VIII ENCONTRO NACIONAL DA ANPEGE
28 de setembro a 02 de outubro de 2009
Curitiba - PR
"Espaço e tempo: Complexidade e desafios do pensar e do fazer geográfico"

(565) A NOVA GEOGRAFIA DAS REDES NO CIBERESPAÇO: IMPASSES NA GESTÃO DOS SISTEMAS DE ZONA RAIZ E DE DNS

GT 22 – GEOGRAFIA DAS REDES E MOBILIDADE POPULACIONAL

Hindenburgo Francisco Pires
Universidade do Estado do Rio de Janeiro
Instituto de Geografia
Departamento de Geografia Humana
www.cibergeo.org/artigos

Objetivos do Tema

a. Ampliar os horizontes teóricos da Geografia nos estudos sobre Governança da Internet (GI) e o ciberespaço.

b. Analisar a representação política dos países na gestão dos sistemas de zona raiz e de concessão de DNS no ciberespaço.

c. Revelar as implicações geopolíticas da GI no desenvolvimento futuro da Internet.

Apresentação dos Tópicos da Temática

1. **A Nova Geografia das Redes no Ciberespaço：**
   Impasses na localização geográfica dos servidores da zona raiz da Internet
2. **Algumas Questões sobre o atual modelo de Governança da Internet**
3. **Geopolítica versus Governança: A localização geográfica dos servidores da zona raiz da Internet**
4. **O Controle dos Servidores da Zona Raiz pelos EUA: O Ciberespaço como campo estratégico e militar da guerra para os EUA**

1. A Nova Geografia das Redes no Ciberespaço:
Impasses na localização geográfica dos servidores da zona raiz da Internet

Milton Santos ao investigar a Geografia das Redes concluiu que as redes no território ao mundializar-se apresentavam características topológicas que favoreciam a extrapolação dos seus limites físicos.

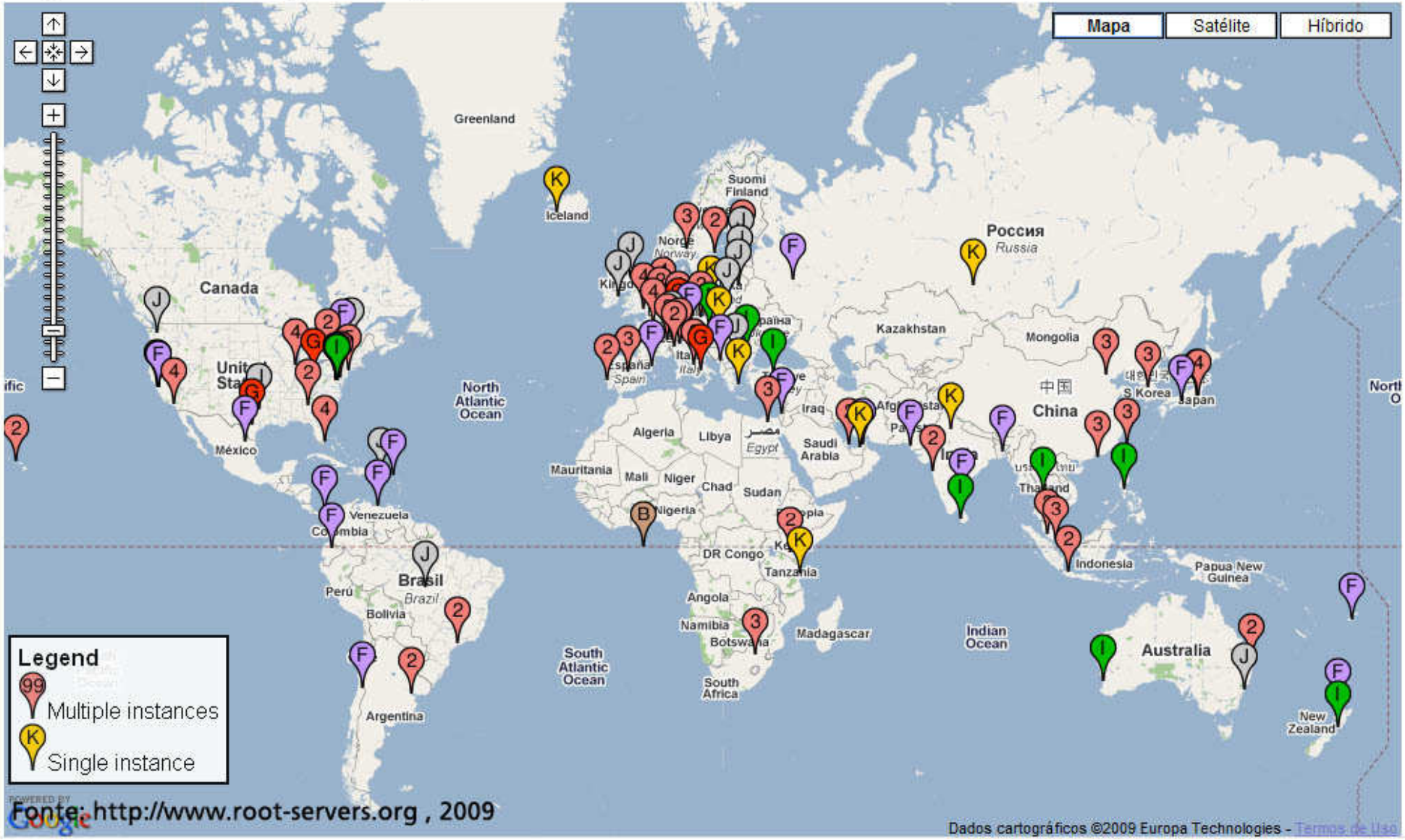
Este processo traria implicações no espaço soberano das fronteiras, pois estas são “os mais eficazes transmissores do processo de globalização a que assistimos” (Santos, 1996:212).

1. A Nova Geografia das Redes no Ciberespaço:
Impasses na localização geográfica dos servidores da zona raiz da Internet

Na análise da globalização 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 (Cf. Figura 1).

Questões geopolíticas são engendradas pelo sistema hierarquizado de parâmetros de concessão de nomes de domínios (DNS) e a política de concessão Regional de Registros da Internet - RIR, concebidos por Jon Postel, ex-diretor da IANA - The Internet Assigned Numbers Authority.

Figura 1- Localização Geográfica Global dos Servidores Raízes da Internet



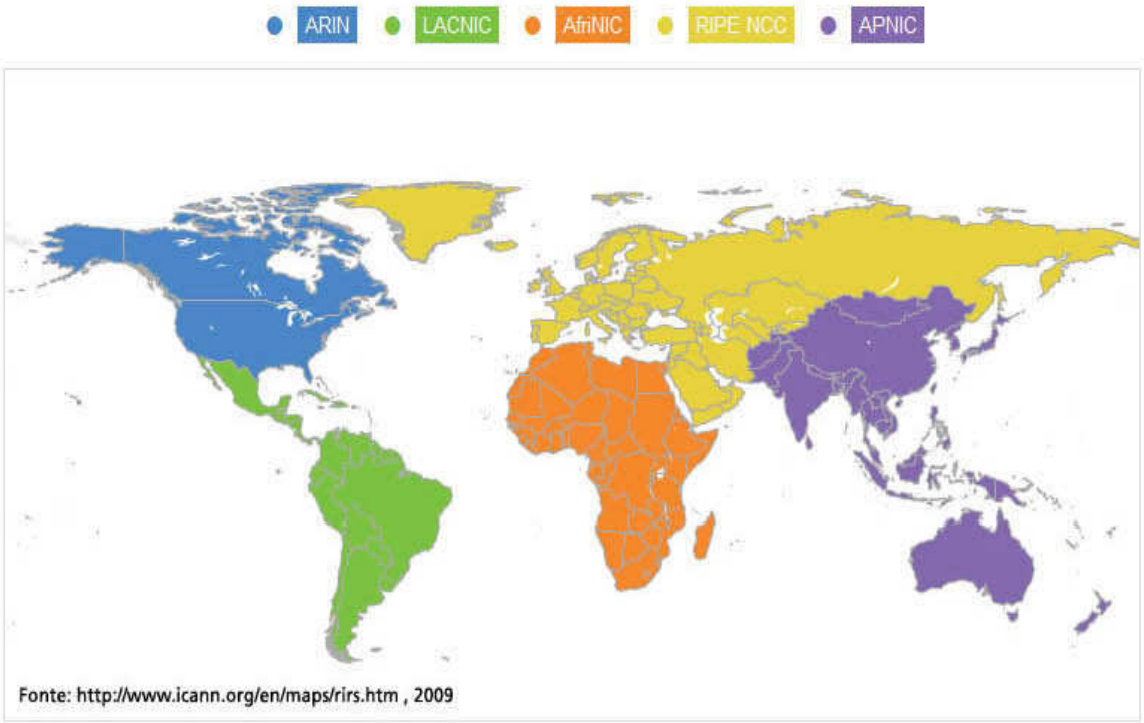
1. A Nova Geografia das Redes no Ciberespaço:
Impasses na localização geográfica dos servidores da zona raiz da Internet

O sistema de concessão de nomes de domínios, concebido por Jon Postel, que permite a articulação e o mapeamento geográfico dos servidores regionais, fortalece e reforça o controle geopolítico dos servidores da zona raiz pelos EUA.

A ICANN controla a concessão de Registros Regionais da Internet (RIRs).

Atualmente esta geopolítica de distribuição de endereços IP é controlado por 5 instituições de concessão de RIRs (Cf. Figura 2).

Figura 2 - Instituições Internacionais da ICANN que regulamentam os Registros Regionais da Internet (RIR)



Fonte: http://www.icann.org/en/maps/rirs.htm , 2009

ARIN - American Registry for Internet number, controla a concessão de RIRs na Região Norte Americana: http://www.arin.net/

LACNIC - Latin-American and Caribbean Internet Adress Registry, controla a concessão de RIRs na Região da América Latina e algumas ilhas do Caribe: http://www.lacnic.net/

RIPE/NCC - Réseaux Ip Européens/Network coordination Center, detém o controle da concessão de RIRs na Europa e Oriente Médio e Ásia Central: http://www.ripe.net/

AfriNIC - Africa Network Information center, mantém o controle da concessão de RIRs na Região da África: http://www.afrinic.net/

APNIC - Asia Pacific Network Information center, controla a concessão de RIRs na Região da Ásia e Pacífico: http://www.apnic.net/

2. Algumas Questões sobre o modelo de Governança da Internet

Com a globalização o atual modelo unilateral de GI, 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;

2. Algumas Questões sobre o modelo de Governança da Internet

c) **a política de concessão de Domain Name Server (DNS)** em relação à atribuição do código de domínio de alto nível dos países (country code top-level domain - ccTLD), baseada em normas geográficas (ISO 3166-1) criadas em 1974, composto por duas letras (br. es, ar, ch, de, etc.);

d) **a política de cibersegurança empreendida desde 2007** pelos EUA através do Plano "The National Strategy For Homeland Security" do Department of Homeland Security, dirigido à proteção da infra-estrutura crítica do território.

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

A localização geográfica dos servidores da zona raiz nos EUA é um fenômeno historicamente estabelecido desde a constituição da Internet como uma rede militar.

O controle dos servidores da zona raiz da Internet é mantido pela tríade: **DoC, ICANN e VeriSign**.

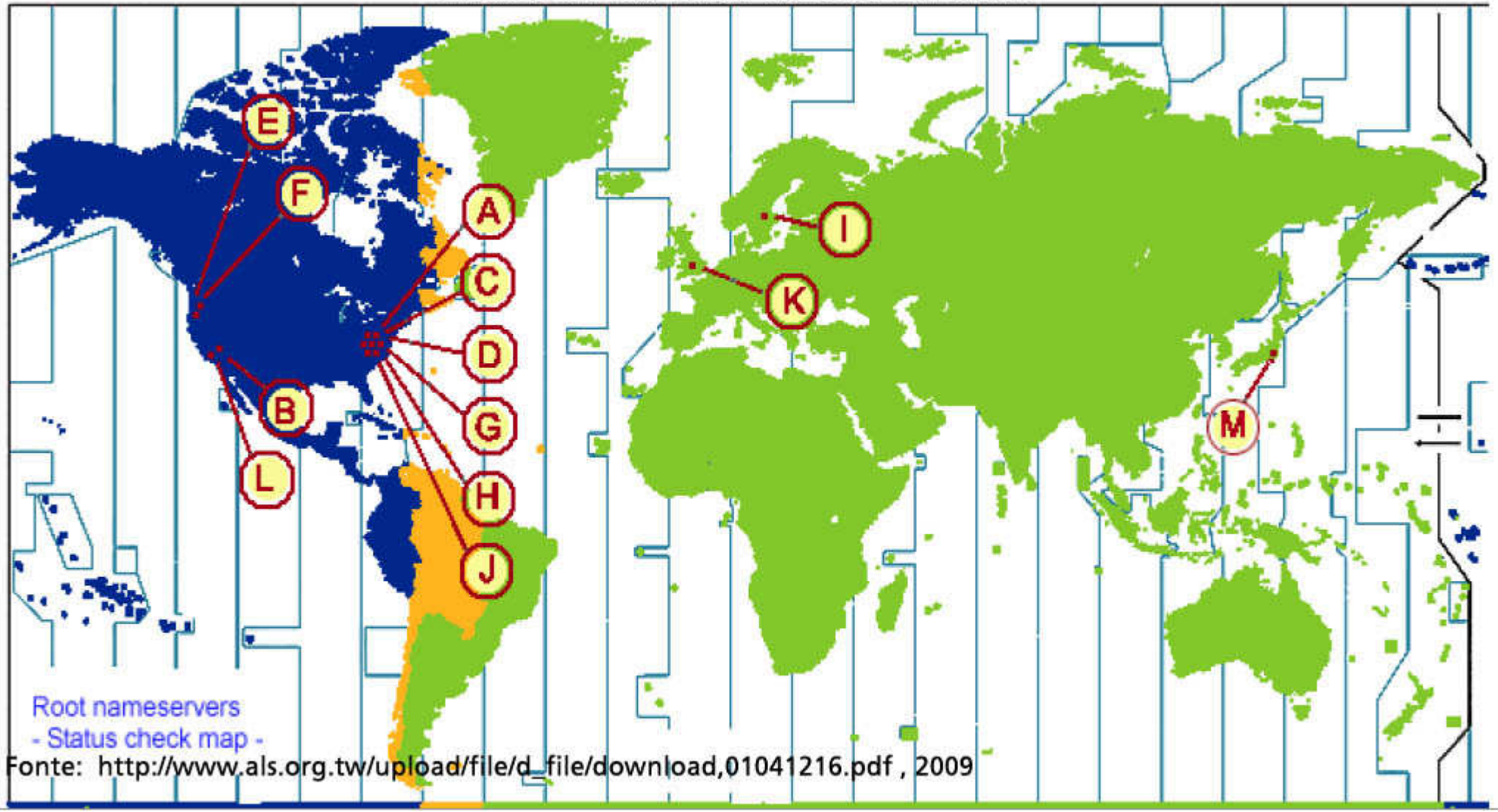
Dos 13 servidores da zona raiz 10, estão localizados fisicamente nos Estados Unidos (A, B, C, D, E, F, G, H, J, L), destes 6 operam dentro dos EUA (A, B, D, E, G, H), para garantir a gestão do sistema de cibersegurança, os 4 outros são servidores anfitriões (C, F, J, L) que operam com sistema de endereçamento descentralizado Anycast distribuídos por vários países, fisicamente instalados fora da região de influência dos EUA (Cf. Figura 3).

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

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 permitem o acesso de centenas de servidores secundários replicantes de outras regiões.

De acordo com **o memorando RFC 1591**, coube também a IANA, a responsabilidade pela concessão do código de domínio de alto nível dos países (ccTLD). Os ccTLD, representados por duas letras (br. es, ar, ch, de, etc.), eram os identificadores oficiais dos topônimos de países.

Figura 3: Localização Geográfica dos 13 principais Servidores da Zona Raiz da Internet



Fonte: http://www.als.org.tw/upload/file/d_file/download,01041216.pdf , 2009

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

As iniciativas de constituição de um novo sistema de zona raiz alternativo para a Internet via IGF, estão sendo rotuladas de promoverem a **fragmentação da Internet** .

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;
b) liberdade de expressão;
c) cibersegurança;
d) concessão de nomes de domínios fora do domínio da zona raiz;
e) soberania na gestão do sistema de concessão de nomes de domínios e países (DNS e ccTLDs);
f) políticas de desenvolvimento do trafego local da Internet e da arquitetura da rede no território.

4. O Controle dos Servidores da Zona Raiz pelos EUA: O Ciberespaço como campo estratégico e militar da guerra para os EUA

A hegemonia dos EUA durante o pós-guerra se estruturou em dois grandes pilares na expansão das atividades comerciais e na acumulação militar.

Com Eisenhower **a acumulação militar passou a ser o resultado da formação de um extraordinário mercado estatal, sem concorrência pública**.

Os contratos de defesa produziram um novo mapa econômico dos EUA, criando um complexo industrial militar 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"** *e* na história industrial do ocidente.

4. O Controle dos Servidores da Zona Raiz pelos EUA: O Ciberespaço como campo estratégico e militar da guerra para os EUA

Esse complexo industrial militar consiste de um conjunto de indústrias locais formado por várias firmas, cuja preocupação central, tem sido a produção de armamentos baseada em alta-tecnologia e inovação.

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

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.

4. O Controle dos Servidores da Zona Raiz pelos EUA: O Ciberespaço como campo estratégico e militar da guerra para os EUA

Por razão de segurança, desde os anos 90, a rede MILNET restringiu o uso de inúmeras aplicações de comunicações, comuns às redes comerciais convencionais.

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).

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

Assim, desde Eisenhower e durante a era Bush, o ciberespaço se transformou no espaço do Estado de guerra, *"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".

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

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.

Figura 4 - Camadas de Conteúdos do Ciberespaço

Fonte: Kurbalija & Gelbstein, 2005

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

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.

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

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."

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

Pelo exposto anteriormente 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.**

Conclusões

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;

Conclusões

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.

Conclusões

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

Mesmo com Barack Obama não houve qualquer modificação da doutrina Bush no que diz respeito a Internet, a nomeação de Rod Beckstrom, ex-coordenador do Department of Homeland Security, para presidir a ICANN, reflete infelizmente o prosseguimento dessa linha doutrinária de cunho eminentemente militar e bélico.

Obrigado!