MONÇÕES
Revista de Relações Internacionais da UFGD
ISSN 2316-8323

GOVERNANÇA DA INTERNET E SEGURANÇA CIBERNÉTICA NO BRASIL

INTERNET GOVERNANCE AND CYBER SECURITY IN BRAZIL

DANIEL OPPERMANN[1]
Doutor em Relações Internacionais pela UNB
E-mail: dan.oppermann@gmail.com

ABSTRACT: Internet Governance and cyber security are related to each other. This observation became clear already in the early days of international debates on Internet Governance which in the first decade of the 21st century were concentrated mainly around the United Nations Internet Governance Forum (IGF). Since then, a constantly growing number of stakeholders from several countries became involved in discussions concerning the Internet. Also in Brazil, there is a growing interest in Internet topics while the country sees increasing numbers of Internet users. However, besides higher user rates there has also been growing concerns regarding cyber security issues in the country. This article analyses the current situation of cyber security in Brazil and integrates the topic into the context of Internet Governance.

Keywords: Internet Governance, cyber security, Brazil

[1] Possui Mestrado em ciência política pela Universidade Livre de Berlim (FUB). Como diretor de uma empresa de TI em São Paulo e pesquisador da Universidade de São Paulo (USP) ele está constantemente observando e analisando os processos de governança da internet em vários países.

RESUMO: A governança da internet e a segurança cibernética estão relacionadas entre si. Essa observação ficou clara já nos primeiros dias dos debates internacionais sobre a governança da internet, que aconteceram durante a primeira década do século XXI principalmente em torno de Fórum de Governança da Internet (FGI) das Nações Unidas. Desde então, o número de atores de vários países envolvidos nos debates sobre a internet está cada vez maior. Também no Brasil o interesse nos tópicos relacionados à internet está aumentando e a quantidade de usuários está crescendo. Ao mesmo tempo, aumenta a preocupação com a segurança cibernética no país. Este artigo analisa a situação atual da segurança cibernética no Brasil e pretende enquadrar o assunto no contexto da governança da internet.

Palavras-chave: Governança da internet, segurança cibernética, Brasil

INTRODUÇÃO

Desde o início do Fórum de Governança da Internet das Nações Unidas (FGI) em 2006, a segurança cibernética era um dos temas centrais discutidos por uma variedade de atores interessados de países diferentes. Na literatura atual esse fenômeno raramente é analisado através do contexto Sul Americano. A maioria das contribuições é orientada pelos desenvolvimentos da América do Norte, da Ásia e da Europa enquanto os problemas e desafios na América do Sul (e especialmente no Brasil) são amplamente negligenciados. Além da pouca atenção que é dada à segurança cibernética na América do Sul, os poucos contribuintes ao debate (especialmente na mídia) estão frequentemente retratando a situação em uma forma menos objetiva e mais espalhafatosa, o que é contra-produtivo para um debate que, de fato, necessita de explicações ao invés de exageros. Sem dúvida a segurança cibernética, assim como outros temas de governança da internet são raramente discutidos entre a comunidade político-científica da América do Sul e também entre a população como um todo. A ideia

deste artigo é apresentar uma contribuição construtiva para informar o leitor interessado sobre os desenvolvimentos de segurança cibernética no Brasil e também estimular um debate que, na segunda década do século 21, mais de 20 anos após a transformação da internet em uma rede-comercial é definitivamente necessário.

GOVERNANÇA DA INTERNET

Desde o início do processo de governança da internet, o Brasil era constantemente envolvido nos debates globais e reuniões que tratavam da sociedade da informação e o desenvolvimento da internet. Em Novembro de 2007, a segunda reunião do FGI aconteceu no Rio de Janeiro. O FGI foi fundado durante a segunda reunião da Cúpula Mundial sobre a Sociedade da Informação (sigla em inglês: WSIS) em Tunis em 2005 (WSIS 2005, par. 72). Sua fundação foi baseada em uma recomendação do Grupo do Trabalho sobre Governança da Internet (sigla em inglês: WGIG), que foi fundado pelo Secretário-Geral das Nações Unidas, Kofi Annan para a discussão e desenvolvimento de estratégias que fortalecessem o debate sobre a governança da internet em uma escala global (WSIS 2003, C6 13b). O primeiro mandato do FGI aconteceu entre 2006 e 2010 (seguido pelo segundo mandato), quando um encontro anual[2] era conduzido para unir todo os grupos de atores interessados e discutir diversas questões que se desenvolveram em torno da internet nos anos e décadas anteriores, assim como os temas e desafios mais recentes da rede global de computadores. O FGI, assim como a maior parte das reuniões e processos sobre a governança da

2 Os encontros do primeiro mandato aconteceram na Grécia (2006), no Brasil (2007), na India (2008), no Egito (2009) e na Lituânia (2010). Os encontros do segundo mandato aconteceram até este momento no Quênia (2011), no Azerbaijão (2012) e na Indonésia (2013). O encontro de 2014 vai acontecer na Turquia.

internet, foi estabelecido a partir de uma abordagem de governança multissetorial, incluindo atores do setor público, do setor privado e da sociedade civil. A ideia básica dessa abordagem é reconhecer a diversidade de grupos de interesse e oferecer oportunidades para que todos podem se encontrar em um ambiente onde discussões e debates entre todos os atores se tornem possíveis em um nível horizontal e não-hierárquico.

A ABORDAGEM MULTISSETORIAL

O processo de governança da internet é um dos ambientes em que a abordagem multissetorial foi aplicada com sucesso no início do século XXI. Desde o papel importante de atores não–governamentais de ambos o setor privado e sociedade civil durante o processo do WSIS, o multissetorialismo se tornou a forma crucial de organização, também no processo do FGI. As razões porque essa abordagem se tornou popular dentro deste contexto podem ser encontradas no desenvolvimento histórico da internet e também nas mudanças de constelações da política global.

A internet teve início como uma rede de computadores criada por pesquisadores dos EUA em universidades diferentes e institutos de pesquisa nos anos 1960 (Kleinrock 2008, p. 10ff). Apesar de o projeto ter sido financiado pelo Departamento de Defesa dos EUA através da *Advanced Research Projects Agency* (ARPA) fundada em 1958, a motivação dos pesquisadores desenvolvendo redes não era de natureza militar. Em um tempo que o conhecimento era mantido em segredo pelos governos e serviços secretos, que temiam a vantagem de um adversário, os engenheiros de TI perceberam que compartilhar o conhecimento era de maior importância que esconde-lo. Por esse motivo eles estabeleceram uma rede que permitia acesso instantâneo a informações, livre de custo (com

exceção do equipamento técnico). A ideia de compartilhamento de informação se espalhou em um nível não-comercial em diversos países, apoiada basicamente por instituições acadêmicas. Em 1987 pesquisadores da Universidade de São Paulo (USP) decidiram promover a ligação de instituições acadêmicas brasileiras à rede internacional, que naquela época já era conhecida como a internet. Depois de uma primeira conexão a BITNET[3] ter sido estabelecida em 1988 no Laboratório Nacional de Computação Cientifica (LNCC) no Rio de Janeiro, a primeira conexão à internet aconteceu em 1991 na Fundação de Amparo à Pesquisa no Estado de São Paulo (FAPESP) (Stanton 1998). Naquele tempo quando o Brasil se tornou conectado à internet, a ideia não-comercial de compartilhamento de conhecimento ainda era um conceito dominante dos programadores envolvidos. No entanto, ao mesmo tempo os primeiros atores comerciais entravam em cenário nos EUA. Depois de Tim Berners-Lee ter desenvolvido a linguagem de programação HTML possibilitando o desenvolvimento de um ambiente amigável ao usuário, um número crescente de companhias reconheceu o potencial econômico que a internet iria implementar nos próximos anos. Fornecedores como Network Solutions Inc (NSI) começaram a lucrar com um número crescente de serviços (Mueller 2002, p. 105ff). Este avanço causou descontentamento, especialmente entre os criadores da internet, que viam a sua função em prestação de serviços em uma base não-comercial acima do que como um negócio lucrativo (Goldsmith; Wu 2006, p. 35f).

Durante os anos de 1990 o conflito entre os grupos de interesse aumentou quando o setor público também se uniu ao cenário. Como naquele tempo a maioria das discussões cruciais em relação a função e a administração da internet aconteceram no EUA, também foi o governo de Washington que se tornou o envolvido mais ativo entre os representantes do setor público. Esta influência

3 BITNET foi uma rede entre um número limitado de insitiuições em países diferentes nos anos 1980 e 1990.

precoce facilitou sua posição dominante na administração técnica da internet, que mais tarde foi criticada por diversos outros atores envolvidos no processo de governança da internet (Klein 2002, p. 201; Mueller 2005, p. 3). Especialmente na segunda metade dos anos 90, mais governos se interessaram pela internet, fortalecendo a posição do setor público no ambiente de governança da internet. A constelação de atores neste contexto é exemplara para o ambiente multissetorial em geral. A coexistência de governos (como representantes de estados-nação), companhias privadas (fornecendo capital de investimento) e da sociedade civil (trazendo conhecimento especializado e representando interesses de usuários) pode ser também observada em outros processos de governança como na Conferência Internacional sobre o Financiamento do Desenvolvimento (Monterrey, México) ou na Cúpula Mundial sobre Desenvolvimento Sustentável (Joanesburgo, África do Sul) que aconteceram ambos em 2002.

Independente do processo de governança da internet, as mudanças das constelações globais também favoreceram a proliferação do modelo multissetorial especialmente depois do fim da Guerra Fria. Enquanto durante as décadas do conflito leste-oeste o problema da segurança dominava os debates e negociações internacionais, o fim da confrontação entre os blocos nos anos 90 possibilitou a aparição de questões que vinham sendo ignoradas pelos governos nos anos antecedentes. Entre elas estavam temas como direitos da minorias, questões ambientais ou desenvolvimento sustentável, em sua maior parte áreas em que os atores da sociedade civil haviam se comprometido há anos e na qual eles obtinham um alto grau de experiência (Fues; Hamm 2001, p. 54). Durante a Conferência das Nações Unidas sobre o Meio Ambiente e o Desenvolvimento que aconteceu no Rio de Janeiro em 1992, um grande número de atores da sociedade civil foi convidado a participar, pela primeira vez em um processo internacional que anos antes era dominado por governos nacionais (Dodds 2002, p. 28).

E a participação do setor privado também cresceu ao longo dos anos, impulsionado pela necessidade de apoio financeiro por uma variedade de programas novos que haviam entrado na agenda internacional. Ao apresentar o Pacto Global em 1999, um programa de cooperação entre as Nações Unidas e companhias privadas, Kofi Annan incluiu o setor privado em uma variedade de questões na agenda internacional (Kell; Ruggie 1999, p. 103). Nesse contexto, a convergência de diferentes grupos de interesse no processo de governança da internet no início do século XXI estava refletindo um desenvolvimento que acontecia globalmente em numerosos processos de governança ao mesmo tempo.

SEGURANÇA CIBERNÉTICA

O processo de governança da internet relatado ao FGI foi de início organizado em uma estrutura clara de tópicos, sendo eles: acesso, diversidade, abertura e segurança. Nos anos seguintes, recursos críticos da internet foram acrescentados à agenda anual (Kleinwächter 2007, p. 16ff). Ao olhar mais de perto aos temas diversos sendo trabalhados, torna-se claro que uma certa parte do debate sobre a proteção dos recursos críticos da internet coincide com o debate sobre a segurança cibernética. Recursos críticos da internet são frequentemente definidos como as partes da infra-estrutura da rede que mantém a internet em funcionamento, sendo especialmente partes técnicas como a Autoridade para Atribuição de Números da Internet (sigla em inglês: IANA) e o Sistema de Nomes de Domínios (sigla em inglês: DNS) ou o próprio Sistema de Servidores-Raiz. Outros incluem também os Registros Regionais da Internet (sigla em inglês: RIR) (Mueller 2010). A definição de WGIG de recursos críticos da internet é:

> resources, including administration of the domain name system and Internet protocol addresses (IP addresses), administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovate and convergent technologies, as well as multilingualization. (WGIG 2005, p. 5)

No entanto, de acordo com Vint Cerf, programador do TCP/IP, antigo presidente do conselho de diretores da ICANN e desde 2005 vice-presidente do Google também existem outros componentes importantes que fazem parte da lista de recursos críticos da internet que são pessoas e conhecimento:

> [...] people play a critical role in the well-being and evolution of the Internet. Without skilled programmers, engineers, operators, equipment makers, application designers, enlightened governmental policymakers, thoughtful legal practitioners, effective and innovative business leaders, researchers, teachers and knowledgeable users, the Internet would not be the remarkable global engine of innovation and utility that it has become. Any consideration of critical Internet resources must take into account the wide range of people resources that are needed to keep the Internet operating and evolving in productive directions. (Cerf, 2007, p. 209).

E Geoff Huston do *Asia-Pacific Network Information Centre* (APNIC) destacou em um artigo de CircleID que os recursos mais críticos da internet são simplesmente "users like you and me" (Huston, 2007).

Ao observar o nível técnico, há uma série de recursos críticos da internet no Brasil que necessitam que seu funcionamento seja garantido para manter a rede trabalhando. Entre eles estão os servidores raiz, que estão localizados em cidades como Brasília, Curitiba, Florianópolis, São Paulo e outras. Os servidores raiz estão no topo da hierarquia do DNS e permitem a comunicação entre

computadores e redes diferentes. Apesar de todos os 13 operadores de servidores raiz estarem localizados fora do Brasil, também é mantida uma série de servidores no país para facilitar o acesso ao serviço do DNS. Além disso o domínio de topo de código de país (sigla em inglês: ccTLD) .br administrado pelo Comitê Gestor da Internet no Brasil (CGI) também é um recurso crítico da internet. O CGI, uma entidade organizada de forma multissetorial, fundado pelo governo em 1995 para administrar e investigar o desenvolvimento da internet no Brasil, é responsável pela coordenação de números de IP no Brasil e pela distribuição de nomes de domínio sob o ccTLD nacional (Ministério das Comunicações 1995). É registrado na IANA como a organização administrativa oficial de ccTDL do Brasil.

Outros recursos críticos da internet importantes são os Pontos de Troca de Tráfego (PTT). PTTs são centros de processamento de dados nos quais os provedores de rede se conectam a outras redes para troca de dados. Dessa maneira os usuários têm acesso a todos os servidores e redes conectados à internet a um custo menor. De forma alternativa, as redes poderiam se conectar umas às outras através de redes terceiras, que demonstra um custo mais dispendioso para os usuários. Os PTTs têm uma alta importância para o funcionamento da internet, já que sua ausência não só causa custos altos para os provedores e usuários, mas também interfere na velocidade do fluxo de informação. Com freqüência a falta de PTTs força os provedores de rede a enviarem suas informações a outros países para a troca de dados com outras redes. Em 2012 o projeto *PTTMetro* do CGI dava suporte aos PTTs em 20 grandes cidades do Brasil. Outros 40 locais estavam sendo analisados para estabelecer mais PTTs[4]. Um estudo de 2012 da *Internet Society* (ISOC) mostrou os efeitos

4 Pela página http://www.ptt.br o CGI está divulgando as informações atualizadas em relação à situação dos PTTs no Brasil.

positivos dos PTTs em relação ao desenvolvimento de mercados crescentes da internet (Kende; Hurpy 2012).

Além de recursos técnicos também existem, como já citado anteriormente, pessoas como um recurso crítico para o desenvolvimento e funcionamento da internet. Os usuários comuns, em especial, têm um papel importante, também relativo a questões de segurança. A internet como ela existe hoje é um produto de milhões de contribuições feitas individualmente. Além de centros de dados e prestadores de serviços, a proteção de cada computador em casa e no trabalho é portanto um aspecto central de segurança cibernética a nível nacional e internacional. Em 2011 foram reportados aproximadamente 400.000 incidentes de segurança cibernética ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT). Comparado aos dados de 2006 isso significa um aumento de mais que 100% em cinco anos (CERT 2012). Como os casos são relatados de forma voluntária, é muito provável que o número real de incidentes seja muito maior. Incidentes cibernéticos direcionados a usuários são em maior parte relacionados a malware de diversos tipos com intenção de cometer fraudes, furto de identidade, furto de senhas (também conhecido como *phishing*) e também a intrusão em redes e computadores vem acontecendo com frequência. Enquanto todos esses acontecimentos fazem com que usuários se tornem vítimas de ataques cibernéticos, que com frequência se encaixa na categoria de crime cibernético, os usuários podem também tornar-se co-autores de outros ataques sem sequer se dar conta do fato. Embora as obstruções e prejuízos deixados pelos ataques cibernéticos mais intensos dos anos passados na Estônia (2007) e na Geórgia (2008) estejam geograficamente distantes da América do Sul, é óbvio que os computadores e redes brasileiros estavam envolvidos nestes incidentes ou em outros similares. Ataques Cibernéticos como estes acontecem como ataques distribuídos de negação de serviço (sigle em

inglês: DDoS) que necessitam de uma alta quantidade de computadores para seu sucesso.

Ataques DDoS são formas comuns de desativar uma rede escolhida por um determinado período de tempo. Em Geórgia ocorreu paralelamente à invasão militar da Rússia no conflito na Ossétia do Sul. Na Estônia, aconteceu durante as tensões políticas entres russos e estonianos causadas por conflitos nacionalistas (Oppermann 2010). O objetivo de um ataque DDoS é enviar uma quantidade enorme de solicitações a uma rede ao mesmo tempo que consequentemente causa um colapso da rede ou do servidor. Para alcançar esse objetivo milhares de solicitações devem ser agrupadas, o que acontece através das *botnets* (Feily; Ramadass; Shahrestani 2009). Botnets são computadores conectados de forma não legítima e são operados por uma só pessoa conhecida como o *bot herder*. Mandando códigos maliciosos (por exemplo pelo spam) o bot herder tem acesso a computadores de toda a parte do mundo, que formam sua botnet. Ao longo dos anos um negócio lucrativo se desenvolveu em torno das botnets. Criminosos cibernéticos ou atacantes motivados por esquemas políticos que necessitam de uma botnet grande em algum período de tempo para lançar um ataque ou conduzir atividades criminosas no espaço cibernético alugam botnets que são oferecidos no espaço cibernético pelos bot herders profissionais. Esses bot herders também estão utilizando redes e computadores pouco protegidos no Brasil para condução de ataques cibernéticos ou atividades de crime cibernético no Brasil e em outros países. O fato de redes brasileiras estarem envolvidas nestas atividades não encaminha diretamente à conclusão de que os bot herders em si estão localizados no país. Um bot herder pode operar sua botnet de qualquer lugar do mundo. O aspecto crucial para o Brasil é que é um dos países mais afetados do mundo em relação às botnets. Segundo analistas de segurança de TI da Microsoft, Symantec, e Trend Micro, redes brasileiras têm uma das maiores taxas de infecção por malware no mundo (Microsoft 2011; Symantec 2011; Trend

Micro 2010). Como conseqüência, o Brasil tem a segunda maior concentração de infecções de botnets no mundo (Symantec 2011, p. 6). Uma razão importante para isto pode ser encontrada na alta taxa de crescimento de usuários da internet nos últimos anos combinado com o baixo nível de proteção pelos usuários (geralmente por falta de conhecimento).

CRESCIMENTO DA INTERNET E AMEAÇAS CIBERNÉTICAS

O crescimento econômico no Brasil se ligou a um aumento constante em relação à quantidade de usuários da internet e à velocidade da internet nos últimos anos. Segundo uma análise do CGI, 46% de todos os domicílios no Brasil tinham um computador em 2012 (CGI 2013, p. 457). A maior parte deles também tinha conexão à internet, formando 40% de todos os domicílios. 51% da população brasileira era considerada usuário da internet.

Proporção de domicílios com computador - Total Brasil (%)

Ano	%
2008	25
2009	32
2010	35
2011	45
2012	46

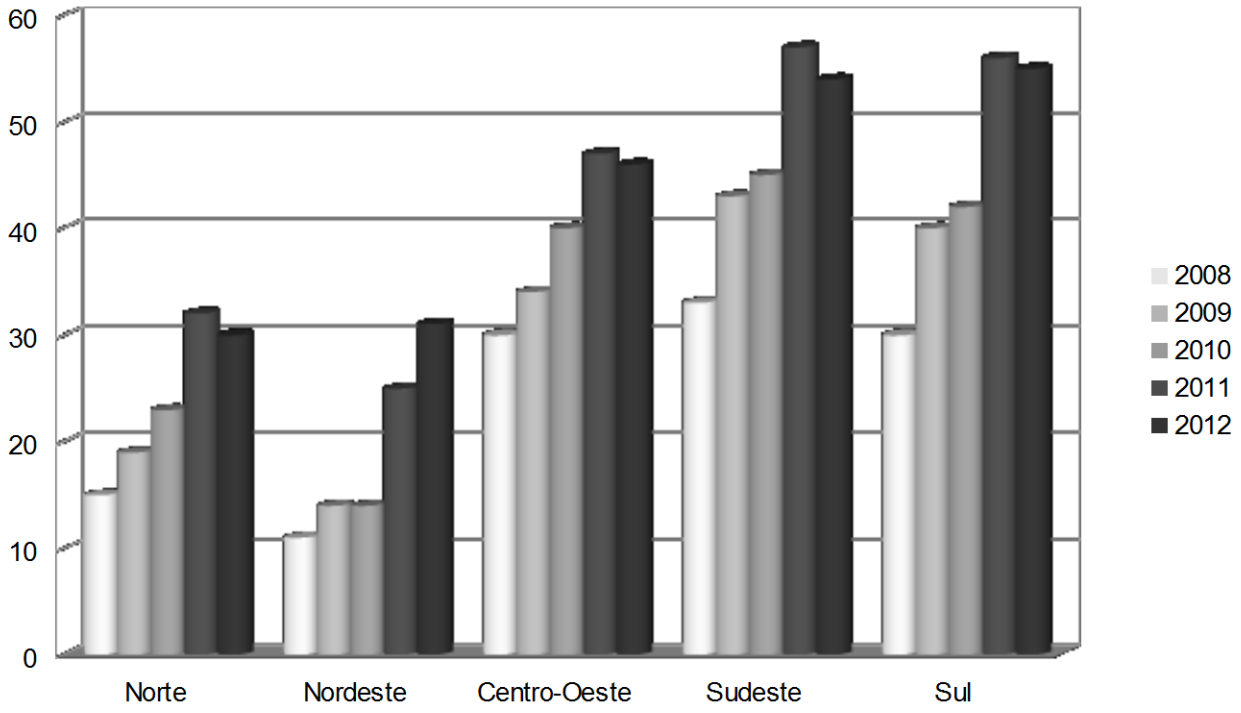
Fonte: CGI

Proporção de domicílios com computador, por região - Total Brasil (%)

	Norte	Nordeste	Centro-Oeste	Sudeste	Sul
2008	15	11	30	33	30
2009	19	14	34	43	40
2010	23	14	40	45	42
2011	32	25	47	57	56
2012	30	31	46	54	55

Fonte: CGI

Proporção de domicílios com computador, por região - Total Brasil (%)



Fonte: CGI

Proporção de domicílios com acesso à internet – Total Brasil (%)

Ano	%
2008	18
2009	24
2010	27
2011	38
2012	40

Fonte: CGI

Desde que o CGI começou a publicar as informações de pesquisa em 2005, um aumento contínuo de usuários da internet pode ser observado. Para apoiar esse desenvolvimento e especialmente para trazer aqueles com um poder aquisitivo menor para o mundo virtual, o governo desenvolveu uma série de programas para facilitar a aquisição do equipamento de TI, para a conexão de escolas e para a extensão de acesso a conexões de banda larga. Em 2010 a banda larga era a forma mais importante de acesso à internet no Brasil. A conexão discada estava em constante declínio e quase alcançou figuras em uma posição tão baixa como o acesso móvel (CGI 2011, p. 146f). Ao implementar o Programa Nacional de Banda Larga (PNBL) o governo planejou conectar até 40 milhões de domicílios e pequenas empresas adicionais à internet através da banda larga até 2014 (Presidência da República 2010; Senado Federal 2011). O PNBL pode diminuir a exclusão digital e expandir o número de usuários da internet no Brasil, especialmente em áreas rurais onde o acesso à internet é mais caro do que em centros urbanos, enquanto o salário médio é menor do que nos centros. Ao

mesmo tempo estes 40 milhões de novas conexões da internet são capazes de piorar a segurança das redes brasileiras, já que entre estes mais de 40 milhões de novos usuários apenas uma pequena porcentagem estará preparada para se proteger da variedade de ameaças cibernéticas que se espalham pelas redes do país já da data atual. O alto nível de computadores infiltrados que colocam o Brasil na liga de países mais afetados por atividades maliciosas é causado pela alta velocidade de novos computadores conectados à internet combinado com a insuficiência de preparo da comunidade de usuários. Apesar de usuários mais frequentes da internet estarem cientes da existência de malware (frequentemente resumidos erroneamente como "vírus") raramente há um conhecimento mais profundo relacionado às possibilidades destes programas afetarem o funcionamento da internet. Dessa forma, um simples clique em uma rede social ou em um e-mail pode entregar um computador em casa, no trabalho ou na escola a um bot herder ou a outro tipo de criminoso cibernético e acabar como um componente em um sistema de amplitude nacional de fraudes bancárias on-line ou um conflito internacional em qualquer parte do planeta.

Além dos riscos para o usuário comum, também o setor público e o setor privado sofrem de grandes dimensões de insegurança no espaço cibernético brasileiro. Como o problema foi amplamente ignorado, não há informações disponíveis em relação a, por exemplo, perdas financeiras em relação a ameaças cibernéticas no setor econômico privado do Brasil. De fato, poucas companhias publicam tais informações simplesmente para não expor sua própria vulnerabilidade ao resto do mundo provocando falta de confiança e portanto evitando uma maior perda financeira. No entanto, dados dos EUA demonstram que a insegurança no espaço cibernético é um problema concreto para a economia privada e causa perdas anuais de milhões de dólares dependendo do tamanho da empresa e dos ataques que elas sofrem (Ponemon 2011). Da mesma forma a economia brasileira está investindo milhões de reais todos os anos para

proteger suas empresas de invasores online. E não somente as grandes empresas sofrem com ameaças virtuais. Negócios pequenos e médios também estão sofrendo ataques on-line. Estas empresas em especial enfrentam problemas de estabelecer um orçamento suficiente para proteger suas redes e computadores.

O grau em que o setor público foi afetado por ataques cibernéticos foi ocultado (ou ignorado) pelo governo nos últimos anos até que uma série de eventos deixou claro que a segurança cibernética era uma questão séria que precisava ser considerada com mais cuidado. Em 2011 uma onda de ataques cibernéticos no Brasil causou invasões de redes imensos (especialmente *web defacements*[5]) em uma série de sites importantes, entre eles ministérios, o senado, universidades e a Receita Federal (Oppermann 2011). Nos anos antecedentes observações ocasionais feitas por analistas políticos considerando a possibilidade de que ataques cibernéticos serem responsáveis por uma série de apagões entre 2005 e 2009 (o que foi negado por parte do governo) e tentativas de extorsão de instituições públicas por hackers (o que foi confirmado por parte do governo) acompanhavam o início de um discurso mais ou menos público sobre a segurança cibernética no Brasil e apoiavam os defensores de uma estratégia de segurança cibernética nacional que foi então levada a caminhar e teve sua primeira versão publicada em 2010 (Rodrigues 2009; Soares 2009).

ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA NACIONAL

Em dezembro de 2010 o Departamento de Segurança da Informação e Comunicações (DSIC) no Gabinete de Segurança Institucional da Presidência da República (GSI/PR) publicou o Livro Verde de Segurança Cibernética no Brasil (Mandarino 2010). Ao fazer isso, o Brasil deu um primeiro passo em uma forma importante de proteção de sua rede de computadores nacionais contra formas

5 Web defacements são atos em que um invasor manipula o visual de uma página incluindo imagens ou textos próprios.

diferentes de ameaças cibernéticas. O objetivo do Livro Verde era a apresentação de um primeiro conceito do que mais tarde viria a se tornar uma estratégia completa chamada Política Nacional de Segurança Cibernética. Segundo recomendações internacionais o DSIC compreende segurança cibernética como um desafio transfronteiriço e internacional ao invés de apenas uma questão exclusivamente nacional.

Portanto o Livro Verde se refere a numerosas estratégias internacionais em maior parte de organizações internacionais como a Organização dos Estados Americanos (OEA), a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a União Internacional de Telecomunicações (UIT) e outras (idem, p. 20ff). Além disso, o DSIC também segue a abordagem multissetorial ao sublinhar a importância da inclusão de atores diferentes da sociedade no processo de desenvolvimento de uma estratégia nacional, que é crucial para alcançar resultados mais efetivos. Neste contexto, o Livro Verde se refere principalmente aos cinco atores principais sendo o governo, o setor privado, academia, o terceiro setor e a sociedade (idem, p. 14). A cooperação desses atores é aspirada nas áreas de políticas e estratégicas, economia, aspectos sociais, ciência, tecnologia & inovação (CT&I), educação, problemas legais, cooperação internacional e segurança das infraestruturas críticas. Aqui é importante diferenciar entre infraestruturas críticas como mencionada no Livro Verde e recursos críticos da internet, como citados acima. A infraestrutura crítica tem um significado mais amplo do que recursos críticos da internet, incluindo energia, transporte, água, telecomunicações, finanças, informação e mais. É definida no Livro Verde como "instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade." (idem, p. 19). Quando se compara a definição anteriormente citada de recursos críticos da internet (em especial a definição sobre as partes técnicas) à definição de

infraestrutura crítica, se torna claro que os recursos críticos da internet são parte da infraestrutura crítica de todos os países. Entre as estratégias de segurança cibernética desempenham um papel central. Por outro lado, obviamente há muito mais em relação à segurança cibernética do que a proteção da infraestrutura técnica.

Não é sem motivo que o fator humano é considerado a parte mais fraca em qualquer ambiente de segurança cibernética (Tech Journal 2011). Como já citado, as botnets e seus resultados (como os ataques DDoS) estão intimamente ligados às lacunas de segurança causadas pelo usuário comum. Como o Brasil tem uma das mais altas concentrações de botnets no mundo, é obvio que as abordagens de segurança incluindo o comportamento do consumidor devem ser uma parte central da estratégia de segurança cibernética brasileira. No Livro Verde o fator humano é considerado diretamente e indiretamente em vários momentos. De forma direta acontece na secção de educação que refere-se a alguns desafios para incluir questões de segurança cibernética nos ambientes de educação básica e superior. Além disso, o Livro Verde introduz as ideias de uma cultura e conscientização nacional de segurança cibernética entre usuários de todas as idades e classes sociais (Mandarino 2010, p. 45). Essa ideia é de grande importância já como a segurança cibernética não pode ser alcançada apenas ao treinar profissionais de TI para proteger pontos estratégicos da infraestrutura nacional. Apesar de isso ser, sem dúvida, também um aspecto muito importante. No entanto, um grande número de ataques cibernéticos (incluindo atividades de criminosos cibernéticos) está acontecendo no nível do usuário privado. De fato, uma variedade de ataques cibernéticos em pontos estratégicos da infraestrutura de telecomunicação nacional e em outras partes da infraestrutura crítica são conseqüências lógicas de ataques cibernéticos que aconteceram em um nível privado anteriormente. O fechamento temporário de serviços públicos e privados pelos ataques DDoS só são possíveis devido a milhares de redes e computadores

que foram infiltrados anteriormente. Por essa razão, o desenvolvimento de uma estratégia de sensibilização é essencial. Especialmente á luz de um crescente aumento de usuários da internet esperado.

O fator humano também é levado em consideração em outras partes do Livro Verde além da educação. Na verdade, em todas as secções mencionadas existem diretivas referentes à necessidade de profissionais treinados para o estabelecimento de órgãos coordenadores como na área de decisão estratégica, a preparação de representantes da economia do setor privado para o desenvolvimento de um ambiente de comércio on-line seguro, a especialização de pesquisadores para investigação da segurança cibernética e criação de soluções, a formação de profissionais para monitoria e resposta de ataques cibernéticos e mais (idem, p. 43ff). Essa necessidade amplamente citada de profissionais preparados e educação da comunidade de usuários destaca um problema fundamental: a falta de conhecimento em relação à segurança cibernética.

Depois da publicação do Livro Verde o DSIC abriu uma discussão pública e convidou diversos grupos de interesse para comentar a edição antes de se tornar um estratégia nacional. Ao fazê-lo, também seguiram as necessidades básicas de uma abordagem multissetorial para o desenvolvimento de um ambiente estável no qual todos os atores teriam seus próprios interesses considerados, sendo esses em especial do setor público, da economia privada e da sociedade civil. No entanto, deve ser mencionado que até agora o debate sobre segurança cibernética é dominado pelo setor público. No Brasil ainda falta uma representação forte nessa área, especialmente na sociedade civil. Há poucas organizações oriundas deste setor da sociedade com envolvimento ativo nos debates. Enquanto o setor privado demonstra grande interesse na segurança cibernética para proteger seus próprios negócios e estruturas financeiras, a

maioria das organizações da sociedade civil no Brasil é mais relutante quando se trata da inclusão de segurança cibernética em sua agenda. No entanto, há uma necessidade crescente de se ter a participação de atores do terceiro setor nos debates. Especialmente porque os regulamentos de segurança cibernética normalmente afetam os direitos do consumidor, a liberdade de expressão, a privacidade e outros tópicos que também devem ser protegidos pela sociedade civil (Deibert 2011). Como mostraram as campanhas em relação aos regulamentos dos EUA PIPA e SOPA em janeiro de 2012, decisões tomadas em outros países podem ter influência nos direitos do usuário no Brasil. A participação de uma grande quantidade de indivíduos nos protestos contra PIPA/SOPA (principalmente por mídias sociais como Facebook e Twitter) mostra que há uma crescente consciência por parte dos usuários de internet no Brasil em relação às políticas da internet. Apesar de PIPA/SOPA não serem tópicos comuns de segurança cibernética, eles definitivamente marcaram um passo importante para a participação da sociedade civil brasileira em questões globais da internet, às quais se inclui a segurança cibernética. A (re)fundação do capítulo brasileiro da ISOC que teve sua primeira assembleia geral ordinária em São Paulo em Fevereiro de 2012[6] também é um passo crucial para o fortalecimento da sociedade civil da internet no Brasil que precisa (e provavelmente irá) considerar questões de segurança cibernética. No fim, a segurança cibernética não é um problema que pode ser deixado apenas para o setor público e atores tradicionais de segurança como polícia e o corpo militar que já tinha estabelecido em agosto de 2010 seu Centro de Defesa Cibernética do Exército (CDCiber) baseado na portaria nº 666, 4 agosto 2010. Assim como todos os temas da esfera da governança da internet a segurança cibernética também exige uma contribuição de todos os setores da sociedade.

6 Em 1998 já havia a fundação de um escritório da ISOC no Brasil, que mais tarde se tornou inativo.

CONCLUSÃO

Desde que em 2006 o FGI posicionou a segurança cibernética como um dos temas centrais da agenda de governança da internet, tem sido dada uma atenção crescente a esse fenômeno em diversos países. O Brasil também começou a se conscientizar da necessidade de discutir os problemas de redes de informação desprotegidas e a dar os passos necessários para proteger suas redes. Um aspecto importante é perceber que a segurança cibernética não é um problema inteiramente técnico e portanto não pode ser resolvido apenas por engenheiros de TI. Também não é uma questão que pode ser resolvida por governos ou forças de segurança mas necessita de esforços de diversos atores da sociedade. É uma questão de formar uma consciência e uma atenção publica na comunidade usuária, que tem crescido em uma taxa impressionante no Brasil nos últimos anos. Ao encorajar grande parte da população a entrar on-line o governo brasileiro está ao mesmo tempo melhorando o desenvolvimento da sociedade de informação e observando a formação de milhões de novos pontos de acesso mal protegidos utilizados por milhões de usuários inadequadamente preparados que podem se tornar vítimas e também participantes nos crimes cibernéticos ou outras atividades maliciosas na internet. O desenvolvimento de uma estratégia de segurança cibernética nacional como iniciada pelo Departamento de Segurança da Informação e Comunicações é um passo importante em direção à proteção de redes de informação e de usuários da internet. Mais uma vez, é necessário destacar que a estratégia do governo não pode se limitar à proteção da infraestrutura crítica de natureza técnica, mas também precisa considerar os usuários como parte fundamental. E na verdade há uma série de passagens no Livro Verde que consideram a necessidade de se desenvolver programas educacionais para usuários de todas as idades e classes

sociais. Nesse contexto é dada uma atenção especial à criação de um programa de conscientização nacional sobre segurança cibernética que poderia contribuir para o desenvolvimento de uma consciência entre a população e especialmente entre os usuários da internet. Além disso, uma série de sugestões é feita para aprimorar a situação de usuários profissionais, que quer desenvolver treinamento e programas de instrução para especialistas de TI com foco em questões de segurança cibernética. Seguindo a abordagem multissetorial o Livro Verde também foi aberto a comentários feitos por qualquer dos grupos de interesse. No entanto, após esse processo de discussão que até agora levou mais de três anos, a estratégia final de segurança cibernética ainda não foi publicada (fevereiro de 2014). Por outro lado, como o Brasil está entre os países do mundo mais infectados por malware e tem um problema sério com as botnets, o governo precisa muito continuar o processo de recaptura das partes de redes nacionais que já estão sob o controle de criminosos cibernéticos. Mas não só o setor público precisa reconhecer sua importância nesse contexto, também a sociedade civil precisa começar a expandir suas atividades relacionadas a questões de segurança cibernética. Especialmente grupos da sociedade civil organizada precisam tomar posições para defender os direitos dos usuários contra possíveis restrições que vão aparecer por parte do governo nos próximos anos. Uma conscientização crítica entre a população não pode ser reduzida a restrições estrangeiras como o SOPA/PIPA, e precisa também considerar desenvolvimentos dentro do país.

BIBLIOGRAFIA

BRASIL – PRESIDÊNCIA DA REPÚBLICA. Decreto N. 7175, Casa Civil, Subchefia para Assuntos Jurídicos, 12 maio 2010. Disponível em: http://bit.ly/cvgQEq. Acesso em: 24 de janeiro de 2014.

BRASIL – MINISTÉRIO DAS COMUNICAÇÕES, Gabinete do Ministro, Portaria Interministerial N° 147, 31 maio 1995. Disponível em: http://bit.ly/I29qAN. Acesso em: 24 de janeiro de 2014.

BRASIL – SENADO FEDERAL. Banda larga chegará a 40 milhões de domicílios até 2014, prevê Paulo Bernardo, Portal de Notícias, 31 agosto 2011. Disponível em: http://bit.ly/IAVhNm. Acesso em: 24 de janeiro de 2014.

CERT. Estatísticas dos Incidentes Reportados ao CERT.br, 1999 a março 2012. Disponível em: http://bit.ly/58IS48. Acesso em: 24 de janeiro de 2014.

CGI. TIC: Domicílios e Empresas 2010, Comitê Gestor da Internet no Brasil, São Paulo, 2011. Disponível em: http://bit.ly/vdo1Ic. Acesso em: 24 de janeiro de 2014.

CGI. TIC: Domicílios e Empresas 2011, Comitê Gestor da Internet no Brasil, São Paulo, 2012. Disponível em: http://bit.ly/1ejzEfE. Acesso em: 24 de janeiro de 2014.

CGI. TIC: Domicílios e Empresas 2012, Comitê Gestor da Internet no Brasil, São Paulo, 2013. Disponível em: http://bit.ly/1ejzEfE. Acesso em: 24 de janeiro de 2014.

CERF, Vint. Critical Internet Resources – A Private Sector Perspective, em: Kleinwächter, Wolfgang: The Power of Ideas. Internet Governance in a Global Multi-Stakeholder Environment, Marketing für Deutschland GmbH, Berlin, 2007, pp. 208-214.

DEIBERT, Ron. Towards a cyber security strategy for global civil society? Global Information Society Watch, 2011. Disponível em: http://bit.ly/IcI3Yu. Acesso em: 24 de janeiro de 2014.

DODDS, Felix. The Context: Multi-Stakeholder Processes and Global Governance, in: Hemmati, Minu: Multi-Stakeholder Processes for Governance and Sustainability, Earthscan, London 2002, pp. 26-38.

FEILY, Maryam; RAMADASS, Sureswaran; SHAHRESTANI, Alireza. A Survey of Botnet and Botnet Detection, Securware, 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 268-273.

FUES, Thomas; HAMM, Brigitte I. Die Weltkonferenzen der 90er Jahre: Baustellen für Global Governance, Dietz, Bonn, 2001.

GOLDSMITH, Jack; WU, Tim. Who Controls the Internet? Oxford University Press, New York, 2006.

HUSTON, Geoff. On the Hunt for "Critical Internet Resources", CircleID, 12 Nov 2007. Disponível em: http://bit.ly/Idprq2. Acesso em: 24 de janeiro de 2014.

KELL, Georg; RUGGIE, John Gerard. Global markets and social legitimacy: the case for the 'Global Compact', Transnational Corporations, Vol 8, No 3, December 1999, pp. 101-120. Disponível em: http://bit.ly/w2nsKy. Acesso em: 24 de janeiro de 2014.

KENDE, Michael; HURPY, Charles. Assessment of the Impact of Internet Exchange Points - Empirical Study of Kenya and Nigeria, Internet Society, April 2012. Disponível em: http://bit.ly/JbE1Oj. Acesso em: 24 de janeiro de 2014.

KLEIN, Hans. ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy, The Information Society, 18, 2002, pp. 193-207. Disponível em: http://bit.ly/rOQwe2. Acesso em: 24 de janeiro de 2014.

KLEINROCK, Leonard. History of the Internet and its Flexible Future, IEEE Wireless Communication, February 2008. Disponível em: http://scr.bi/sYzMoh. Acesso em: 24 de janeiro de 2014.

KLEINWÄCHTER, Wolfgang. The Power of Ideas. Internet Governance in a Global Multi-Stakeholder Environment, Marketing für Deutschland GmbH, Berlin, 2007.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. Livro Verde: Segurança Cibernética no Brasil, Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, Brasília 2010. Disponível em: http://bit.ly/e5Iif8. Acesso em: 24 de janeiro de 2014.

MICROSOFT. Security Intelligence Report, Volume 12, July-December 2011. Disponível em: http://bit.ly/4fxWfo. Acesso em: 24 de janeiro de 2014.

MUELLER, Milton *et al*. Political Oversight of ICANN: A Briefing for the WSIS Summit, Concept Paper by the Internet Governance Project, 1 November 2005. Disponível em: http://bit.ly/ulRsDG. Acesso em: 24 de janeiro de 2014.

MUELLER, Milton. Ruling The Root, Internet Governance and the Taming of Cyberspace, MIT Press, Cambridge 2002.

OPPERMANN, Daniel. Entre hackers e botnets: a segurança cibernética no Brasil, Boletim OPSA, No 2, abril/junho 2011, pp. 12-16. Disponível em: http://bit.ly/tqsqQD. Acesso em: 24 de janeiro de 2014.

OPPERMANN, Daniel. Virtual attacks and the problem of responsibility: the case of China and Russia, em: Carta Internacional, Núcleo de Pesquisa em Relações Internacionais, Universidade de São Paulo, Vol. 5, No 2, Dez 2010, pp 11-25. Disponível em: http://www.usp.br/nupri/. Acesso em: 24 de janeiro de 2014.

PONEMON INSTITUTE. Second Annual Cost of Cyber Crime Study, August 2011. Disponível em: http://bit.ly/pftNlW. Acesso em: 24 de janeiro de 2014.

RODRIGUES, Fernando. Hacker troca senha de servidor de um ministério e exige US$ 350 mil, Folha de São Paulo, 8 de novembro de 2009.

SOARES, Marcelo. Brazilian Blackout Traced to Sooty Insulators, Not Hackers, Wired.com, 9 November 2009. Disponível em: http://bit.ly/1c3Frl. Acesso em: 24 de janeiro de 2014.

STANTON, Michael A. A Evolução das Redes Acadêmicas no Brasil: Parte 1 - da BITNET à Internet (1987 a 1993), RNP News Generation, Rio de Janeiro, RJ, v. 2, n. 6, 1998. Disponível em: http://bit.ly/JNeLhF. Acesso em: 24 de janeiro de 2014.

SYMANTEC. Symantec Intelligence Quarterly, July-September 2011. Disponível em: http://bit.ly/IQox12. Acesso em: 24 de janeiro de 2014.

TECH JOURNAL. Cyber security must focus on users, not just attackers, 29 November 2011. Disponível em: http://bit.ly/JNLV0t. Acesso em: 24 de janeiro de 2014.

TREND MICRO. TrendLabs. Global Threat Trends 1H 2010. Disponível em: http://bit.ly/JcRlya. Acesso em: 24 de janeiro de 2014.

WGIG: Report of the Working Group on Internet Governance, Château de Bossey, June 2005. Disponível em: http://bit.ly/dxGmEp. Acesso em: 24 de janeiro de 2014.

WSIS: Geneva Plan of Action, WSIS-03/GENEVA/DOC/5-E, 12 December 2003. Disponível em: http://bit.ly/vNs6xW. Acesso em: 24 de janeiro de 2014.

WSIS: Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 November 2005. Disponível em: http://bit.ly/tAnjdR. Acesso em: 24 de janeiro de 2014.

Recebido em 05 de março de 2014

Aceito em 24 de março de 2014