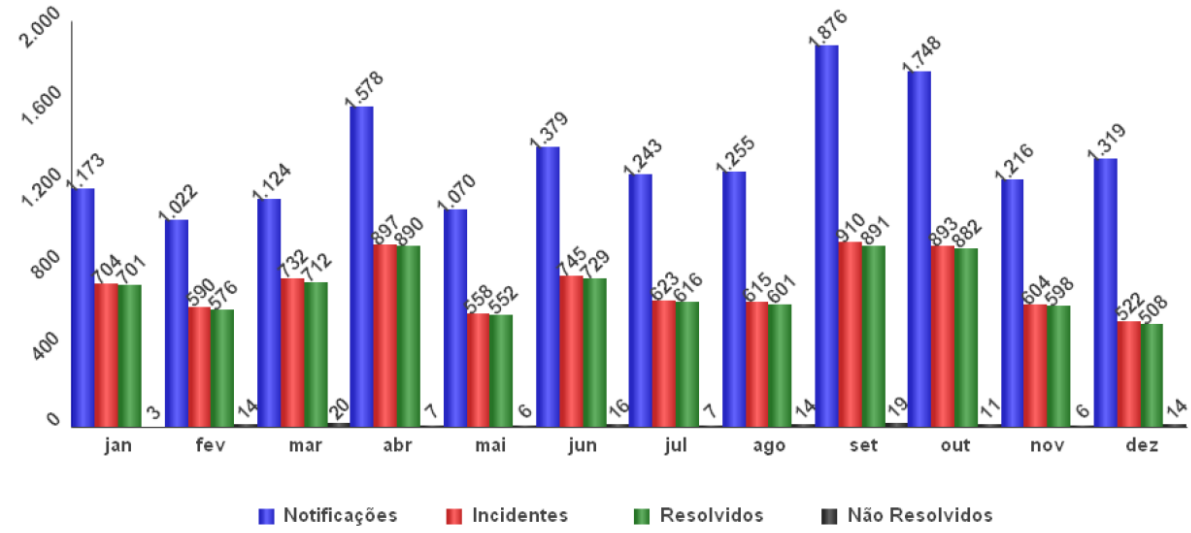
Fonte: BRASIL (2014b).

Gráfico 4 - Número de notificações e incidentes à APF – terceiro trimestre de 2014



Fonte: BRASIL (2014c)

Gráfico 5 - Número de notificações e incidentes à APF - 2013



Fonte: BRASIL (2013)

Desse modo, com base no critério do *Military Balance* (IISS, 2014) entende-se que um aumento ou uma estabilização no número de invasões ou incidentes notificados devem demonstrar de uma estagnação ou carência nos investimentos em certas capacidades defensivas no campo cibernético, bem como na melhoria dos procedimentos de segurança e

arquitetura da rede nacionalmente.[74] Assim, evidencia-se, ainda que haja crescente esforço para com o tema da cibersegurança em geral, a insuficiência do desenvolvimento de capacidades nacionais, a fim da estruturação de uma ciberestratégia sólida e com objetivos à altura do país e da inserção internacional brasileira.

Logo, na análise do Brasil como ator detentor de relativo ciberpoder no cenário mundial, acredita-se que o país possua grande potencial para o atingimento de um melhor lugar entre os maiores influentes do ciberespaço e, principalmente da Internet. A seguir, um quadro de referência dos diversos indicadores que podem ser analisados:

Quadro 3 - Capacidades Cibernéticas do Brasil

Posição Internacional	Inserção internacional crescente e grande influenciador em termos de iniciativas para a governança da Internet.
Ações Regulatórias e Liberdade na Rede	O Marco Civil figura importante medida recente, entretanto o país demonstra níveis médios de liberdade na Internet (vide figura 5).
Doutrina de Ciberestratégia	Doutrina em fase de desenvolvimento, com grande destaque à criação do CDCiber.
Infraestrutura e Investimentos	Investimentos ainda não suficientes em infraestrutura e em sua proteção.
Número de ISPs	148 (YAHOO, 2014)
Velocidade de Acesso	84 no ranking global, com média de 2.7 Mbps (megabytes por segundo) (AKAMAI, 2013).
Penetração da Internet	Relativamente baixa. 53,37% (107.822.831 usuários) (INTERNET LIVE STATS, 2014).

Fonte: Elaboração própria.

Além dos indicadores já mencionados, ponderam-se outros passíveis de consideração, como o progresso do número de domínios ".br" registrados até o momento - 3.527.301

[74] "A decline in the number of successful intrusions by aggressors should demonstrate the merit of continued investment in defensive capabilities, as well as improvements to security procedures and network security architecture". (IISS, 2014, p.14)

(REGISTROBR, 2014) -, e o número de PTTs (Pontos de Troca de Tráfego)[75] - 24 pontos (PTTBR, 2014) - a ser incluído como infraestrutura essencial também, além do crescimento notável, entre 2000 e 2009, dos serviços de TIC de 795 mil para 1,2 milhão (4,7% a.a.), chegando a corresponder, em 2010, a 1,4% do total da força de trabalho (1.172.800 especialistas) (DUARTE; PORCARO, 2014). Contudo, no mesmo ano de 2010, no que tange à política de recursos humanos, em 20% das instituições do governo brasileiro, os gestores de TI não foram selecionados com base em sua competência, 35% das instituições da APF não preencheram pelo menos 75% dos papéis gerenciais de TI, e 75% também não mantiveram política de incremento de gestores (CRUZ JÚNIOR, 2013), demonstrando um vácuo de especialistas a longo prazo ou, no mínimo, a necessidade de mais gastos.

Mais uma vez, se faz importante ressaltar o fato de que a análise de capacidades cibernéticas não representa todas as faces do ciberpoder. Tais referências estariam relacionadas com a primeira camada do ciberespaço, com algumas extrapolações à terceira (ou até mesmo a quarta, porém de maneira ainda não completas). A dificuldade de mensuração continua presente, contudo, o exercício é valido para as primeiras percepções acerca de onde se encontra o país no cenário internacional em relação ao campo aludido e que nível de importância apresenta o tema nacionalmente. A influência brasileira, em vista dos últimos acontecimentos e da crescente inserção do país em nível mundial, em defesa da promoção da pluralidade de direitos dos atores estatais sobre a Internet, se mostra evidente e a tendência é que, com uma política externa constante, tal situação se mantenha sustentável e próspera, desde que internamente os vários entraves sejam superados.

[75] PTT é uma infraestrutura física, através da qual ISPs promovem entre suas redes uma interconexão direta para troca de tráfego de Internet (PTTBR, 2014).

4. CONCLUSÕES

Mesmo com o advento do campo da cibernética em meados da década de 1940, desde os tempos das primeiras máquinas de telégrafo, o ciberespaço já figurava nos intercâmbios sociais e econômicos dos países. À medida que a esfera "ciber" foi crescendo em tamanho e importância, questões acerca de sua funcionalidade para com as interações humanas e políticas na rede foram aparecendo. Mas, somente com o advento da Internet, após o fim da Guerra Fria, a essencialidade do tema foi percebida por todos.

Por conseguinte, esse trabalho adotou o conceito de ciberespaço como "uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar a informação através de redes interdependentes e interligadas usando tecnologias de informação e comunicação" (KUEHL, 2009), centrando a caracterização do campo na ocorrência da movimentação de elétrons por algum meio.

Desse modo, a partir do crescimento da ARPANET e o afloramento na Internet como conhecemos hoje, a delimitação do que é o ciberespaço e o que seria a Internet por vezes foi confundida (CANABARRO; BORNE, 2013), uma vez que até mesmo suas divisões de domínios se assemelham. Logo, entende-se pela análise, que, hierarquicamente, o ciberespaço possui um espectro mais amplo do que a Internet, e esta, por sua vez, é incluída como mais uma rede dentre as diversas que são usadas no espaço cibernético. No entanto, o grande diferencial da Internet, dentro do ciberespaço e entre todas as outras redes, é o seu caráter inclusivo, convergente e ubíquo. Nesse ponto, inicialmente percebe-se a rede das redes como instrumento de projeção dos Estados Unidos ao redor do mundo, uma vez que este país foi o berço da ARPANET e de toda a construção da Internet, física e institucional.

Por meio dos protocolos disseminados ao redor do mundo, o TCP/IP foi grande responsável pela alavancagem da rede como principal ferramenta de integração da atualidade, uma vez que padronizou a comunicação entre os computadores em uma só "linguagem", perpetuando assim a ubiquidade (onipresença e compatibilidade) da rede. A Web, por sua vez, mantendo a mesma relação de confinamento existente entre a Internet e o ciberespaço, se mostra como principal promotora da integração social da rede e, a partir disso, os diferentes intercâmbios e possibilidades se universalizam entre os indivíduos.

Dessas interações, as que se dão entre Estados manifestam as relações de Poder mais importantes dentre os atores do sistema global, evidenciando a importância do estudo para o entendimento das influências e poder no âmbito cibernético. Com isso, a teorização do ciberpoder ganha seus primeiros contornos e herda diversas características das relações de poder tradicionais, descritas por Hobbes (1651), Weber (1947), Lasswell e Kaplan (1950) e, de grande importância para o debate demonstrado nesse trabalho, a crítica de Dahl (2012) sobre a mensurabilidade do Poder.

A partir disso, compreende-se que ciberpoder é a capacidade de uso, ou ameaça de uso, do ciberespaço para criar vantagens e afetar outros atores e eventos em todos os ambientes operacionais e por meio dos instrumentos desse ambiente obter os resultados pretendidos. Do encontro de ciberpoderes, os Estados encontram ameaças e constrangimentos, os quais demandam uma reação para a securitização do tema dentro de suas políticas interna e externa. O ciberespaço não existe por si só, logo sua dependência está ligada ao sua primeira camada, a física, que está submetida à jurisdição de um ou outro Estado, dependendo de sua localização geográfica. Assim, a cibersegurança trata da defesa dessas estruturas físicas, para que, desse modo, as interações no nível cibernético possam ocorrer e todos os serviços – que hoje são muitos – ligados às redes de comunicação (em especial, à Internet) possam funcionar plenamente. Mais uma vez, os Estados Unidos são pioneiros no tema da cibersegurança, o qual se refere à proteção e garantia de utilização de infraestruturas críticas da informação, conjuntos de ativos essenciais para a consecução da missão do Estado.

A governança da Internet entra em cena como uma iniciativa de diminuição dos polos de Poder e influência na camada mais ampla da rede e do ciberespaço. Nesse ponto, o Brasil se mostra um dos grandes promotores dessa pluralidade de atores e poderes no sistema internacional em relação ao domínio da governança da Internet. Ao tempo que a influência estadunidense na rede vai diminuindo, atores estatais reivindicam espaço para com os assuntos de gestão da rede, manifestado com destaque na transferência de controle da ICANN (*Internet Corporation for Assigned Numbers and Names*) e na neutralidade da rede.

Assim, a posição brasileira faz forte crítica ao domínio americano em certas faces da rede e incentiva outros governos na participação dos debates acerca da maior multilateralidade da Internet. Com a aprovação do Marco Civil da Internet, o país lidera uma articulação das forças políticas nacionais para garantir uma resposta à sociedade a respeito do tema e, assim, proporcionar uma melhor inserção brasileira ao nível das discussões internacionais. Desse modo, o Marco Civil serve de modelo para outros países a respeito das

garantias e deveres na Internet e, acima disso, representa ferramenta de política externa para entrada brasileira no sistema internacional.

O encontro promovido pelo Brasil da NETmundial mostra, mais uma vez, o papel de liderança do país no tema. O diálogo com Estados Unidos por vezes se manifesta um processo lento e com alguns entraves, mas a perspectiva nesse sentido é otimista em termos da inserção brasileira e da governança multissetorial, porém não tanto quanto se espera na diminuição da influência dos grandes atores do ciberespaço, como os Estados Unidos e atores não-estatais relacionados.

De qualquer modo, a aspiração brasileira de maior representatividade e de melhor imagem perante a comunidade mundial necessita ter bases mais sólidas do que a simples retórica ou iniciativas. Logo, a sustentação da cibersegurança em espectro nacional é extremamente necessária para que o Brasil mantenha e almeje uma posição de destaque dentro do tema do ciberespaço. Nesse aspecto, o país peca pela ainda insuficiência de esforços para a securitização plena de suas infraestruturas críticas. O Brasil vem adequando suas políticas públicas com destaque à questão cibernética desde 2008, na Estratégia Nacional de Defesa (BRASIL, 2008), porém não possui ainda um documento que delimite as diretrizes próprias do país para a cibersegurança. Assim, verifica-se, antes mesmo das ocorrências de espionagem brasileira pela NSA, a existência de grandes brechas pondo em risco a integralidade dos ativos de informação brasileiros.

Grande parte das redes da APF, como demonstrado ao longo do trabalho, confirmam níveis de segurança insuficientes para a proteção plena dos ativos da maquina estatal. A capacitação de pessoas, aspecto muito importante no desenvolvimento de capacidades cibernéticas pelos países, apesar de apresentar crescimento ao longo dos últimos anos no mercado, dentro do governo é posta de lado muitas vezes, dificultando muito avanços sólidos na área. A criação do CDCiber explicita uma iniciativa frutífera para a defesa no campo, contudo, de acordo com o orçamento anual do governo, os investimentos decrescentes e não concretizados barram a possibilidade de crescimento do Brasil nesses termos, e a sua arquitetura organizacional dificulta avanços no sentido da coordenação de esforços para a evolução no espectro da segurança.

Enfim, apreende-se da análise desse trabalho que existe uma aspiração brasileira de inserção internacional que se traduz como forte liderança no tema da governança da Internet. Contudo, internamente os avanços do Brasil para o sustento de sua solidez nas outras camadas do ciberespaço e da Internet demonstram um descompasso com os anseios do país. Acredita-se na existência de um "*gap*", ou espaço, entre a promoção de uma política externa assertiva e

o desenvolvimento de mecanismos que garantam a posição brasileira como capaz de defesa e segurança nesse âmbito. Se não houver uma convergência entre estes elementos, o país poderá, no futuro, ter de prescindir do projeto de se constituir em um ator relevante no ciberespaço.

REFERÊNCIAS

ABBATE, Janet. **Inventing the Internet.** Massachussetts: The MIT Press, 1999.

AKAMAI. **The State of the Internet:** 3rd Quarter, 2013 Report. 3. ed. Cambridge, 2013. 6 v.

AMORIM, C. Segurança Internacional : Novos Desafios para o Brasil. **Contexto Internacional**, v. 35, n. 1, p. 287–311, Rio de Janeiro, 2013.

ARON, R. **Paz e Guerra entre as Nações.** São Paulo: Universidade de Brasília, 2002. Tradução de: Sergio Bath.

BADII, Farzaneh. **The UN and the Future of the Internet Governance Forum.** 2014. Disponível em: <http://www.internetgovernance.org/2014/09/28/the-un-and-the-future-of-the-internet-governance-forum/>. Acesso em: 22 nov. 2014.

BERNERS-LEE, Tim. **Weaving the Web**: The Original Design and Ultimate Destiny of the World Wide Web. New York: HarperCollins Publishers, 2000.

BLUMENTHAL, Marjory S.; CLARK, David D.. The Future of the Internet and Cyberpower. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security**. Washington D.c.: National Defense University, 2009. Cap. 8, p. 31.

BOWLES, Samuel; GINTIS, Herbet. **Power.** Massachussetts, 2007.

BRASIL. **Estatísticas de Incidentes de Rede na APF:** 2013. Brasília, 2013.

BRASIL. **Estatísticas de Incidentes de Rede na APF:** 1° Trimestre/2014. Brasília, 2014a.

BRASIL. **Estatísticas de Incidentes de Rede na APF:** 2° Trimestre/2014. Brasília, 2014b.

BRASIL. **Estatísticas de Incidentes de Rede na APF:** 3° Trimestre/2014. Brasília, 2014c.

BRASIL. **Estratégia Nacional de Defesa**. Brasília, 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007- 2010/2008/Decreto/D6703.htm>. Acesso em: 24 nov. 2014.

BRASIL. **Livro Branco de Defesa Nacional**. Brasília, 2012a. Disponível em: <https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 24 nov. 2014.

BRASIL. Lei nº 12.598, de 21 de março de 2012. **Estabelece Normas Especiais Para As Compras, As Contratações e O Desenvolvimento de Produtos e de Sistemas de Defesa; Dispõe Sobre Regras de Incentivo à área Estratégica de Defesa; Altera A Lei no 12.249, de 11 de Junho de 2010; e Dá Outras Providências.** Brasília, 2012b.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasília, 2014d.

BRASIL. **Lei Orçamentária Anual 2013.** Brasília: 2014e.

BRASIL. **Política Nacional de Defesa**. Brasília, 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em: 22 nov. 2014.

BRASIL. **Portaria no 666, de 4 de agosto de 2010**. Brasília, 2010a. Disponível em: <http://tinyurl.com/aebz5yw>. Acesso em: 22 nov. 2014.

BRASIL. **Portaria no 667, de 4 de agosto de 2010**. Brasília, 2010b. Disponível em: <http://tinyurl.com/aebz5yw>. Acesso em: 22 nov. 2014.

BRASIL. **Projeto de Lei Orçamentária Anual 2014.** Brasília: 2014f.

CANABARRO, D. R.; BORNE, T. Ciberespaço e Internet: Implicações Conceituais para os Estudos de Segurança. **Mundorama**, v. 69, p. 1-4, Brasília, 2013.

CANABARRO, D. R. A governança da Internet: atores, aspectos institucionais e questões políticas em confronto. *In*: ENCONTRO DA ASSOCIAÇÃO BRASILEIRA DE CIÊNCIA POLÍTICA, 8., 2012, Gramado, Rio Grande do Sul. **Anais**... Gramado: ABCP, 2012. Disponível em: <http://goo.gl/VDif3>. Acesso em: 24 nov. 2014.

CANABARRO, D. R. **Governança Global da Internet:** tecnologia, poder e desenvolvimento. 2014. 431 f. Tese (Doutorado) - Curso de Ciência Política, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

CANALTECH. **Empresas brasileiras investem mais em segurança da informação.** 2014. Disponível em: <http://corporate.canaltech.com.br/noticia/protecao-de-dados/Empresas-brasileiras-investem-mais-em-seguranca-da-informacao/>. Acesso em: 20 nov. 2014.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parceria Estratégica,** Brasília, v. 14, n. 29, p.21-46, jul. 2009.

CAVELTY, M. The militarisation of cyber security as a source of global tension. *In*: MÖCKLI, D. **Strategic trends 2012**: key developments in global affairs. Zurich: Center for Security Studies (CSS), 2012. Disponível em: <http://goo.gl/tBmeiu>. Acesso em: 24 nov. 2014.

CDN. Portaria nº 34, de 05 de agosto de 2009. **Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação**. Brasília, 2014.

CEPIK, M.; ARTURI, C. S. Tecnologias de Informação e Integração Regional: Desafios Institucionais para a Cooperação Sul-Americana na Área de Segurança*. **DADOS - Revista de Ciências Sociais**, v. 54, n. 4, p. 651–691, Rio de Janeiro: UERJ, 2011.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. A Securitização do Ciberespaço e o Terrorismo: Uma Abordagem Crítica. In: SOUZA, André Mello e; NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi de. **Do 11 de Setembro de 2001 à Guerra ao Terror:** reflexões sobre o terrorismo no século XXI. Brasília: Ipea, 2014. p. 161-186.

CLARKE, R. A.; KNAKE, R. **Cyber war**: the next threat to national security and what to do about it. [s.l.]: Ecco, 2011.

CONTAS ABERTAS. **Apesar de espionagem dos EUA, orçamento para defesa cibernética é reduzido em R$20 milhões.** 2013. Disponível em: <http://www.contasabertas.com.br/website/arquivos/747>. Acesso em: 22 nov. 2014.

CRUZ JÚNIOR, Samuel César da. **A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual.** Brasília: Ipea, 2013.

CZOSSECK, Christian. Introduction to Cyberspace: Sociological Facets and Technical Features. In: ZIOLKOWSKI, Katharina. **Peacetime Regime for State Activities in Cyberspace:** International Law, International Relations and Diplomacy. Tallinn: Nato Cooperative Cyber Defence Centre Of Excellence, 2013. p. 32-64.

DAHL, Robert. **A Democracia e seus Críticos.** São Paulo: Wmf, 2012. Tradução de: Patrícia de Freitas Ribeiro.

DEFESANET (Brasília). **CDCiber:** Portaria de criação do Centro de Defesa Cibernética do Exército. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1633/cdciber---portaria-de-criacao-do-centro-de-defesa-cibernetica-do-exercito>. Acesso em: 22 nov. 2014.

DODGE, Martin; KITCHIN, Rob. **Atlas of Cyberspace.** London: Pearson Education, 2001.

EISENBERG, J.; CEPIK, M. **Internet e política**: teoria e prática da democracia eletrônica. Belo Horizonte: Editora da UFMG, 2002.

EM DISCUSSÃO. **Brasil investe pouco em inteligência.** 2013. Disponível em: <http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/materia.html?materia=brasil-investe-pouco-em-inteligencia.html>. Acesso em: 21 nov. 2014.

FREEDOM HOUSE. **Freedom on the Net 2013.** 2013. Disponível em: <https://www.freedomhouse.org/sites/default/files/resources/FOTN 2013_Map.pdf>. Acesso em: 22 nov. 2014.

GIBSON, Willian. **Neuromancer**. São Paulo: Aleph, 2003.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. **EUA espionaram milhões de e-mails e ligações de brasileiros.** 2013. Disponível em: <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em: 24 nov. 2014.

GREENWALD, Glenn; MACASKILL, Ewen. **NSA Prism program taps in to user data of Apple, Google and others**. 2013. Disponível em: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 22 nov. 2014.

GROSSMANN, Osvaldo. **NetMundial preserva transição da ICANN e faz leve menção à neutralidade.** 2014. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36577&sid=4#.VHhK5NLF-T->. Acesso em: 22 nov. 2014.

HANSEN, L.; NISSENBAUM, H. Digital disaster, cyber security, and the Copenhagen School. **International studies quarterly**, v. 53, n. 4, p. 1.155-1.175, Tucson: 2009.

HAUBEN, Ronda. The Birth and Development of the ARPANET. In: HAUBEN, Michael; HAUBEN, Ronda. **Netizens**: On the History and Impact of Usenet and the Internet. Los Alamitos: IEEE Computer Science Press, 1997.

HOBBES, Thomas. **Leviatã**. 1651. Tradução de João Paulo Monteiro e Maria Beatriz Nizza da Silva.

HUNKER, Jeffrey. Cyber War and Cyber Power: Issues for Nato Doctrine. **Research Paper,** Rome, v. 62, 22 nov. 2014.

ICANN. **Qual o papel da ICANN?** 2012. Disponível em: <https://www.icann.org/resources/pages/what-2012-02-25-pt>. Acesso em: 22 nov. 2014.

IISS. **The Military Balance.** London: Routledge, 2011.

IISS. **The Military Balance.** London: Routledge, 2014.

INTERNET LIVE STATS. **Internet Users.** 2014. Disponível em: <http://www.internetlivestats.com/internet-users/>. Acesso em: 20 nov. 2014.

INTERNET SOCIETY (Reston). **Who We Are.** 2014. Disponível em: <http://www.internetsociety.org/who-we-are>. Acesso em: 20 nov. 2014.

ITAMARATY. . **Transcrição da Audiência Pública com o Ministro de Estado da Relações Exteriores, Luiz Alberto Figueiredo Machado, na Comissão de Relações Exteriores e Defesa Nacional do Senado Federal (6/2/2014).** 2014. Disponível em: <http://www.itamaraty.gov.br/sala-de-imprensa/discursos-artigos-entrevistas-e-outras-comunicacoes/ministro-estado-relacoes-exteriores/transcricao-da-audiencia-publica-com-o-ministro-de-estado-da-relacoes-exteriores-luiz-alberto-figueiredo-machado-na-comissao-de-relacoes-exteriores-e-defesa-nacional-do-senado-federal-2014-6-2-2014/?searchterm=cibernética>. Acesso em: 20 nov. 2014.

ITAMARATY. **Reunião de Ministros das Relações Exteriores do BRICS à margem da 68ª Assembleia-Geral das Nações Unidas – Comunicado à imprensa.** 2013. Disponível em: <http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/reuniao-de-ministros-das-relacoes-exteriores-do-brics-a-margem-da-68a-assembleia-geral-das-nacoes-unidas-comunicado-a-imprensa-nova-york-26-de-setembro-de-2013/?searchterm=cibernética>. Acesso em: 20 nov. 2014.

KELION, Leo. **Future of the internet debated at NetMundial in Brazil.** 2014. Disponível em: <http://www.bbc.com/news/technology-27108869>. Acesso em: 22 nov. 2014.

KLEINWÄCHTER, W. The history of Internet governance. *In*: OSCE. **Governing the Internet**: freedom and regulation in the OSCE region. Vienna: OSCE, 2007. Disponível em: <http://www.osce.org/fom/26169>. Acesso em: 15 nov. 2014.

KRAMER, Franklin D.; WENTZ, Larry K.. Cyber Influence and International Security. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security.** Washington D.c.: National Defense University, 2009. Cap. 14, p. 16.

KRAMER, F. D.; STARR, S. H.; WENTZ, L. (Ed.). **Cyberpower and National Security**. Washington: National Defense University Press, 2008.

KRAMER, Franklin D. Policy Recommendations for a Strategic Framework. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security**. Washington D.C.: National Defense University, 2009. Cap. 1, p. 18.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security**. Washington D.C.: National Defense University, 2009. Cap. 2, p. 17.

LASSWELL, Harold D.; KAPLAN, Abraham. **Power and Society:** A Framework for Political Inquiry. [S.l], 1950.

LEE, Timothy B.. **40 maps that explain the Internet.** 2014. Disponível em: <http://www.vox.com/a/internet-maps>. Acesso em: 22 nov. 2014.

LEWIS, James A.. **Cybersecurity and Critical Infrastructure Protection.** Washington D.C: Center for Strategic and International Studies, 2006.

LIBICKI, Martin C.. **Cyberdeterrence and Cyberwar.** Santa Monica: Rand Corporation, 2009.

LICKLIDER, J. C. R; TAYLOR, Robert W.. **The Computer as a Communication Device. [**S.l]: Science And Technology, 1968.

MAZONI, Ana Carolina. **Crimes na Internet e a Convenção de Budapeste.** 2009. 65 f. TCC (Graduação) - Curso de Direito, Centro Universitário de Brasília, Brasília, 2009.

MÖLLER, C. Governing the Domain Name System: An Introduction to Internet Infrastructure. *In*: **OSCE**. **Governing the Internet**: freedom and regulation in the OSCE region. Vienna: OSCE, 2007. Disponível em: <http://www.osce.org/fom/26169>. Acesso em: 21 nov. 2014.

NETMUNDIAL. **NETmundial Multistakeholder Statement.** 2014. Disponível em: <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>. Acesso em: 22 nov. 2014.

NETMUNDIAL (São Paulo) (Org.). **Discurso da Presidenta da República, Dilma Rousseff, durante cerimônia de abertura do Encontro Global Multissetorial sobre o Futuro da Governança da Internet.** 2014. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/15102/NET-MUNDIAL---Discurso-Dilma-Rousseff/>. Acesso em: 2 nov. 2014.

NETMUNDIAL (São Paulo). **NETmundial:** o início de um processo. 2014. Disponível em: <http://netmundial.br/pt/about/>. Acesso em: 22 nov. 2014.

NTIA. **NTIA Announces Intent to Transition Key Internet Domain Name Functions.** 2014. Disponível em: <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>. Acesso em: 22 nov. 2014.

NYE JR., Joseph. **Cyber Power.** Cambridge: Belfer Center For Science And International Affairs, 2010.

PIMENTEL, C. Notas analíticas sobre os conceito dissuasão aplicado ao fenômeno da cibersegurança. In: **IX ENCONTRO DA ABCP**. Brasília, 2014.

PRESCOTT, Roberta. **Governança da Internet:** EUA se opõem ao modelo multilateral e conflitam com o Brasil. 2014. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36692#.VHhLL9LF-T9>. Acesso em: 22 nov. 2014.

PRIBERAM. **Cibernética.** 2013. Disponível em: <http://www.priberam.pt/dlpo/cibernética>. Acesso em: 20 nov. 2014.

PTTBR. **Localidades atuais do PTTMetro.** Disponível em: <http://ptt.br/localidades/atuais>. Acesso em: 22 nov. 2014.

RATTRAY, Gregory J.. An Environmental Approach to Understanding Cyberpower. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security.** Washington D.C.: National Defense University, 2009. Cap. 10, p. 19.

REGISTROBR. **Domínios .br registrados até o momento.** 2014. Disponível em: <http://registro.br/estatisticas.html>. Acesso em: 22 nov. 2014.

ROUSSEFF, Dilma. Leia a Íntegra do discurso da Dilma na Assembleia-Geral da Onu. Em: Folha de São Paulo, 2013. Disponível em: <http://www1.folha.uol.com.br/mundo/2013/09/1346617-leia-a-integra-do-discurso-de-dilma-na-assembleia-geral-da-onu.shtml>. Acesso em: 30 out. 2014.

RUSSELL, Bertrand. **Power:** A new social analysis. London: Routledge, 1938.

SÁ, Nelson de. **CDCIBER:** Centro de Defesa Cibernética inicia em junho. 2012. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/5954/cdciber---centro-de-defesa-cibernetica-inicia-em-junho->. Acesso em: 10 maio 2014>. Acesso em: 25 nov. 2014.

SENADO. **General pede mais recursos para segurança cibernética.** 2013. Disponível em: <http://www12.senado.gov.br/jornal/edicoes/2013/10/03/general-pede-mais-recursos-para-seguranca-cibernetica>. Acesso em: 20 nov. 2014.

SKOUDIS, Edward. Evolutionary Trends in Cyberspace. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security**. Washington D.C.: National Defense University, 2009. Cap. 6, p. 20.

SKOUDIS, Edward. Information Security Issues in Cyberspace. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security**. Washington D.C.: National Defense University, 2009. Cap. 7, p. 29.

STARR, Stuart H. Toward a Preliminary Theory of Cyberpower. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security**. Washington D.C.: National Defense University, 2009. Cap. 3, p. 38.

STOPPINO, Mario. Poder. In: BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. **Dicionário de Política.** 11. ed. Brasília: Unb, 1998. p. 943-952.

TELEGEOGRAPHY. **Submarine Cable Map.** 2014. Disponível em: <http://www.submarinecablemap.com/>. Acesso em: 22 nov. 2014.

UNITED STATES. **International strategy for cyberspace**. Washington D.C. 2011. Disponível em: < http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf%3E>. Acesso em: 22 nov. 2014.

UNITED STATES. **National Security Strategy**. Washington D.C. 2010. Disponível em: <http://goo.gl/pBBP>. Acesso em: 22 nov. 2014.

UNITED STATES. NSPD nº 54/HSPD nº 23 of jan. 8th, 2008. **Cybersecurity Policy**. Washington D.C, 2008.

WEBER, Max. **The Theory of Social and Economic Organization.** Illinois: The Falcon's Wing Press, 1947. Edited with an introduction by Talcott Parsons.

WIENER, Norbert. **Cybernetics or control and communication in the animal and the machine**. Cambridge, Massachusetts: The M.I.T Press, 1948.

YAHOO. **Internet Service Providers.** 2014. Disponível em: <https://dir.yahoo.com/business_and_economy/business_to_business/communications_and_networking/internet_and_world_wide_web/network_service_providers/internet_service_providers__isps_/by_region/countries/?o=a>. Acesso em: 22 nov. 2014.

ZIMET, Elihu; SKOUDIS, Edward. A Graphical Introduction to the Structural Elements of Cyberspace. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry.**Cyberpower and National Security.** Washington D.c.: National Defense University, 2009. Cap. 4, p. 19.

ZIOLKOWSKI, Katharina. **Peacetime Regime for State Activities in Cyberspace:** International Law, International Relations and Diplomacy. Tallinn: Nato Cooperative Cyber Defence Centre Of Excellence, 2013. 782 p.