Gestão dos Sistemas de Zona Raiz e de DNS no Ciberespaço: impasses e controvérsias.

4-Avances en el uso de las tecnologías de información geográfica
Pires, Hindenburgo Francisco
1 - Universidade do Estado do Rio de Janeiro | Brazil

Resumo

Com a globalização e o crescimento da Internet, o atual modelo unilateral de Governança da Internet (GI), constituído e mantido, desde 1998, pelo Departamento de Comércio do Estados Unidos (DoC), pela *Internet Corporation for Assigned Names and Numbers* (ICANN) e pela VeriSign, passou a ser questionado a partir de 2002.

Os alvos centrais destes questionamentos foram: a) o controle excessivo dos 13 servidores da zona raiz efetuado pelos Estados Unidos; b) a localização geográfica da grande maioria desses servidores no território dos Estados Unidos; c) a política de concessão de *Domain Name Server* (DNS) efetuada somente pela ICANN e pela VeriSign, principalmente em relação à atribuição do código de domínio de alto nível dos países (*country code top-level domain* - ccTLD), identificados por um conjunto de normas geográficas (ISO 3166-1), criadas em 1974, representado por duas letras (br. es, ar, ch, de, etc.); d) a política de cibersegurança empreendida desde 2007 pelas autoridades estadunidenses através do Plano "*The National Strategy For Homeland Security*" do *Department of Homeland Security*, dirigido à proteção da infra-estrutura crítica do território dos EUA, vinculada à Internet.

Os questionamentos geraram vários impasses e controvérsias que abrangem uma gama variada de temas não apenas vinculados à questão do desenvolvimento tecnológico, mas também às questões políticas, geografias, economias, que dizem respeito à soberania, segurança, cidadania e a liberdade de expressão. Nesse sentido, críticas e movimentos de emancipação emergiram, obrigando a Assembléia Geral das Nações Unidas – ONU a organizar algumas Cúpulas, Conferências e Fóruns Mundiais. Estes fóruns coletivos discutiram propostas e reformas ao modelo vigente de GI, tendo ocorrido em: Genebra, 2003; Tunes, 2005; Rio de Janeiro, 2007 e em Hyderabad/Índia, 2008.

A autoridade historicamente constituída pelos EUA na GI encontra-se desgastada porque a Internet não pode continuar sendo vista como o espaço do estado de guerra. Os países não desejam serem controlados por empresas estrangeiras que se instalam fora do domínio de seus espaços políticos. Não há mais como continuar impedindo a participação dos países nos fóruns de decisão da GI, é preciso criar meios e canais para garantir a autonomia dos países na elaboração de políticas públicas para o desenvolvimento da Internet.

Atualmente existe uma grande mobilização dos atores políticos - governos, setores públicos, setores privados e organizações da sociedade civil, para o estabelecimento de uma nova estrutura de regulação global baseada em um sistema de GI multilateral.

Mesmo assim, com todos esses impasses, a ICANN e a VeriSign pretendem dar continuidade ao modelo de GI, conforme anunciaram recentemente através do Documento "*Root Zone Signing Proposal*", publicado pela VeriSign em 22 de Setembro de 2008.

Sendo assim, este trabalho é uma continuidade da pesquisa que venho desenvolvendo "Governança Global da Internet: a representação de topônimos de países no ciberespaço", financiada pela FAPERJ através do Programa de Pró-ciência, e que tem como objetivo contribuir para ampliar os horizontes teóricos da Geografia, no âmbito das ciências humanas que se dedicam a investigar a GI.

Esta pesquisa tem como objetivo debater e analisar o atual cenário político de representação dos países, promovido pela tríade DoC, ICANN e VeriSign, e evidenciar os instrumentos reais de participação e decisão dos países soberanos na gestão dos sistemas de zona raiz e de concessão de DNS no ciberespaço.

Palavras Chave: Ciberespaço, Governança da Internet, Sistema de Zona Raiz da Internet, Geopolítica, Geografia das Redes.

1. Geopolítica versus Governança: A localização geográfica dos servidores da zona raiz da Internet:

A globalização recente da Internet está pondo em cheque a arquitetura de localização e concentração geográfica dos servidores da zona raiz da Internet (Cf. Figura 1, In: www.root-servers.org), evidenciando questões geopolíticas engendradas pelo sistema hierarquizado de parâmetros de concessão de nomes de domínios (DNS) e a política de concessão Regional de Registros da Internet - RIR, ambos concebidos em março de 1994 por Jon Postel, quando ele ainda estava na direção da IANA - *The Internet Assigned Numbers Authority*[1].

Figura 1 - Localização Geográfica Global dos Servidores da Zona Raiz da Internet e seus 73 replicadores anycast regionais

Fonte: http://www.root-servers.org/ (2009)

A localização e a concentração geográfica dos servidores da zona raiz nos EUA (Cf. Tabela 1) é um fenômeno historicamente estabelecido desde a constituição da Internet como uma rede militar, que posteriormente se tornou uma rede acadêmica e comercial (PIRES, 2008)[2]. O controle dos servidores da zona raiz da Internet é mantido pela tríade: DoC, ICANN e VeriSign, conforme iremos destacar mais a frente.

Como se pode observar na Figura 2 abaixo, os 13 servidores da zona raiz são identificados pelas letras do alfabeto de A a M. Dos 13 servidores da zona raiz 10, 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 4 outros são servidores anfitriões (C, F, J, L) que operam com sistema de endereçamento descentralizado Anycast[3], viabilizando o acesso a um aglomerado de servidores secundários replicantes distribuídos por vários países, fisicamente instalados fora da região de influência dos servidores da zona raiz da Internet nos EUA.

Figura 2 - Localização Geográfica dos 13 principais Servidores da Zona Raiz da Internet

Fonte: MONIKA, Ermert. Ein Königreich für einen (Internet-)Namen, 2007, In: http://www.heise.de/ct/00/25/066/

Os 3 servidores restantes da zona raiz que operam fora do território dos EUA (I, K, M), localizados respectivamente na Inglaterra, 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 Tabela 1 abaixo.

Tabela 1 – Principais Operadores dos Servidores da Zona Raiz, Localização e Atividades

Servidor, Operador, Domínio e Endereço de IP	**Localização e Atividades**
Servidor **A** VeriSign, Inc.: www.verisign.com/ IPv4:198.41.0.4. Operador voltado à regulação de registros comerciais.	Situado no estado da Virginia, este servidor é controlado pela VeriSign, empresa fundada em 1995[4], responsável pela identificação, certificação de segurança e concessão de quase todos registros comerciais, para os serviços de telecomunicações e para as empresas de e-commerce da Internet.
Servidor **B** Information Sciences Institute – USC-ISI: http://www3.isi.edu/home/ IPv4:92.228.79.201 IPv6:001:478:65::53. Operador voltado para gestão do sistema de cibersegurança dos EUA.	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 20 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.[5]
Servidor **C** Cogent Communications: www.cogentco.com/htdocs/index.php/ IPv4:192.33.4.12. Operador voltado à regulação de registros comerciais.	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 10Gbs). [6]
Servidor **D** University of Maryland: http://www.umd.edu IPv4:128.8.10.90	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.[7]
Servidor **E** NASA Ames Research Center: http://www.nasa.gov/home/index.html IPv4:192.203.230.10. Operador voltado para gestão do sistema de cibersegurança dos EUA.	Localizado em Edwards no estado da Califórnia, este servidor é utilizado pela NASA - National Aeronautics and Space Administration, agência criada em 1958, patrocina pesquisas e o desenvolvimento de tecnologias direcionadas para o fortalecimento do programa espacial estadunidense.
Servidor **F** Internet Systems Consortium, Inc: http://www.isc.org/ IPv4:192.5.5.241 IPv6:2001:500::1035	Localizado em San Jose, 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 ISC fornece o acesso a 46 sítios da Internet localizados em**:** Otawa, Canadá ; Palo Alto, CA, E.U. ; San Jose, CA, E.U.; New York, NY, E.U. ; San Francisco, CA, E.U. ; Madrid, ES; Hong Kong, Hong Kong, Los Angeles, CA, E.U. ; Roma, Itália; Auckland, Nova Zelândia , São Paulo, BR; Pequim, NC; Seul, KR ; Moscou, Rússia, Taipei, TW; Dubai, AE; Paris, FR ; Singapura, SG; Brisbane, AU , Toronto, CA ; Monterrey, MX; Lisboa, PT ; Joanesburgo, ZA; Tel Aviv, IL; Jacarta, ID; Munique, DE ; Osaka, JP ; Praga, República Checa , Amesterdão, NL ; Barcelona, ES ; Nairobi, KE; Chennai, EM; Londres, Reino Unido ; Santiago do Chile, CL; Dhaka, BD; Karachi, PK; Torino, IT, Chicago, IL, E.U. ; Buenos Aires, AR; Caracas, VE; Oslo, NO; Panamá, PA; Quito, CE; Kuala Lumpur, Malásia ; Suva, Fiji, no Cairo, Egipto.
Servidor **G** U.S. DOD Network: http://www.nic.mil IPv4:192.112.36.4 Operador voltado para gestão do sistema de cibersegurança dos EUA.	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).
Servidor **H** U.S. Army Research Lab: http://www.arl.army.mil/main/Main/default.htm IPv4:128.63.2.53 IPv6: 2001:500:1::803f::235	Este servidor, situado em Aberdeen no estado de Mariland, é controlado pelo Laboratório de Pesquisas do Exército dos Estados Unidos (ARL). 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 de 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 (2008, p.81): *"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".* [8]
Servidor **I** Autonomica: http://www.netnod.se/dns_root_nameserver.shtml IPv4:192.36.148.17	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. Este provedor opera na concessão de DNS a vários servidores secundários fora da zona raiz dos EUA, fornecendo o acesso a 31 sítios da Internet localizados em**:** Estocolmo, Suécia, Helsinki, FI; Milão, Itália, Londres, Reino Unido; Genebra, CH; Amsterdam, NL; Oslo, NO; Bangkok, TH; Hong Kong, HK; Bruxelas, BE; Frankfurt, Alemanha; Ankara, TR; Bucareste , RO; Chicago, IL, E.U.; Washington, DC, E.U.; Tokyo, JP; Kuala Lumpur, MY; Palo Alto, CA, E.U.;

	Jacarta, ID; Wellington, Nova Zelândia; Joanesburgo, ZA; Perth, AU, San Francisco, CA, E.U.; Singapura, SG; Miami, FL, E.U.; Ashburn, VA, E.U.; Mumbai, EM; Pequim, NC; Manila, PH; Doha, GQ; Colombo, LK.
Servidor **J** VeriSign, Inc.: http://www.verisign.com/ IPv4:192.58.128.30	Situado no estado da Virginia, este servidor opera através do sistema de endereçamento descentralizado Anycast. Administrado pela VeriSign este servidor fornece acesso a 52 sítios da Internet localizados em**:** Dulles, VA, E.U. (3 sites); Ashburn, VA, E.U. ; Vienna, VA, E.U.; Miami, FL, E.U.; Atlanta, GA, E.U.; Seattle, WA, E.U.; Chicago, IL, E.U.; Nova Iorque, NY, E.U.; Los Angeles, CA, E.U.; Honolulu, HI, E.U.; Mountain View, CA, E.U. (2 sites), San Francisco, CA, E.U. (2 sites) ; Dallas, TX, E.U.; Amsterdam, NL; Londres, Reino Unido; Estocolmo, Suécia (2 sites); Tokyo, JP; Seul, KR; Pequim, NC; Singapura, SG; Dublin, IE; Kaunas, LT; Nairobi, KE; Montreal, CA; Quebec, CA; Sydney, AU; Cairo, EG; Varsóvia, PL; Brasília, BR; São Paulo, BR; Sofia, BG; Praga, CZ; Joanesburgo, ZA; Toronto, CA; Buenos Aires, AR; Madrid, ES; Viena, AT; Friburgo, CH; Hong Kong, HK; Turim, IT; Mumbai, EM; Oslo, NO; Bruxelas, BE; Paris, FR; Helsinki, FI; Frankfurt, Alemanha; Riga, LV.
Servidor **K** http://www.ripe.net/ Reseaux IP Europeens - Network Coordination Centre: www.ripe.net/info/ncc/index.html IPv4: 193.0.14.129 IPv6: 2001:7fd::1	Situado em Londres, na Inglaterra, este servidor opera através do sistema de endereçamento descentralizado Anycast. Administrado pela RIPE NCC, instituição independente, sem fins lucrativos, este servidor opera oferecendo, 17 sítios de organizações de telecomunicações e grandes empresas localizadas na Europa, Oriente Médio e em partes da Ásia Central, a concessão pública de Registro Regional para Internet (RIR) e Protocolos de acesso a Internet (IPv4, IPv6), para os membros conveniados: Londres, Reino Unido , Amesterdam, NL ; Frankfurt, Alemanha; Atenas, GR; Doha, GQ, Milão, IT ; Reykjavik, IS; Helsinki, FI ; Genebra, CH ; Poznan, PL; Budapest, HU ; Abu Dhabi, AE; Tokyo, JP; Brisbane, AU ; Miami, FL, E.U. ; Delhi, IN; Novosibirsk, EF.
Servidor **L** Internet Corporation for Assigned Names and Numbers - ICANN: http://www.icann.org IPv4:198.32.64.12	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 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 ajudam os computadores a se comunicarem pela Internet.
Servidor **M** WIDE Project: http://www.wide.ad.jp/ IPv4:202.12.27.33 IPv6:2001:dc3:35	Localizado em Tokyo, no Japão, este servidor opera através do sistema de endereçamento descentralizado Anycast. Administrado pela WIDE Project, este servidor entrou em operação, em agosto de 1997, para prover e conceder registros a inúmeros servidores secundários na região do oeste do pacífico. Desde 2002, fornece acesso a 6 grandes sítios da Internet localizados em**:** Tóquio, Japão (3 sites); Seul, KR; Paris, FR; San Francisco, CA, E.U.

Baseado em: http://www.root-servers.org/(2009)

Conforme já evidenciado anteriormente, de acordo com o memorando RFC 1591, coube também a IANA, 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.), eram os identificadores oficiais dos topônimos de países. A escolha dessa metodologia de designação dos topônimos de países segue um conjunto de normas geográficas, criadas em 1974, que valida os códigos para os nomes de países e dependências, o ISO 3166-1 (PIRES, 2008).

Os parâmetros do sistema hierarquizado de concessão de nomes de domínios, concebidos 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.

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 (IGF - *Internet Governance Foruns*) ou as já consolidadas como *Open Root Server Network* (ORSN), estão sendo rotuladas de promoverem a fragmentação da Internet.

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:
a) jurisprudência no ciberespaço: pode-se afirmar que falta uma declaração internacional dos direitos sociais e comerciais dos países no ciberespaço;
b) liberdade de expressão: segundo o sítio dos Repórteres Sem Fronteiras, pelo menos 15 países censuram ou praticam a censura parcial ou completa de conteúdos da Internet no seu território (cyber-censorship)[9];
c) cibersegurança: as autoridades públicas internacionais estão mobilizadas no combate a pedofilia, os cibercrimes e proteção de recursos críticos contra ataques provenientes de potenciais inimigos externos (hackerismos[10], atentados e ciberterrorismos). Nos EUA, desde os anos 90 a força aérea havia criado um cibercomando (*Air Force Cyber Command*)[11] localizado na base da Força Aérea de Barksdale, na Louisiana, onde são treinados ciberguerreiros (*Cyber Warriors*) voltados para proteger o território estadunidense contra um eventual ataque ou uma guerra centrada nas redes. Neste item, o governo do presidente George W. Bush gastou o equivalente a seis (6) bilhões de dólares em investimentos militares. Já o atual Presidente dos EUA, Barack Obama, declarou recentemente que pretende criar um conselho nacional para atuar também na área de cibersegurança[12];
d) concessão de nomes de domínios fora do domínio da zona raiz: a soberania territorial na gestão de servidores raízes e o estabelecimento do sistema de concessão de nomes de domínios;
e) soberania na gestão do sistema de concessão de nomes de domínios e países (DNS e ccTLDs): alguns atores políticos - governos, setores públicos, setores privados e organizações da sociedade civil, desejam descentralizar e reformar o modelo de concessão de DNS, através da implantação do sistema mais seguro de resolução de nomes, o *Domain Name System Security Extensions* – DNSSEC, que permite a criptografia das assinaturas, a redução dos riscos de manipulação de dados e a falsificação de domínios; desejam também debater o aperfeiçoamento e a substituição do protocolo IPv4, que suporta aproximadamente 4 x 109 de endereços, pelo protocolo de registro IPv6, que suportará algo em torno de 3.4 x 1038 endereços. Em resposta ao crescimento do uso de DNSSEC pelos países, a VeriSign e a ICANN lançaram em setembro de 2008 - antes do IGF de Hyderabad, a proposta "*Root Zone Signing Proposal*", cujo objetivo era permanecer controlando e regulando o processo de registros e de concessão de DNS de servidores e provedores na zona raiz da Internet.
f) políticas de desenvolvimento do trafego local da Internet e da arquitetura da rede no território: O crescimento e a globalização da Internet propiciaram a formação de estruturas virtuais de acumulação (EVAs) nas diferentes economias-mundo. Estas EVAs passaram a requerer instrumentos territorializados de regulação e gestão do ciberespaço (PIRES, 2006).

2. O Controle dos Servidores da Zona Raiz pelos EUA: O Ciberespaço como campo estratégico e militar da guerra sem fim dos EUA

Para se compreender essas questões geopolíticas da GI é preciso fazer-se uma pequena retrospectiva.

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.

A 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 general 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*[13] (MARKUSEN et al,1991). 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 locais formado por várias firmas, cuja preocupação central, desde o período a 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*" (Harrison & Bluestone, 1984), que explica a expansão industrial regional do *Sunbelt* e sua relação com os investimentos militares do Pentágono.

Muitos estudiosos na 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 13% do PIB para investimentos militares nos EUA (MARKUSEN et al, 1991, p.10).

A formação do ciberespaço, desde o período da Guerra Fria (1958 a 1983), sempre esteve atrelada a demandas de cunho militar.

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.

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

Em 1957, a URSS efetuaram o lançamento do satélite militar "Sputinik". Procurando fazer frente a esta iniciativa, o presidente Eisenhower resolveu criar, em 1958, a *Advanced Research Projects Agency Avançada* – ARPA (Agência de Projetos de Pesquisa). Nos anos 60, esta preocupação com a questão da segurança territorial dos EUA foi mantida e aperfeiçoada pela Administração Kennedy.

De 1958 a 1965, a ARPA atuou centrada em grandes questões de defesa nacional, como a proteção do espaço aéreo dos EUA, míssil balístico de defesa, e experimentos nucleares. Em 1960, todos os seus programas espaciais civis e os programas espaciais militares foram transferidos para a Administração Nacional Aeronáutica e Espaço (NASA), criada também em 1958.

Durante a Guerra Fria, o objetivo da ARPA era atuar com o apoio das Universidades, através do desenvolvimento de pesquisas, na promoção de tecnologias que detivesse o avanço soviético no campo da corrida espacial.

No final dos anos 60, a ARPA se tornou a mais importante empresa da história da computação nos Estados Unidos. Vários fatores promoveram esse crescimento, mas o fator mais importante foi a criação de uma rede militar de computadores, chamada de ARPANET. Essa rede foi aperfeiçoada com a utilização do programa de comutação de computadores chamado de "*Information Processing Techniques Office*" IPTO, que permitiu o surgimento de uma rede de computadores integrada no território em tempo real.

Em 1972, a ARPA foi renomeada e se transformou na Defense *Advanced Research Projects Agency* - DARPA (Agência de Projetos de Pesquisa Avançada de Defesa), e continuou sendo regulada pelo Departamento de Defesa dos EUA (DoD), com um orçamento anual de US$ 238 milhões de dólares. Neste período, os investimentos da DARPA foram orientados para programas de tratamento da informação e para o desenvolvimento de um sistema de Controle e Comando de Comunicações.

Assim, em cooperação com o Laboratório Bell, com a General Electric e com o Massachusetts Institute of Technology - MIT, na área do processamento da informação, a DARPA fez grandes progressos em suas pesquisas para aperfeiçoar o sistema de defesa dos EUA.

Nesta mesma época, o exército dos EUA também já havia desenvolvido, com o apoio da IBM e do laboratório Lincoln do MIT, um projeto ambicioso de proteção continental do espaço aéreo estadunidense, chamado de SAGE (*Semi-Automatic Ground Environment*). O sistema SAGE foi concebido para coordenar estações de radares voltadas para interceptar aviões que pretendessem efetuar um possível ataque aéreo. Foram implantados, no território, 23 centros de controle equipados com o sistema SAGE, que poderiam monitorar até 400 aviões cada.

No início dos anos 70, a ARPANET desenvolveu, conjuntamente com a IBM, o "*NCP-Network Control Program*". O NCP foi o primeiro programa com um protocolo padrão de rede que executava as funções de e-mail, telnet e de protocolos transferências de arquivos – FTP, entre servidores. Este programa ajudou a integrar, em rede, quinze importantes instituições acadêmicas, militares e de pesquisas: 1. Bolt Baranek and Newman; 2. Carnegie Mellon University; 3. Case Western Reserve University; 4. Harvard University; 5. Lincoln Laboratories; 6. Massachusetts Institute of Technology; 7. NASA e AMES; 8. RAND Corporation; 9. Stanford Research Institute; 10. Stanford University; 11. System Development Corporation; 12. University of California at Los Angeles; 13. University of California of Santa Barbara; 14. University of Illinois at Urbana; 15. University of UTAH. Estas instituições formaram o embrião do que hoje conhecemos como Internet ou Inter-Networking.

Esta rede da ARPANET, constituída via NCP, tinha por objetivo propiciar a conexão de bases militares com os departamentos de pesquisa do governo americano, agregando mais de 100 sítios.

Em 1983, o NCP deixou de ser utilizado pela ARPANET que, em seu lugar, resolveu instalar definitivamente um protocolo de rede mais poderoso, eficiente e flexível, chamado TCP/IP. Concebido em 1974, este protocolo foi desenvolvido pelos cientistas da ARPANET: Vinton Cerf, Yogen Dalal e Carl Sunshine, em estreita colaboração com especialistas da Universidade de

Stanford. O TCP/IP, como um conjunto de protocolos de controle e transmissão entre protocolos da Internet, permitia que diferentes redes se comunicassem umas com as outras. Esta linguagem inaugurou uma revolução na era da comunicação em rede e tornou-se o protocolo de rede mais utilizado no mundo.

O crescimento espontâneo do número de instituições universitárias e civis nesta rede forçou o departamento de Defesa a criar, em 1983, uma rede eminentemente militar chamada de MILNET, que congregava apenas instituições do complexo industrial militar dos EUA e sítios militares em sua rede.

Durante os anos 80, a MILNET expandiu-se e formou a Defense Data Network – DDN, que foi utilizada pelo DoD de 1983 a 1995. A DDN oferecia um protocolo de rede que interligava as bases militares dos EUA no exterior.

No final dos anos 80, a rede MILNET subdividiu-se em um conjunto de quatro grandes redes militares: NIPRNET - Non-Classified Internet Protocol Router Network, SIPRNET - Secret Internet Protocol Router Network, JWICS - Joint Worldwide Intelligence Communications System e, mais recentemente, em 2007, a RIPRNET- Radio over Internet Protocol Routed Network, que operam cada uma com níveis diferenciados de segurança e, âmbito mundial.

De 1984 a 1991, a Internet adquiriu um caráter científico-militar e manteve-se regulada por instituições acadêmicas e civis vinculadas a National Science Foundation (NSFNET).

Por razão de segurança, desde os anos 90, a rede MILNET restringiu o uso de inúmeras aplicações de comunicações, comuns às redes comerciais convencionais, passando a ter um funcionamento diferente das redes acadêmicas e corporativas.

Mesmo aparentemente saindo de cena da Internet comercial, que é um campo estratégico e de interesse econômico dos EUA, e por considerar o ciberespaço também como um campo virtual de guerra sobre o qual deve manter um sistema militar permanente de segurança, vigilância e de proteção das redes, o DoD criou uma dominância informacional, articulada através do princípio da "*Network-Centric Warfare*" (Guerra Baseada em Redes), criado pelo Command and Control Research Program – CCRP (Programa de Pesquisa de Comando e Controle do DoD).

Segundo Luc Mampaey e Claude Serfati, no artigo: "Os grupos armamentistas e os mercados financeiros: Rumo a um compromisso 'guerra sem limites'". *A finança mundializada* In: CHESNAIS, François (org.) São Paulo: Boitempo, 2005:

> *"Junto com as modificações das ligações da finança e da política com o armamento, o terceiro fator que favorece a emergência de um sistema militar e de segurança está relacionado ao papel que a segurança tem no domínio das tecnologias de informações e da comunicação (TIC). Assumindo legalmente as potencialidades dessas tecnologias, os militares americanos desenvolveram, a partir do fim dos anos 80, a noção de dominância informacional. Importantes programas de P&D consagrados aos TIC e ao espaço foram lançados pelo DoD; eles foram menos afetados pelas reduções no orçamento militar (1986-1998) do que os destinados à produção de armas. As barreiras à entrada que protegem os grandes grupos (ver a primeira parte) são reforçadas pelo tipo de competências necessárias para pôr em prática novas doutrinas experimentadas na Sérvia, no Afeganistão e no Iraque. A 'guerra baseada nas redes' (NCW, Network Centric Warfare), que sustenta as novas doutrinas militares dos Estados Unidos, auxilia os principais grupos, cuja 'vantagem comparativa' se sustenta geralmente em sua competência nos domínios de sistemas integrados. A aplicação da NCW exige, com efeito, mais estrutura organizacional, mais integração de 'sistemas de sistemas' e uma proteção e uma segurança muito acentuada das*

redes, e, por conseqüência, da produção de programas para computadores e de materiais altamente seguros." (2005, p.244).

Assim, desde Eisenhower e durante a era Bush, o ciberespaço se transformou no espaço do Estado da guerra sem fim, *"the cyberwar"*. Em 2007, ainda sob administração Bush, o Department of Homeland Security lançou a política nacional de cibersegurança através do Plano "*The National Strategy For Homeland Security*" do *Department of Homeland Security*, dirigido à proteção da infra-estrutura crítica do território dos EUA, vinculada à Internet, "A Estratégia Nacional para Segurança Doméstica" orienta, organiza e unifica os esforços para segurança doméstica nacional".

Este plano, em relação aos outros planos estratégicos dos EUA, tem um componente extremamente importante, diferente e atualizado em relação ao ciberespaço dos EUA, na parte referente à *"Cibersegurança: Uma consideração especial/Cyber Security: A Special Consideration",* (2007, p.36). O plano revela uma 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 ciberredes 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."*

Pelo exposto acima pode-se compreender que esta tem sido a ideologia que vem norteando a política de Governança da Internet nos EUA, efetuada pelo Department of Homeland Security, vinculado ao DoD. Daí essas mesmas estratégias de segurança se refletem no controle dos servidores da zona raiz, mantidas pela ICANN, VeriSign e pelo DoC na concessão de DNS e nos registros de códigos de países - ccTLDs, que vêm dificultando a implantação de uma governança multilateral da Internet, como reivindicam todos os países.

3. Uma rápida análise comparativa dos IGFs do Rio de Janeiro (2007) e de Hyderabad (2008)

Efetuando uma rápida análise do programa do IGF (*Internet Governance Forum*) de Hyderabad e comparando-o com os anteriores IGFs, constatou-se que a programação do IGF de Hyderabad deslocou os temas Acesso (*Acess*) e Abertura (*Openness*) para o interior dos Painéis de Discussão: Alcançando o Próximo Bilhão (*Reaching the Next Billion*) e Promover a Ciber-Segurança e

Confiança (*Promoting Cyber-Security and Trust*), no subitem: Promover a segurança, a privacidade e abertura (*Fostering security, privacy and openness*).

Em 2007, o IGF, que se realizou no Rio de Janeiro, os principais temas foram (Cf. Tabela 2, abaixo):

Tabela 2 – Principais Temas do IGF do Rio de Janeiro (2007)

Temas
1. Recursos Críticos da Internet /*Critical Internet Resources*
2. Acesso /*Access*
3. Diversidade / *Diversity*
4. Abertura / *Openness*
5. Segurança / *Security*
6. Balanço e caminho a seguir / *Taking Stock and the way forward*
7. Questões emergentes / *Emerging Issues*

Fonte: http://www.intgovforum.org/Rio_Schedule_final.html (2007)

No IGF 2008, realizado em Hyderabad, os temas escolhidos foram divididos nos seguintes Painéis de Discussão:

Tabela 3 – Temas do IGF de Hyderabad (2008)

Temas
1. Alcançando o Próximo Bilhão / *Reaching the Next Billion*
2. Promover a Ciber-Segurança e Confiança / *Promoting Cyber-Security and Trust*
3. Gerenciamento de Recursos Críticos da Internet / *Managing Critical Internet Resources*
4. Questões emergentes - a Internet do Futuro / *Emerging Issues - the Internet of Tomorrow*
5. Balanço e caminho a seguir / *Taking Stock and the Way Forward*

Fonte: http://www.intgovforum.org/cms/hyderabad_prog/Workshop_Schedule.htm (2008)

Portanto o IGF, no Rio, contemplou mais intensamente o tema Abertura. Foram 19 horas de debate, desenvolvidos entre 18 Grupos de trabalho. Os temas debatidos eram profundamente polêmicos, tais como: Respostas Jurídicas as Ciber-ameaças, Cibersegurança e Privacidade; Privacidade na Internet e Gestão da Identidade; TIC e os desafios da Cibersegurança; DNSSEC; Política de Desenvolvimento *Multi-stakeholder*; O papel das Instituições multilaterais: UNESCO, OCDE, Nações Unidas; *Child Online Protection*; A internacionalização dos Registros dos Nomes de Domínio dos Países - ccTLD, etc. Como o IGF no Rio não conseguiu concluí-los, foi proposto a continuidade do debate para 2008, no entanto os fóruns para organização do IGF de 2008 modificaram os temas.

Anteriormente, a escolha desses temas pela ONU era no sentido de permitir o debate democrático de questões importantes, que afetavam diretamente as nações e toda a sociedade humana.
O tema Abertura gerou discussões interessantes no IGF da Grécia e não deixou de ser incluído na

agenda do IGF do Brasil.

A impressão que fica quando analisa-se o programa do IGF de Hyderabad é que este polêmico tema foi relegado intencionalmente e considerado um subtema do tema: Promover a Ciber-Segurança e Confiança: Promover a segurança, a privacidade e a abertura (*Promoting Cyber-Security and Trust no Panel Discussion: Fostering security, privacy and openness*).

O tema abertura gerou uma gama variada de debates no IGF no Rio, alguns representantes de países desejavam que fossem discutidom formas e meios de preservar a identidade do usuário na rede enquanto outros não demonstraram qualquer interesse em desenvolver estes mecanismos de proteção da privacidade do usuário.

Outro conteúdo que virou objeto de discussão foi a questão da Internacionalização dos Registros dos Nomes de Domínio dos Países - ccTLDs e o papel das Instituições: UNESCO, OECD, Nações Unidas.

A questão da internacionalização dos ccTLDs deveria retornar à mesa de discussão, porque, segundo Pires (2008), alguns países não aceitam serem vistos apenas como topônimos na Internet. O controle e a extrema centralização da Governança da Internet por um só país colocam em risco a soberania das nações, abrem margem para que se continue a por em dúvida a capacidade dos países de se fazerem representar politicamente na era da sociedade do conhecimento colaborativo.

É importante retomar o debate sobre a Política de Desenvolvimento Multilateral – "*Multi-stakeholder Policy Development"*, esta discussão poderá permitir a democratização da governança entre as nações.

A idéia do tema abertura era buscar soluções e elementos de mediação para a proteção do direito da liberdade de expressão e respeito aos direitos humanos, através da Internet.

A ênfase temática dada pelo programa do IGF de Hyderabad indicou uma intencionalidade direcionada para discutir temas mais técnicos do que para temas polêmicos que exige a criação de instrumentos de mediação e desmonte do poder centralizador exercido na governança da Internet pela ICANN.

A quase retirada do tema Abertura reflete nitidamente uma tendência de negligenciar os temas que dizem respeito aos direitos humanos e a soberania dos países na Internet.

Conclusão

Em 2008, quando examinamos o contexto de governança da Internet mantido pela ICANN, acreditávamos que a globalização da Internet iria erodir este modelo ultrapassado de governança, ingenuamente acreditávamos também que os fóruns promovidos pela ONU para discutir a Governança da Internet (*Internet Governance Forum* – IGF), poderiam acelerar a consolidação de uma GI multilateral e democrática, constituída a partir de um consenso global.

Hoje, o que infelizmente constatamos é que:
a) o controle e a extrema centralização da Governança da Internet por um só país (EUA), continua mais forte do que antes, a despeito da legitimidade da autoridade da ICANN, neste modelo de GI, ser amplamente questionada;
b) a participação do Department of Homeland Security, na elaboração do plano "*The National Strategy For Homeland Security*", passou a considerar o ciberespaço como fator estratégico para a segurança dos EUA;

c) 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;
d) o malogro do IGF de Hyderabad revelou as dificuldades para implementar, através da ONU, um debate internacional para a implantação de uma Governança Multilateral e Democrática;
e) alguns países estão preferindo estabelecer a sua própria estrutura de regulação e controle da Internet, a revelia das decisões da ONU.
f) o legado da era Bush sobre o ciberespaço transformou o discurso da governança democrática multilateral na ONU, em uma ideologia da geopolítica de segurança.

O consenso dos países é que o ciberespaço não pode continuar sendo gerenciado por um único país, principalmente quando este detem o poder econômico e militar da Internet, assim, esperamos que o próximo IGF leve em conta o debate dessas reivindicações.

Notas

---

[1] . Cf. O memorando RFC 1591 Domain Name System Structure and Delegation, In: http://*www*.ietf.org/rfc/rfc1591.txt, sítio acessado em fevereiro de 2009.
[2] . PIRES, Hindenburgo Francisco. Governança Global da Internet: A representação de topônimos de países no ciberespaço. X Coloquio Internacional de Geocrítica, Barcelona, Universitat de Barcelona, 2008. In: http://www.ub.es/geocrit/-xcol/415.htm
[3] . Mais informações sobre servidores que operam com o sistema Anycast, conferir In: http://en.wikipedia.org/wiki/File:Root-current.svg e http://wapedia.mobi/en/Anycast/, sítio acessado em janeiro de 2009.
[4] . In: http://en.wikipedia.org/wiki/VeriSign e http://en.wikipedia.org/wiki/File:Verisignheadquarters.jpg, sítios acessados em fevereiro de 2009.
[5] . Cf. In: http://www3.isi.edu/about-isi_profile.htm, sítio acessado em fevereiro de 2009.
[6] . Cf. In: http://www.cogentco.com/us/about_history.php
[7] . PIRES, Hindenburgo Francisco. A produção morfológica do ciberespaço e a apropriação dos fluxos informacionais no Brasil, Santiago de Chile,VII Coloquio Internacional de Geocrítica, 2005. In: http://www.cibergeo.org/artigos/MORFOLOGIA_2005.pdf
[8] . TANCMAN, Michele. Geopolítica da Governança Global de Internet, São Paulo, Tese de Doutoramento, 2008, pp. 253.
[9] . Cf. a) First Online Free Expression Day launched on Reporters Without Borders website, In: http://www.rsf.org/article.php3?id_article=26086; b) BARATA, Germana. Governos e mercado impulsionam censura na Internet, In: http://comciencia.br/comciencia/?section=8&edicao=20&id=220, sítios acessados em fevereiro de 2009.
[10] . QIU, Jack Linchuan. Chinese Hackerism in Retrospect: The Legend of a New Revolutionary Army, In: http://ncsi-net.ncsi.iisc.ernet.in/cyberspace/societal-issues/Qiu1.pdf, sítio acessado em fevereiro de 2009.
[11] . Cf. In: http://www.areamilitar.net/noticias/noticias.aspx?NrNot=435, sítio acessado em fevereiro de 2009.
[12] . GORMAN, Siobhan, Hathaway to Head Cybersecurity Post, In: http://online.wsj.com/article/SB123412824916961127.html, sítio acessado em fevereiro de 2009.
[13] Cf. In: 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.

Bibliografia

BLUESTONE, Barry and HARRISON, Bennett. The Deindustrialization of America. New York, Basic Books, 1st edition, 1984.
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.
PIRES, Hindenburgo Francisco. A produção morfológica do ciberespaço e a apropriação dos fluxos informacionais no Brasil, Santiago de Chile,VII Coloquio Internacional de Geocrítica, 2005. In: http://www.cibergeo.org/artigos/MORFOLOGIA_2005.pdf
_____. Digital migration and regulation of the virtual structures of accumulation in Brazil. In: Growth and Crisis: Social Structure of Accumulation Theory and and Analysis. Edited by: Terrence McDonough, Michael Reich, David M. Kotz and Maria-Alejandra Gonzalez-Perez. First Published, Galway, 2006. In: http://www.nuigalway.ie/ssrc/documents/SSA_Conference_E-Book.pdf
_____. Governança Global da Internet: A representação de topônimos de países no ciberespaço. X Coloquio Internacional de Geocrítica, Barcelona, Universitat de Barcelona, 2008. In: http://www.ub.es/geocrit/-xcol/415.htm
SILVA Jr., Kenneth J. Root Zone Signing Proposal, ICANN/VeriSign, 2008. In: http://www.ntia.doc.gov/DNS/VeriSignDNSSECProposal.pdf
TANCMAN, Michele. Geopolítica da Governança Global de Internet, São Paulo, Tese de Doutoramento, 2008, pp. 253.
THE DEPARTMENT OF HOMELAND SECURITY. The National Strategy for Homeland Security, 2007. In: http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf