ESTADOS NACIONAIS, SOBERANIA E REGULAÇÃO DA INTERNET

Hindenburgo Francisco Pires
Instituto de Geografia da Universidade do Estado do Rio de Janeiro
Bolsista do Programa de Estudos para Estágio Pós-Doutoral no Exterior
da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes)
hindenburgo@uerj.br - http://www.cibergeo.org

Estados nacionais, soberania e regulação da Internet (Resumo)

A história recente da atuação dos Estados Nacionais para a promoção de mecanismos que estabeleçam uma jurisprudência normatizadora de regulação do ciberespaço e da Internet no século XX, passou a ser justificada ideologicamente pela crescente influência da Internet na soberania e no cotidiano de suas relações sociais. Esta atuação controladora, mantida atualmente pelos EUA, afeta uma gama variada de questões que dizem respeito à soberania, segurança, infraestrutura, economia, geopolítica, educação, cidadania, privacidade, democracia, entre outras.
Por isso, este artigo tem por objetivos, em primeiro lugar, analisar os impactos dos usos sociais da Internet na soberania dos Estados Nacionais; em segundo lugar, examinar como historicamente foram instituídas, pelos EUA, a autoridade política e controle do sistema na zona raiz da Internet; em terceiro lugar, investigar a atuação e a interferência atual dos atores políticos, para o estabelecimento de uma nova estrutura de regulação global baseada em um sistema de gestão multilateral da Internet.

Palavras Chave: estados nacionais, soberania, regulação, ciberespaço, imperialismo digital, governança da Internet.

National states, sovereignty and regulation of the Internet (Abstract)

The recent history of the nation states actions to promote mechanisms to establish a normative jurisprudence for cyberspace and the Internet regulation in the twentieth century became ideologically justified by the Internet growing influence on sovereignty and in their everyday social relations. This controlling action, which is still maintained by the U.S., affects a wide

range issues that concern the sovereignty, security, infrastructure, economy, geopolitics, education, citizenship, privacy, democracy, imperialism digital, inter alia.
Therefore, this paper aims, first, to analyze the Internet social uses impacts in the nation states sovereignty, and secondly, to examine how the political authority and control system historically has been imposed by the U.S. in the Internet root zone; in third, to investigate the actions and interference of the current political actors to establish a new global regulatory structure based on an Internet multilateral management system.

Keywords: national states, sovereignty, regulation, cyberspace, imperialism digital, Internet governance.

Los Estados nacionales, la soberanía y la regulación de Internet (Resumen)

La historia reciente de las acciones de los Estados nacionales para promover los mecanismos para establecer una jurisprudencia normativa para la regulación del ciberespacio y la Internet en el siglo XX, se justificó ideológicamente por la creciente influencia de Internet en la soberanía y en sus relaciones sociales cotidianas. Esta acción controlada por los EE.UU. afecta a una amplia gama de cuestiones relativas a la soberanía, seguridad, infraestructura, economía, geopolítica, educación, ciudadanía, a la intimidad, la democracia, el imperialismo digital, entre otros.

Por lo tanto, este artículo tiene como objetivo, en primer lugar, analizar los impactos de los usos sociales de Internet en la soberanía de los estados-nación, y en segundo lugar, examinar cómo históricamente se ha impuesto por los EE.UU., la autoridad política y el sistema de control en la zona de las raíces Internet y en tercer lugar, investigar las acciones y la interferencia de los actores políticos actuales para establecer una nueva estructura global de regulación basada en un sistema de gestión multilateral de Internet.

Palabras clave: estados nacionales, soberanía, regulación, ciberespacio, imperialismo digital, gobernanza de Internet.

O uso social de, pelo menos, cinco inovações tecnológicas[1] provocou uma revolução na área das comunicações mundiais que modificou a realização e o desempenho de várias esferas de produção social e afetou a dinâmica das relações internacionais contemporâneas[2]. O objeto de investigação da presente pesquisa[3], será apenas uma dessas inovações, quando se destacará o impacto produzido pela Internet na dinâmica relação constituída entre o poder dos Estados Nacionais e seus territórios nos séculos XIX e XX.

Para se compreender essas questões geopolíticas da governança da Internet é preciso fazer-se uma pequena retrospectiva para verificar como a hegemonia dos EUA, durante o pós-guerra, se estruturou em dois grandes pilares na expansão das atividades comerciais e, acima de tudo, na acumulação militar[4].

Essa acumulação militar foi o resultado da formação de um extraordinário mercado estatal, sem concorrência pública, para a produção de artefatos e tecnologias voltadas para a defesa dos EUA. O maior incentivador desta orientação econômica beligerante foi o presidente

Dwight Eisenhower. Os contratos de defesa produziram um novo mapa econômico dos EUA, criando um complexo industrial que ajudou a consolidar um conjunto de cidades que formam um imenso perímetro regional de defesa denominada de *Gunbelt*. Esse cinturão de armas "é o maior fenômeno no mapa econômico contemporâneo da América" porque se pode afirmar, sem receio, que não há precedente igual de criação de uma zona industrial militar deste tipo e tamanho na história industrial do ocidente.

Esse complexo industrial militar consiste de um conjunto de indústrias globais formado por várias firmas locais, cuja preocupação central, desde o período da guerra fria, tem sido a produção de armamentos compostos de alta-tecnologia e inovação.

O impacto territorial de implantação desse complexo industrial militar nos EUA foi profundamente estudado por Benneth Harrison e Barry Bluestone, no livro *Deindustrialization of America*[5], que explica a expansão industrial regional do *Sunbelt* e sua relação com os investimentos militares do Pentágono.

Muitos estudiosos na área da geografia atribuíram a Eisenhower a formação do *Welfare State* mas, contrariando esta orientação, pode-se constatar que ele contribuiu mais para a formação do *Warfare State* do que para a formação do *Welfare State*. Para provar esta assertiva, basta analisar os orçamentos destinados à despesa militar nos diferentes governos da história dos EUA para verificar que nenhum governo repassou tantos recursos quanto o governo de Eisenhower que, durante o pós-guerra, destinou mais treze por cento do produto interno bruto para investimentos militares nos EUA[6].

O crescimento da produção de computadores e de radares nos Estados Unidos também esteve relacionado com investimentos no setor de defesa e com a corrida militar; este crescimento se acentuou ainda mais quando os soviéticos detonaram sua primeira bomba atômica, em 1949, e também fizeram o lançamento do satélite Sputnik em 1957.

Naquela época, os radares[7], baseados em sistemas de telecomunicações, seriam o único meio capaz de prevenir contra um possível ataque aéreo; nesse sentido, foi criado pelo Departamento de Defesa dos EUA e pela força aérea dos EUA, com o apoio da RAND Corporation, um sistema de defesa que monitoraria os sinais enviados pelos radares no território.

No final dos anos 1960, coube a Agência de Projetos de Pesquisas Avançados – ARPA do DoD, o comando e a coordenação para o desenvolvimento de uma rede de comunicação militar voltada para a proteção do território dos EUA. Um grupo de pesquisadores, a partir do uso de sistemas de computadores, aperfeiçoou uma rede chamada de *Intergalactic Computer Network* [8].

Posteriormente, a partir de grandes investimentos e transferências de recursos estatais, foi criada uma complexa rede de computadores no território estadunidense que passou a ser chamada de ARPANET; essa rede interconectava empresas privadas, universidades, centros de pesquisas e laboratórios, utilizando redes de pacotes de rádio (*packet radio network* - PRNET) [9].

Assim, a história da formação da Internet, desde o período da Guerra Fria, esteve atrelada às demandas de cunho militar mas, com o crescimento da participação das instituições universitárias e de pesquisa, a Internet se expandiu numa velocidade extraordinária dentro dos EUA[10] e fora deles em outros países; essa participação contribuiu, no final dos anos 80 e início dos anos 90, para a disseminação e propagação internacional de uma nova forma de trabalho colaborativa, realizada em rede fora do domínio territorial dos EUA.

No final dos anos noventa, ocorreu um intenso debate, entre cientistas sociais e especialistas em direito no ciberespaço, sobre a repercussão da Internet na soberania dos Estados Nacionais. Os argumentos predominantes que nortearam esse debate[11] foram que, em primeiro lugar, a Internet tal como vinha se desenvolvendo enfraqueceria a soberania do Estado Nacional[12], contra esse argumento havia os que sustentavam utopicamente que a expansão dos usos sociais da Internet fortaleceria a democracia, a liberdade de organização e a socialização da informação[13]; em segundo lugar, os que se colocaram na defesa do argumento de que era quase impossível regular a Internet, contra também havia aqueles que defendiam que os Estados Nacionais desenvolveram vários mecanismos jurídicos para regular as atividades e os serviços realizados a partir do uso da Internet.

Alguns autores que defenderam a tese do primeiro argumento, afirmaram que o crescimento do comércio eletrônico através de trocas de bens intangíveis e a expansão do uso da Internet podem "ameaçar"[14] o poder soberano do Estado porque este não consegue mais controlar inteiramente os limites fronteiriços das relações que se estabelecem sob sua jurisdição geográfica[15], nem consegue mais com normas de jurisprudência local controlar processos, condutas e operações que se realizam virtualmente fora do contexto de seu domínio soberano, o território.

As interpretações negativas dos impactos da Internet na soberania territorial do Estado nacional serviram como justificativa e fundamentação ideológica para a promoção de políticas favoráveis ao controle da Internet. Há quem defenda[16] a regulação unilateral estatal da Internet, afirmando que a atuação do Estado melhora o combate ao crime organizado, a pirataria, aos delitos realizados em operações financeiras, ao terrorismo, pedofilia, ao tráfico de pessoas, entre outros.

Mas será que todos esses argumentos explicam e justificam o controle e gestão da Internet por um único país (os EUA)?

A mundialização incompleta da Internet sob a égide estadunidense

Quando Milton Santos investigou a Geografia das Redes concluiu que as redes inscritas no território ao mundializar-se apresentavam características topológicas que favoreciam a extrapolação dos seus limites físicos. Este processo traria implicações que afetaria o espaço soberano das fronteiras, tendo em vista que as redes são *"os mais eficazes transmissores do processo de globalização a que assistimos"*[17].

Neste sentido, quando analisamos a mundialização recente da Internet, contatamos que este processo está pondo em cheque a arquitetura de localização, de controle e de concentração geográfica dos servidores da zona raiz da Internet[18], evidenciando questões geopolíticas

engendradas pelo sistema hierarquizado de parâmetros de concessão de nomes de domínios[19] e a política de concessão Regional de Registros da Internet, ambos concebidos em março de 1994 por Jon Postel, quando ele ainda estava na direção da IANA (*The Internet Assigned Numbers Authority*).

Essa localização e a concentração geográfica dos servidores da zona raiz nos EUA é um fenômeno historicamente estabelecido desde a constituição da Internet como uma rede militar, que posteriormente se tornou uma rede acadêmica e comercial.

Os parâmetros do sistema hierarquizado de concessão de nomes de domínios, concebidos em 1981 por David L. Mills e aperfeiçoado por Jon Postel, permitem a articulação e o mapeamento geográfico dos servidores regionais interconectados no ciberespaço, fortalecendo e reforçando o controle geopolítico e a concentração dos servidores da zona raiz pelos EUA.

Em 1986, segundo Kurbalija e Gelbstein, o Departamento de Defesa que gerenciava a concessão de nomes de domínios, havia transferido essa responsabilidade para a Fundação Nacional de Ciências dos Estados Unidos, mas:

> "...em 1994, a Fundação Nacional de Ciências dos Estados Unidos decidiu envolver o setor privado, terceirizando a administração do Sistema de Nomes de Domínio (DNS) para a Network Solutions Inc. (NSI). A decisão não foi bem recebida pela comunidade da Internet, e assim começou a "Guerra do DNS".
> Esta "Guerra do DNS" pôs outros atores em cena: o setor empresarial, organizações internacionais e Estados-nação. Ela terminou em 1998, com o estabelecimento de uma nova organização, a Corporação da Internet para Atribuição de Nomes e Números (ICANN).
> Desde 1998 e da fundação da ICANN, o debate sobre a Governança da Internet tem se caracterizado pelo envolvimento mais intensivo de governos nacionais, principalmente através da estrutura da ONU".[20]

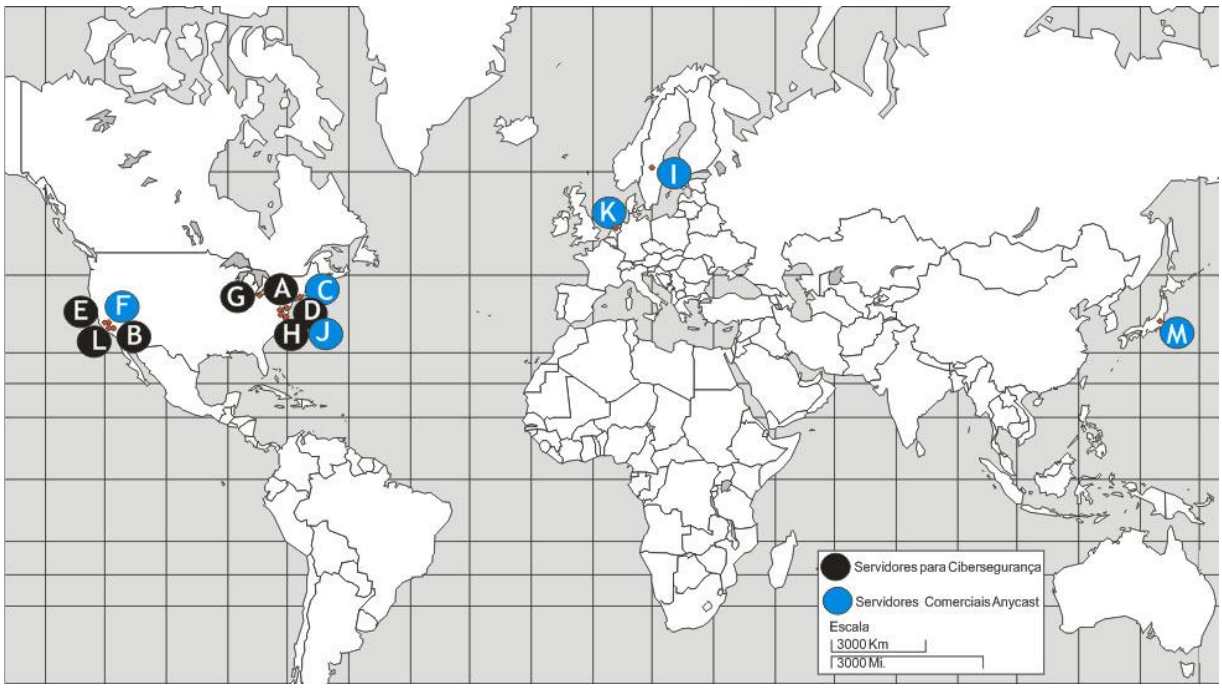
Assim, quatro anos depois da Fundação Nacional de Ciências dos Estados Unidos terceirizar a gestão de nomes de domínios à Network Solutions Inc., a comunidade da Internet, principalmente através da Internet Society[21], conseguiu estabelecer, com a criação da Corporação da Internet para Atribuição de Nomes e Números (ICANN), um novo panorama de concessão de nomes de domínios [22], a partir de muitas articulações diplomáticas, negociações, formação de coalizões, uso de pressões, construção de consensos, com os setores públicos governamentais e privados, e também com parte dos setores da sociedade civil organizada e das organizações internacionais.

O atual modelo unilateral de governança da Internet, constituído desde 1998, pelo Departamento de Comércio dos Estados Unidos, pela ICANN e pela VeriSign, foi o resultado de uma política de dominação voltada para consolidar uma nova forma de imperialismo digital, compelido pela mundialização e o crescimento comercial da Internet. Assim, o desenvolvimento dessa política de imperialismo digital, a partir do controle dos servidores da zona raiz da Internet pela tríade: Departamento de Comércio, ICANN e VeriSign, fez emergir uma nova forma de dominação jurídica, econômica, tecnológica e cultural. Neste sentido a ICANN através da IANA (*The Internet Assigned Numbers Authority*), continua controlando a concessão de Registros Regionais da Internet (*Regional Internet Registry* - RIR)[23].

Como se pode observar na Figura 1, os treze servidores da zona raiz são identificados pelas letras do alfabeto de A a M. Dos treze servidores da zona raiz dez, estão localizados

fisicamente nos Estados Unidos (A, B, C, D, E, F, G, H, J, L); destes, 6 operam dentro do ciberespaço estadunidense (A, B, D, E, G, H), voltados para garantir a gestão do sistema de cibersegurança, os quatro outros são servidores anfitriões (C, F, J, L) que operam com sistema de endereçamento descentralizado Anycast, viabilizando o acesso a um aglomerado de servidores comerciais secundários replicantes distribuídos por vários países, fisicamente instalados fora da região de influência dos servidores da zona raiz da Internet nos EUA.

Figura 1.
Localização Geográfica dos treze principais Servidores
da Zona Raiz da Internet



Elaboração própria, 2012.

Os três servidores restantes da zona raiz que operam fora do território dos EUA (I, K, M), localizados respectivamente na Holanda, na Suécia e no Japão, são servidores anfitriões que operam com sistema de endereçamento descentralizado Anycast e também permitem o acesso de centenas de servidores secundários replicantes de outras regiões, conforme Quadro 1.

Quadro 1.
Principais Operadores dos Servidores da Zona Raiz, Localização e Atividades

Servidor, Operador, Domínio e Endereço de IP	**Localização e Atividades**
Nome: **Servidor A:** VeriSign, Inc.: http://www.verisign.com/ Endereço: IPv4:198.41.0.4; IPv6: 2001:503:ba3e::2:30.	Descrição: Situado no estado da Virginia, este servidor é controlado pelo Departamento de Comércio dos Estados Unidos e pela VeriSign, esta última fundada em 1995, responsável pela certificação de segurança e pela identificação do registro de todos os domínios utilizados na Internet. Este

Nome antigo: ns.internic.net.	servidor interliga seis sítios-webs de quatro cidades estadunidenses e duas cidades globais (Hong Kong e Frankfurt). Atua como operador voltado à regulação de **registros comerciais**[24].
Nome: **Servidor B:** *Information Sciences Institute – USC-ISI:* http://www3.isi.edu/home/ Endereço: IPv4:92.228.79.201; IPv6: 2001:478:65::53. Nome antigo: ns1.isi.edu	Descrição: Localizado em Marina Del Rey, no estado da Califórnia, este servidor é controlado pelo Instituto de Ciência da Informação - Information Sciences Institute da University of Southern Califórnia. O ISI emprega mais de 350 engenheiros da área de tecnologia da informação e tem como missão contribuir para o desenvolvimento da defesa do ciberespaço dos EUA. Atuando no setor de defesa e de recursos críticos desde 1972, presta consultoria a mais de vinte agências e departamentos do governo estadunidense: *DARPA - Defense Advanced Research Projects Agency; RAND Corporation; the Department of Homeland Security, The Department of Energy;National Science Foundation*, etc[25]. Este servidor opera apenas nos EUA. Atua como operador voltado para gestão do sistema de **cibersegurança**.
Nome: **Servidor C:** *Cogent Communications:* http://www.cogentco.com/htdocs/index.php/ Endereço: IPv4:192.33.4.12; IPv6: 2001:500:2::c. Nome antigo: c.psi.net	Descrição: Servidor que opera sistema de endereçamento descentralizado Anycast, situado em NewYork no estado de New York. Este servidor é mantido pela empresa multinacional Cogent, fundada em 1999, provedora de acesso à Internet de nível T1 (mais de 10 Gbs)[26]. Este servidor interliga seis sítios-webs de quatro cidades estadunidenses e duas cidades européias (Madrid e Frankfurt). Atua como operador voltado à regulação de **registros comerciais**.
Nome: **Servidor D**: *University of Maryland:* http://www.umd.edu Endereço: IPv4:128.8.10.90; IPv6: 2001:500:2d::d. Nome antigo: terp.umd.edu	Descrição: Servidor localizado no College Park da University of Maryland, no estado de Maryland. A Universidade de Maryland opera o servidor da IANA. Em setembro de 1988, esta Universidade foi responsável pelo estabelecimento da primeira conexão à rede BITNET com as instituições científicas brasileiras, usando para isto um enlace de 9.600 bps. O Laboratório Nacional de Computação Científica (LNCC), localizado no Rio de Janeiro, foi a primeira instituição científica do Brasil a receber esta conexão[27]. Este servidor opera apenas nos EUA. Atua como operador voltado para gestão do sistema de **cibersegurança**.
Nome: **Servidor E:** *NASA Ames Research Center:* http://www.nasa.gov/home/index.html Endereço: IPv4:192.203.230.10; IPv6: Não declarado. Nome antigo: ns.nasa.gov	Descrição: Localizado em Mountain View no Estado da Califórnia, este servidor é utilizado pela *NASA - National Aeronautics and Space Administration*, criada em 1958. A NASA patrocina pesquisas e o desenvolvimento de tecnologias direcionadas para o fortalecimento do programa espacial estadunidense. Este servidor opera apenas nos EUA. Atua como operador voltado para gestão do sistema de **cibersegurança**.
Nome: **Servidor F:** *Internet Systems Consortium, Inc*: http://www.isc.org/ Endereço: IPv4:192.5.5.241, IPv6: 2001:500:2f::f. Nome	Descrição: Localizado em Palo Alto, no estado da Califórnia, este servidor opera desde 1994 pela IANA através do sistema de endereçamento descentralizado Anycast, mantido pelo Internet Systems Consortium, Inc. O servidor do ISC interliga 49 sítios-web, alguns de várias

antigo: ns.isc.org	partes do mundo. Atua como operador voltado à regulação de **registros comerciais**.
Nome: **Servidor G:** *U.S. DOD Network*: http://www.nic.mil Endereço: IPv4:192.112.36.4; IPv6: Não declarado. Nome antigo: ns.nic.ddn.mil	Descrição: Localizado em Columbus, no estado de Ohio, este servidor é mantido pela Agência do Sistema de Informação de Defesa, que tem a responsabilidade de efetuar o planejamento e o desenvolvimento das operações de cibersegurança para o governo dos EUA e o Departamento de Defesa (DoD). Este servidor opera em quatro cidades estadunidenses e duas européias (Sturttgart e Napoles). Atua como operador voltado para gestão do sistema de **cibersegurança**.
Nome: **Servidor H:** *U.S. Army Research Lab*: http://www.arl.army.mil/main/Main/default.htm Endereço: IPv4:128.63.2.53; IPv6:2001:500:1::803f:235. Nome antigo: aos.arl.army.mil	O servidor H do exército dos EUA, interconecta duas áreas de operações, a primeiro situado em Aberdeen região de Mariland e a segunda em San Diego na Califórnia. Este servidor é controlado pelo Laboratório de Pesquisas do Exército dos Estados Unidos (*U.S. Army Research Lab*). O ARL também conhecido como Laboratório de Pesquisas Balísticas (BRL), tem uma longa história na concepção de tecnologias de informação. Nos anos 50, o BRL ajudou a conceber o primeiro computador eletrônico digital, o ENIAC. Na época, o objetivo principal, para construção do ENIAC, era auxiliar a produção de armas, ou seja, este faria os cálculos necessários para a criptoanálise, confecção de bombas atômicas, cálculos das tabelas balísticas e dos primeiros mísseis nucleares. A grande maioria das pesquisas científicas deste laboratório esteve voltada para auxiliar o desenvolvimento da indústria de defesa. Muitos pesquisadores desses dois laboratórios também estiveram envolvidos em projetos para o desenvolvimento militar da Internet, estes ajudaram a conceber: o sistema operacional UNIX; o sistema de protocolos TCP/IP; os parâmetros de registro do DNS. No final dos anos 70 e início dos anos 80, o BRL coordenou pesquisas para a organização das redes militares. Segundo Tancman: "*O ARL passou a sediar um dos servidores-raiz original na MILNET e foi desvinculado da Internet. Atualmente, ARL é a base de um dos maiores supercomputadores do mundo. O ARL continua a operar com um servidor-raiz de nome com serviços de segurança para Internet*"[28]. Este servidor opera apenas em duas cidades estadunidenses (Aberdeen e San Diego). Atua como operador voltado para gestão do sistema de **cibersegurança**.
Nome: **Servidor I:** Autonomica: http://www.netnod.se/dns_root_nameserver.shtml Endereço: IPv4:192.36.148.17; IPv6: 2001:7fe::53. Nome antigo: nic.nordu.net	Descrição: Localizado em Estocolmo, na Suécia, este servidor opera através do sistema de endereçamento descentralizado Anycast, administrado pelo provedor públicos de Internet de alta velocidade: Autonomica. Sua atuação se dá na concessão de DNS a vários servidores secundários fora da zona raiz dos EUA, fornecendo o acesso a trinta e oito sítios-webs da Internet de várias partes do mundo. Este servidor atua como operador voltado à regulação de **registros comerciais**.

Nome: **Servidor J:** VeriSign, Inc.: http://www.verisign.com/ Endereço: IPv4:192.58.128.30; IPv6: 2001:503:c27::2:30.	Descrição: Situado no estado da Virginia, este servidor opera através do sistema de endereçamento descentralizado Anycast, administrado pela VeriSign, fornecendo acesso a setenta sítios da Internet de várias partes do mundo. Este servidor atua como operador voltado à regulação de **registros comerciais**.
Nome: **Servidor K:** *Reseaux IP Europeens - Network Coordination Centre*: http://www.ripe.net/info/ncc/index.html Endereço: IPv4:193.0.14.129; IPv6:2001:7fd::1	Descrição: Situado em Amsterdam, na Holanda, este servidor opera através do sistema de endereçamento descentralizado Anycast. Administrado pela RIPE NCC. O servidor desta instituição opera interligado a 18 sítios de organizações de telecomunicações e grandes empresas localizadas na Europa, Oriente Médio e em partes da Ásia Central. A RIPE também oferece a concessão pública de registro regional para Internet (RIR) e protocolos de acesso a Internet (IPv4, IPv6), para os membros conveniados. Este servidor atua como operador voltado à regulação de **registros comerciais**.
Nome: **Servidor L:** *Internet Corporation for Assigned Names and Numbers - ICANN*: http://www.icann.org Endereço: IPv4:198.32.64.12; IPv6: 2001:500:3::42.	Descrição: Situado em Los Angeles, no estado da Califórnia, este servidor opera através do sistema de endereçamento descentralizado Anycast. Administrado pela ICANN, este servidor oferece roteamento e interligação física a vários servidores clientes de noventa e sete sítios-webs, através do Border Gateway Protocol (BGP), nos seguintes pontos de troca: *Equinix Internet Exchange - Los Angeles; Pacific Wave Internet Exchange - Los Angeles; LAIIX-Los Angeles International Internet Exchange - Los Angeles; Pacific Wave Internet Exchange - San Jose; Pacific Wave Internet Exchange – Seattle; PAN das Américas – Miami.* A ICANN é responsável pela coordenação global do sistema de identificadores da Internet, como nomes de domínio e endereços usados em vários protocolos que permitem os computadores se comunicarem pela Internet. Este servidor atua como operador voltado à regulação de **registros comerciais**.
Nome: **Servidor M:** *WIDE Project:* http://www.wide.ad.jp/ Endereço: IPv4:202.12.27.33; IPv6:2001:dc3::35.	Descrição: Localizado em Tokyo, no Japão, este servidor opera, desde 1997, através do sistema de endereçamento descentralizado Anycast. Administrado pela WIDE Project, atuando para prover e conceder registros a inúmeros servidores secundários na região do oeste do pacífico. Desde 2002, fornece acesso a seis grandes sítios da Internet localizados em: Tóquio, Japão (três sítios); Seul, KR; Paris, FR; São Francisco, CA, E.U. Este servidor atua como operador voltado à regulação de **registros comerciais**.

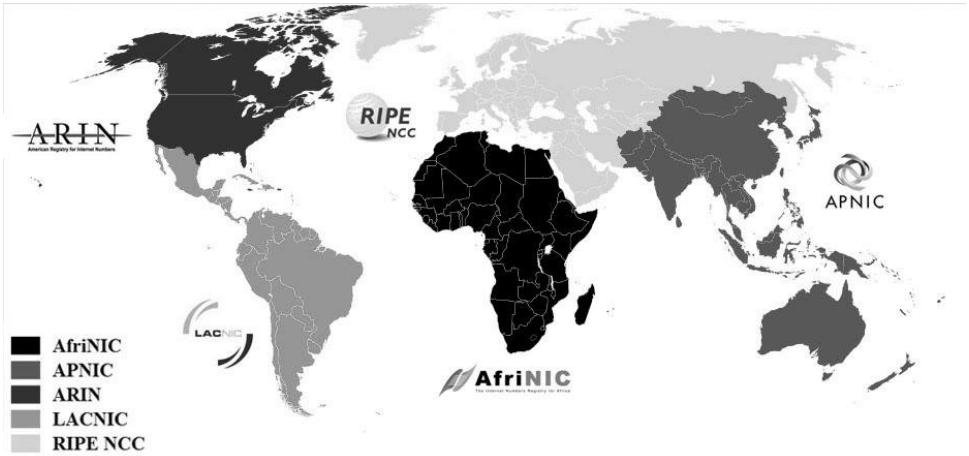
Elaboração própria, atualizada em 2012 a partir de consulta ao sítio-web: http://www.root-servers.org/

Conforme já evidenciado anteriormente, de acordo com o memorando RFC 1591[29], coube também a IANA (*The Internet Assigned Numbers Authority*), a responsabilidade pela concessão do código de domínio de alto nível dos países (country *code top-level domain - ccTLD*). Os ccTLD, representados por duas letras (br. es, ar, ch, de, etc.) que eram os identificadores oficiais dos topônimos de países. A escolha dessa metodologia de designação

dos topônimos de países[30] segue um conjunto de normas geográficas, criadas em 1974, que valida os códigos para os nomes de países e dependências, o ISO 3166-1 Apha-2[31].

Como se pode observar na Figura 2, atualmente esta geopolítica de distribuição de endereços protocolos de Internet - IPs é controlado por cinco instituições de concessão de registros regionais da Internet: a) *Africa Network Information center* - AfriNIC , que mantém o controle da concessão de registros regionais da Internet na Região da África: http://www.afrinic.net/; b) *Asia Pacific Network Information center* - APNIC, que controla a concessão de registros regionais da Internet na Região da Ásia e Pacífico: http://www.apnic.net/; c) *American Registry for Internet number* - ARIN, que controla a concessão de registros regionais da Internet na Região Norte Americana: http://www.arin.net/; d) *Latin-American and Caribbean Internet Address Registry* - LACNIC, que controla a concessão de registros regionais da Internet na Região da América Latina e algumas ilhas do Caribe: http://www.lacnic.net/; e) *Réseaux Ip Européens/Network coordination Center* - RIPE/NCC, que detém o controle da concessão de registros regionais da Internet na Europa e Oriente Médio e Ásia Central: http://www.ripe.net/.

Figura 2.
Instituições de Registros Regionais da Internet



Fonte: http://en.wikipedia.org/wiki/Regional_Internet_registry , 2011.

Neste sistema de regionalização da concessão global de Registros Regionais da Internet (RIRs), a ICANN também indica os representantes das cinco instituições reguladoras.

No final dos anos 1990, ocorreu uma grande mobilização dos atores políticos dos Estados nacionais, através dos governos, setores públicos, setores privados, organizações da sociedade civil e organismos internacionais (Associação de Nações do Sudeste Asiático - ASEAN, Ásia-Pacífico Cooperação Econômica - APEC; Conselho da Europa - CoE; União Internacional de Telecomunicações - UIT; Escritório do Alto Comissariado da ONU para os Direitos Humanos - ACDH, Organização para a Cooperação Econômica e Desenvolvimento - OCDE; Comissão das Nações Unidas sobre o Direito Comercial Internacional - UNCITRAL; Escritório das Nações Unidas sobre Drogas e Crime - UN-ODC, Patrimônio Mundial da UNESCO; Organização Mundial da Propriedade intelectual - OMPI, Organização Mundial do Comércio - OMC; etc.[32]), para o estabelecimento de fórum internacional, voltado para discutir uma nova

estrutura de regulação global da Internet, baseado em um sistema consensuado de gestão multilateral.

O ciberespaço como o novo anfiteatro da guerra no século XXI

O ciberespaço continua sendo, na atualidade, um terreno estratégico de interesses econômicos e militares dos EUA, e também um campo virtual de guerra, sobre o qual estes interesses devem manter um sistema militar permanente de segurança, vigilância e de proteção de suas redes, articulados através do princípio da Guerra Baseada em Redes ou *Network-Centric Warfare*[33], criado pelo Programa de Pesquisa de Comando e Controle do Departamento de Defesa (*Command and Control Research Program* – CCRP).

Neste sentido, o Departamento de Defesa ficou com o controle militar do ciberespaço e a ICANN juntamente com a VeriSign ficaram com o controle comercial e, por isso, vêm sendo os organismos formais responsáveis exclusivos pela atribuição de parâmetros de protocolo da Internet, pela regulação do sistema de nome de domínio, pela alocação blocos de números de endereços IP e pela gestão do servidor raiz do sistema.

O sistema de designação genérico de nomes e domínios (*generic top-level domain* - gTLD) e o sistema de Registro Regional da Internet (*Regional Internet Registry* - RIR) se transformaram, sob a chancela da trindade (Departamento de Comércio/ICANN/Verisign) da Internet, em um negócio altamente lucrativo. Esta atuação controladora afeta uma gama variada de questões que dizem respeito à soberania, segurança, geopolítica, educação, cidadania, privacidade, liberdade de expressão, democracia, entre outras. Segundo Proulx e Millette, esta forma de imperialismo digital é contrária ao espírito da Internet:

> "Este dominio tecnológico y jurídico facilita el dominio comercial. ... Sin embargo su predominio comercial no sólo entraña la capacidad de influir decisivamente en los principales mercados de Internet: es toda la arquitectura de la red que se encuentra cercada por los intereses de las compañías estadounidenses. Ese poder menoscaba el proyecto inicial de los pioneros de Internet, que era el de considerar la información como un bien común. Esta forma digital de imperialismo cultural impide el desarrollo del ciberespacio como servicio público y fermento de la democracia".[34]

A despeito das várias iniciativas de 2003 até 2011 para reformar o modelo atual de governança unilateral da Internet, através da realização de oito fóruns para debater a governança da Internet (Quadro 2), os EUA publicaram no mesmo período, quatro importantes documentos de estratégias políticas de manutenção do controle da Internet. Estes documentos, elaborados pelo Departamento de Segurança Doméstica, pela Casa Branca e pelo Departamento de Defesa, são utilizados como componentes doutrinários que vem norteando a atual política global de controle da Internet pelos EUA.

Quadro 2.
Fóruns da Governança da Internet e Estratégias Políticas dos EUA para Internet

Fóruns da Governança da Internet (IGF)	**Ano**	**Local de realização**	**Estratégias Políticas dos EUA para Internet (Documentos)**
1º IGF	2003	Genebra, Suíça	Gestão Bush: *National Strategy to*

			Secure Cyberspace[35]
2º IGF	2005	Tunes, Tunísia	
3º IGF	2006	Atenas, Grécia	
4º IGF	2007	Rio de Janeiro, Brasil	Gestão Bush: *The National Strategy for Homeland Security*[36]
5º IGF	2008	Hyderabad, Índia	
6º IGF	2009	Sharm El Sheikh, Egito	
7º IGF	2010	Vilnius, Lituânia	
8º IGF	2011	Nairobi, Quênia	Gestão Obama*: International Strategy for Cyberspace*[37] e *Strategy for Operating in Cyberspace*[38]

Elaboração própria. Quadro elaborado a partir de informações fornecidas pelo Departamento de Defesa dos EUA e pelo Secretariado do Fórum da Governança da Internet nas Nações Unidas: http://www.intgovforum.org/cms/

Essas mesmas estratégias de segurança se refletem no controle dos servidores da zona raiz, mantidas pela ICANN, VeriSign e pelo Departamento de Comércio na concessão de nomes de domínios e nos registros de códigos de países, que vêm dificultando a implantação de uma governança multilateral da Internet, como reivindicam quase todos os países.

Em fevereiro de 2003, a Casa Branca lançou através do Departamento de Defesa o documento "A Estratégia Nacional para Segurança do Ciberespaço" (*The National Strategy to Secure Cyberspace*)[39]. Os principais objetivos eram[40]: a) impedir a ocorrência de ataques cibernéticos contra infra-estruturas críticas dos EUA; b) reduzir a vulnerabilidade nacional a ataques cibernéticos; e c) minimizar os danos e antever ações para reduzir a freqüência desses ataques. O ciberespaço, neste documento, passou a ser considerado como uma rede interdependente de infraestruturas de tecnologias de informação e uma das principais infra-estruturas críticas dos interesses dos EUA.

Este plano estratégico articulava cinco importantes prioridades nacionais:

I. "Sistema de resposta de segurança do ciberespaço;
II. Um programa de redução de vulnerabilidade e ameaça à segurança do ciberespaço nacional;
III. Um programa de treinamento e consciência de segurança do ciberespaço nacional e;
IV. Proteção aos ciberespaços dos governos, e
V. Cooperação em segurança do ciberespaço nacional e internacional"[41].

Uma das justificativas para implantação desse plano estratégico de segurança foi que alguns dos treze (13) servidores raízes da Internet haviam sofrido um ataque no dia 21 de outubro de 2002[42].

Em 2007, ainda sob a gestão de Bush, o Departamento de Segurança Doméstica (*Department of Homeland Security)* lançou a política nacional de cibersegurança através do documento "A Estratégia Nacional para Segurança Doméstica" (*The National Strategy For Homeland Security)*. Esta estratégia orienta, organiza e unifica os esforços para segurança doméstica nacional, objetivando a proteção da infra-estrutura crítica do território dos EUA, vinculada à Internet. Neste mesmo ano, a força aérea havia criado um cibercomando (*Air Force Cyber* - AFCYBER), localizado na base da Força Aérea de Barksdale, na Louisiana, onde são

treinados ciberguerreiros (*Cyber Warriors*) que tem como função a proteção do território estadunidense contra um eventual ataque ou uma guerra centrada nas redes.

Este plano, em relação aos outros planos estratégicos dos EUA, na parte referente à Cibersegurança: Uma consideração especial *(Cyber Security: A Special Consideration),* revela um componente diferente e atualizado em relação ao ciberespaço dos EUA, devido à preocupação com a segurança da infra-estrutura cibernética dos EUA:

> "Muitos dos serviços essenciais e emergenciais da Nação, bem como as nossas infra-estruturas críticas, utilizam ininterruptamente a Internet e os sistemas de comunicações, de dados, de acompanhamento, de controle e sistemas que compõem a nossa infra-estrutura cibernética. Um ataque cibernético poderia debilitar profundamente a nossa interdependente infra-estrutura crítica (CI) e recursos chaves (KR) e, finalmente, a nossa economia e segurança nacional.
> Uma variedade de atores ameaça a segurança da nossa infra-estrutura cibernética. Terroristas exploram cada vez mais a Internet para se comunicar, recrutar, arrecadar fundos, realizar treinamento e planejamento operacional. Governos estrangeiros hostis têm os recursos técnicos e financeiros para apoiar uma rede avançada de exploração e lançar ataques contra os elementos informacionais e físico de nossa infra-estrutura cibernética. Hackers criminosos ameaçam a economia de nossa Nação e as informações pessoais dos nossos cidadãos, estes também podem vir a ser uma ameaça, se conscientemente ou inconscientemente são recrutados pela inteligência estrangeira ou grupos terroristas. Nossas ciber-redes também são vulneráveis a desastres naturais.
> A fim de garantir a nossa infra-estrutura cibernética contra estas ameaças produzidas pelo homem e pela natureza, os governos federal, estadual e local, trabalham conjuntamente com o setor privado, para evitar danos contra a utilização não autorizada e a exploração de nossos sistemas cibernéticos. Nós também estamos aumentando a nossa capacidade e procedimentos para responder no caso de um ataque ou incidente grave cibernético. A Estratégia Nacional para a Segurança do Ciberespaço e o Setor de Cibersegurança do Plano Nacional de Proteção da Infra-estrutura (NIPP) estão orientando os nossos esforços"[43].

Por isso, durante a era Bush, o ciberespaço se transformou no espaço do Estado da guerra sem fim à ciberguerra ou *Cyberwarfare*[44]. Esta guerra vem sendo construída para ser deflagrada através de complexos aparatos tecnológicos, utilizados por um exército de cibercombatentes, que estão sendo preparados em universidades para destruírem os territórios-rede. Segundo Baldi, Gelbstein e Kurbalija, um contexto de ciberguerra envolve componentes de espionagens, várias formas de atividades de contra-informação e o uso de armas "inteligentes" destrutivas e não destrutivas[45]. Devido a essas ações dos EUA, a China[46] e outros países (Rússia e Brasil) também já estão treinando um exército de Hackers.

Dando continuidade a essas políticas do *Cyberwarfare*, em maio de 2011, o governo dos EUA sob a gestão de Barack Obama, lançou o documento Estratégia Internacional para o Ciberespaço: Prosperidade, Segurança, e Abertura em um Mundo Conectado e em Rede (*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World).* Este documento é repleto de eufemismos e de contradições, pois ao mesmo tempo em que admite, pela primeira vez, que a governança da Internet não pode continuar sendo efetuada por um único país, afirmando que:

> "Os Estados Unidos vão trabalhar internacionalmente para promover uma infraestrutura de comunicações e informação, aberta, interoperável, segura, e confiável, que suporte as trocas e o comércio internacional, fortaleça a segurança internacional, e promova a livre expressão e inovação. Para alcançar essas metas, iremos construir um ambiente em que as normas de comportamento responsável oriente as ações dos Estados, matenha as parcerias, e garanta a regra

da lei no ciberespaço[47]. ... As normas emergentes, também essenciais para este espaço (**ciberespaço**), incluem:

- Interoperabilidade Global: Os Estados devem agir dentro de suas autoridades para ajudar a garantir a interoperabilidade de ponta a ponta de uma Internet acessível a todos.
- Estabilidade da Rede: Os Estados devem respeitar o livre fluxo de informações nas configurações de redes nacionais, assegurando que eles não interferiram arbitrariamente com infra-estrutura internacionalmente interligados.
- Acesso Confiável: os Estados não devem privar arbitrariamente ou interromper o acesso de indivíduos à Internet ou outras tecnologias de rede.
- Governança Multilateral: os esforços de governança da Internet não devem ser limitados aos governos, mas deve incluir todos empreendedores apropriados.
- Cibersegurança Devido Diligência: Os Estados devem reconhecer e agir sobre sua responsabilidade de proteger infra-estruturas de informação e a segurança de sistemas nacionais de danos ou uso indevido"[48].

Mas o documento entra em contradição quando afirma:

> "Quando garantido, os Estados Unidos responderão a atos hostis no ciberespaço como faríamos com qualquer outra ameaça ao nosso país. Todos os estados possuem o direito inerente de legítima defesa, e reconhecemos que certos atos hostis realizados através do ciberespaço podem obrigar às ações no âmbito dos compromissos que temos com os nossos parceiros de tratados militares. Reservamo-nos o direito de utilizar todos os meios necessários diplomático, informativo, militar e econômico, adequados e compatíveis com o direito internacional aplicável, a fim de defender a nossa nação, nossos aliados, nossos parceiros e nossos interesses. Ao fazer isso, vamos esgotar todas as opções antes de força militar sempre que possível; vai pesar cuidadosamente os custos e riscos de ação contra os custos da inação, e vai agir de uma maneira que reflita nossos valores e fortalece a nossa legitimidade, buscando um amplo apoio internacional sempre que possível".[49]

No documento Estratégia Internacional para o Ciberespaço: Prosperidade, Segurança, e Abertura em um Mundo Conectado e em Rede, o estilo modificou, mas o tom imperialista e belicista permanece o mesmo, continua a mesma concepção unilateral das iniciativas de auto defesa que inspiram desconfiança e receios.

Alternativas contrahegemônicas de governança da Internet

Há uma crescente percepção, entre Estados nacionais, que o ciberespaço não poderá continuar sendo controlado por um único país, principalmente quando este detém o poder econômico e militar da Internet. Mas como se constituirá a gestão de fato dos Estados Nacionais do ciberespaço e da Internet?

As iniciativas de constituição de um novo sistema de zona raiz alternativo para a Internet, menos dependente dos EUA, promovidas pela ONU através dos Fóruns de Governança da Internet (*Internet Governance Forum* – IGF)[50] e dos Projetos Alternativos de governança da Internet, estavam sendo rotuladas como iniciativas que promovem a fragmentação da Internet. A primeira grande iniciativa de estruturação de uma rede independente de raiz de nomes de domínios para a Internet[51], ocorreu oficialmente em 2002 com a criação da Rede Aberta do Servidor de Raiz (*Open Root Server Network –ORSN)*[52]. Esta iniciativa durou apenas seis anos porque, em dezembro de 2008, a ORSN foi formalmente desligada (*shutdown*), mas as razões e justificativas do desligamento da ORSN ainda são obscuras[53]; mesmo assim, outras

redes alternativas de servidores raízes de nomes para a Internet[54] continuam em operação nos EUA, mas sem o caráter e a filosofia de independência política que foi mantida pela ORSN.

É importante salientar que as principais questões geopolíticas que dominam o debate sobre a localização dos servidores da zona raiz da Internet são referentes aos seguintes temas: jurisprudência no ciberespaço, liberdade de expressão, cibersegurança e combates às práticas de delitos na Internet, soberania e gestão do sistema de concessão de nomes de domínios e países, e políticas de desenvolvimento do tráfego local da Internet e da arquitetura da rede no território.

Com relação à cibersegurança e combates às práticas de delitos na Internet, as autoridades públicas internacionais estão mobilizadas no combate à pedofilia, aos ciberdelitos e proteção de recursos críticos e contra ataques provenientes de potenciais inimigos externos (hackerismos[55], atentados e ciberterrorismos). Neste item, durante a gestão de Bush, foi gasto o equivalente a seis bilhões de dólares em investimentos militares e na gestão de Barack Obama, além de manter esses gastos, foi criado um conselho nacional para atuar também na área de cibersegurança[56].

Na questão da soberania e gestão do sistema de concessão de nomes de domínios e países, alguns atores políticos - governos, setores públicos, setores privados e organizações da sociedade civil, desejam descentralizar e reformar o modelo de concessão de nomes de domínios, através da implantação do *Domain Name System Security Extensions* – DNSSEC que é um sistema mais seguro de resolução de nomes e que permite a criptografia das assinaturas, a redução dos riscos de manipulação de dados e a falsificação de domínios. Esses atores desejam também debater o aperfeiçoamento e a substituição do protocolo *Internet Protocol Version 4* - IPv4, que suporta aproximadamente 4 x 109 de endereços, pelo protocolo de registro *Internet Protocol Version 6* - IPv6, que suportará algo em torno de 3.4 x 1038 endereços. Em resposta ao crescimento do uso do *Domain Name System Security Extensions* – DNSSEC em vários países (Brasil, Bulgária, República Checa, Puerto Rico e Suécia), a VeriSign e a ICANN lançaram, em setembro de 2008, a proposta *Root Zone Signing Proposal*[57], cujo objetivo foi manter a permanência do controle do processo de registros e de concessão de nomes de domínios de servidores e provedores na zona raiz da Internet, absorvendo, na sua proposta o DNSSEC.

Nas políticas de desenvolvimento do tráfego local da Internet e da arquitetura da rede no território, o crescimento e a mundialização da Internet propiciaram a formação de contextos virtuais de acumulação em diferentes economias-mundo. Estas passaram a requerer instrumentos territorializados de regulação e gestão do ciberespaço.

Por isso, os Estados nacionais reivindicam, através da ONU, um espaço soberano de decisão e participação multilateral na gestão da Internet. No final dos anos 1990, esses atores sociais rejeitaram o modelo de gestão estabelecido pelos EUA através da ICANN, e exigem a promoção do diálogo na direção da construção de um novo modelo de gestão consensuado e multilateral, que envolva democraticamente todos os Estados membros da ONU.

Com relação à liberdade de expressão na Internet, esta está cada vez sendo mais sendo vigiada e controlada. O mundo tem acompanhado as represálias dos Estados Unidos com relação ao sítio-web WikiLeaks[58] que está impedido de se expressar, outros países estão também

estabelecendo censuras à livre manifestação e organização na Internet. Segundo o sítio dos Repórteres Sem Fronteiras, pelo menos 15 países[59] censuram ou praticam a censura parcial ou completa de conteúdos da Internet no seu território (*cyber-censorship*)[60], mas alguns Estados nacionais justificam que esse controle é para evitar a influência ideológica de outros países que estão ferindo sua soberania. Os EUA estão no topo da lista dos países que praticam políticas draconianas contra Internet[61], justificando também a censura que pratica como uma questão de segurança.

Conclusão

Quando analisamos os instrumentos e os fóruns reais de decisão do atual sistema de governança da Internet, chegamos à constatação de que pouco se fez para torná-los mais democráticos, participativos e multilaterais.

Ao examinamos o contexto de governança da Internet, mantido pela ICANN, acreditávamos que a mundialização da Internet iria erodir este modelo ultrapassado de governança, ingenuamente acreditávamos também que os fóruns, promovidos pela ONU para discutir a governança da Internet, poderiam acelerar a consolidação de uma governança da Internet multilateral e democrática, constituída a partir de um consenso global.

Mas ainda hoje, o que infelizmente constatamos é que, em primeiro lugar, o controle e a extrema centralização da governança da Internet por um só país continuam tão intransponíveis quanto antes, a despeito da legitimidade da autoridade da ICANN, neste modelo de governança da Internet, ser amplamente questionada; em segundo lugar, as participações do Departamento de Segurança Doméstica, da Casa Branca e do Departamento de Defesa, na elaboração da atual política global de controle da Internet, considerando esta como um recurso crítico para a segurança dos EUA, acirram o *Cyberwarfare*; em terceiro lugar, os canais para garantir a autonomia dos países para a elaboração de propostas de políticas públicas para o desenvolvimento da Internet estão sendo cada vez mais restringidos, principalmente nos IGF; em quarto lugar, há uma enorme dificuldade para programar, através da ONU, um debate internacional que envolva todos os Estados nacionais à consolidação de uma instituição internacional encarregada de promover uma governança global multilateral; em quinto lugar, alguns países estão preferindo estabelecer a sua própria estrutura de regulação e controle da Internet, a revelia das decisões da ONU; em sexto lugar, o legado da era Bush sobre o ciberespaço transformou o discurso da governança democrática multilateral na ONU, em uma ideologia da geopolítica de segurança que vem sendo continuada na gestão atual de Obama.

No entanto, a maioria das representações diplomáticas dos países acredita que o ciberespaço não pode continuar sendo controlado por um único país, principalmente quando este detém o poder econômico e militar da Internet e, também, porque como ainda não existem instituições internacionais multilaterais que decidam democraticamente na gestão da Internet global, as soberanias de todos os Estados nacionais continuam sob a ameaça desse imperialismo digital.

Notas

[1] As cinco inovações foram: em primeiro lugar, o telégrafo inventado pelo estadunidense Samuel Morse em 1832; em segundo lugar, o telefone inventado pelo italoamericano Antonio Santi Giuseppe Meucci, em 1854, e não por Alexander Graham Bell considerado durante muitos anos como inventor do telefone (Cf. em: http://pt.wikipedia.org/wiki/Antonio_Meucci) em terceiro lugar, o radio concebido em 1891, pelo austríaco Nikola Tesla; em quarto lugar, a televisão desenvolvida industrialmente em 1928, pelo engenheiro sueco Ernst F. W. Alexanderson, da General Eletric; em quinto lugar, a Internet, criada no final dos anos 60 pela ARPANET, como o resultado de uma fusão de várias redes militares voltada para a proteção do território dos EUA, a Internet ou *Inter-Networking* passou a ser reconhecida como a rede das redes, a sua expansão e o seu crescimento no território estadunidense foi um resultado de imensas transferências de recursos estatais destinadas a promoção, sem licitação ou concorrência pública, de empresas privadas, universidades, centros de pesquisas e laboratórios pertencentes ao complexo militar.

[2] Fidler, 1998 p.415.

[3] Iniciada em 2009, esta pesquisa agora revisada e ampliada, para o *XII Coloquio Internacional de Geocrítica de Bogotá*, é o fruto do aprofundamento das reflexões parcialmente desenvolvidas no XII Encontro de Geografos da America Latina - XII EGAL Mesa: Región y Globalización. Desafíos epistemológicos y políticos de las nuevas espacialidades de Montevideo, e no VIII Encontro Nacional da ANPEGE de Curitiba.

[4] Para quem deseja ter informações mais aprofundadas sobre a história da governança da Internet ler o meu artigo "Governança Global da Internet: A representação de topônimos de países no ciberespaço", publicado na revista Scripta Nova em 2008: http://www.ub.edu/geocrit/sn/sn-270/sn-270-151.htm

[5] Harrison & Bluestone, 1984.

[6] Markusen et al, 1991, p.10.

[7] Segundo McNeil, 1989, p. 401:

> *"... el radar constituyó la más notable de estas innovaciones, científicos e ingenieros británicos descubrieron cómo utilizar la reflexión de ondas cortas de radio para localizar aviones a una distancia que permitiera a pilotos de cazas interceptarios durante la batalla de Inglaterra. El radar siguió desarrollándose muy rápidamente durante la guerra y encontró nuevos usos en la navegación y la puntería de los aviones, pero otros avances tecnológicos – aviones a reacción, espoletas de proximidad, vehículos anfibios, misiles dirigidos, cohetes, y lo más complicado de todo, cabezas atómicas – pronto compitieron en importancia con el radar".*

[8] Ryan, 2010, p.25.

[9] Ryan, 2010, p.34.

[10] Conferir através de mapas a evolução da ARPANET de 1969 até 1977 em: http://som.csudh.edu/cis/lpress/history/arpamaps/

[11] Trata-se do debate promovido no *The Indiana Journal for Global Legal Studies*, sobre os impactos da Internet na soberania dos Estados Nacionais. Ver em Sassen, 2000 p.195.

[12] Perritt, 1998 p. 424.

[13] Barlow, 1996.

[14]. Ler em Perritt, 1998 p. 425 e 426:

> *"Later, the development of radio, telegraph, telephone, and then television technologies also confronted those in power and privilege with new threats to their traditional status. The Internet joins a long historical heritage of new information technologies threatening to upset the existing nature of politics within nation-states".*

[15] Post, 1997.

[16] Veja como Goldsmith defende a regulação unilateral dos EUA, 2000, p. 136.

[17] Santos, 1996 p.212.

[18] Conferir a localização geográfica global dos servidores da Zona Raiz da Internet e seus replicadores anycast regionais em: http://www.root-servers.org/

[19] O Sistema de Nomes de Domínios ou *Domain Name System - DNS*, também chamado de *Internet Name Domains*, foi concebido em setembro de 1981, por David Mills da COMSAT Laboratories, através d o memorando RFC (Request for Comments) número 799. Conferir o memorando RFC 799 em: http://www.faqs.org/rfcs/rfc799.html

[20] Ver Kurbalija e Gelbstein, 2005, pp.10-11.

[21] A Internet Society (ISOC), constituída em 1992, teve um importante papel na abertura de discussões sobre os processos de concessão de DNS e de governança da Internet. Ver mais sobre a História da ISOC no seu sítio-web, em: http://www.internetsociety.org/20th

[22] Conferir o "Anexo II – Uma síntese da evolução da governança da Internet", no livro de Kurbalija e Gelbstein, 2005, pp.160-161.

[23] Em relação ao sistema de códigos de nomes dos países, a ICANN preferiu dar continuidade à política da IANA e continuou seguindo o conjunto de normas geográficas da ISO 3166-1. A única alteração foi burocrática, correspondente à criação da Organização de Suporte aos Códigos de Nomes dos Países ou *Country Code Names Supporting Organisation* – CCNSO e a constituição de um conselho de administração de políticas globais para elaborar, de forma "consensuada", o código dos domínios de nível superior dos países, o ccTLD. Portanto, a essência do sistema permaneceu a mesma da IANA, ou seja, os países não são países, são apenas topônimos de países sujeitos a mercantilização. Ler em Pires, 2008.

[24] Ler em: http://en.wikipedia.org/wiki/VeriSign e http://en.wikipedia.org/wiki/File:Verisignheadquarters.jpg

[25] Conferir em: http://www3.isi.edu/about-isi_profile.htm

[26] Conferir em: http://www.cogentco.com/us/about_history.php

[27] Pires, 2005.

[28] Tancman, 2008, p.81.

[29] Conferir o memorando RFC 1591 *Domain Name System Structure and Delegation*, In: http://www.ietf.org/rfc/rfc1591.txt

[30] Existe uma variedade de possibilidades de designações de topônimos de países, ver o Dicionário de Unidade de Mesuração ou *Dictionary of Units of Measurement*, elaborado pelo Professor Russ Rowlett, diretor do *Center for Mathematics and Science Education* da *University of North Carolina at Chapel Hill* em: http://www.unc.edu/~rowlett/units/codes/country.htm

[31] Conferir a tabela *ISO-3166-1 alpha-2* em: http://www.iso.org/iso/country_codes/iso-3166-1_decoding_table.htm

[32] Conferir os nomes e as siglas em Inglês dos organismos internacionais que participam do fórum global pela governança da Internet:
Association of Southeast Asian Nations – ASEAN; Asia-Pacific Economic Cooperation - APEC; Council of Europe - CoE; International Telecommunication Union – ITU; Office of the United Nations High Commissioner for Human Rights - OHCHR; Organisation for Economic Co-operation and Development - OECD; United Nations Commission on International Trade Law - UNCITRAL; United Nations Office on Drugs and Crime – UN-ODC; UNESCO World Heritage Site; World Intellectual Property Organization – WIPO; World Trade Organization - WTO; etc.

[33] Sobre a nova política do *Network-Centric Warfare*, vale a pena conferir o artigo *Os grupos armamentistas e os mercados financeiros: Rumo a um compromisso 'guerra sem limites*, de Mampaey e Serfati, 2005, p.244.

[34] Proulx e Millette, 2011 pp.181-182.

[35] Ler este documento em:
http://www.cyber.st.dhs.gov/docs/National%20Strategy%20to%20Secure%20Cyberspace%202003.pdf

[36] Conferir este documento em: http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

[37] Ler este documento em:
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[38] Ler este documento em: http://www.defense.gov/news/d20110714cyber.pdf

[39] Uma versão resumida desse documento foi difundida pela Universidade de Harvard em:
http://cyber.law.harvard.edu/cybersecurity/The_National_Strategy_to_Secure_Cyberspace

[40] Conferir a página VIII do documento *The National Strategy to Secure Cyberspace* em:
http://www.cyber.st.dhs.gov/docs/National%20Strategy%20to%20Secure%20Cyberspace%202003.pdf

[41] Conferir a página X desse documento em:
http://www.cyber.st.dhs.gov/docs/National%20Strategy%20to%20Secure%20Cyberspace%202003.pdf

[42] Ler a justificativa na página 30 desse documento:

> *"Attackers can disrupt the DNS by flooding the system with information or requests or by gaining access to the system and corrupting or destroying the information that it contains. The October 21, 2002 attacks on the core DNS root servers revealed a vulnerability of the Internet by degrading or disrupting some of the 13 root servers necessary for the DNS to function. The occurrence of this attack punctuates the urgent need for expeditious action to make such attacks more difficult and less effective".*

[43] Conferir em inglês o documento *National Strategy for Homeland security*, 2007, p.28, em: http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

"Cyber Security: A Special Consideration

Many of the Nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent CI/KR and ultimately to our economy and national security.

A variety of actors threaten the security of our cyber infrastructure. Terrorists increasingly exploit the Internet to communicate, proselytize, recruit, raise funds, and conduct training and operational planning. Hostile foreign governments have the technical and financial resources to support advanced network exploitation and launch attacks on the informational and physical elements of our cyber infrastructure. Criminal hackers threaten our Nation's economy and the personal information of our citizens, and they also could pose a threat if wittingly or unwittingly recruited by foreign intelligence or terrorist groups. Our cyber networks also remain vulnerable to natural disasters.

In order to secure our cyber infrastructure against these man-made and natural threats, our Federal, State, and local governments, along with the private sector, are working together to prevent damage to, and the unauthorized use and exploitation of, our cyber systems. We also are enhancing our ability and procedures to respond in the event of an attack or major cyber incident. The National Strategy to Secure Cyberspace and the NIPP's Cross-Sector Cyber Security plan are guiding our efforts".

[44] Sobre *Cyberwarfare* ver em: http://en.wikipedia.org/wiki/Cyber_arms_control

[45] Ler em Baldi, Gelbstein and Kurbalija, 2003, pp.46-47.

[46] Ler em: http://www.areamilitar.net/noticias/noticias.aspx?NrNot=435

[47] Ler em inglês na página 8 do documento *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*:

"The United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace".

[48] Ler em inglês na página 10 do documento:

"Emerging norms, also essential to this space, include:

- *Global Interoperability: States should act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all.*
- *Network Stability: States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure.*
- *Reliable Access: States should not arbitrarily deprive or disrupt individuals' access to the Internet or other networked technologies.*
- *Multi-stakeholder Governance: Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders.*
- *Cybersecurity Due Diligence: States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse".*

[49] Ler em inglês na página 14 do documento:

"When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible".

[50] Para quem deseja efetuar um estudo introdutório sobre Governança da Internet, ler o livro de Kurbalija & Gelbstein, 2005.

[51] Este assunto também já foi preliminarmente tratado o meu artigo "Governança Global da Internet: A representação de topônimos de países no ciberespaço", publicado em 2008.
[52] *European Open Root Server Network*, In: http://european.ch.orsn.net/about.php - (Sítio-web retirado de services em 2008)
[53] Sobre o shutdown da ORSN, é importante conferir:
   a. A carta de Paul Vixie *"[dns-operations] Open Root Server Network project shutdown by 31.12.2008 00:00 UTC*". Em: https://lists.dns-oarc.net/pipermail/dns-operations/2008-October/003339.html
   b. A Wikipédia: http://en.wikipedia.org/wiki/Open_Root_Server_Network
[54] Mais sobre o assunto conferir em: http://en.wikipedia.org/wiki/Alternative_DNS_root
[55] Conferir o artigo de Jack Linchuan QIU *Chinese Hackerism in Retrospect: The Legend of a New Revolutionary Army*, In: http://ncsi-net.ncsi.iisc.ernet.in/cyberspace/societal-issues/Qiu1.pdf
[56] Ver o artigo de Siobhan Gorman *Hathaway to Head Cybersecurity Post*, In: http://online.wsj.com/article/SB123412824916961127.html
[57] Silva Jr, 2008.
[58] Pires, 2011.
[59] Deibert, 2008, p.327.
[60] Conferir o artigo de Germana Barata "*Governos e mercado impulsionam censura na Internet*", In: http://comciencia.br/comciencia/?section=8&edicao=20&id=220
[61] Conferir o artigo *Draconian cyber security bill could lead to internet surveillance and censorship,* in: http://en.rsf.org/etats-unis-draconian-cyber-security-bill-06-04-2012,42283.html

Bibliografia

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. Davos, Suiça. 1996. <https://projects.eff.org/~barlow/Declaration-Final.html>

BALDI, Stefano; GELBSTEIN, Eduardo and KURBALIJA, Jovan. Hacktivism, Cyber-terrorism and Cyberwar: The activities of the uncivil society in cyberspace. Malta: DiploFoundation. 2003, pp.46-47.

BLUESTONE, Barry and HARRISON, Bennett. The Deindustrialization of America. New York, Basic Books, 1st edition, 1984.

DEIBERT, Ronald J. The geopolitics of Internet control Censorship, sovereignty, and cyberspace. In Andrew Chadwick and Philip N. Howard, (eds.). *Routledge Handbook of Internet Politics*, New York: Routledge, 2008. <http://www.handbook-of-internet-politics.com/pdfs/chapter_23.pdf>

FIDLER, David. Introduction: The Internet and the Sovereign State: The Role and Impact of Cyberspace on National and Global Governance Symposium, *Indiana Journal of Global Legal Studies*: Vol. 5: Iss. 2, Article 3, 1998, pp. 415-420. <http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1127&context=ijgls>

GOLDSMITH, Jack. Unilateral Regulation of the Internet: A Modest Defence. *The European Journal of International Law - EJIL*, Vol. 11, Nº 1, pp.135-148, 2000. <http://ejil.oxfordjournals.org/content/11/1/135.full.pdf

KURBALIJA, Jovan & GELBSTEIN, Eduardo. Governança *da Internet: Questões, atores e cisões*. DiploFoundation, 2005. <http://archive1.diplomacy.edu/poolbin.asp?IDPool=590>

RYAN, Johnny. *A history of the Internet and the digital future*. London: Reaktion Books, 2010.

MAMPAEY, Luc e SERFATI, Claude. Os grupos armamentistas e os mercados financeiros: Rumo a um compromisso 'guerra sem limites. In: Chesnais, François (org.) *A finança mundializada*. São Paulo: Boitempo, 2005.

MARKUSEN, Ann; HALL, Peter; CAMPBELL, Scott and DEITRICK, Sabina. *The Rise of the Gunbelt: The Military Remapping of Industrial America. New York,* Oxford Press, 1991.

PERRITT, Henry H. Jr. The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance, *Indiana Journal of Global Legal Studies*; Vol. 5: Iss. 2, Article 4, 1998, pp.423-442. <http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1128&context=ijgls>

PIRES, Hindenburgo Francisco. A produção morfológica do ciberespaço e a apropriação dos fluxos informacionais no Brasil. *Scripta Nova. Revista Electrónica de Geografía y Ciencias Sociales.* [En línea]. Barcelona: Universidad de Barcelona, 1 de agosto de 2005, vol. IX, núm. 194 (19). <http://www.ub.es/geocrit/sn/sn-194-19.htm> .

PIRES, Hindenburgo Francisco. Governança Global da Internet: A representação de topônimos de países no ciberespaço. *Scripta Nova. Revista Electrónica de Geografía y Ciencias Sociales*. [En línea]. Barcelona: Universidad de Barcelona, 1 de agosto de 2008. <http://www.ub.es/geocrit/-xcol/415.htm>.

PIRES, Hindenburgo Francisco. WikiLeaks e Redes Sociais: A publicização de conteúdos da SIPRnet. Ar@cne. Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales. [En línea. Acceso libre]. Barcelona: Universidad de Barcelona, nº 143, 15 de enero de 2011. <http://www.ub.es/geocrit/aracne/aracne-143.htm>

POST, David G. The Cyberspace Revolution. Keynote Address, Computer Policy & Law Conference Cornell University, July 9, 1997. Available at: <http://www.temple.edu/lawschool/dpost/Cornell.html>

PROULX, Serge e MILLETTE, Mélaine. El imperialismo digital estadounidense. *El Estado do mundo: Anuario económico geopolítico mundial*, Madrid: Ediciones Akal S.A, 2011, pp. 179-182.

SANTOS, Milton. A Natureza do Espaço. São Paulo: Hucitec, 1996.

SASSEN, Saskia. On the Internet and Sovereignty, *Indiana Journal of Global Legal Studies*: Vol. 5: Iss. 2, Article 9, 1998, pp. 545-559. <http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1133&context=ijgls>

SASSEN, Saskia. The Impact of the Internet on Sovereignty: Unfounded and Real Worries. In: Engel, Christoph and Heller, Kenneth H. (eds). *Understanding the Impact of Global Networks in Local Social, Political and Cultural Values*. Baden-Baden: Nomos

Verlagsgesellschaft, 2000, pp.195-209. <http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/sassen.pdf>

SILVA Jr., Kenneth J. Root Zone Signing Proposal, *ICANN/VeriSign*, 2008. <http://www.ntia.doc.gov/DNS/VeriSignDNSSECProposal.pdf>

TANCMAN, Michele. *Geopolítica da Governança Global de Internet*. São Paulo: USP, Tese de Doutorado, 2008, pp. 253.

THE DEPARTMENT OF HOMELAND SECURITY. *National Strategy to Secure Cyberspace*, February 2003. <http://www.cyber.st.dhs.gov/docs/National%20Strategy%20to%20Secure%20Cyberspace%202003.pdf>

THE DEPARTMENT OF HOMELAND SECURITY. *The National Strategy for Homeland Security*, 2007. <http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf>

U.S. WHITE HOUSE, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

U.S. DEPARTMENT OF DEFENSE, *Strategy for Operating in Cyberspace*, July 2011. <http://www.defense.gov/news/d20110714cyber.pdf>