

O Lado Benevolente do Conflito Cibernético

Panayotis A. Yannakogeorgos, PhD

Administração da Rede *Internet* é definida como amplo campo que inclui questões jurídicas, infraestruturais, socioculturais, econômicas, bem como de padronização e desenvolvimento. Mas os elementos relacionados à administração de recursos vitais da Rede e seu impacto na segurança nacional norte-americana muitas vezes são ignorados. Os empreendimentos estrangeiros para alterar seu gerenciamento técnico e projeto de padrões técnicos contam com o potencial de solapar os interesses nacionais dos EUA a longo prazo. Esse artigo trata do contexto de diretrizes de segurança nacional norte-americano e apresenta o conceito de conquista benevolente e um formato administrativo com interessados múltiplos, o que permite o livre fluxo de informação.

Existem muitos obstáculos globais ao *status quo*, inclusive a emergência de redes ciberespaciais alternativas que necessitam de recomendações para uma solução viável.

A Administração e a Estratégia Cibernética Nacional

Os padrões e protocolos técnicos não exigem a mesma atenção que as ameaças mais visíveis à segurança cibernética do país. Em ambiente de capital humano e recursos restritos, a atenção enfoca-se em delitos, espionagem e outras formas de conflito cibernético, não em assuntos relativos à administração de recursos vitais da Rede, desenvolvimento de padrões técnicos e projetos de novo equipamento em telecomunicações. Em domínio que até mesmo confunde as pessoas que estudam e desenvolvem estratégias e diretrizes, e que possuem alto interesse e aptidão para detalhes técnicos, a complexidade da administração da *Rede* é ainda mais difícil para aqueles que desenvolvem diretrizes e alocam recursos a campo que não possui analogia física.

Durante a era nuclear, não havia debate a respeito da possibilidade de reprojetermos as propriedades físicas do urânio para que pudéssemos empregá-lo universalmente, a fim de eliminarmos a possibilidade de seu emprego em fabricação de armamentos. A terminologia subjacente de o conflito nuclear fica restrita pelas leis da Física (e.g., fissão nuclear, gravidade). Os limites físicos também

existem no ciberespaço, quando se restringem os fluxos de informação às leis da Física—a dualidade onda-partícula [dualidade matéria-energia] da radiação que, quando modulada em *bits* cria um fluxo de informação.

No entanto, os elementos da “lógica” cibernética que permitem o fluxo da informação através de redes e sua presença em aplicativos, a fim de criar efeitos no mundo físico, são restritos somente pela inovação humana. Isso afeta o caráter do ciberespaço. Sua configuração atual é livre e aberta, mas isso não significa, necessariamente, que sempre continuará sendo assim. A percepção de questões de nível estratégico da administração da *Internet* é tão vital quanto compreender o impacto das vulnerabilidades que os agressores podem explorar para causar incidentes de segurança nacional.

No contexto da segurança nacional, o gerenciamento técnico da *Internet* é importante porque permitiria às nações autoritárias exercer poder e influência sobre a infraestrutura subjacente. Em contexto de segurança global, a manutenção de valores em livre fluxo de informação, dentro dos órgãos administrativos da *Internet*, continuarão a fomentar inovação e prosperidade econômica, tanto em nações desenvolvidas, como naquelas em processo de desenvolvimento.

Várias estratégias nacionais atuais articulam reações através de toda a nação para reagir à ameaças cibernéticas.¹ Tendem a manter o enfoque em incidentes catastróficos de segurança nacional e não em batalhas dentro das organizações que demarcam padrões técnicos ou gerenciam a operação do dia a dia da *Internet*.

A Casa Branca destaca a importância de foros de multi-interessados para projetar e padronizar os padrões técnicos, via “desenvolvimento colaborativo de padrões internacionais para informação e tecnologia de comunicações baseados em consenso (. . .) algo essencial para preservar a transparência e interoperabilidade, manter o crescimento das economias digitais e promover o avanço da sociedade”.² Além do mais, as dificuldades que encaramos em órgãos de demarcação de padrões internacionais são reconhecidas, assim que “ao projetar a próxima geração desses sistemas, devemos promover o interesse comum, apoiando os padrões técnicos e estruturas administrativas mais salutares, e não aquelas que simplesmente aumentarão o prestígio nacional ou o controle político”.³ No entanto, essas questões são reprimidas pelas situações hipotéticas mais sensacionais de um provável Dia de Julgamento Cibernético Final.

As exigências de segurança exigem que a terminologia empregada pela *Internet*—os padrões técnicos e protocolos subjacentes—continue a

suster o livre fluxo da informação. Se “código é lei” no ciberespaço, como dizem alguns, então os padrões e protocolos formam o tecido da realidade cibernética que dão significado aquele código.⁴

Em círculos de formuladores de diretrizes, o ciberespaço já é considerado um “domínio invisível”. Os padrões técnicos e protocolos são, por conseguinte, duplamente invisíveis. No entanto, esses protocolos definem o caráter da *Internet* e suas infraestruturas essenciais subjacentes. Como observado por todos, “Os protocolos subjacentes aos quais se conformam os projetos de *software* e *hardware* são uma forma mais invisível e mais arraigada para restringir o comportamento e estabelecer diretrizes públicas (. . .) Nesse sentido os protocolos possuem agência política—não uma agência desincorporada, mas aquela derivada de projetistas e executores de protocolo”.⁵

Antigamente, eram os Estados Unidos que lideravam o mundo em desenvolvimento de protocolos e padrões. Como resultado, os princípios de liberdade estavam incorporados no projeto e caráter da *Rede*, o que gera a inovação que continua a impulsionar o desenvolvimento sócio-econômico global.

O Lado Benevolente do Conflito Cibernético

Batalhas iminentes acerca de padrões e corpos administrativos determinarão o caráter futuro da *Internet*. O destacamento avançado de *IPv6* na Rússia e China e o desenvolvimento de novos padrões pelos países poderosos que concorrem com os Estados Unidos quase em paridade tecnológica, criam novos padrões técnicos, disseminando-os em todos os mercados mundiais, possibilitando assim, conflito cibernético benevolente.

A conquista benevolente ocorre quando um operador de sistema não essencial entra em parceria com um operador essencial em câmbio de acesso a sistema de informática desejado. O teórico cibernético Martin Libicki observa:

Aquele que controla um sistema pode permitir acesso a outros para que possam utilizar o conteúdo, serviços e conexões. Com o tempo, se tal acesso for útil (. . .) os usuários ficarão cada vez mais dependentes do mesmo, inclusive aprofundando essa dependência, adotando padrões e protocolos para os próprios sistemas e investindo, a fim de melhor utilizar o conteúdo, serviços ou conexões.⁶

O sócio principal em tal coalizão emerge para dominar os outros membros que agora dependem do serviço oferecido, contudo sem certa vulnerabilidade à rede do parceiro principal. Existe o temor de que “a

completa dependência que permeia seus sistemas internos pode fazer com que fique exposto à conspícua manipulação (. . .) A fonte de tal vulnerabilidade pode abranger o conhecimento geral de um dos sócios, indo da segurança da infraestrutura a acesso privilegiado à infraestrutura, o que permite que ataque de inicialização de computador à força ocorra com maior facilidade”.⁷

A *Internet* e sua infraestrutura técnica formam a potente manifestação de como os Estados Unidos, em sua função de operador essencial do sistema de informática, estenderam o domínio benevolente sobre aliados e adversários, através do desenvolvimento de tecnologia e demarcação de regras para sua operação. A *Internet* baseia-se em produtos designados e operados pelas entidades baseadas nos EUA, tais como *Domain Name System – DNS* e *Internet Corporation for Assigned Names and Numbers – ICANN*, *Microsoft* e *Cisco*. Os usuários ao redor do mundo, tais como *Google* e *Facebook* passaram a depender dos serviços oferecidos por essa plataforma. A posição dominante que as entidades baseadas nos EUA agora possuem não é permanente. *Skype*, baseado na Estônia, é indicação clara de que nem todos os serviços são de origem norteamericana. Ainda assim, quando o serviço baseado em *Internet* é criado por entidades estrangeiras, a maior parte da informação que flui através de tal aplicativo passa pelo *hardware* norteamericano. Quando se percebem vulnerabilidades, outras nações podem tentar sair de nosso sistema, a fim de preservar a soberania cibernética e expandir a influência, atraindo clientes aos próprios sistemas, fora da *Internet*.⁸ Assim, a vantagem estratégica ciberespacial dos EUA não é infinita. Está sendo contestada, em vários graus, por entidades que estão alcançando paridade competitiva. Assim, devemos compreender as reações atuais ao domínio da tecnologia norteamericana, a fim de refinar nossa estratégia cibernética dentro do contexto de conquista cibernética benevolente.

A conquista benevolente abrange muito mais do que adversários, que meramente contam com a capacidade de infiltrar a cadeia de suprimento e criar acesso “pelos fundos” de importantes provedores de segurança nacional, antes de sua entrada nos Estados Unidos propriamente dito.⁹

A ameaça também ocorre com o lançamento de nova tecnologia da qual os EUA não são os operadores básicos. No entanto, podem vir a depender da mesma.

Com o enfoque em ataques cibernéticos maliciosos, não se presta suficiente atenção aos pontos fracos do mundo cibernético – a tecnologia e padrões que permitem ao ciberespaço emergir do espectro

eletromagnético.

A China está dando grandes passos, plantando as sementes de conquista ciberespacial benévola. Como relatado pela *US-China Economic and Security Review Commission*, “Se a presente tendência continuar, a China (juntamente com seus representantes) será a propulsora principal do mercado em muitos setores, inclusive telecomunicações, com base em consumo, produção e inovação”.¹⁰

Os EUA adquirem pastilhas para computadores e outros fins, da China, bem como outros tipos de *hardware* em informática e comunicações [*information and communications technology – ICT*]. Isso permite a entrada de vírus e “acesso pelos fundos” a equipamento utilizado por entidades baseadas nos EUA, inclusive as forças armadas.

O extraordinário é que o *hardware* para computadores manufaturado na China, e vendido a baixo custo é aquisição lucrativa na Ásia e no resto do mundo em desenvolvimento.¹¹ Além do mais, as entidades chinesas, tais como *Huawei*, lideram o mundo em desenvolvimento de padrões para a próxima geração de redes de celulares *4G LTE*.¹²

Multi-interessados e a Administração da Internet

As entidades mercantis, tais como empresas multinacionais contribuem à formulação de diretrizes que regulam as comunicações internacionais, formalmente, no Sindicato Internacional de Telecomunicações [*International Telecommunications Union – ITU*] e, informalmente, através de contribuições pessoais de seus empregados dentro do *ICANN*, *Internet Engineering Task Force (IETF)* e outras organizações.

Nos Estados Unidos, os provedores de serviço de telecomunicações (desde a era de sistemas de telégrafos elétricos) nunca fizeram parte de monopólio estatal. Esse não foi o caso no restante do mundo.¹³ A *British Telecom* e a *Deutsche Telekom*, por exemplo, foram entidades estatais antes de sua privatização na década de 1990. Admitimos que, embora não haja controle estatal direto nos Estados Unidos, as companhias de telecomunicações são regidas pelo Estado.

Em negociações internacionais relacionadas à telecomunicações, um estado e suas empresas *ICT* possuem relação simbiótica.¹⁴ Isso acontece desde que a *International Telegraph Union*, predecessor da *International Telecommunications Union*, iniciou reuniões na metade do Século *XIX*, a fim de regulamentar as diretrizes telegráficas.¹⁵ Assim, a

perspectiva mundial é de que “atualmente (. . .) é a lei norteamericana que se aplica globalmente por falta de outra, porque a maioria das empresas da *Internet* são baseadas nos Estados Unidos”.¹⁶

Se o comércio é uma atividade política, então as empresas são protagonistas políticos. Os estados utilizam empresas para distribuir ou recompensar poder, a fim de satisfazer os objetivos políticos.¹⁷ Uma vez que os estados e as empresas afetam o comportamento entre si, uma interação dinâmica bidirecional existe entre o estado e o *MNC*.

Os dispositivos importantes de diretrizes que afetam o comportamento de *MNCs* incluem controles de exportação, protecionismo e diretrizes de comércio estratégico.

Os controles de exportação tendem a possuir um propósito político uma vez que, como observa certo especialista, “são projetados para evitar que nações rivais ganhem acesso a recursos e tecnologia vitais” ou, a fim de punir dada nação.¹⁸ As empresas que manufaturam mercadoria estratégica baseiam-se em governos para adotar diretrizes mercantis que apoiam a postura competitiva da empresa no mercado global.¹⁹ No entanto, os países impõem restrições naquilo que pode ser exportado, mesmo se for para o detrimento da empresa relacionado à concorrência em mercados estrangeiros. Por conseguinte, o governo federal norteamericano perdeu as denominadas guerras de criptografia na década de 90, quando a indústria privada protestou contra diretrizes que proibiam a exportação de ótimo *software* para criptografia devido a motivos estratégicos.²⁰

A fim de evitar que elementos delinquentes entrassem em comunicação via códigos impregnáveis, certas empresas colocaram em execução mecanismos [*Law Enforcement Intercept - LEI*] para que as agências de segurança nacional pudessem monitorar as comunicações entre pessoas suspeitas e terroristas.²¹ As empresas norteamericanas e associados, que desenvolvem, mantêm e revisam padrões básicos e infraestruturas tecnológicas são estigmatizadas por tais alegações que descrevem um aparato de segurança nacional trapaceiro, juntamente com um setor privado em conluio, que captam os dados de todo o planeta. Isso não reflete o fato de que, ao contrário de estados autoritários, a observação cuidadosa de leis norteamericanas projetadas para proteger a privacidade do usuário mantém a linha divisória entre o governo e o setor privado.²² A mídia, que prefere alegações em manchetes gritantes, simplesmente para atrair atenção, diminui a confiança mundial no setor privado norteamericano e valida as narrativas de que os mecanismos administrativos da *Internet* devem ser internacionalizados.

A percepção global de que o governo norteamericano possui o controle, *de facto*, dos recursos vitais da Internet é vastamente moldado pelas experiências de outras nações do relacionamento íntimo entre as empresas de telecomunicações e seus governos. De maneira singular, o governo norteamericano nunca foi o proprietário ou gerente executivo de empresas de telecomunicações. Como o resto do mundo seguiu o exemplo norteamericano de telecomunicações privatizada, a experiência antiga de controle governamental daquele setor não deixou seu equilíbrio cognitivo. Hoje, esse tipo de experiência lança sombra de suspeita sobre o acordo especial entre o *ICANN* e o Departamento de Comércio dos Estados Unidos.

Recursos e Infraestrutura Vitais da Internet

Com o enfoque de debates em atividades maliciosas, existe pouca consideração referentes às inferências de trabalho pacífico de projetar e manter a *Internet* e da mudança que essas atividades produzirão em prosperidade e inovação global. O gerenciamento técnico do *Domain Name System*, inventado pelo *DoD* e por ele administrado durante seus anos formativos, foi assumido pelo Departamento de Comércio em 1998. Subsequentemente evoluiu ao modelo atual não governamental, composto de multi-interessados.²³ A descrição oferece breve recapitulação da tecnologia subjacente e das organizações que desempenharam funções para demarcar os padrões que permitem o funcionamento técnico da *Internet*. Assim, o propósito desta seção é apresentar uma descrição da administração da *Internet* como fonte de preocupação em segurança econômica global.

Critical Internet Resources (CIR) “no contexto administrativo da *Internet* normalmente refere-se a seus recursos lógicos singulares e não aos componentes da infraestrutura física ou recursos virtuais não exclusivos àquela *Rede*. Os *CIRs* devem providenciar um requisito técnico de singularidade global que requer certo grau de coordenação central: O endereço *Internet*; *DNS*; *Autonomous System Numbers*”.²⁴ Ao contrário do conceito popular de *Internet* ilimitada, a capacidade do endereço subjacente é limitada. De fato, o alcance do endereço *IP* já foi praticamente superado. Antecipando o fato, os engenheiros desenvolveram o *IPv6* que, dentre outras melhorias, aumenta o número total de endereços *IP* em potencial – de 4.294.967.296 no *IPv4* a 2^{128} no *IPv6*. Reconhece-se hoje que: “O lançamento do *IPv6* é o único meio perene de aliviar a pressão no conglomerado do *IPv4* público (. . .)”²⁵ Quando iniciar a transição do *IPv4* ao *IPv6*, i.e., o protocolo dominante em comunicações para a *Internet* global, os Estados Unidos não

desempenharão a função de liderança. Atualmente, a Rússia está em primeiro lugar, em termos de penetração de mercado. A China possui o maior lançamento em números absolutos.²⁶ As consequências de lançamento retrasado estão relacionadas, tanto à administração, como às ameaças mais tradicionais à segurança. Para esse último problema o *National Institute for Standards* nota que a “prevenção de acesso não autorizado às redes *IPv6* provavelmente será mais difícil nos anos iniciais do lançamento”.²⁷ Assim, as nações concorrentes com maior experiência em lançamentos *IPv6* nacionalmente, possuem também maior percepção técnica acerca de suas operações no mundo real. A rede *NIPR* da *USAF* só estará completamente capacitada para o *IPv6* em 2014. Mesmo então, nota-se que o plano é empregar ambos, o *IPv4* e o *IPv6*, paralelamente durante os próximos 10-15 anos.²⁸ À medida que continua o lançamento do *IPv6*, a espinha dorsal da *Internet*, a percepção geral provavelmente será de que a Rússia e a China lideram em *IPv6*. É probabilidade é que aproveitarão a oportunidade para mudar o controle desses escassos espaços de endereços do *ICANN* rumo a controle de órgão intergovernamental, tais como as Nações Unidas.

O ICANN e a Estrutura Administrativa Atual da Internet

Como o ciberespaço é um domínio artificial, a infraestrutura e a padronização possuem importância vital. Os grupos de cientistas (Informática) e engenheiros criam os padrões e regras sob as quais opera a *Internet* – a manifestação mais potente do ciberespaço. De fato, grande número desses órgãos globais tiveram início como programas da *DISA*, *DARPA*, e outros do *USG* e foram privatizados em meados da década de 90. Assim, o desenvolvimento da próxima fase da *Internet* não conta com os Estados Unidos como principal propulsor. Pelo contrário, os padrões e processos estão sendo desenvolvidos pelos cientistas e engenheiros russos, chineses e outros estrangeiros. Atualmente, as máquinas comunicam-se entre si, utilizando terminologia baseada em Inglês. Se a excelência norteamericana continuar seguindo seu rumo degenerativo é provável que futuras redes dependerão de máquinas que falam idiomas estrangeiros. Além disso, a administração de alocação de endereços *DNS* e *IP* está sendo pressionada para passar de uma abordagem de multi-interessados a mecanismo intergovernamental dentro da *ITU*. Esse é o lado benevolente do conflito cibernético.

O *DNS* permite que as pessoas utilizem o *Uniform Resource Locators (URL)* para comunicação com outros dispositivos da *Internet*. Em lugar de sermos obrigados a digitar um endereço de *website IP*—uma sequência de números—pode-se digitar um *URL* em linguagem

natural, tais como *www.af.mil*, em navegador para obter a conexão ao endereço *IP* correspondente. Isso faz com que a rede seja de fácil uso. Ao usuário comum, a canalização da informação ao seu computador pode muito bem parecer um toque de mágico. No entanto, os endereços *IP* são escassos, especialmente em *IPv4*. Os processos de designação de endereços *IP*, permitindo que a *Internet* sirva de plataforma global, são complexos, técnica e politicamente.

A alocação de espaços para endereço *IPv4* a vários registros é outorgada pela *ICANN* via *Internet Assigned Numbers Authority (IANA)*.²⁹ Globalmente, os endereços *IP* roteáveis fazem parte da base de dados *DNS* em bancos de dados de zona-raiz e permitem a tradução de *URLs* aos endereços *IP*.³⁰ Os nomes de domínio de nível superior, tais como *.com* or *.org*, são mantidos e atualizados pelo *ICANN*, antigamente sob a direção do Departamento de Comércio [*Department of Commerce – DoC*. Atualmente operando sob memorando de acordo com o *DoC*, o *ICANN* continua a ser a única fonte de alocação de endereços a *DNSs* específicos e registros regionais de *Internet*, a fim de assegurar a todos uma experiência uniformizada. O *ICANN* garante que se nome de domínio estiver disponível, qualquer pessoa pode adquiri-lo, vinculando-o a endereço *IP*, a fim de gerar presença *online*, administrando e mantendo as bases de dados centrais da zona-raiz, e instalando-as em servidores *DNS* ao redor do globo.³¹

A Força-Tarefa de Engenharia Internet: Regentes do TCP/IP

O grupo de protocolo de comunicações padronizado internacionalmente, denominado *Transmission Control Protocol and Internet Protocol (TCP/IP)*, permite o fluxo de feixes de dados e informação pelas redes de computadores, inclusive *Internet*. O *TCP/IP* é padronizado com a utilização do modelo *International Organization of Standards for the Open Systems Interconnection (OSI)* como base da rede *Internet*.

É necessária breve descrição de como a informação é enviada pelas redes para melhor compreender o significado de *TCP/IP*. Os feixes de dados são as unidades básicas do tráfego em rede. São os meios padrão para dividir a informação em unidades menores, o que permite seu envio por dada rede. Um componente significativo de redes de computadores é o cabeçalho *IP*, que contém informação pertinente à fonte e endereços destinatários. As máquinas requerem essa sequência de números para possibilitar sua conexão com outros computadores na *Internet* ou outras redes.³² O *hardware* em rede deve possuir um válido endereço *IP* para funcionar em dada rede. Os feixes de dados são

recriados pelo dispositivo receptor, baseado na informação contida no cabeçalho de cada feixe que indica ao receptor como recriar a informação, utilizando o feixe de dados. Sem protocolos internacionalmente padronizados, tais como *TCP/IP*, seria impossível assegurar que os feixes poderiam ser lidos pelo dispositivo receptor.³³

O mais esotérico de todos os recursos vitais da *Internet* são os números do sistema autônomo [*autonomous system numbers – ASN*]. Esses números são empregados pelos provedores da rede em “pontos de inspeção” [*“peering points”*], a fim de permitir que a informação possa fluir de, digamos, *Verizon* à *ATT*, entre outros. Os protocolos de portais de perímetro [*Border gateway protocols*] são um dos aspectos de *ASNs*.

Os debates acerca de diretrizes da *Internet* comprovaram a ineficácia de multi-lateralismo, à medida que os Estados Unidos tentam liderar e outros deixam de seguir. A inovação tecnológica norteamericana em desenvolvimento e manutenção da *espinha dorsal* da *Internet* está sendo questionada. No entanto, empreendimentos globais para promover a reforma regulamentar, como incluir instituições de administração global, tais como *ITU* como entidades responsáveis pela monitoria do *ICANN*, são questões que causam tensão política, intimamente relacionadas às preocupações de segurança nacional em regimes democráticos e autocráticos. Em suma, a “liderança” norteamericana, a primeira entre seus pares, levou a uma sucessão de becos sem saída. Estamos presenciando contramedidas por amigos e concorrentes que ganharão impulso durante a Conferência Mundial de Telecomunicações Internacionais [*World Conference on International Telecommunication*] de 2012.³⁴

Objecções Globais ao *Status Quo*

A informação global que flui através de dispositivos ciberespaciais livres, tais como a *Internet*, é regulamentada pelos órgãos nacionais e regionais que coordenam suas diretrizes internacionalmente. Os padrões criados por dispositivos ciberespaciais requerem processos prolongados em diferentes órgãos, como a *International Organization for Standardization* e a *ITU*, para assegurar suficiente cooperação técnica e política entre as nações-estados. Enquanto que as entidades baseadas nos EUA demarcam os padrões para a tecnologia *Internet*, as entidades baseadas na China, tais como *Huawei* e a *ZTE Corporation*, cada vez mais estão tomando funções em órgãos administrativos da *Internet* para redigir importantes padrões internacionais que moldarão a futura geração de redes mundiais. Não é ocorrência recente. Já em 2004, o pessoal chinês desempenhava funções avançadas no *ITU*. O

Telecommunication Standardization Sector começou a mencionar a transição ao *IPv6* como meio de corrigir uma percepção de desequilíbrio em alocação de endereços entre os Estados Unidos e o mundo em desenvolvimento. “A alocação prévia de endereços *IPv4* resultou em desequilíbrios geográficos e excessiva posse de espaço pelos que primeiro haviam adotado a medida. A situação foi reconhecida e abordada pelos *Regional Internet Registries (RIR)* (. . .) Alguns países em desenvolvimento levantaram questões acerca da alocação de endereços *IP*. É importante assegurar que apreensões similares não surjam com respeito ao *IPv6*.”³⁵ A indicação é que alguns países desejam mudar a administração da alocação de endereços *IPv6* à instituição global, tais como o *ITU*.

Os foros políticos aceleram cada vez mais o impulso relacionado à administração da *Internet* nos Estados Unidos. Liderado pelas iniciativas russas e chinesas, os concorrentes e parceiros, igualmente, trabalham para internacionalizar a administração técnica da *Internet*. A China e a Rússia, juntamente com a Índia, África do Sul e o Brasil deram início à iniciativas contra o domínio norteamericano do *ICANN*. Essas tentativas já estão a caminho há quase uma década.³⁶ À medida que o experimento do *DoD ARPAnet* surgiu para vir a ser componente significativo do desenvolvimento sócio-econômico global e os governos cada vez mais se tornaram cientes de sua importância, o impulso para internacionalizar o *ICANN* aumentou. Lembremo-nos de que esses pequenos *empurrões* a favor da internacionalização são devidos, em parte, à percepção de controle governamental pelos EUA sobre o *ICANN* via o *DoC* e a *NTIA*, seguindo o histórico de relacionamentos especiais entre as empresas de telecomunicações estatais que existem em outros países.

Uma direção mais plausível de controle do *ITU* sobre o espaço *IPv6* é fazer com que a *ICANN* forneça ao *ITU* seu próprio bloco de endereços *IP*, servindo de seu próprio *RIR* para alocar, ao nível nacional, registros de *Internet*. Serviria para manter a estrutura atual de multi-interessados que governa os recursos vitais da *Internet*, ao mesmo tempo equilibrando as necessidades da China e do mundo em desenvolvimento. Permitiria a redução de fricção e faria com que aqueles que preferem o modelo atual continuem a servir de mecanismo para regulamentar às operações técnicas cotidianas da *Internet*.

A Tirania (em Potencial) do ITU Sobre os Recursos Vitais da Internet

Durante os preparativos para o *World Summit for the Information Society (WSIS)* ficou claro o campo de batalha relacionado a debates sobre a internacionalização do *ICANN*, quando surgiu grande oposição à administração atual da *Internet*. Por exemplo, em março de 2004, durante um dos Foros Globais em Administração da *Internet* presididos pela ONU³⁷ a delegada brasileira, Maria Luiza Viotti declarou que a administração da *Internet* necessitava de reforma, uma vez que não incluía os países em desenvolvimento. Muito pelo contrário, parecia estar sob o controle de um grupo de países ou interessados.³⁸ Lyndall Shope-Mafole, presidente da Comissão Nacional da África do Sul [*South Africa's National Commission*], empregou quase as mesmas palavras, alegando que a legitimidade dos processos *ICANN*, e não seu funcionamento, era a maior preocupação dos países em desenvolvimento.³⁹ Por conseguinte, após rigorosa comunicação, os delegados concluíram que o *ICANN* requeria maiores reformas, baseado em inquietudes do mundo em desenvolvimento. Através de todo o processo *WSIS* e continuando em outros foros que discutem a administração da *Internet* e a segurança cibernética global, o Brasil continuou a propor contra a posição dos EUA no *ICANN*. Em 2011, a Índia uniu-se à África do Sul e ao Brasil para apresentar a “execução da Agenda de Túnis”

Mantendo em mente a necessidade de mecanismo multilateral transparente, democrático e multilateral que permite a participação de todos os interessados em suas respectivas funções, para tratar das muitas questões acerca de diretrizes públicas internacionais transversais que requerem atenção; e que não estão sendo tratados de maneira adequada pelos mecanismos atuais; e a necessidade de maior cooperação para que os governos, em paridade, possam levar avante suas funções e responsabilidades em questões de diretrizes públicas internacionais pertinentes à *Internet*, a Índia propõe o estabelecimento de novo mecanismo institucional nas Nações Unidas para diretrizes relacionadas à *Internet* global, com a denominação de *United Nations Committee for Internet-Related Policies (CIRP)*.⁴⁰

A ideia *CIRP* foi incentivada em países em desenvolvimento como contramedida ao atual gerenciamento técnico. De fato, reflete muito bem as inquietudes da China declaradas pela *China Organizational Name Administration Center (CONAC)* de que “o governo dos EUA possui controle soberano sobre os recursos da *Internet*. Sugerimos, assim, fazer com que o plano de segurança Informática seja colocado à disposição

para comentários de todos os interessados, pois manter a segurança do espaço cibernético não é uma missão somente do governo dos Estados Unidos, e não pode ser realizado por uma só nação”.⁴¹

Da Rússia o então Primeiro Ministro, Vladimir Putin, declarou: A *International Telecommunication Union* é uma das organizações internacionais das mais antigas; duas vezes mais antiga do que as Nações Unidas. A Rússia foi um de seus co-fundadores e seu intento é permanecer como membro ativo. Somos gratos pelas ideias propostas para discussão. Uma delas é o estabelecimento de controle internacional sobre a *Internet*, utilizando a capacidade de monitoria e supervisão da *International Telecommunication Union (ITU)*.⁴²

Consequentemente, os Estados Unidos enfrentam grandes obstáculos dentro da *ITU* da parte de regimes autocráticos que lideram o mundo em desenvolvimento no movimento para transferir os recursos vitais da *Internet* a órgão multilateral. O perigo implícito é o distanciamento da característica que define a *Internet*, i.e., o livre fluxo de dados rumo a modelo no qual as agendas políticas não democráticas tentam exercer controle sobre o fluxo de dados. Assim, os Estados Unidos e nações da mesma índole devem unir-se diplomaticamente para assegurar que o caráter da *Internet* permanecerá livre dos controles políticos de instituição multilateral.

Essa luta diplomática pelo controle da *Internet* também ocorre em outros foros, como a *Commission on Science and Technology for Development da ONU*. As sugestões feitas incluem:

O estabelecimento de grupo de trabalho *ad hoc* sob a *Commission on Science and Technology for Development*, tendo em vista o desenvolvimento de projeto institucional e roteiro para aumentar a cooperação em questões de diretrizes públicas relacionadas à *Internet* com o apoio do Secretário-Geral (. . .)

A criação de um comitê mais permanente em questões de diretrizes públicas internacionais pertinentes à *Internet* dentro do sistema norteamericano, possivelmente de acordo com o modelo do *Committee on Information, Communications and Computer Policy of the Organization for Economic Cooperation and Development* (...)

E, de forma mais concreta, as questões sobre diretrizes

globais devem ser solucionadas por entidade com representação global, tais como as Nações Unidas, e as questões regionais por entidades com representação regional, tais como o Conselho Europeu (. . .) [e] a participação de organizações relevantes durante discussões à respeito da administração da *Internet* na *ITU Plenipotentiary Conference*, quadrienal, e o processo de revisão pública e o *Governmental Advisory Committee* do *ICANN*.⁴³

Com a *World Conference on Telecommunications* em dezembro de 2012, tais declarações indicam que essas ideais virão à tona uma vez mais como parte da tentativa da *ITU* em revisar as *International Telecommunications Regulations (ITR)*, a fim de incluir a administração de recursos vitais futuros da *Internet* dentro do mandado da *ITU*, e assumir maiores funções na administração da *Internet*.⁴⁴

Fazer com que a administração da *Internet* fique aberta a processos intergovernamentais colocaria a segurança econômica global em perigo, dado o potencial de que protagonistas estatais menos que responsáveis adotem a atual abordagem privada de *laissez-faire* no que diz respeito à administração da *Internet*, deixando que nações-estados e suas entidades empresariais tomem controle administrativo dos recursos vitais da *Rede*.

A Sombra “DNS” em Ascensão

Como descrito acima, os recursos vitais da *Internet* que permitem a solução de *URL* universais e comunicações globais existem devido ao sistema básico gerenciado pelo *ICANN* e protocolos projetados, desenvolvidos e debatidos dentro do *IETF* (entre outras organizações). Embora isso permita a operabilidade livre e aberta da *Internet*, os padrões e protocolos que o *ICANN* emprega para manter o domínio de registros de nomes podem ser usados por indivíduos, redes *ad hoc* e nações-estados para projetar e lançar sistema *DNS* alternativo que pode ser independente ou transitar “de garupa” na *Internet*. Um *LAN* empresarial, tais como “.nome da empresa” para o uso interno da empresa, é um exemplo do primeiro. Quando um grupo deseja transitar acima da base *DNS* global e incorporar seu próprio pseudo-domínio de nível superior, os operadores originais dos pseudo-domínios podem empregar recursos de *software* específicos para solucionar os domínios globalmente acessíveis dentro de seu sistema *DSN* alternativo. Os clientes norteamericanos poderiam experimentar o que seria como ingressar a universo *DNS* alternativo via rede *The Onion Router (TOR)*.

Quando se baixa o pacote do *Onion Router* pode-se navegar a *websites* desejadas, de forma anônima, (o uso típico do *TOR*), direcionando o navegador *TOR* a *websites* no domínio “.*onion*” e mesclando-se onde o submundo cibernético começou a transferir o gerenciamento de suas operações comerciais atuais, a fim de evitar problemas de infração de ordem pública, e adicionar outra camada de proteção aos seus disfarces.

Se ocorrer grande uso desse tipo de emprego de *Internets* obscuras, isso levaria à perda de confiança e de utilidade da *Internet* em si. O maior perigo existe, quando nações-estados desenvolvem e lançam seus próprios sistemas *DNS* alternativos, separando-se assim da *Internet* global. Não é como controlar os pontos de acesso e de fato desenvolver *intranets* dentro do país que podem ou não estar conectadas à *Internet* global.⁴⁵ O enfoque do debate abaixo é a Rússia e a China e relaciona-se aos respectivos sucessos em lançar possíveis *intranets* para seu uso interno. Outros países, tais como o Irã estão seguindo os mesmos passos.

O envolvimento dos EUA em *abertamente* promover e organizar “ativistas digitais” na luta pelo livre fluxo de informação gera fricção internacional, emitindo \$30 milhões de dólares em subsídios para aumentar o acesso livre à *Internet*, apoio a ativistas digitais, e combater a repressão da *Internet* onde quer que ocorra”.⁴⁶ Isso é contraproducente se a meta for promover cooperação internacional em questões de segurança cibernética internacional. A “*Internet Freedom Agenda*” é um exemplo desse fenômeno.⁴⁷ Tal tecnologia eficazmente permite que cidadãos-ativistas passem ilegalmente (hakear) sentinelas digitais governamentais, a fim de disseminar informação proibida. Outros dispositivos permitem aos ativistas utilizar disfarces digitais, organizando-se em movimentos sociais projetados para derrubar (diferentes) regimes. O resultado foi o aparecimento de redes nacionais alternativas que essencialmente criam sistemas de domínio de nome alternativo para uso interno, permitindo a censura de conteúdo e sufocando a produtividade que a topologia atual da *Internet* permite. A China é um país que colocou em execução tudo isso em escala nacional.⁴⁸ Com a autorização do *State Commission Office for Public Sector Reform (SCPSR)* e do *Ministry of Industry and Information Technology (MIIT)*, a *CONAC* opera o registro para “.*政务.cn*” (Assuntos Governamentais) e “.*公益.cn*” (Interesse Público).

A ascensão de *Internet* dissidente certamente mudará o caráter da *Rede* atual, com consequências negativas para a inovação e a prosperidade ao redor do mundo. Aqueles que desejarem que a *Internet*

se mantenha livre e aberta serão beneficiados, projetarão contraste nítido e moral aqueles que desejarem controlar o *interruptor de força* principal. Consequentemente, manter o modelo administrativo atual, ao mesmo tempo, tratando das inquietudes legítimas de amigos e aliados garantirá que a *Internet* continuará a servir de potente plataforma para o desenvolvimento econômico humano.

Conclusão

Deixar de prestar atenção as nossas vulnerabilidades em administração da *Internet* e a conquista benéfica darão aos adversários vantagem estratégica em conflito cibernético. Nossas próprias tentativas em agressão cibernética também ficarão complicadas, pois as redes não baseadas em protocolos e padrões desenvolvidos pelas entidades baseadas nos EUA são lançadas pelos rivais. Para que possamos conceber o ciberespaço, adaptando-nos à mudança do ambiente cibernético, deve haver amplo diálogo a respeito. Apesar do fato de que a *Internet* teve origem no Departamento de Defesa, não existe tentativa organizada para influenciar o desenvolvimento de diretrizes e padrões técnicos que afetam o gerenciamento da Rede. Atualmente, o *DoD* permanece em situação reativa, coordenando e tecendo comentários a respeito das várias normas e padrões globais sob consideração dentro dos processos do *USG* relacionados à administração da Rede. Devido a essa abordagem, o *DoD* e a *USAF* são vistos como organismos sem competência jurídica ou reputação técnica em gerenciamento da Rede. O *DoD* e a Força Aérea norteamericana, em particular, devem exercer liderança e tomar um papel mais ativo no desenvolvimento de padrões para a infraestrutura tecnológica da Informática, como antes. Além do mais, devem documentar suas funções com maior esmero e providenciar a métrica de participação e posição junto aos órgãos de gerenciamento da Rede. A Força Aérea deve desempenhar função de liderança dentro do *DoD* e em todo o governo, explicitamente mantendo o enfoque em conceito mais amplo de conquista benéfica o que implicitamente existe em diretrizes estratégias e doutrinas. A *World Telecommunications Conference* dezembro próximo talvez seja o local apropriado para dar início a essa tentativa.

À medida que o *hardware* e o *software* nos quais se baseia a *Internet* global evoluem e as entidades fora dos EUA começam a investir em novo *hardware*, padrões e protocolos, potencialmente removendo o quinhão do mercado para longe das entidades norteamericanas, a posição dos EUA como operador central da infraestrutura cibernética diminuirá. Os Estados Unidos atualmente desfrutam de domínio

técnico, através de sua posição como criadores e provedores centrais de serviços possibilitados pelo *ICANN* e pelo nível superior do *Domain Name System*. Mas a segurança de nossas estratégias cibernéticas não se dirigem adequadamente à ameaças que possam advir do desenvolvimento de protocolos, padrões e tecnologia de outros países, nos quais se baseará a próxima geração de Redes. A Força Aérea possui função vital, dada a riqueza de excelência técnica que reside em nossa fonte de cientistas e engenheiros. No entanto, não pode agir sozinha e o *DoD* necessitará manter parte de seus recursos financeiros cibernéticos já limitados em administração da *Internet*. Se deixar de fazer isso, arriscará que os padrões e protocolos técnicos projetados por estrangeiros formem a *espinha dorsal* da próxima geração *IT*, colocando as operações do *DoD* possivelmente em risco, revertendo o que é agora uma *Internet* caracterizada pelo livre fluxo de informação do qual depende o Departamento. A *USAF* continua a liderar as forças armadas norteamericanas em impacto ciberespacial. Por conseguinte, os debates referentes à ações ou omissões em administração da *Internet* são importantes.

Notas

1. The *National Strategy to Secure Cyberspace (NSSC)*, (Washington: The White House, y 2003); John Rollins and Anna C. Henning, *Comprehensive National Cybersecurity Initiative (CNCI)*, (Washington: Congressional Research Service, 10 March 2009; regime de segredo abolido em março 2010); o *International Strategy for Cyberspace* (Washington: The White House, May 2011); e o *Department of Defense Strategy for Operating in Cyberspace* (Washington: DoD, July 2011) são até hoje as diretivas relevantes que lideram a segurança cibernética.

2. *International Strategy for Cyberspace*, 12.

3. *Ibid.*, 15.

4. Lawrence Lessing, “Code is Law,” in *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006), 11–10.

5. Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge: MIT Press 2009), 11.

6. Libicki, *Conquest in Cyberspace*, 12.

7. *Ibid.*, 137.

8. O sistema de posicionamento global (GPS) é um exemplo onde o controle do *software* e *hardware* está sendo disputado. Embora acesso ao *GPS* seja gratuito ao

serviço básico, aliados e rivais notam sua vulnerabilidade devido a dependência no sistema norteamericano. A Rússia está modernizando seu GPS e a União Europeia e a China estão desenvolvendo sistemas independentes. O longo ciclo, da ideia à execução desses novos sistemas é devido ao imenso custo financeiro para o lançamento de rede espacial. Os ciclos cibernéticos podem ser mais curtos em matéria de tempo, em vista de custos mais baixos associados ao lançamento de rede nacional de informática, quando comparado ao de múltiplos satélites, altamente tecnológicos. Para debate mais completo, referente a sistemas GPS alternativos, ver *GPS versus Galileo: Balancing for Position in Space* do TenCel Scott W. Beidleman, (Base Aérea Maxwell AFB, AL: Air University Press, 2006).

9. Bruce Rayner, "Ferretting out the Fakes," *Electronic Engineering Times*, 15 August 2011, 24. Ver também John Markoff, "Computer Gear may Pose Trojan Horse Threat to Pentagon," *New York Times*, 10 May 2008, 12.

10. *The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector*, U.S.-China Economic and Security Review Commission Staff Report, January 2011, 7, http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf

11. LCDR A. Anand, "Threats to India's Information Environment," em *Information Technology: The Future Warfare Weapon* (New Delhi: Ocean Books Pvt. Ltd., 2000), 56–62.

12. "Huawei Conducts World's First Commercial Network LTE Category 4 Trial," *Cellular News*, 9 May 2012, <http://www.cellular-news.com/story/54329.php>.

13. Anton A Huurdeman, *The Worldwide History of Telecommunications* (Hoboken, NJ: John Wiley & Sons, 2003), 91–146, 153–85. Ver também Jill Hills, "International Market Structure and the ITU," em *Telecommunications and Empire* (Champaign: University of Illinois Press, 2007) 91–116.

14. Edward Comor, "Communication Technology and International Capitalism: The Case of DBS and US Foreign Policy," in *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy*, ed. Comor (New York: St Martin's Press, 1994), 83–102.

15. Jill Hills, *The Struggle for Control of Global Communications: The Formative Century* (Champaign: University of Illinois Press, 2002.)

16. Parminder Jeet Singh, "India's Proposal Will Help Take the Web out of U.S. Control," *Hindu Online*, 17 May 2012, <http://www.thehindu.com/opinion/op-ed/article3426292.ece>.

17. Debora L. Spar, "National Policies and Domestic Politics," em *The Oxford Handbook of International Business*, ed. Alan M. Rugman (New York: Oxford University Press, 2008), 207.

18. *Ibid.*, 209.

19. Ibid., 212.

20. Richard C. Barth and Clint N. Smith, "International Regulation of Encryption: Technology Will Drive Policy," em *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, eds. Brian Kahin e Charles Nesson (Cambridge: MIT Press 1998), 283–99.

21. James Bamford, *The Shadow Factor: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2009). Ver também Claude Crépeau e Alain Slakmon, "Simple Backdoors for RSA Key Generation," em *CT-RSA'03: Proceedings of the 2003 RSA conference on the Cryptographers' Track* (Berlin: Springer-Verlag, 2003), 403–16; e Benjamin J. Romano, "Microsoft device helps police pluck evidence from cyberscene of crime," *Seattle Times*, 29 April 2008, http://seattletimes.nwsourc.com/html/microsoft/2004379751_msftlaw29.html

22. Ver Foreign Intelligence Surveillance Act, Electronic Communications and Privacy Act, and Communications Assistance for Law Enforcement Act.

23. Department of Commerce, *Management of Internet Names and Addresses*, 63 *Fed. Reg.* 31741 (1998).

24. DeNardis, *Protocol Politics*, 11.

25. Ver M. Ford, M. Boucadair, A. Durand, P. Roberts Issues with IP Address Sharing (Internet Engineering Task Force, RFC 6269) June 2011 <http://www.hjp.at/doc/rfc/rfc6269.html>

26. Ingrid Marson, "China launches largest IPv6 network," *CNET News*, 29 December 2004, http://news.cnet.com/China-launches-largest-IPv6-network/2100-1025_3-5506914.html

27. Sheila Frankel et al., *Guidelines for the Secure Deployment of IPv6* (Gaithersburg, MD: National Institute of Standards, December 2010).

28. Katherine Kebisek, "AFNIC prepares Air Force for IPv6 transition" Air Force Space Command(4 April 2011) <http://www.afspc.af.mil/news1/story.asp?id=123249968>

29. Este acordo foi renovado em 2 de julho de 2012: <http://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm>.

30. Robert E. Molyneux, *The Internet under the Hood: An Introduction to Network Technologies for Information Professionals* (Westport, CT: Libraries Unlimited, 2003), 86.

31. ICANN, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority," 1 March 2000, <http://www.icann.org/en/general/ietf-icann-mou-01mar00.htm>.

32. Elihu Zimet e Edward Skoudis, “A Graphical Introduction to the Structural Elements of Cyberspace,” in *Cyber Power and National Security*, 91–112. Ver também Molyneux, *Internet under the Hood*, 85–86.

33. Molyneux, *Internet under the Hood*, 27.

34. Os debates acerca da administração iniciaram há cerca de uma década e certamente continuarão. A próxima fase do *World Summit for the Information Society* será realizada em 2015.

35. H. Zhao, “ITU and Internet Governance—input to the 7th meeting of the ITU Council Working Group on WSIS, 12–14 December 2004,” <http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov02.doc>

36. Panayotis A. Yannakogeorgos, “Cyberspace: The New Frontier and the Same Old Multilateralism,” em *Global Norms, American Sponsorship, and the Emerging Pattern of World Politics*, ed. Simon Reich (New York: Palgrave, 2010).

37. “UN ICT Task Force Global Forum on Internet Governance to be Held in March,” Comunicado de imprensa pela ONU em Paris, 13 de fevereiro de 2004, http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html

38. “Global Internet Governance System is Working But Needs to Be More Inclusive, UN Forum on Internet Governance Told” Comunicado de imprensa pela ONU em Paris, 26 de março de 2004, <http://www.un.org/News/Press/docs/2004/pi1568.doc.htm>

39. Ibid.

40. “Statement by Mr. Dushyant Singh, Member of Parliament, on Agenda Item 16—Information and Communication Technologies for Development, at the 66th Session of the United Nations General Assembly on October 26, 2011,” <http://content.ibnlive.in.com/article/21-May-2012documents/full-text-indias-un-proposal-to-control-the-internet-259971-53.html>

41. A reação da China, Yang Yu, “Further Notice of Inquiry on the Internet Assigned Numbers Authority Functions,” China Organizational Name Administration Center (CONAC), http://www.ntia.doc.gov/files/ntia/conac_response_to_fnoi.pdf.

42. “Prime Minister Vladimir Putin meets with Secretary General of the International Telecommunication Union Hamadou Toure,” *Working Day*, 15 June 2011, <http://premier.gov.ru/eng/events/news/15601/>

43. UN General Assembly, “Enhanced Cooperation on Public Policy Issues Pertaining to the Internet,” Report of the Secretary-General, http://unctad.org/meetings/en/SessionalDocuments/a66d77_en.pdf.

44. Assinado pelos 178 países, o ITR é um acordo global empregado ao redor do mundo.

45. Isso é diferente do que Chris Demchak assinala em "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32–61.

46. US Department of State, Internet Freedom Fact Sheet (15 February 2011) <http://www.state.gov/r/pa/prs/ps/2011/02/156623.htm>.

47. Spencer Ackerman, "Does Obama's 'Net Freedom Agenda' Hurt the U.S.?" *Wired*, 28 January 2011, <http://www.wired.com/dangerroom/2011/01/does-obamas-internet-freedom-agenda-hurt-the-u-s-without-helping-dissidents/>.

48. Ye Tian, Ratan Dey, Yong Liu, Keith W. Ross, "China's Internet: Topology Mapping and Geolocating" <http://cis.poly.edu/~ratan/topologymappingchinainternetshort.pdf>
Cyrus Farivar, "Security researcher unearths plans for Iran's halal Internet" *Ars Technica* (17 April 2012).