Segurança cibernética: o desafio da nova Sociedade da Informação

Claudia Canongia[1] & *Raphael Mandarino Junior*[2]

Resumo

O artigo introduz o tema da segurança cibernética, sua importância no cenário atual, e os desafios da nova Sociedade da Informação, que tem a revolução tecnológica e a inovação como fatores críticos de desenvolvimento. Apresenta quadro resumo da estratégia nacional de segurança cibernética dos EUA e do Reino Unido como visão panorâmica, além de apresentar como o Brasil vem construindo os passos iniciais de sua trilha de segurança cibernética, propondo, ao final, focos chaves para a formulação da Estratégia Brasileira de Segurança Cibernética.

Palavras-chave: Sociedade da Informação. Segurança Cibernética. Segurança da Informação e Comunicações. Inovação.

Abstract

This paper introduces the subject of cibersecutity, its importance in the actual scenario, and the challenges of the new Information Society, which has technological revolution and innovation as critical factors of the development. Presents summary table of the National Strategy for Cibersecurity of the USA and UK, as a panoramic view, and shows how the Brazil has been building the initial steps of its tracks of cibersecurity, proposing, at the end, key focus for the formulation of the Brazilian Strategy Cibersecurity.

Keywords: *Information Society. Cybersecurity. Information and Communications Security. Innovation.*

1 Claudia Canongia é doutora em gestão da inovação pela Escola de Química (EQ) da Universidade Federal do Rio de Janeiro, pesquisadora tecnologista do Instituto Nacional de Metrologia, Normalização, e Qualidade Industrial (Inmetro). Atualmente está cedida ao Gabinete de Segurança Institucional da Presidência da República (GSIPR), atuando na assessoria técnica do Departamento de Segurança da Informação e Comunicações (DSIC/GSIPR). Email: claudia.canongia@planalto.gov.br

2 Raphael Mandarino Junior é diretor do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR). Especialista em Ciência da Computação: Gestão da Segurança da Informação e Comunicações pela Universidade de Brasília (UnB), atua há mais de 35 anos em TI, e formação básica em matemática. Email: raphael.mandarino@planalto.gov.br

1. Introdução

A revolução que as tecnologias de informação e comunicação, as chamadas TICs, já alcançaram na sociedade moderna, é sem dúvida mais do que perceptível e concreta para a sociedade, com resultados bastante satisfatórios em vários campos, como: comércio eletrônico, educação à distância, atendimento médico à distância, redes sociais, desenvolvimento científico-tecnológico, desenvolvimento econômico, promoção do desenvolvimento sustentável, dentre outros. O setor das TICs é muito dinâmico e exige um ritmo acelerado de inovações e de ações multi e interdisciplinares. Todos os movimentos baseados fortemente no intercâmbio rápido de informações de toda ordem, de toda parte do mundo, com diferentes níveis de qualidade, de integridade, de confiabilidade e de segurança, daquela informação que flui, "navega" na rede mundial Internet. Sem dúvida, a problemática referente à inclusão digital permanece viva, assim como as questões sobre a privacidade na Internet, e fazem parte das múltiplas agendas internacionais, as quais se somam, ainda, a questão da preservação das especificidades regionais, e dos valores culturais das economias menos desenvolvidas e emergentes.

Porém, estas abordagens fazem parte de nosso dia-a-dia, mais fortemente, desde o final da década de 1990. Os jargões como sociedade da informação e economia globalizada, ficaram comuns, e em certa medida até banalizados pelo uso excessivo dos mesmos.

O mundo, em especial, aquela parte que congrega países desenvolvidos, em muito se beneficiou e continua a se beneficiar dos avanços que as TICs vêm promovendo.

É, marcadamente, o terreno da alta tecnologia e da inovação constantes, com domínio claro de empresas de países desenvolvidos. A convergência tecnológica bombardeando com novidades antes nem imaginadas, como, por exemplo, acessar Internet do celular, permitindo acompanhar emails e até realizar transações bancárias, enfim, múltiplas aplicações, serviços, e negócios que as TICs vêm proporcionando, são crescentes mundialmente. A inovação nesta nova ordem econômica vem promovendo, então, por meio do uso intensivo das TICs, um fortalecimento das redes sociais, das trocas de informação e conhecimento *just in time*, bem como a geração de novos hábitos e meios de vida, aumentando cada vez mais a tendência da "inovação aberta" como motor dos sistemas nacionais de inovação, conforme defendido primeiramente por Chesbrough. (SOUZA E CANONGIA, 2007).

Neste ponto cabe considerar o outro lado da moeda, uma vez que tais avanços das TICs permitiram também que os chamados ataques cibernéticos, no cenário atual, apresentem escala mundial crescente e se caracterizem como o grande desafio do século. Portanto, assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação é essencial para

a formulação de estratégias e para o processo decisório, especialmente no âmbito do amplo espectro de competências da administração pública federal. Esforços são empreendidos objetivando a segurança da sociedade e dos interesses do Estado, porém, as vulnerabilidades e ameaças são crescentes na Sociedade da Informação.

Está lançado o grande desafio, harmonizar duas dimensões, a primeira dimensão diz respeito à cultura do compartilhamento, da socialização, da transparência, da criação de conhecimento, e a segunda dimensão refere-se às questões de proteção, segurança, confidencialidade, e privacidade.

O texto está organizado em cinco sessões, em que na primeira apresenta-se o contexto e conceitos da segurança da cibernética, na segunda evidencia-se uma visão panorâmica, realçando a motivação e a justificativa da prioridade do tema na cenário atual, na terceira apresenta-se a estratégia nacional de segurança cibernética dos EUA e do Reino Unido, na quarta destaca-se o Brasil frente à esta problemática e esboça-se uma proposta dos eixos fundamentais para a estratégia nacional de segurança cibernética do Brasil, e finalmente na quinta apresentam-se as considerações finais.

2. Entendendo a segurança cibernética

Em decorrências de tantas mudanças socioeconômicas e tecnológicas o que se percebe é uma nova configuração da Sociedade da Informação[1].

Tim Berners-Lee, considerado o pai da *World Wide Web*, promotor da grande revolução da Sociedade da Informação, recentemente rememorou o início de seu trabalho, há 20 anos, que tinha o objetivo de reunir dados dispersos e incompatíveis, dando origem ao conhecido "www". Os avanços tecnológicos ora alcançados estão permitindo que a Web Semântica ou Internet 3.0, extensão da Internet atual, seja colocada em prática, em futuro breve, o que poderá permitir aos computadores e humanos trabalharem em estreita cooperação. A internet 3.0 será capaz de organizar e usar todo o conhecimento disponível na Rede de forma mais inteligente, misturando dados de fontes diferentes instantaneamente, a partir de dados abertos e *linkados* entre si. Segundo Berners-Lee, o mais importante ao se desenvolver "alguma coisa" na web é a universalidade, ou seja, todos têm que ser capazes de utilizá-la independentemente da plataforma, do sistema operacional, do *browser*, ou da cultura[2].

1 Lembra-se que a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida (NBR 17999, 2003).

2 Tim Berners-Lee convoca participantes da Campus Party Brasil para construir o futuro da Internet. (acesso em: 02/09/2009; Disponínel em: <**http://www.campus-party.com.br/index.php/release-5.html**>)

Neste sentido cabe dizer que a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Rede, crescem em igual medida aos desenvolvimentos tecnológicos e ao número de usuários, observados ao longo dos últimos anos.

O nível de preocupação da atualidade é marcante, exemplifica-se com as recomendações resultantes da reunião da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) ocorrida em março de 2009[3], em que os pontos a serem destacados sobre esta nova Sociedade da Informação, lá apresentados foram: a) convergência de tecnologias, aumento significativo de sistemas e redes de informação, aumento crescente de acesso à Internet, avanços das tecnologias de informação e comunicação; b) aumento das ameaças e das vulnerabilidades, apontando para a urgência de ações na direção da criação, manutenção e fortalecimento da cultura de segurança; e, c) ambiente em constante, e rápidas mudanças.

Soma-se que, naquela mesma reunião da OCDE, foi realçado o tema Cultura de Segurança como vetor estratégico das Nações, e os seguintes aspectos foram colocados em evidência: a) cada parte envolvida tem um importante papel para assegurar a segurança em função de suas competências, e devem ser sensibilizados sobre os riscos associados à segurança de sistemas e redes de informação; e, b) as questões de segurança devem ser objeto de preocupação e responsabilidade de todos os atores, seja governamental, empresarial, e de outros (pesquisa e terceiro setor).

Os países membros da OCDE, no que se refere à temática da segurança na Sociedade da Informação, estão desenvolvendo suas estratégias baseados em nove princípios, quais sejam: 1) sensibilização sobre riscos – seguir normas e boas práticas, implantar controles, e estar em alerta sobre todo tipo de interconectividade e interpendência de sistemas e redes de informação; 2) responsabilidade – entender a importância de avaliar e atualizar sistematicamente as políticas, práticas, medidas e procedimentos de segurança adotados para sistemas e redes de informação; 3) resposta – agir próativamente e em cooperação, prevenindo, detectando e respondendo aos incidentes; 4) ética – respeitar interesses legítimos de todas as partes envolvidas; elaborar e adotar práticas exemplares na condução da segurança de sistemas e redes de informação; 5) democracia – seguir e fortalecer valores fundamentais de uma sociedade democrática na segurança de sistemas e redes de informação; 6) avaliação de riscos – minimizar ameaças e vulnerabilidades por meio de ações que sejam amplas o bastante para englobar os fatores críticos internos e externos (tecnologias, físicos, humanos, políticos, serviços de terceiros). A avaliação de risco tanto permitirá determinar o nível de risco aceitável quanto facilitará a adoção de medidas de controle apropriadas ao tipo de informação a ser protegida; 7) concepção – integrar segurança como elemento essencial no processo de planejamento, modelagem, criação e gestão de sistemas e rede

3 Organization for Economic Co-Operation and Development (OECD) - Guidelines for the Security of Information Systems and Networks: Towards a culture of security. (Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002). Paris: OECD. 2002. 28p

de informação, com soluções inovadoras; 8) gestão da segurança – coordenar e integrar a avaliação de riscos e a capacidade de resposta e resolução de incidentes, bem como a auditoria de sistemas e redes de informação, para criar um sistema coerente de segurança da informação; e, 9) reavaliação – examinar e reavaliar a segurança de sistemas e redes de informação, e introduzir as necessárias mudanças nas respectivas políticas, estratégias, medidas e procedimentos.

Cabe acrescentar que o documento OECD *Recommendation of the Council on the Protection of Critical Information Infrastructure*[4], apresenta as seguintes recomendações aos países membros da OCDE no que tange a proteção das infraestruturas de informação: a) adotar política, com objetivos claros, no mais alto nível de governo; b) identificar agências de governo e organizações com competência (responsabilidade e autoridade) para implantar a política e seus objetivos; c) estabelecer mútua cooperação entre os *stakeholders* – setor privado, agências, terceiro setor, governo – visando à efetiva implantação da política; d) garantir transparência na delegação de competência – governança – facilitando e fortalecendo a cooperação, em especial entre governo & setor privado; e) rever sistematicamente a política e respectivo marco(s) legal(is), com especial atenção às ameaças, minimizando riscos e/ou desenvolvendo novos instrumentos; e, f) estabelecer níveis de segurança em sistemas e redes de informação e comunicações.

A Segurança Cibernética vem, assim, se caracterizando cada vez mais como uma função estratégica de governo, e essencial à manutenção e preservação das infraestruturas críticas de um país, tais como saúde, energia, defesa, transporte, telecomunicações, da própria informação, entre outras.

2.1. Construindo conceitos

O ciberespaço (ou espaço cibernético) é considerado como a metáfora que descreve o espaço não físico criado por redes de computador, notadamente a internet, onde as pessoas podem se comunicar de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros. O termo foi criado por Willian Gibson em seu romance "Neuromancer". (APDSI, 2005).

Em relação aos conceitos tanto de Segurança Cibernética quanto de Defesa Cibernética, cabe colocar que estes vêm sendo construídos com a presença de diferentes e importantes agentes, no país. Entende-se que o escopo de atuação da Segurança Cibernética compreende aspectos e

4 Organization for Economic Co-Operation and Development (OECD) Committee for Information, Computer and Communication Policy (ICCP Committee) – OECD Recommendation of the Council on the Protection of Critical Information Infrastructure. (Adopted as a Recommendation of the OECD Council at its 1172th Session on 30 April 2008). Seoul/Korea. June. 2008.

atitudes tanto de prevenção quanto de repressão. E para a Defesa[5] Cibernética entende-se que a mesma compreende ações operacionais de combates ofensivos.

Como um ponto de partida para a constituição de uma base conceitual nesta temática, ainda em construção no país, a seguinte conceituação de segurança cibernética, vem sendo adotada na esfera pública, mais focadamente na comunidade de segurança da informação e comunicações, qual seja, "segurança cibernética é entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas"[6]. É, portanto, maior que segurança em TI, pois envolve pessoas e processos.

Acrescenta-se que o conceito, em inglês, de *Cybersecurity* inclui, segundo o *Department of Homeland Security (DHS)*, a prevenção aos danos causados pelo uso não autorizado da informação eletrônica e de sistemas de comunicações e respectiva informação neles contida, visando assegurar a confidencialidade, integridade, e disponibilidade, incluindo, também, ações para restaurar a informação eletrônica e os sistemas de comunicações no caso de um ataque terrorista ou de um desastre natural." [7]

Vale refletir sobre o conceito colocado na perspectiva da *International Communications Union (ITU)* em que *Cybersecurity* significa basicamente prover proteção contra acesso, manipulação, e destruição não autorizada de recursos críticos e bens. Tais recursos e bens variam e dependem do nível de desenvolvimento dos países. Dependem, também, do que cada país considera como sendo recurso crítico, os esforços que podem e estão dispostos a realizar, bem como da avaliação do risco que estão dispostos a aceitar em conseqüência das inadequadas medidas de segurança cibernética. Adicionalmente, para certo número de países desenvolvidos, há outras ameaças tais como fraude, proteção do consumidor, e privacidade, as quais consideram também como soluções da cybersecurity, forma de proteger e manter a integridade das infraestruturas críticas nos setores financeiro, de saúde, da energia, do transporte, das telecomunicação, da defesa, e de outros."[8]

Ainda de acordo com o *ITU*, as áreas consideradas foco, dos países membros da OCDE, para a promoção da *cybersecurity* são: a) Áreas de elevada atenção: Combate ao crime cibernético,

5 De acordo com o Glossário das Forças Armadas (MD35-G-01;2007) o termo defesa é entendido como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança", ou ainda, como "reação contra qualquer ataque ou agressão real ou iminente".

6 MANDARINO, R. **Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro.** 2009. Monografia (especialização). Universidade de Brasília (UnB). Departamento de Ciência da Computação - DCE:Brasília. Jun. 2009. p. 29.

7 NATIONAL INFRASTRUCTURE PROTECTION PLAN. **Partnering to enhance protection and resiliency.** DHS, 2009. p.12.

8 ITU GLOBAL CYBERSECURITY AGENDA (GCA). **Framework for International Cooperation in Cybersecurity.** ITU, 2007. p. 10.

Criação em nível nacional de *CERTs/CSIRTs* (*Computer Emergency Response Teams/Computer Security Incident Response Teams*); Aumento da cultura de segurança cibernética e suas atividades; e Promoção da educação; b) Áreas com menos atenção: Pesquisa e Desenvolvimento; Avaliação e monitoramento; e Atendimento às pequenas e médias empresas (PMEs)."[9]

Tem-se que dois conceitos adotados no Brasil na esfera pública dão sustentação à abordagem da segurança cibernética, quais sejam, "infraestrutura crítica da informação", bem como "ativos de informação". No âmbito do governo federal brasileiro, considera-se "infraestrutura crítica da informação" o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. E, complementarmente, consideram-se "ativos de informação", os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios, e as pessoas que a eles têm acesso[10].

3. O porquê da "bola da vez" ser a segurança cibernética: visão panorâmica

Chama a atenção neste ano de 2009, no âmbito dos debates da sociedade globalizada, que emerge, além da grande crise econômica mundial, o emprego, cada vez mais intenso, de expressões como ataques cibernéticos, segurança cibernética, espaço cibernético, regulamentação da Internet, direitos de privacidade, crimes cibernéticos, violação de direitos de propriedade intelectual, dentre outros, quer sejam nas mídias convencionais e digitais, quer em fóruns e eventos de governo e da academia, nacionais e internacionais. Enfim, uma miríade de termos que colocam o uso da Internet, a interconectividade das redes, e a convergência digital, na linha de frente das atenções das lideranças de vários países, a nova Sociedade da Informação e seus desafios.

Um bom retrato da atualidade, a exemplificar, foi o ocorrido em julho de 2009, em que o sítio do Departamento de Defesa dos EUA foi invadido por 4 dias consecutivos, numa ação que atualmente tem sido comum por parte dos chamados *hackers*, de tentativa de saturação de acesso e conexão a um determinado sítio da Internet até que o mesmo seja interrompido e seu acesso bloqueado. E, da mesma forma, sítios do governo da Coréia do Sul sofreram com ação similar, tornando lento o acesso à Internet naqueles mesmos dias do início de julho. Dados dos serviços de inteligência de ambos os países informaram que tal ataque cibernético partiu de 16 países,

9 SUND, Christine. Promoting a Culture of Cybersecurity. In. ITU REGIONAL CYBERSECURITY FORUM FOR EASTERN AND SOUTHERN AFRICA. Lusaka, 25-28 Aug 2008.

10 BRASIL. Portaria nº. 34, de 05 de agosto de 2009. Diário Oficial da República Federativa do Brasil, Brasília, 06 ago 2009.

inclusive dos EUA e da Coréia do Sul, fazendo uso de cerca de 20 mil computadores domésticos e 80 provedores da Internet. (SILVA; 2009)

Soma-se que os crimes na internet, segundo dados recentes revelados pelo governo britânico, geram um prejuízo global de 52 bilhões de libras (U$ 84,2 bilhões), por ano, sendo 20 bilhões de libras (U$ 32,5 bilhões) para o Reino Unido. O ministro de Segurança Cibernética do Reino Unido, Lord West, revelou que a agência britânica já vem atuando em conjunto com sua equivalente nos Estados Unidos em estratégias de defesa e segurança do ciberespaço[11].

Reconhecidamente uma das mais importantes e grandes empresas de TI do mundo, a Microsoft, destaca em seu último relatório *Microsoft Security Intelligence Report*, 16 pontos críticos relativos à segurança e à privacidade na Internet, nos últimos seis meses. Entre os quais, para reflexão, exemplificam-se quatro, a seguir: 1) exploração de vulnerabilidade de *browser*: as máquinas baseadas no Windows XP foram as mais atacadas, representando cerca de 40,9% do total de ataques monitorados pela empresa; 2) exploração de vulnerabilidade do sistema *Office*: a vulnerabilidade mais freqüentemente explorada foi uma simples e antiga, representando 91,3% dos ataques examinados, mesmo que a solução de tal vulnerabilidade tenha sido disponibilizada pela empresa há dois anos (CVE-2006-2492), indicando por conseqüência uma ameaça, qual seja, a ação dos usuários de não atualização das versões do sistema *Office* de forma sistemática; 3) softwares maliciosos: a tendência mais significativa observada foi a detecção de aumento bastante expressivo de *softwares* maliciosos em muitos países e regiões no mundo, sendo que a depender da cultura de cada Nação há um tipo que mais se salienta. Por exemplo, na China *malwares* que modificam *browsers* prevalecem, ao passo que no Brasil os alvos são *malwares* para captura de senha e fraudes bancárias prevalecendo o cavalo de tróia conhecido como Trojanspy:win32/Bancos, e na Coréia os vírus são os mais comumente disseminados, em especial os conhecidos Win32/Virut e o Win32/Parite; e, 4) emails: mais de 97% dos emails que trafegaram na Internet, mais especificamente no *Hotmail* que é o monitorado pela empresa, foram indevidos, ou seja, foram enviados por meio de spams ou de ataques cibernéticos nos casos de intenção maliciosa. (MICROSOFT; 2008[12])

Uma investigação de crimes digitais, no âmbito do projeto de pesquisa do grupo SecDev Group, da Universidade de Toronto, Canadá, descobriu que 1.295 computadores em 103 países estavam sendo espionados. Segundo o relatório divulgado no final de março 2009, 30% dos PCs invadidos pertencem a ministérios de relações exteriores, embaixadas, organizações internacionais, empresas de comunicação e organizações não-governamentais, inclusive com acesso à

11 INGLATERRA e EUA se aliam na Segurança Cibernética. (Disponível em: <*http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=19362&sid=18&tpl=printerview*>. Acesso em: 02 set. 2009.

12 MICROSOFT. **Microsoft Security Intelligence Report.** EUA, Jul-Dec 2008. 183p. 6.v.

conhecimento sensível[13]. O relatório fornece evidências detalhadas sobre ação de crackers, com motivação política, ao mesmo tempo em que levanta dúvidas sobre a relação destes criminosos com governos. A rede de espionagem, chamada *GhostNet*, utiliza o *malware* denominado *ghost RAT* (*Remote Access Tool*) para roubar documentos sensíveis, acessar *Web Cams* e assumir completamente o controle de máquinas infectadas. (SECDEV GROUP; 2009)[14]

No que se refere ao cenário do governo brasileiro, os resultados de uma pesquisa realizada em 2007 pelo Tribunal de Contas da União (TCU) em 250 órgãos públicos, apresentou uma série de deficiências na gestão de Governança de Tecnologia da Informação, sendo que os itens mais expressivos foram aqueles relativos à Segurança da Informação. A pesquisa mostrou que 80% dos órgãos pesquisados não classificam a informação[15], 75% não fazem análise de riscos, e 64% não possuem política de segurança da informação.

Segundo as palavras de Raphael Mandarino Junior[16], em entrevista realizada em 2009 para a Revista Galileu[17], "Nós temos 320 grandes redes. Chamo-as de grandes redes porque cada uma pode ter suas sub - redes: o Exército, por exemplo, tem redes no Brasil inteiro, mas eu conto como uma só. O Brasil recebe 2.000 (dois mil) ataques por hora nessas redes – isso são apenas tentativas de invasão para roubar dados, não estou contando vírus e spams. (...) Nem sempre é uma pessoa que faz o ataque. Em muitos casos alguém invade um computador, usa um software – robô, e fica tentando atacar as redes do governo várias vezes. Eu detecto o ataque e identifico de que computador ele vem, então notifico o administrador daquela rede. Normalmente eu chego no computador que foi invadido para invadir o nosso, não ao computador do hacker. Mas ao menos eu fecho essa porta".

Woloszin apresenta que os ataques cibernéticos e o ciberterrorismo são uma tendência mundial com perspectivas sombrias. E o especialista complementa, que a maior preocupação para o Brasil reside no fato de que os conhecimentos específicos sobre o tema ainda são do domínio de poucos, assim como, os recursos financeiros são insuficientes. (WOLOSZIN, 2009)[18]

13 Conhecimento sensível segundo a Portaria GSIPR No. 42 publicada no DOU de 17/08/2009 é todo conhecimento, sigiloso ou estratégico, cujo acesso não autorizado pode comprometer a consecução dos objetivos nacionais e resultar em prejuízos ao País, necessitando de medidas especiais de proteção.

14 THE SEC DEV GROUP. **Tracking GhostNet: Investigating a Cyber Espionage Network.** Mar. 2009. 53p. (Disponível em: <*http://www.infowar-monitor.net/ghostnet*>. Acesso em: 08 abr 2009.)

15 Ver detalhes no Decreto No. 4553 publicado no DOU de 27 de dezembro de 2002.

16 Diretor do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.

17 ENTREVISTA de Mariana Lucena sobre Segurança Cibernética. In: Revista Galileu. (Disponível em: <*http://dsic.planalto.gov.br/noticias/65-entrevista-do-diretor-do-dsic-a-revista-galileu*>. Acesso em: 02 set 2009.)

18 WOLOSZIN, A. L.. **A ameaça invisível do terror cibernético.** Jornal do Brasil-Internacional, A3, 14 ago 2009.

Não é sem razões fortes e fatos contundentes que o tema segurança cibernética vem sendo tratado cada vez mais intensamente nas esferas de governo, no mundo, sendo considerado, portanto, "a bola da vez".

4. Estratégia nacional dos EUA e do Reino Unido

Inicialmente, e sem polemizar, apenas para dar início a um amplo processo de reflexão, debate, e construção de opiniões sobre o tema, observa-se que os contornos do espaço cibernético ainda são fluídos e não definidos para uma Nação, dado o elevado grau de interdependência e interconectividade das redes e sistemas de informação em termos mundiais.

Economias desenvolvidas estão, exatamente neste momento, como por exemplo EUA e Reino Unido, revisando ou lançando, respectivamente, suas estratégias nacionais de segurança cibernética, com uma sinalização forte do quanto há por fazer, principalmente em termos de cooperação internacional, legislação, normalização, e capacitação de recursos humanos especializados.

O que não quer dizer que o tema não faça parte das agendas anteriores de fóruns de governo, da iniciativa privada, das ONGs, nacionais e internacionais. As questões correlacionadas à segurança cibernética, em grande medida, tanto em termos de tecnologia quanto em termos de diretrizes, normalização e metodologias, ao longo dos últimos anos, vinham sendo tratadas, mundialmente, no escopo da segurança da informação e comunicações, inclusive no Brasil.

Em relação aos EUA vale citar o documento *Securing Cyberspace for the 44th. Presidency*, que ao ser lançado no final de 2008, traz um panorama daquele país no tema, suas prioridades e carências.

No que diz respeito ao Reino Unido, pode-se destacar que sua primeira estratégia nacional de segurança cibernética foi lançada em junho de 2009, e denominada *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.*

No Quadro 1, a seguir, apresenta-se demonstrativo das recomendações dos EUA e do Reino Unido, para a Estratégia Nacional de Segurança Cibernética adotada por aquelas Nações, quadro que caracteriza um breve resumo dos entendimentos da autora deste artigo.

Estratégia Nacional de Segurança Cibernética

Quadro 1: Demonstrativo das Recomendações dos EUA[19] e do Reino Unido[20]
Resumo dos entendimentos da autora

EUA	Reino Unido
Criação de uma estratégia integrada e detalhada de segurança nacional dos EUA para o ciberespaço O governo deveria promover ajuste na atual Estratégia, e estabelecer uma Estratégia Nacional de Segurança do Ciberespaço, integrada e detalhada, na qual a macro coordenação seja realizada por órgão/agência especificamente criado para tal finalidade, no âmbito da Casa Branca, órgão este que promoveria a devida sinergia do tema, prioritariamente, nos meios: diplomático quanto à inserção internacional, militar relativo à doutrina e ao planejamento, econômico no que tange à política, inteligência em suas atividades, e marcos legais no tocante à atualização e dinamização dos mesmos;	**Desenvolvimento da estratégia de segurança cibernética do Reino Unido** A primeira Estratégia Nacional de Segurança Cibernética do Reino Unido lançada em junho de 2009, tem os seguintes objetivos: a) estabelecer programa intragoverno e intergovernos em áreas prioritárias da segurança cibernética, provendo fundos adicionais para a pesquisa, desenvolvimento e inovação (P,D&I), bem como para o desenvolvimento e promoção das habilidades e competências críticas; b) estreitar os trabalhos de cooperação entre o setor público com o setor privado, as organizações-não governamentais, e os parceiros internacionais; c) criar órgão central específico, neste caso o Office Cyber Security (OCS), para prover a liderança e macro coordenação necessárias; e, d) criar órgão operacional específico, neste caso o Cyber Security Operations Centre (CSOC), para prioritariamente monitorar o espaço cibernético e coordenar respostas à incidentes, estabelecer melhores condições de entendimento e conhecimento sobre os ataques cibernéticos contra as redes e usuários do Reino Unido, e prover informações sobre os riscos, tanto para as transações comerciais e negócios, quanto para o setor público no que se refere ao espaço cibernético.
Organização das estruturas nacionais para a segurança cibernética O Presidente deveria estabelecer no âmbito do National Security Council (NSC) uma Diretoria de Segurança Cibernética que absorveria as funções atualmente exercidas pela Homeland Security Council (HSC). Além disso, o novo Órgão/ Agência Nacional do Ciberespaço deveria apoiar os trabalhos da nova Diretoria de Segurança Cibernética da NSC, e deveria atuar na assessoria direta do Presidente para tal assunto. O Presidente deveria, ainda, promover a fusão entre os já existentes órgãos National Cyber Security Center (NCSC) e a Joint Inter-Agency Cyber Task Force (JJACTF – criada pelo Diretor Nacional de Inteligência). O Department of Homeland Security (DHS) deveria permancer responsável pelo United States Computer Emergency Readiness Team (US-CERT) bem como pelo respectivo Programa US-CERT Einstein.	**Novas estruturas de governo para atuação em cibernética** O governo estabelecerá o *Office of Cyber Security (OCS)*, que atuará no *Cabinet Office*, e será o órgão responsável pela liderança estratégica do tema, promovendo maior sinergia e macro coordenação dos vários programas de governo na direção da segurança cibernética, sem duplicação de esforços, porém com a devida priorização dos objetivos nacionais no tema. O governo estabelecerá, também, uma multiagência, o *Cyber Security Operations Centre (CSOC)*, para monitorar o espaço cibernético, analisar tendências, e fortalecer a coordenação de respostas técnicas aos ciber incidentes. O CSOC será também responsável por disseminar informação para o governo, a indústria, e aos parceiros internacionais, sobre os riscos e oportunidades da segurança cibernética. As novas estruturas serão estabelecidas em setembro de 2009 e colocadas em efetiva operação até final da março de 2010.

Continua...>>

19 CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. **Securing Cyberspace for the 44th.** Presidency: a report of the CSIS Commission on Cybersecurity for the 44th. Presidency. CSIS_Washington. Dec. 2008. 88p.

20 CABINET OFFICE. **Cyber Security Strategy of the United Kingdom:** safety, security and resilience in cyber space. (UK Office of Cyber Security (OCS) and UK Cyber Security Operations Centre (CSOC)). UK: TSO – The Parliament Bookshop. June. 2009. 25p.

...Continuação

Parcerias com o setor privado O governo americano deveria "reconstruir" as parcerias entre os setores público-privado, em cibersegurança, no sentido de focar as infraestruturas chaves/ críticas da Nação. Para tanto, deveria ser formado Comitê Assessor para atuar em nível presidencial, com representantes seniores das infraestruturas chave/ críticas cibernéticas. Neste sentido, este novo Comitê deveria incorporar tanto o National Security and Telecommunications Advisory Committee (NSTAC) quanto o National Infrastrustructure Advisory Council (NIAC).	**Defesa, segurança e sistema de resistência** O governo focará na preparação e proteção contra ataques cibernéticos em todos os setores, provendo uma maior capacidade de resistência e resposta. Para tanto envidará esforços para ampliar o entendimento sobre potenciais vulnerabilidades e impactos, bem como para desenvolver medidas de mitigação apropriadas.
Regulação da segurança cibernética Deveria ser desenvolvido pelo novo Órgão/ Agência Nacional de Segurança Cibernética uma macro-coordenação sobre os aspectos de normas e padrões da segurança para a infraestrutura crítica cibernética, no sentido de que as diferentes agências reguladoras em seus escopos de atuação tenham suas atividades alinhadas ao objetivo comum da segurança cibernética	**Política, doutrina, e marcos legais e regulatórios** O novo Office of Cyber Security (OCS) identificará lacunas nas atuais doutrina, política, legislação e regulação por meio de um framework que aponte o cenário doméstico e internacional. O OCS será o melhor local para liderar tanto o desenvolvimento de políticas específicas e promover a maior interação no governo, quanto o desenvolvimento e implantação da estratégia industrial de segurança cibernética, em estreita colaboração com atores chaves da indústria. Assim, o fortalecimento das parcerias com o setor privado será fundamental no sentido de sustentar e promover as capacidades nacionais no tema, e estimular a inovação. Para o desenvolvimento do framework dos marcos legais e regulatórios, tais parcerias também serão essenciais, somadas ao estreito trabalho com os atores e órgãos que detenham tais competências e escopo de atuação.
Segurança nos sistemas de controle industrial e SCADA (Supervisory Control and Data Acquisition) O novo Órgão/ Agência Nacional de Segurança Cibernética deveria trabalhar em conjunto com as agências reguladoras adequadas e o National Institute for Standards and Technology (NIST), no desenvolvimento de normas, regulamentos técnicos e padrões metrológicos de segurança para a certificação dos sistemas de controle industrial.	**Compreensão e cultura** O novo Office of Cyber Security (OCS) liderará o trabalho de ampliar a compreensão e fortalecer a cultura de segurança cibernética, identificando mudanças ambientais e de trabalho a serem incorporadas, tanto quanto priorizará os vários aspectos relacionados à segurança cibernética na formulação da política. Dentre as medidas, salienta-se a de desenvolver o processo de tomada de decisão baseado em risco. Tal prática representa uma substancial e desafiadora mudança de cultura, e prescindirá de trabalhos específicos na direção de que a informação certa e consistente, chegue no momento certo e nas mãos certas, visando garantir maior eficácia e eficiência decisória no campo sensível que é o da segurança cibernética.
Fortalecimento da segurança nas aquisições e usos de serviços e produtos de TI O novo Órgão/ Agência Nacional de Segurança Cibernética deveria trabalhar em parceria estreita com o setor privado na direção de estabelecer um guia básico para aquisição e uso de tecnologia da informação, dando especial atenção aos softwares. Além disso, esforços para o aumento da segurança da Internet deveriam ser priorizados, contemplando dentre as necessárias ações, o desenvolvimento de regulamentos técnicos mandatórios de protocolos de segurança da Internet. Tal medida, inclusive, deveria fazer parte de uma estratégia de articulação internacional para a segurança da Internet.	**Habilidades e educação** O governo examinará os requisitos e passos necessários ao desenvolvimento de capacidades, habilidades e formação de especialistas em segurança cibernética para atuação no governo e na indústria. Não se limitará aos aspectos técnicos requeridos, mas sim em combinar diferentes abordagens e cobrir as lacunas existentes neste campo. Serão desenvolvidos treinamentos, estímulo à certificação e desenvolvimento de carreira específica para atuação dentro e fora do governo.

Continua...>>

...Continuação

Gestão e credenciamento

Deveria ser reforçado o sistema de autenticação das identidades, em especial daquelas pessoas que atuam nas infraestruturas críticas cibernéticas (TICs, energia, finanças, serviços essenciais do governo). Além do que deveria ser cobrada com ênfase a adoção da Política de Padrão de Identificação Comum para os Empregados e Contratados no âmbito do Governo Federal dos EUA, conforme a Homeland Security Presidential Directive: HSPD-12. Soma-se que, o credenciamento do governo deveria, também, apoiar os consumidores em atividades online, observados os direitos da privacidade individual e da liberdade civil.

Capacidades técnica, de pesquisa e desenvolvimento (P&D)

O governo aportará e proverá significantes contribuições para o trabalho de atualização da doutrina, política, marcos legal e regulatório, bem como para a implementação da estratégia de segurança cibernética na indústria, com destaque para as infraestruturas críticas nacionais como saúde, energia e outras. Para tanto, esforços e priorização da P&D promoverão melhores efeitos, em especial ao se considerar as parcerias internacionais ocorridas no meio acadêmico. No primeiro momento, recursos adicionais serão alocados para apoiar e expandir o trabalho colaborativo de proteção das redes de governo e industriais. O novo Office of Cyber Security (OCS) trabalhará também em forte cooperação com a Network Security Innovation Plataform (NSIP) na Technology Strategy Board, visando prover oportunidades para as empresas de alta tecnologia do Reino Unido.

Modernização

O Presidente, em conjunto com o Ministério da Justiça, deveria reexaminar os estatutos e processos de investigação de ciber crimes, no sentido de torná-los mais claros, mais ágeis, e com melhor proteção da privacidade. Em paralelo, deveria lançar guia básico com indicações de circunstâncias e requisitos para uso e cumprimento da lei, bem como uso das autoridades militares e de inteligência nos ciber incidentes.

Exploração

O Reino Unido desenvolverá ações para entendimento e identificação das necessárias capacidades e competências para exploração do espaço cibernético, no sentido de combater ameaças de criminosos, terroristas, e de outros atores, por meio de um trabalho eficaz e eficiente de combate aos ataques cibernéticos, conferindo a devida defesa dos interesses nacionais e da sociedade.

Revisão do Ato Normativo Federal de Gestão da Segurança da Informação (FISMA 2002)

O Presidente deveria trabalhar juntamente com o Congresso na direção de "reescrever" o Federal Information Security Management Act – 2002 (FISMA), marco normativo americano da segurança da informação, do National Institute of Standards and Technology (NIST), de forma que o mesmo contemple os aspectos relativos à segurança cibernética.

Engajamento internacional

O novo Office of Cyber Security (OCS) será o responsável pela construção coerente e sinérgica dos trabalhos de segurança cibernética do Reino Unido vis a vis políticas, estratégias e boas práticas de parceiros e de organizações internacionais. Neste primeiro momento o OCS não fará parte dos numerosos acordos bilaterais e multilaterais que cada agência ou órgão já realiza. E sim, exercerá uma macro coordenação dessas atividades na direção de desenvolver uma visão e mensagem única do Reino Unido à respeito da segurança cibernética, alinhada às visões de aliados estratégicos, e se fazendo presente em comissões e fóruns internacionais.

Eliminar a divisão entre diretrizes e normas de segurança de sistemas civis e nacional

O Presidente deveria propor legislação que eliminasse a distinção existente entre normas e regulamentos técnicos de segurança de sistemas nacional e sistemas de agências civis, adotando abordagem baseada em risco.

Governança, papéis e responsabilidades

Será modelada a governança do Reino Unido para todos os aspectos relacionados à segurança cibernética, desenvolvendo um arcabouço teórico-referencial que contemple as lições aprendidas, as melhores práticas, os parceiros considerados chave, e as iniciativas de mudanças requeridas. Uma das áreas críticas, a dos ciber crimes, exigirá uma revisão breve dos papéis e responsabilidades dos atores diretamente envolvidos, bem como dos requisitos estratégicos, sob a liderança e macro coordenação do OCS, para assegurar a Estratégia Nacional de Segurança Cibernética do Reino Unido. No âmbito desta recomendação encontram-se também os esforços intra-governo de promoção e priorização da Estratégia Nacional de Segurança Cibernética , que contará com a participação e colaboração de stakeholders, de órgãos não governamentais, e da sociedade.

Continua...>>

...Continuação

Treinamento e educação em cibernética e desenvolvimento de força de trabalho O Presidente deveria por meio do novo Órgão/ Agência de Segurança Cibernética, e operando juntamente com agências de formação e gestão de pessoal do governo, criar programas de treinamento para as atividades de governo no campo da cibernética. E, ainda, deveria trabalhar juntamente com o National Science Foundation (NSF) para desenvolver um programa nacional de educação no tema.	
Pesquisa e desenvolvimento (P&D) em cibernética O novo Órgão/ Agência de Segurança Cibernética, trabalhando juntamente com o Office of Science and Technology Policy (OSTP), deveria realizar macro coordenação da P&D em cibernética.	

Ainda a título de exemplo da dinâmica do tema e seu impacto, em especial, nas infraestruturas críticas de uma Nação, o documento elaborado em atendimento à demanda do atual Presidente dos EUA, Barack Obama, no início de seu governo, que incluiu a segurança cibernética no rol das grandes ameaças globais, foi concluído em junho de 2009, e intitula-se "*US Cyberspace Policy Review: assuring a trusted and resilient information and communications infrastructure*". Seu sumário executivo apresenta 10 recomendações para a revisão da estratégia daquele país, quais sejam: 1) criação de órgão específico, na Casa Branca, para exercer efetivamente macro coordenação entre as agências de governo americanas, com atuação em segurança cibernética, visando maior sinergia na estratégia nacional e nas respectivas políticas; 2) atualização breve da estratégica nacional de proteção da infraestrutura de informação e comunicações; 3) designação da segurança cibernética como uma das prioridades chaves de gestão da Presidência do país, e estabelecimento de mecanismos de medidas de avaliação e de auditorias; 4) observância da liberdade civil e da privacidade dos profissionais do órgão específico criado no tema; 5) formulação de política clara quanto aos papéis, responsabilidades, e tipo de atuação de cada agência do governo com autoridade de ação em segurança cibernética e áreas correlatas, e criação de mecanismos entre as agências de gestão, de monitoramento, e de avaliação; 6) promoção da segurança cibernética por meio de campanhas nacionais públicas e programas de educação; 7) desenvolvimento de posicionamento dos EUA em segurança cibernética, e fortalecimento de parcerias e da cooperação internacional na construção de uma política internacional no tema; 8) fortalecimento e elaboração de plano de resposta a incidentes de segurança cibernética, com forte interação e diálogo entre os setores público-privado; 9) desenvolvimento de *framework* de pesquisa, desenvolvimento, e inovação (PD&I), nos vários campos de aplicação da segurança cibernética, como por exemplo, soluções tecnológicas integradas, ferramentas, metodologias de segurança e contingência da infraestrutrura digital; e, 10) construção de uma visão de gestão e de uma estratégia nacional baseada na segurança cibernética, observando a privacidade e os direitos civis.

Bezerra, em seu texto disseminado no Blog Segurança Digital, pondera muito bem os acontecimentos internacionais recentes de ataques cibernéticos, como os ocorridos na Estônia em 2007 (talvez o primeiro grande marco de ataque cibernético no mundo), e o já citado na Coréia do Sul, mais recentemente neste ano de 2009, dentre outros, o que vem para alertar o fato de que não se trata de um modismo ou mero exagero, mas de uma nova realidade que vem desencadeando um leque de possibilidades e situações.

Pode-se perceber, como sendo o desafio, saber lidar fortemente com tal aspecto, o da segurança cibernética na sociedade globalizada, nova onda que realça a necessidade de estudos de impactos econômico-sociais e prospectivos, bem como a formulação de políticas públicas e de estratégias nacionais.

Nos EUA, encontra-se, atualmente, em debate no Congresso uma série de novas legislações a respeito do tema, como por exemplo: a) o Projeto de Lei conhecido como *Cybersecurity Act 2009 (S.773)*, defendido pelo Senador Jay Rockefeller, que daria ao Presidente dos EUA autoridade para declarar situação de *cyber emergence*, se tráfico na Internet indicasse risco de ataque aos sistemas e redes de governo e às infraestruturas críticas da Nação, medida considerada controversa na medida em que daria àquele Presidente condições de interromper totalmente o tráfico da Internet do país, o que seria em tese "proibitivo' em termos econômicos e também sociais, e não somente para aquela Nação, dado o nível de interdependência dos sistemas e redes de informação em nível global; b) revisão e atualização do *Federal Information Security Management Act of 2002*, na nova denominação *US Information and Communications Enforcement Act of 2009 (S.921)*, com apoio e defesa dos Senadores Carper e Burris, que modifica o capítulo 35 da legislação de 2002, caracterizando a competência do novo órgão específico de segurança cibernética americano no que se refere à segurança, proteção, e recuperação das infraestruturas de informação e comunicações do país, com compromisso de desenvolver ambiente seguro aos cidadãos, de prosperidade econômica, e de defesa dos interesses da Nação, diante de qualquer ataque cibernético. Esta legislação reforça o papel das equipes de tratamento e resposta a incidentes em redes computacionais e exalta a necessidade de recursos humanos altamente especializados; c) no que se refere ao escopo da educação, o *H.R 266 Cyber Education and Enahncement Act 2009*, introduzido por Sheila Jackson-Lee, defende duas vertentes principais, quais sejam, a de contar com programas efetivos de fomento da *National Science Foudation (NSF)* para a formação de recursos humanos e atualização de infraestrutura tecnológica de cursos de graduação e pósgraduação especializados em segurança cibernética, contando a coordenação geral do *Department of Homeland Security (DHS)*; e, uma segunda vertente, a de estabelecer programa de cooperação e intercâmbio técnico e científico, nos níveis local, setorial e regional, com forte parceria com o setor privado, na formação de talentos.

Alerta-se para o fato de que uma série de desdobramentos na temática ora em análise, merecem reflexão e debates no país, neste momento de construção de novos paradigmas da Sociedade da Informação.

5. Governo brasileiro: passos iniciais para a trilha da segurança cibernética

O Livro Verde da Sociedade da Informação no Brasil[21], já em 2000 quando de seu lançamento, apresentava que "No Brasil, governo e sociedade devem andar juntos para assegurar a perspectiva de que seus benefícios efetivamente alcancem a todos os brasileiros. O advento da Sociedade da Informação é o fundamento de novas formas de organização e de produção em escala mundial, redefinindo a inserção dos países na sociedade internacional e no sistema econômico mundial. Tem também, como conseqüência, o surgimento de novas demandas dirigidas ao Poder Público no que respeita ao seu próprio funcionamento".

No entanto, apesar da expansão do uso da Internet nos últimos anos no Brasil, o país ocupa ainda um posicionamento considerado "ruim" em termos do *ranking* mundial daqueles países mais conectados na Rede, ocupando atualmente o 590. lugar, segundo o *World Economic Forum-WWF* (WWF apud SILVA, 2009[22]).

Mesmo diante deste posicionamento no *ranking* mundial, segundo Alexandre Sanches Magalhães, gerente de análise do Ibope/*NetRatings*, o ritmo de crescimento da Internet brasileira é intenso. Em julho de 2009 foram contabilizados 64,8 milhões de internautas no Brasil, conforme dados do *Ibope Nielsen Online*, ou seja, um aumento de 2,5 milhões de pessoas em relação ao mês anterior. Em relação ao acesso via banda larga, o país atingiu 10,04 milhões de conexões em junho de 2008: um ano e meio antes do previsto, já que essa era a projeção para 2010[23].

Relatório de ameaças à segurança, produzido pela Sophos no início de 2007, aponta que a China foi responsável pela produção de 30% dos *softwares* maliciosos virtuais espalhados pelo mundo em 2006. Em segundo lugar aparece o Brasil, com carga de responsabilidade de cerca de 14,2%,

21 **Sociedade da informação no Brasil:** livro verde. TADAO, Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000. 195p.

22 SILVA, P. F. Ameaça Cibernética: a ciência e a tecnologia significam progresso mas também criam vulnerabilidades e ameaças. In.: **Defesa Latina.** Jul-Set 2009.p. 52-54.

23 Estatísticas, dados e projeções atuais sobre a Internet no Brasil. (Disponível em: <*http://www.tobeguarany.com/internet_no_brasil.php*> Acesso em: 02 set 2009.)

conforme amplamente divulgado naquela época pelo Núcleo Operacional da Sociedade da Informação no Brasil[24].

Ainda no caso do Brasil, este tem história na Sociedade da Informação, e no campo da segurança da informação e comunicações tem governança estabelecida, legislação vigente, vem construindo seu arcabouço normativo no âmbito do governo federal, e apesar de recente, se comparado ao arcabouço de leis, normas, padrões dos países desenvolvidos, tem destaque de atuação e reconhecimento nacional e internacional de sua competência em temas diretamente correlacionados à segurança cibernética. Vale aqui destacar, a competência técnica nacional de tratamento e resposta a incidentes de redes computacionais de governo, (o que significa, em resumo, ações de segurança contra ataques dos chamados malwares[25]), reconhecida em nível nacional e internacional.

Outrossim, como passos iniciais para a construção da trilha da segurança cibernética no âmbito da administração pública federal, direta e indireta (APF), o Gabinete de Segurança Institucional da Presidência da República (GSIPR), por intermédio de seu Departamento de Segurança da Informação e Comunicações (DSIC), vem articulando e promovendo com a efetiva colaboração de representantes de vários órgãos da APF, membros do Comitê Gestor de Segurança da Informação (CGSI), um conjunto de normas visando assegurar a segurança da informação e comunicações no governo, bem como, vem, alavancando a instituição de grupos de trabalhos e técnicos, e a formação de recursos humanos, para o tratamento de temas relacionados à segurança cibernética[26].

Apresenta-se, a seguir, a série disciplinar mais recentemente publicada no país, no sentido de ampliar a disseminação de tal marco normativo, bem como, estimular que a sociedade participe de perto desta construção, notadamente, tanto a comunidade científica e tecnológica, com sua P&D de excelência, na proposição e desenvolvimento da(s) melhor(es) solução(ões) tecnológica(s) e metodológica(s), quanto a comunidade do setor privado, atuando de forma inovadora, no lançamento no mercado de novos produtos, processos e serviços de valor agregado.

Como marco mais recente e relevante para o tema em pauta pode-se citar a publicação da Instrução Normativa IN GSIPR No. 01/2008, que disciplina compulsoriamente a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, a qual define que "Segurança da Informação e Comunicações (SIC) são ações que objetivam viabilizar

24 Brasil é o segundo na lista dos países que mais produzem malware. (Dinponível em: <http://www.nosi.cv/index.php?option=com_content&task=view&id=189> Acesso em: 02 set 2009.)

25 Artefatos maliciosos que são entendidos em geral como qualquer programa de computador construído com a intenção de provocar danos, obter informações não autorizadas, ou interromper o funcionamento de sistemas e/ou redes de computadores.

26 A competência e o escopo de atuação dos órgãos citados, são definidos nos seguintes instrumentos legais: a) criação do GSIPR: Lei No. 10.683 de 28/05/2003; b) criação do DSIC/GSIPR: Decreto No. 5.772 de 08/05/2006; e, c) criação do CGSI: Art. 6o. do Decreto No. 3.505 de 13/06/2000.

e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações", inovando e ampliando, portanto, o escopo tradicionalmente conhecido e adotado na segurança da informação.

Os conceitos definidos na citada IN GSIPR 01/2008, permitem evidenciar os parâmetros e os valores prioritários de SIC, conforme apresentados a seguir: "a) disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade; b) integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental; c) confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado; e, d) autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou *entidade*".

Os desdobramentos necessários à implementação do que é disciplinado pela citada IN são produzidos e publicados na forma de Normas Complementares (NC), colocadas como ações adicionais e compulsórias para a APF.

No que se refere aos temas mais diretamente correlacionados ao desenvolvimento e implantação da SIC nos órgãos e entidades da APF, a produção e respectiva publicação no D.O.U de NCs ocorreu em 2009, com as seguintes publicações:

1. NC 03/IN01/DSIC/GSIPR "Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal", Portaria No. 29, publicada no D.O.U No. 125, de 03 de julho de 2009;

2. NC 04/IN01/DSIC/GSIPR "Gestão de Risco de Segurança da Informação e Comunicações - GRSIC nos Órgãos e Entidades da Administração Pública Federal", Portaria No. 37, publicada no D.O.U No. 156, de 17 de agosto de 2009; e,

3. NC 05/IN01/DSIC/GSIPR "Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos Órgãos e entidades da Administração Pública Federal," Portaria No. 38, publicada no D.O.U No. 156, de 17 de agosto de 2009.

Este marco disciplinar certamente representará um desafio a ser enfrentado pela APF, porém, é sabido que no cenário atual não é plausível aceitar certas vulnerabilidades, e, portanto, meios e mecanismos deverão ser articulados para o sucesso das novas implementações em todos os órgãos e entidades da APF.

Neste contexto, destacam-se os avanços até então alcançados, como resposta à percepção de necessidade de prover quadros no campo de conhecimento de SIC, desde 2006 até julho de 2009, pelo DSIC/GSIPR, em que foram utilizados recursos orçamentários destinados à formação de recursos humanos da seguinte forma: a) eventos de sensibilização tipo palestras sobre o tema para um público estimado de 24 mil pessoas tanto no Brasil quanto no exterior; b) eventos de conscientização tipo seminários, oficinas e congressos para 2.372 servidores públicos distribuídos por mais de 40 instituições da administração pública federal espalhados em diversas capitais pelo Brasil; c) eventos de capacitação tipo cursos básicos e de fundamentos para 395 servidores públicos de 38 instituições da administração pública federal em Brasília, Rio de Janeiro, São Paulo, Porto Alegre e Fortaleza; e, d) eventos de especialização tipo curso de pósgraduação para 80 servidores públicos e militares de 23 instituições da administração pública federal, em duas turmas. No processo de evolução, está planejado para 2009 a formatação e execução de cursos básicos de fundamentos e de especialização à distância.

O Curso de Especialização em Gestão da Segurança da Informação e Comunicações, iniciado em 2007, no âmbito da Universidade de Brasília (UnB), Departamento de Ciência da Computação (DCE), conta, atualmente, com uma carga horária de 375 horas/aula, turmas presenciais de 40 alunos cada, seleção de alunos da APF, está na sua 2a. edição, e tem previsão de lançamento da 3a turma no final deste ano, com novo modelo de desenvolvimento, passando a ser disponibilizado à distância. Além disso, avançar na modelagem e na articulação deste curso de especialização para um mestrado profissional, faz parte dos desafios colocados para 2010, aos parceiros da academia que colaborarão e participarão do novo processo. Vale dizer que dos 40 alunos da primeira turma deste curso de especialização, 34 servidores públicos e militares concluíram o mesmo, tendo depositado suas monografias nas bibliotecas da UnB e da Presidência da República.

Soma-se o fato de que outros temas e campos de atuação continuarão a serem desenvolvidos e disciplinados, sempre na direção de disciplinar a SIC na APF, e de contribuir com a evolução das práticas governamentais ao nível de mercado, criando um ambiente propício à trilha da segurança cibernética nacional.

Diante dos temas novos e desafiadores, bem como da necessária atualização conceitual, metodológica e respectiva proposição de ações continuadas, outras iniciativas que visam promover a SIC na APF, já incorporando a segurança cibernética como pano de fundo, estão sendo empreendidas com apoio e no âmbito do Comitê Gestor de Segurança da Informação, como é o caso da Portaria No. 34 que institui o "Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação" e da Portaria No. 35 que institui o "Grupo de Trabalho de Criptografia", publicadas no D.O.U. No. 149 e 150, de 06 e 07 de agosto de 2009.

5.1. E o Brasil frente ao problema

Acostumou-se, regra geral, a entender que as grandes questões que habitam a agenda internacional são internalizadas no país com certo atraso. Isso não corresponde à verdade neste caso. Pode-se perceber, nas sessões anteriores , que as ações nos países ditos mais desenvolvidos ainda se encontram em uma fase, preparatória, incipiente.

No país está sendo acompanhado par e passo a evolução do tema e seus desdobramentos. Vale notar que em 8 de outubro de 2008, após cerca de um ano de estudos realizados pelo Gabinete de Segurança Institucional da Presidencia da Republica (GSIPR), por intermédio do Departamento de Segurança da Informação e Comunicações (DSIC) a respeito do tema, o assunto foi apresentado na forma de uma proposta para a elaboração de uma Estratégia de Segurança e de Defesa Cibernética para o País em uma reunião extraordinária da Câmara de Relações Exteriores e Defesa Nacional (Creden), do Conselho de Governo convocada extraordinariamente para este fim. Naquela ocasião, após a apresentação do assunto e do modelo proposto, os membros daquela Câmara, após uma discussão breve deliberaram pela aprovação da iniciativa proposta por unanimidade.

Para dar mais consistência àquela decisão, durante os oito meses seguintes, por determinação do GSIPR, o DSIC ampliou o estudo buscando nesta fase inicial, principalmente, entender como os demais países estavam se preparando e que metodologia estavam empregando para fazer frente à esta ameaça. Foram realizadas visitas técnicas e consultas a alguns Governos e a conclusão a que se chegou é de que não existem modelos totalmente prontos e nem um entendimento consensado de como enfrentar a questão de forma estruturada.

Em agosto do corrente ano o assunto foi apresentado ao Presidente da República, Luiz Inácio Lula da Silva, que deu a sua aprovação para que o tema fosse formalmente introduzido na agenda da Administração Pública Federal. Assim, o Diário Oficial da União de 9 de setembro de 2009 publicou a Portaria No. 45, do Ministro Chefe do GSIPR, que também é o Presidente da Creden instituindo no âmbito daquela Câmara de Relações Exteriores e Defesa o Grupo Técnico de Segurança Cibernética.

Este Grupo, composto por representantes dos Ministérios da Justiça, da Defesa, das Relações Exteriores, e dos Comandantes da Marinha; do Exército e da Aeronáutica. Coordenados pelo representante do Ministro Chefe do GSIPR, terá como objetivo propor diretrizes e estratégias para a Segurança Cibernética, no âmbito da Administração Pública Federal, uma missão considerada de relevante interesse público e do Estado. A designação da Coordenação é do GSIPR, com a indicação de que a mesma será exercida por intermédio do DSIC, bem como, há a

oportunidade de que sejam convidados especialistas, da academia e do setor privado, visando uma construção participativa.

Os pressupostos que levaram a criação deste grupo podem ser encontradas naquela proposta original à Creden e foram resumidas nos "considerando" da citada Portaria. Merece destaque naquele texto legal o fato de ter sido explicitado a salvaguarda de que a preocupação com a segurança das informações não pode servir de excusas à necessaria transparência dos atos públicos.

Os conceitos sobre Seguranca Cibernética; Infraestruturas Críticas e Ativos de informação, apresentados neste artigo, também foram explicitados naquela Portaria.

Apesar do Grupo ainda está em processo de nomeação com os inícios dos trabalhos previstos para a primeira semana de novembro de 2009, já existe um documento base para auxiliar o inicio dos trabalhos, o qual ainda não conta com a aprovação do GT, a quem caberá complementar e aprimorar as idéias nele contida.

Este documento apresenta, em essência os primeiros passos para a construção de uma Estratégia Nacional de Segurança Cibernética, tomando como base a monografia do autor, citada na nota de rodapé no. 08. .

O modelo preconiza desde medidas de proteção, passando pelo desenvolvimento da capacidade de dissuasão, e propõem um amplo programa de capacitação, que se inicia nas ações de conscientização e tem seu auge no preparo específico e aprofundado de todos que têm responsabilidade pela gestão da infraestrutura crítica de informação na APF.

Não se pode deixar de registrar como mais um importante passo na trilha da segurança e da defesa cibernética do país o Decreto Nº 6.703/2008[27] que aprova a Estratégia Nacional de Defesa, e tem em sua dimensão a questão cibernética tratada no que se refere às tecnologias, capacitações, parcerias estratégicas e intercâmbios com nações amigas, neste último caso particularmente com as nações do entorno estratégico brasileiro e as da Comunidade de Países de Língua Portuguesa.

5.2. Esboço de uma estratégia de segurança cibernética para o Brasil

Ao se propor a definição para Estratégia de Segurança Cibernética optou-se por iniciá-la com a palavra "arte" tendo em mente que se tratava de uma tarefa única. Não existem modelos a serem seguidos, pois, como apresentado , são poucas as nações que se debruçaram sobre o tema,

27 ESTRATÉGIA Nacional de Defesa (Disponível em: <*http://www.fab.mil.br/portal/defesa/estrategia_defesa_nacional_portugues.pdf*> Acesso em: 07 mai 2009)

e aquelas que o fizeram ainda estão construindo seus referenciais teóricos e práticos. Mesmo se houvessem referências elas ajudariam em parte, pois essa tarefa, que exige muita criatividade, tem que ser construída baseada, sobretudo em muito conhecimento das características próprias de cada Estado e Sociedade. Assim, para que a arte de assegurar a existência e a continuidade da Sociedade da Informação da nação brasileira, garantindo e protegendo, no Espaço Cibernético, os ativos de informação e as infraestruturas críticas do país, seja efetiva, sem a pretensão de esgotar o assunto, indicam-se as seguintes condições essenciais:

- conhecer o grau de vulnerabilida de do país em relação aos seus sistemas de informação e as suas infraestruturas críticas de informação;
- Identificar os serviços críticos essenciais da infraestrutura de informações para o funcionamento da infraestrutura crítica;
- determinar o grau de dependência dos serviços das infraestruturas críticas de informações sobre as infraestruturas críticas;
- desenvolver uma metodologia comum para avaliar a vulnerabilidade das infraestruturas críticas de informação dos seus sistemas e de seus serviços;
- elaborar uma metodologia para avaliações de risco em segurança cibernética;
- conceber um sistema de medidas preventivas contra ataques cibernéticos;
- compreender que a segurança cibernética só se dará plenamente se, na informatização de seus sistemas críticos, o conceito de segurança da informação e comunicações forem observados de forma eficiente;
- estabelecer que às aquisições de produtos e serviços usados em sistemas críticos devam ser testados e certificados por critérios próprios à APF;
- desenvolver algoritmos criptográficos próprios e estabelecer critérios para seu uso;
- construir o marco legal contra ataques cibernéticos;
- estabelecer programas de cooperação entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional;
- estreitar parcerias e ações colaborativos com o setor privado;
- desenvolver programa nacional de capacitação em segurança cibernética e recrutamento, que seja construído à partir da visão interdisciplinar que o tema requer, nos níveis básico técnico, graduação, especialização, mestrado e doutorado; e,
- promover e fortalecer a pesquisa, o desenvolvimento, e a inovação em segurança cibernética e temas correlatos.

6. Considerações finais

É essencial em termos políticos, econômicos e sociais, na era atual da nova Sociedade da Informação, que depende fortemente da base educacional, do desenvolvimento científico e tecnológico, e da capacidade de articulação e de promoção de parcerias de uma nação, que seja formulada a estratégia de segurança cibernética brasileira.

Certamente, a segurança cibernética requer um maior diálogo e consequente fortalecimento nas relações da tríplice hélice (governo, academia e setor privado), bem como, o fortalecimento, em nível nacional e internacional, da cooperação técnica e da inserção do país em fóruns de formação de opinião e de decisão.

Frisa-se que para tanto a cooperação internacional e o desenvolvimento de *framework* harmonizado, tornaram-se requisitos essenciais para enfrentar os desafios de segurança das infraestruturas críticas dos países, em especial da infraestrutura crítica da informação de cada nação, de cada região econômica, enfim, da "aldeia global".

A segurança cibernética, e as respectivas derivações oriundas da complexidade da mesma, permitem depreender que a comunidade global, em especial de governo, de pesquisa, de ensino, da iniciativa privada e do terceiro setor, deverá entender concretamente a envergadura deste tema estratégico. E, consequentemente, deverá empreender esforços de mobilização e de articulação de mecanismos para compartilhar soluções e melhores práticas de segurança da infraestrutura crítica da informação, fortalecendo, assim, a vigilância, a próatividade, e a inovação, de forma a responder e minimizar os riscos cibernéticos.

No atual cenário é preciso, sem qualquer sombra de dúvidas, aumentar significativamente a formação de recursos humanos especializados em segurança cibernética e em áreas correlatas, em todos os níveis, desde a formação básica, passando pela técnica, e alcançando até o mais alto nível da pósgraduação. Pois, de nada vale a melhor capacitação técnica se não se conscientizar o usuário, o profissional o cidadão, destas tecnologias, e de que a segurança da informação e, conseqüentemente, a segurança cibernética, é um problema de todos. Assim sendo, esta conscientização deve ser iniciada desde o ensino fundamental, criando uma cultura orientada a esta abordagem, pois é inegável que a cada dia a iniciação digital se dá em idades mais precoces.

O Brasil tem, portanto, o desafio a enfrentar, qual seja, ao mesmo tempo em que vem se organizando e ganhando espaço de reconhecido destaque de sua atuação no tema, vê ampliada sua responsabilidade, dado seu papel de destaque no processo de tomada de decisão no contexto das nações.

Finalmente, muito há ainda que ser dialogado e construído, o desafio é realmente de todos, e, claro, do mundo. Este artigo não pretendeu ser exaustivo em relação às estratégias e às ações do governo brasileiro, e de outras economias, no âmbito deste tema tão complexo, portador de futuro, e instigante, e sim, pretendeu, disseminar uma síntese do cenário mundial atual, e os passos mais recentes do governo brasileiro, realizados no âmbito do GSIPR , em prol da construção da trilha da segurança cibernética para o país, como forma de subsidiar o debate nacional e a criação de agenda específica.

Referências

ANTONIOLI, Leonardo. **Estatísticas, dados e projeções atuais sobre a Internet no Brasil.** Disponível em: <http://www.tobeguarany.com/internet_no_brasil.php>. Acesso em: 02 set. 2009.

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (APDSI). **Glossário da Sociedade da Informação.** Portugal: APDSI. 2005.

BRASIL. Decreto n. 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa e dá outras providências. Disponível em: <http://www.fab.mil.br/portal/defesa/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 07 maio 2009.

BRASIL é o segundo na lista dos países que mais produzem malware. Disponível em: http://www.nosi.cv/index.php?option=com_content&task=view&id=189. Acesso em 02 set. 2009.

BRASIL. Gabinete de Segurança Institucional da Presidência da República (GSIPR). Lei n. 10.683 de 28 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.683.htm>. Acesso em: 17 dez. 2009.

BRASIL. Instrução Normativa de 13 de junho de 2008. Disciplina a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta. **Diário oficial da União**, n. 115, 18 jun. 2008.

BRASIL. Norma Complementar 03/IN01/DSIC/GSIPR. Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. **Diário oficial da União,** n. 125, 03 jul. 2009.

BRASIL. Norma Complementar 04/IN01/DSIC/GSIPR. Gestão de Risco de Segurança da Informação e Comunicações – GRSIC nos Órgãos e Entidades da Administração Pública Federal. **Diário oficial da União,** n. 156, 17 ago. 2009.

BRASIL. Norma Complementar 05/IN01/DSIC/GSIPR. Criação de Equipes de Tratamento e resposta a Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal. **Diário oficial da União** n. 125, 03 jul. 2009.

BRASIL. Portaria n. 34, de 05 de agosto de 2009. Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. **Diário oficial da União,** n. 149, 06 ago. 2009.

BRASIL. Portaria n. 35, de 06 de agosto de 2009, Institui Grupo de Trabalho de Criptografia, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Diário oficial da União, n. 150, 07 ago. 2009.

BRASIL. Portaria n. 45, de 08 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Diário Oficial da União, n. 172, 09 set. 2009.

BRASIL. Presidência da República. **Portal do Departamento de Segurança da Informação e Comunicações.** Disponível em: <http://dsic.planalto.gov.br>. Acesso em 17 dez. 2009.

CABINET OFFICE. **Cyber security strategy of the United Kingdom:** safety, security and resilience in cyber space. UK Office of Cyber Security (OCS) and UK Cyber Security Operations Centre (CSOC). UK: TSO, Jun. 2009. 25 p.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. **Securing Cyberspace for the 44th**. Report of the CSIS Commission on Cybersecurity for the 44th. Washington: Presidency, Dec. 2008. 88 p.

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI). **Art. 6º**. Decreto n. 3.505 de 13 jun. 2000.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (DSIC/GSIPR). Decreto n. 5.772 de 08 maio 2006.

DEPARTMENT OF HOMELAND SECURITY. **National infrastructure protection plan:** partnering to enhance protection and resiliency. EUA: DHS, 2009. p. 12.

ENTREVISTA de Mariana Lucena sobre Segurança Cibernética. **Revista Galileu**. Disponível em: <http://dsic.planalto.gov.br/noticias/65-entrevista-do-diretor-do-dsic-a-revista-galileu>. Acesso em: 02 set. 2009.

GLOSSÁRIO das Forças Armadas: MD35-G-01. 2007.

INGLATERRA e EUA se aliam na Segurança Cibernética. Convergência digital, 26 jun. 2009. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=19362&sid=18&tpl=printerview>. Acesso em: 02 set. 2009.

INTERNATIONAL TELECOMMUNICATION UNION. **Global Cybersecurity Agenda (GCA)**: framework for international cooperation. Switzerland: ITU, 2007. p. 10.

MANDARINO JR., R. Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro. Monografia aprovada no Curso de Especialização em Gestão da Segurança da Informação e Comunicações. Brasília: Universidade de Brasília - UnB/ Departamento de Ciência da Computação, jun. 2009. p. 29.

MICROSOFT. Microsoft security intelligence report. EUA: Microsoft. Jul.-Dec. 2008. 183 p. 6.v.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Guidelines for the security of information systems and networks:** towards a culture of security. Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002. Paris: OECD, 2002. 28p

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) **Recommendation of the council on the protection of critical information infrastructure**. Adopted as a Recommendation of the OECD Council at its 1172th Session on 30 April 2008. Seoul, Jun. 2008.

SILVA, P. F. Ameaça Cibernética: a ciência e a tecnologia significam progresso mas também criam vulnerabilidades e ameaças. In: DEFESA Latina, jul.-set. 2009. p. 52-54.

SOUZA, Taynah Lopes de; CANONGIA, Claudia. **Technical infrastructure and its importance to national systems of innovation in BRICS**. Projeto "Estudo Comparativo dos Sistemas de Inovação no Brasil, Rússia, Índia, China e África do Sul" – BRICS – Nota Técnica Final em Inglês. Brasília: CGEE, jul. 2007. 29p. Disponível em: <http://www.cgee.org.br/atividades/consultaProduto.php?f=1&idProduto=4111>. Acesso em: 17 dez. 2009.

SUND, Christine. Promoting a culture of Cybersecurity. In.: ITU REGIONAL CYBERSECURITY FORUM FOR EASTERN AND SOUTHERN AFRICA, Lusaka, 25-28 Aug. 2008. Lusaka: ITU, 2008.

TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil**: Livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. 195p.

THE SEC DEV GROUP. **Tracking GhostNet**: investigating a cyber Espionage network. Mar. 2009. 53 p. Disponível em: <http://www.infowar-monitor.net/ghostnet>. Acesso em 08 abr. 2009.

TIM Berners-Lee convoca participantes da **Campus Party Brasil** para construir o futuro da Internet. Campus Party Brasil, 2009. (acesso web em 02/09/2009; http://www.campus-party.com.br/index.php/release-5.html)

WOLOSZIN, A. L. A ameaça invisível do terror cibrnético. **Jornal do Brasil-Internacional,** ano 3, 14 ago. 2009.