em discussão!
Os principais debates do Senado Federal
Ano 5 - Nº 21 - julho de 2014

ESPIONAGEM CIBERNÉTICA

Rede vulnerável

Para CPI, é preciso aparelhar inteligência nacional e melhorar gestão da internet

REDISCUSSÃO

Peças de motos terão padrão de qualidade

PRÓXIMA EDIÇÃO

O futuro do lixo

O SENADO VOTOU. AGORA É LEI

Resolução da Participação Popular nos Projetos de lei do Senado

Secom | Criação e Marketing

Projetos de Lei do Senado Federal: Opinar é um ato de cidadania

O Senado Federal aprovou resolução que torna mais fácil a participação popular durante a tramitação de uma lei. Agora, qualquer pessoa pode entrar no Portal e-Cidadania, ler na íntegra os projetos de lei e expressar sua concordância ou não em relação a eles.

É o Senado Federal cada vez mais próximo e conectado com as necessidades da população.

Saiba mais em:
www.senado.leg.br/agoraelei

SENADO FEDERAL

Aos leitores

Em duas décadas, a internet invadiu o dia a dia de pelo menos metade dos mais de 7 bilhões de habitantes do planeta. Ofereceu serviços preciosos e hoje é a principal fonte de informações em diversos países. Textos, áudios, vídeos são publicados continuamente na rede, causando grande impacto na economia, chacoalhando as tradicionais mídias de massa, diminuindo a leitura de jornais e a audiência da televisão.

Ao mesmo tempo em que tomou o mundo de assalto, garantindo liberdade de expressão nunca antes vista, a ubíqua internet trouxe consigo a possibilidade de controle do trânsito de dados e até mesmo dos conteúdos que circulam pela rede, trazendo riscos à confidencialidade de informações de empresas e governos e à privacidade dos cidadãos.

O que era uma suspeita tornou-se certeza com as revelações do ex-técnico da Agência de Segurança Nacional (NSA) dos Estados Unidos Edward Snowden. Segundo ele, o governo norte-americano, sob a justificativa de garantir a segurança do país contra o terrorismo, bisbilhotou as comunicações eletrônicas não apenas de suspeitos, mas de pessoas, autoridades e instituições de países amigos, como Brasil e Alemanha.

Mas o que viria a seguir talvez tenha sido ainda mais revelador. Apesar de as iniciativas americanas terem sido classificadas no campo diplomático como grande ofensa à soberania de nações amigas, nada de prático aconteceu para que ações como aquelas não se repetissem. Pelo contrário, a influência norte-americana sobre a internet ficou óbvia. Pior, as propostas de alterar a governança da internet não prosperaram. Diante dessa realidade, resta aos países que foram — e são — vítimas das invasões das agências de espionagem dos EUA protegerem-se.

O diagnóstico da situação e as propostas para que o Brasil melhore a segurança das próprias informações estão amplamente descritos no relatório final da Comissão Parlamentar de Inquérito (CPI) da Espionagem, que funcionou no Senado Federal a partir das denúncias de Snowden. O melhor aparelhamento do Sistema Brasileiro de Inteligência (Sisbin) — hoje carente de regras, estrutura e orçamento — é um dos focos do relatório.

O documento, de autoria do senador Ricardo Ferraço (PMDB-ES), é a base para esta edição de **Em Discussão!**, que apresenta a vulnerabilidade da informação na internet, o jogo de poder sobre a rede e o que pode ser feito para que a liberdade dos usuários não seja tolhida por medidas justificadas pela necessidade de segurança.

Boa leitura!

SUMÁRIO

Mesa do Senado Federal

Presidente: Renan Calheiros
Primeiro-vice-presidente: Jorge Viana
Segundo-vice-presidente: Romero Jucá
Primeiro-secretário: Flexa Ribeiro
Segunda-secretária: Ângela Portela
Terceiro-secretário: Ciro Nogueira
Quarto-secretário: João Vicente Claudino
Suplentes de secretário: Magno Malta, Jayme Campos, João Durval e Casildo Maldaner

Diretor-geral e secretário-geral da Mesa: Luiz Fernando Bandeira

Expediente

Secretaria de Comunicação Social

SENADO FEDERAL

Diretor: Davi Emerich
Diretor-adjunto: Flávio de Mattos
Diretor de Jornalismo: Eduardo Leão

A revista **Em Discussão!** é editada pela Secretaria Agência e Jornal do Senado

Diretor: Marco Antonio Reis
Diretor-adjunto: Flávio Faria
Editor-chefe: João Carlos Teixeira
Editores: Janaína Araújo, Joseana Paganine, Thâmara Brasil e Sylvio Guedes
Reportagem: Janaína Araújo, Joseana Paganine, Thâmara Brasil e Sylvio Guedes
Capa e página 3: Priscilla Paz sobre imagens de freeimages.com
Diagramação: Bruno Bazílio e Priscilla Paz
Arte: Bruno Bazílio, Cássio Sales Costa, Diego Jimenez e Priscilla Paz
Revisão: Fernanda Vidigal, Juliana Rebelo, Pedro Pincer e Tatiana Beltrão
Pesquisa de fotos: Bárbara Batista, Braz Félix e Leonardo Sá
Tratamento de imagem: Edmilson Figueiredo
Circulação e atendimento ao leitor: (61) 3303-3333

Tiragem: 2.500 exemplares

Site: www.senado.leg.br/emdiscussao
E-mail: emdiscussao@senado.leg.br
Twitter: @jornaldosenado
www.facebook.com/jornaldosenado
Tel.: 0800 612211
Praça dos Três Poderes, Anexo 1 do Senado Federal, 20º andar, 70165-920, Brasília, DF

Impresso pela Secretaria de Editoração e Publicações (Seep)

REPRODUÇÃO

Contexto

PETE MAROVICH

Mundo

Realidade Brasileira

MARCOS OLIVEIRA/AGÊNCIA SENADO

MARCOS OLIVEIRA/AGÊNCIA SENADO

Propostas

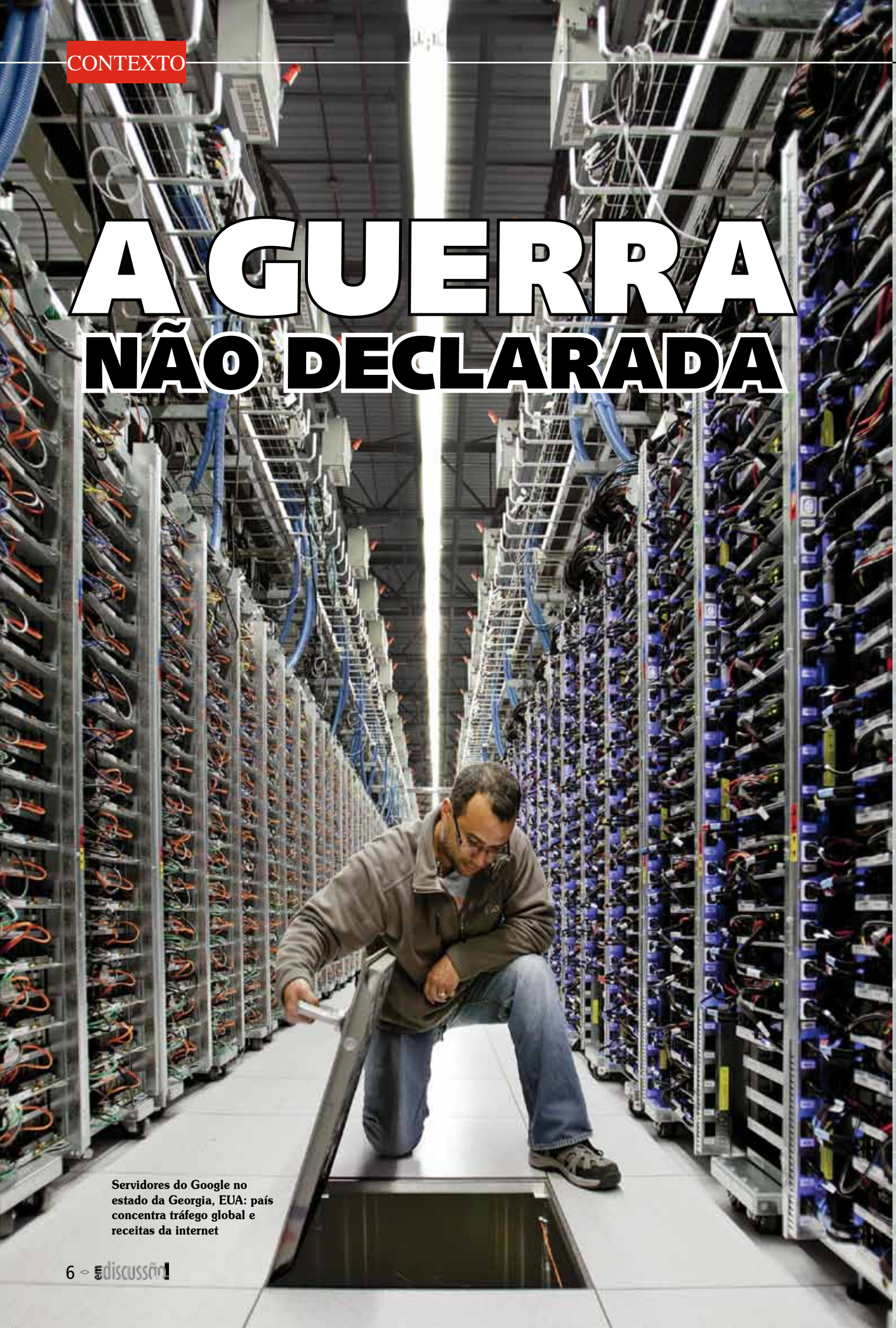
Rediscussão

Próxima edição

A tramitação dos projetos pode ser acompanhada no site do Senado: www.senado.leg.br

Veja e ouça mais em:

A GUERRA NÃO DECLARADA



Servidores do Google no estado da Georgia, EUA: país concentra tráfego global e receitas da internet

Sociedade moderna desfruta os avanços proporcionados pela tecnologia, mas interconexão global também abre caminho para invasão da privacidade e para corrida entre potências pelo controle da informação

Em vários campos, as tecnologias de informação e comunicação promoveram uma revolução na sociedade moderna. A educação e o atendimento médico a distância, o acelerado desenvolvimento científico-tecnológico e o comércio eletrônico são alguns exemplos.

Ao mesmo tempo, a interconexão abriu caminho para novos e alarmantes níveis de invasão de privacidade. Expressões como crimes cibernéticos e espionagem cibernética já fazem parte do dia a dia. É o dilema contemporâneo que opõe a cultura do compartilhamento à necessidade de segurança e confidencialidade.

Já havia sinais claros de crescimento preocupante dos incidentes de invasão de computadores e redes, os chamados ataques. O que poucos podiam imaginar é que dezenas de milhões de cidadãos em todo o mundo estariam expostos, diariamente, à vigilância de seus passos por programas que vasculham e espionam tudo o que se escreve, se lê ou se fala pela internet ou ao telefone celular.

A confirmação veio em junho do ano passado, na forma de uma denúncia do ex-agente norte-americano Edward Snowden, hoje provisoriamente asilado na Rússia: a Agência de Segurança Nacional (NSA) dos Estados Unidos dispõe de um sistema que monitora as comunicações dentro e fora do país. Ninguém estaria seguro, nem mesmo dirigentes de nações amigas, como ficou evidente. As motivações para a espionagem podem ser estratégicas, políticas ou meramente comerciais — tanto que, no caso brasileiro, a presidente da República, Dilma Rousseff, e a Petrobras foram alguns dos alvos.

O clamor internacional contra a espionagem cibernética, que se tornou mais forte a partir das denúncias de Snowden, se voltou especificamente contra os Estados Unidos, mas, na verdade, os especialistas não têm dúvidas de que a prática está disseminada mundo afora.

"Não é segredo para ninguém que os governos são capazes de interceptar ligações telefônicas e mensagens de texto. Hoje em dia, já existem várias empresas que oferecem aos governos programas capazes de invadir seu computador, usar sua *webcam*, ler seus e-mails, copiar documentos, fazer o que quiser, sem serem detectados", disse o pesquisador e ativista cibernético da União Americana pelas Liberdades Civis Christopher Soghoian.

Reações contundentes

Hegemônicos após a ruína do bloco soviético, os Estados Unidos se veem cada vez mais desafiados em termos econômicos e políticos pela China, mas ainda preservam grande influência global, especialmente no que diz respeito às tecnologias da informação, até por causa das origens da internet, nas Forças Armadas americanas.

A reação brasileira foi contundente, mas limitada à esfera diplomática. Em nota oficial, a Presidência afirmou que "as práticas ilegais de interceptação das comunicações e dados de cidadãos, empresas e membros do governo brasileiro constituem fato grave, atentatório à soberania nacional e aos direitos individuais e é incompatível com a convivência democrática entre países amigos". Dias

CONNIE ZHOU/GOOGLE

depois, a presidente Dilma Rousseff adiou a visita oficial aos EUA que estava programada para outubro (em 3 de junho deste ano, Dilma reiterou que "ainda não existem condições para uma visita de Estado a Washington").

Em setembro de 2013, ao discursar na abertura da 68ª Assembleia Geral das Nações Unidas (ONU), em Nova York, Dilma condenou as práticas de espionagem. "Jamais pode o direito à segurança de cidadãos de um país ser garantido mediante a violação de direitos humanos e fundamentais dos cidadãos de outro país", afirmou. "Não se sustentam argumentos de que a interceptação ilegal de informações e dados destina-se a proteger as nações contra o terrorismo. O Brasil repudia, combate e não dá abrigo a grupos terroristas".

Protestos nas ruas e manifestações oficiais de repúdio ocorreram ao redor do mundo, inclusive entre tradicionais aliados de Washington. A Justiça da Alemanha decidiu, em junho de 2013, investigar as escutas ao celular da chanceler Angela Merkel pela NSA.

No continente americano, a União de Nações Sul-Americanas (Unasul) e o Mercosul emitiram declarações condenando a espionagem das comunicações. Somente em janeiro deste ano o presidente dos Estados Unidos, Barack Obama, prometeu colocar um fim à espionagem de dirigentes de nações aliadas, "a menos que a segurança nacional esteja em jogo".

ROBERTO STUCKERT FILHO/PR

Dilma na Assembleia Geral da ONU, em Nova York, três meses após as denúncias: presidente critica interceptações ilegais de dados feitas pelos Estados Unidos

Resolução da ONU

Na ONU, Brasil e Alemanha apresentaram uma proposta de resolução, aprovada por consenso entre os 193 integrantes da Assembleia Geral, pela qual o mesmo direito à privacidade de que as pessoas devem desfrutar fora da rede deve ser protegido on-line. O texto conclama os países-membros a cessarem eventuais violações e a criarem mecanismos independentes de supervisão de modo a assegurar transparência e responsabilização por possíveis transgressões.

"A proposta dá o tom do que se deseja: ampliar e reafirmar na era digital o direito à privacidade, contemplado em distintos instrumentos internacionais. É o primeiro passo no sentido de conter, ainda que minimamente, a intrusão de determinados órgãos de governo de diferentes países nas comunicações, sobretudo on-line, de estrangeiros", realçou o relator da CPI da Espionagem, senador Ricardo Ferraço (PMDB-ES). "É um avanço contra as flagrantes ações de espionagem que visam atingir governos e economia de diversos países", completou Vanessa Grazziotin (PCdoB-AM), que presidiu a CPI da Espionagem.

MARCOS OLIVEIRA/AGÊNCIA SENADO

Vanessa Grazziotin considera resolução aprovada na ONU avanço contra flagrantes ações de espionagem

JOSÉ CRUZ/AGÊNCIA SENADO

Proposta apresentada por Brasil e Alemanha amplia e reafirma o direito à privacidade na era digital

Fato é que, há muito tempo, a guerra cibernética está, ainda que informalmente, declarada. O primeiro relatório global sobre ciberdefesa, publicado em 2012 pela Security & Defence Agenda (centro de estudos do setor, com sede em Bruxelas), revelou que 57% dos especialistas mundiais confirmaram essa sensação, enquanto 43% deles apontaram danos ou inoperância de estruturas críticas de informação como a maior ameaça representada pelos ciberataques.

Os eventos relacionados ao ambiente cibernético nos últimos anos mostram que há países que já vivem uma "Guerra Fria cibernética", afirma Samuel César da Cruz Júnior, pesquisador do Instituto de Pesquisa Econômica Aplicada (Ipea), no estudo *A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual*.

Atraso na segurança

Desde a década passada, entidades como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) — que reúne as mais ricas nações do Ocidente e alguns países emergentes, como Turquia e México — já alertavam para as vulnerabilidades. Um documento de 2009 recomendava aos países-membros estabelecer níveis de segurança em sistemas e redes de informação e comunicações e explicava por quê: pesquisa da Universidade de Toronto, no Canadá, descobriu que 1.295 computadores em 103 países estavam sendo espionados — desses, 30% pertenciam a ministérios de Relações Exteriores, embaixadas, organizações internacionais, empresas de comunicação e organizações não governamentais, inclusive com acesso a conhecimento sensível.

No caso brasileiro, há um longo caminho a ser percorrido. A maior parte das redes da administração pública federal apresenta níveis inaceitáveis de segurança, como revela pesquisa divulgada em 2012 pelo Tribunal de Contas da União (TCU) junto a 337 instituições públicas: 73% dos órgãos pesquisados não classificam a informação, 90% não fazem análise de riscos e 55% não possuem política de segurança da informação.

BRIZZA CAVALCANTE/CD

Vigilância indiscriminada feita por governos é chocante, diz o especialista em segurança da informação Peter Gill

As medidas adotadas pelos órgãos de governo e pelo TCU estariam surtindo efeito, mas lentamente. "Há bastante espaço para melhoria, haja vista que muitas instituições ainda possuem nível de capacidade baixo para muitos aspectos avaliados", disse o presidente do TCU, Augusto Nardes.

Para Samuel César da Cruz Júnior, do Ipea, tanto a segurança quanto a defesa cibernética do Brasil ainda se encontram em estágio embrionário de organização, mesmo que algumas ações já venham sendo tomadas. "Por outro lado, nota-se que as maiores economias mundiais, bem como demais países em desenvolvimento, também não estão muito avançados em relação à sistematização e organização dos mecanismos de proteção cibernética. A começar pelos Estados Unidos, que apenas em 2009 criaram, oficialmente, o Comando de Defesa Cibernética", diz ele, em estudo publicado em julho de 2013, um mês após as denúncias de Snowden.

JANE ARAÚJO/AGÊNCIA SENADO

Presidente do TCU, Augusto Nardes vê possível melhoria nos atuais níveis de segurança das redes do governo federal

Em outubro do ano passado, o governo brasileiro anunciou que iria criar um sistema nacional de e-mail criptografado para evitar que autoridades sejam alvo de espionagem. O sistema será desenvolvido pelo Serviço Federal de Processamento de Dados (Serpro), em parceria com os Correios, e terá uso obrigatório no governo. Até hoje, no entanto, o sistema não foi implantado.

"A construção de um ambiente digital seguro depende do pleno controle sobre a rede de comunicações digitais e do tráfego de aplicações nessa rede. Porém, a lógica do modelo em nuvem mantém a produção e o desenvolvimento tecnológico no país de origem do fornecedor", disse Rafael Moreira, secretário-adjunto de Política de Informática do Ministério da Ciência, Tecnologia e Inovação.

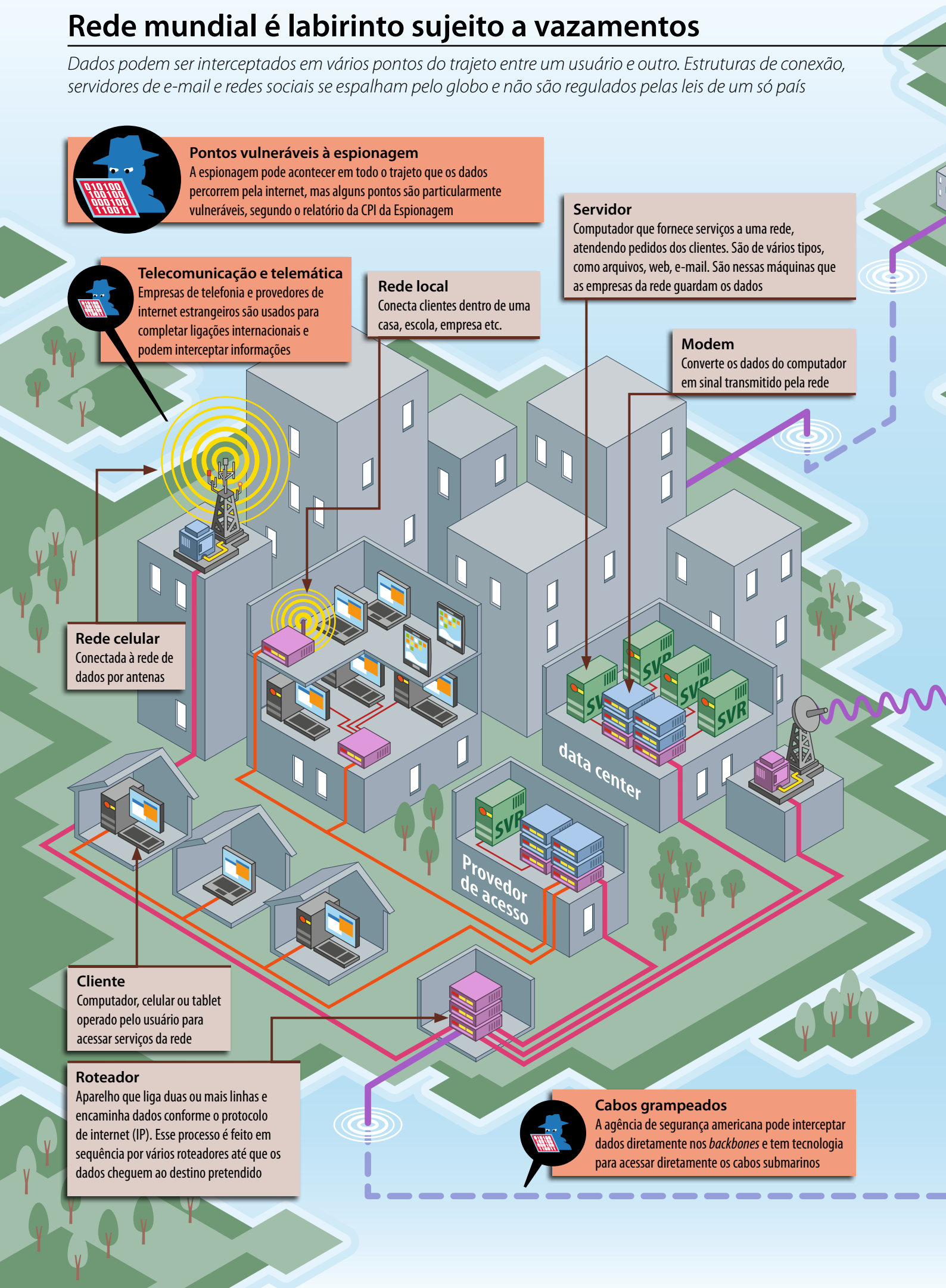
Tecnologia nacional

Na CPI da Espionagem, o presidente da Agência Nacional de Telecomunicações (Anatel), João Batista de Rezende, identificou que há concentração de tráfego e das receitas nos Estados Unidos, sede das principais empresas da internet. "O desequilíbrio do tráfego global da internet em direção aos EUA aumenta a vulnerabilidade das comunicações de brasileiros", admitiu, ressaltando que "nenhuma prestadora de serviços de telecomunicações associada provê ou facilita informações que possam quebrar o sigilo dos usuários, salvo mediante ordem judicial na forma da lei brasileira".

As soluções propostas passam, basicamente, por investir em tecnologia nacional (cabos submarinos de comunicação e satélites, segurança da nuvem no país,

Rede mundial é labirinto sujeito a vazamentos

Dados podem ser interceptados em vários pontos do trajeto entre um usuário e outro. Estruturas de conexão, servidores de e-mail e redes sociais se espalham pelo globo e não são regulados pelas leis de um só país

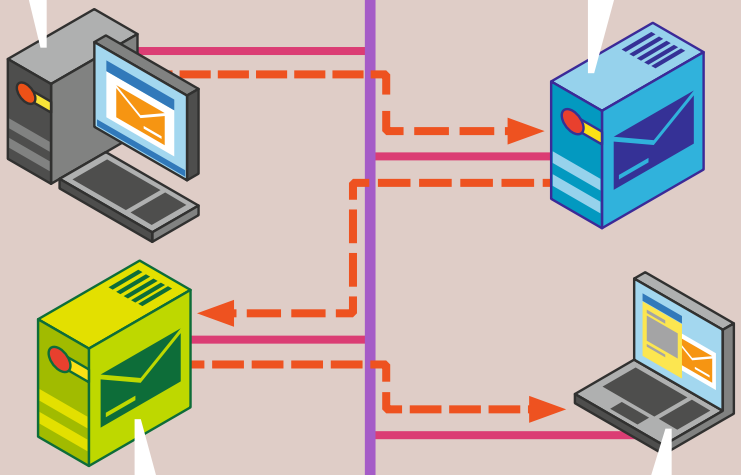


Entre um computador e outro, um longo caminho

Qualquer serviço de rede é uma troca de informações entre clientes e servidores, com uma sucessão de idas e vindas de dados. Veja um exemplo do caminho percorrido por uma mensagem eletrônica:

1. O remetente digita a mensagem de correio eletrônico no computador, indicando o endereço do destinatário

2. A mensagem é enviada aos servidores da empresa responsável pelo serviço de e-mail do remetente, que, em muitos casos (Gmail, Hotmail etc.), se situam no exterior

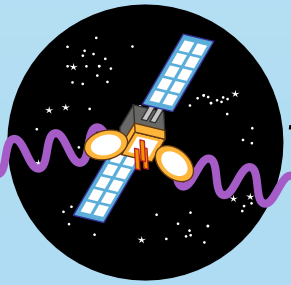


3. A mensagem vai para outro servidor de e-mail, agora da conta do destinatário. Esse servidor pode ser de uma empresa e estar em outro local

4. Quando o destinatário abre a caixa de entrada, todas as mensagens endereçadas a ele são exibidas ou baixadas do servidor no computador

Internet

A rede mundial é uma grande teia de conexões entre todas as outras redes menores

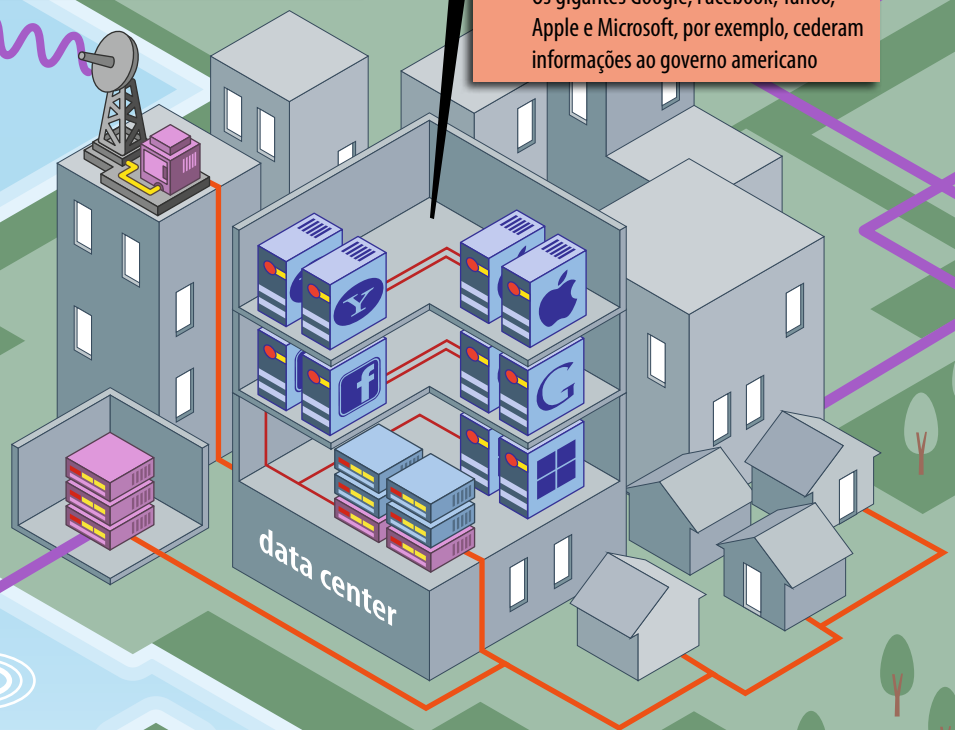


Satélites estrangeiros

O Brasil não possui satélites próprios em número suficiente. Por isso, usa os de outros países para suprir a demanda

Data centers no exterior

Muitos serviços usados em um país estão instalados em servidores em outro país, sujeitos a regras próprias. Os gigantes Google, Facebook, Yahoo, Apple e Microsoft, por exemplo, cederam informações ao governo americano



Conexões

Podem ser feitas por cabos (rede telefônica, fibra óptica e até rede elétrica) ou ondas de radiofrequência (3G, 4G, wi-fi, via satélite etc.)

Backbone

Cabeamento de alta capacidade que conecta os principais roteadores do mundo. Permite grande fluxo de dados entre cidades, países e continentes. Passam, inclusive, no fundo dos oceanos

Fonte: Relatório da CPI da Espionagem

LIA DE PAULA/AGÊNCIA SENADO

Celso Amorim, ministro da Defesa, afirma que investimento nacional em segurança cibernética é baixo

softwares de comunicação brasileiros e produtos de segurança e de monitoramento de redes).

— O que investimos na segurança cibernética é relativamente pouco, mais ou menos um quarto do que investe o Reino Unido. É absolutamente essencial investirmos nessa área, que reúne defesa, ciência e tecnologia e toda a cidadania brasileira — disse, no Senado, o ministro da Defesa, Celso Amorim.

Segundo afirmou à CPI o especialista em segurança da informação Paulo Pagliusi, "há sinais de que alguns equipamentos de computação montados nos EUA já saem de fábrica com dispositivos de espionagem instalados".

O jornal *The New York Times* diz que isso foi feito com pelo menos um governo estrangeiro, sem revelar qual. A matéria mostrou que a criptografia fornecida por operadoras de internet já vem com uma vulnerabilidade inserida propositalmente pela NSA, que permite que os espiões entrem no sistema e façam alterações, sem rastros.

O professor Peter Gill, da Faculdade de Ciências Sociais de Liverpool, autor do livro *Intelligence in an Insecure World (Inteligência em um Mundo Inseguro)*, avaliou cautelosamente a alegação da NSA de que interceptaria apenas 1,6% de todo o tráfego de dados, dos quais só 0,00004% seria analisado.

"Se 2 bilhões de registros são coletados diariamente, mesmo os meros 32 bilhões selecionados excedem e muito aquilo que poderia ser de fato analisado. Que 80 mil sejam analisados todos os dias parece também pouco provável se considerarmos que análise pressupõe um ser humano capaz de decidir a relevância daquela informação, por mais eficiente que seja o programa de computador", raciocina Gill. "Ninguém discute a legitimidade de os governos realizarem vigilância de alvos específicos sobre os quais existe suspeita. O que causa choque e decepção é a descoberta de que os governos aparentemente vigiam todos", critica o professor.

Denúncias de Snowden revelam amplo monitoramento

As primeiras denúncias feitas pelo ex-técnico da NSA Edward Snowden, de 29 anos, foram publicadas no início de junho no jornal inglês *The Guardian*. Ele mostrou como alguns dos programas de vigilância são usados pelos Estados Unidos para espionar a população americana — utilizando servidores de empresas como Google, Apple e Facebook — e de vários países da Europa e da América Latina, entre eles, o Brasil, inclusive fazendo o monitoramento de conversas da chanceler alemã Angela Merkel e da presidente Dilma Rousseff.

Reportagens publicadas pelo jornal *O Globo*, com base em dados coletados por Snowden, mostraram depois que milhões de e-mails e ligações de brasileiros e estrangeiros em trânsito no país foram monitorados.

Em seguida, a revista *Época* também publicou reportagem sobre documento secreto que revela como os Estados Unidos espionaram ao menos oito países — entre eles o Brasil — para aprovar sanções contra o Irã.

Por fim, o programa *Fantástico*, da TV Globo, mostrou, em setembro de 2013, que o esquema teria espionado ligações telefônicas e mensagens eletrônicas entre a presidente Dilma Rousseff e seus assessores diretos. Conversas entre os assessores e entre eles e terceiros também teriam estado na mira do serviço secreto dos Estados Unidos.

Nas semanas seguintes, mais notícias revelaram que a Petrobras e o Ministério de Minas e Energia também foram alvo de espionagem. Os dois nomes figuravam em um plano de treinamento de agentes da NSA, identificados como alvos em uma apresentação classificada como ultrassecreta. Não há confirmação de que o conteúdo das comunicações monitoradas tenha sido acessado. Sabe-se que os metadados das ligações e mensagens foram captados, indicando quem falou com quem, quando, onde e como.

HACKING STUFFS

Americano Edward Snowden, hoje refugiado na Rússia: denúncias afetam relações dos EUA com os aliados

Informação vale ouro na guerra e nos negócios

A atividade de inteligência, expressão tão associada aos filmes de espionagem e conspirações, nada mais é que a produção de conhecimentos e de dados e a proteção daqueles que o Estado ou uma corporação tem interesse em preservar. Obter informações que possam dar vantagem política, estratégica ou comercial frente às demais nações ou contribuir para uma maior segurança a cidadãos é o foco principal.

Nas grandes agências de inteligência, métodos e técnicas voltados para a produção desse conhecimento são cuidadosa e insistentemente ensinados aos agentes, retratados na ficção como glamorosos personagens, mas que, em geral, não vivem as situações de extremo perigo das telas do cinema.

Embora tenha ganhado destaque e relevância a partir do final do século 19, registros de atividades de inteligência podem ser encontrados em civilizações antigas. O livro *A Arte da Guerra*, do general chinês Sun Tzu, escrito 510 anos antes de Cristo, é apontado por muitos como o primeiro tratado oficial de inteligência. Durante as guerras, tais atividades são essenciais para obter informações privilegiadas dos inimigos — não por acaso, as maiores agências foram criadas justamente entre a 1ª e a 2ª Guerras Mundiais, quando ficou célebre a quebra pelos agentes ingleses (matemáticos recrutados junto às melhores universidades) dos códigos usados pelos alemães para orientar as tropas (a máquina Enigma).

Os mais famosos serviços de inteligência governamentais são o MI6, do governo britânico, e o Mossad, de Israel, além, é claro, da Agência Central de Inteligência norte-americana, a CIA. Durante a Guerra Fria, espiões americanos duelaram contra os soviéticos da KGB, oficialmente extinta.

Atualmente, a estrutura de inteligência nos Estados Unidos envolve 16 agências e 107.035 funcionários, que consumiram nada menos que US$ 52,6 bilhões do orçamento do país no ano passado, segundo reportagem publicada pelo jornal *The Washington Post*. No Brasil, essas atividades têm uma dimensão bem menor e ficam a cargo da Agência Brasileira de Inteligência (Abin), órgão central do Sistema Brasileiro de Inteligência — Sisbin *(veja mais em Glossário, na pág. 16, e em Realidade Brasileira, na pág. 47)*.

Países e empresas se "espionam" mutuamente e isto é, por mais paradoxal que pareça, uma prática corriqueira. Em debate no Senado, José Elito Carvalho Siqueira, ministro-chefe do Gabinete de Segurança Institucional (GSI) da Presidência da República, admitiu e classificou como natural a movimentação diplomática de adidos e pessoas da área de inteligência creditadas em território nacional, a exemplo do que ocorre nos demais países.

REPRODUÇÃO

Sede da Agência de Segurança Nacional: estrutura de inteligência dos EUA tem mais de 100 mil funcionários

— Temos 20 países com 40 representantes de órgãos de inteligência. Não há nenhum problema em ter isso conduzido dessa forma — afirmou.

Contrainteligência

Ainda que os principais interessados e protagonistas das notícias sobre atividades de inteligência sejam os governos, há pelo mundo empresas privadas especializadas na atividade. As grandes corporações utilizam cada vez mais serviços privados de inteligência para buscar informações privilegiadas para suplantar os concorrentes.

Como reação natural ao desenvolvimento dos serviços de inteligência, a partir do século passado Estados e organizações passaram a investir em mecanismos para proteger informações estratégicas. É a chamada contrainteligência, cujo objetivo é identificar, neutralizar ou até mesmo contra-atacar as tentativas de acesso. A técnica mais usada é a desinformação, permitindo o vazamento de dados sem muita relevância ou cuidadosamente plantados para confundir e desorientar serviços de espionagem adversários. Durante a Guerra Fria, ficaram famosas as trocas, entre americanos e soviéticos, de planos militares e projetos bélicos fabricados para despistar os inimigos.

Em tempos de espionagem cibernética, uma das formas de se proteger, no contexto governamental ou no privado, é a conscientização: entender a tecnologia, os riscos envolvidos e as medidas que garantam o nível de segurança desejado. Nos anos recentes, especialistas têm dado ênfase ao aumento da legalidade das operações de inteligência. "A direção dominante dos debates é de ter um maior controle e responsabilização sobre as agências que operam na área, cujas atividades passadas foram marcadas pela espionagem de adversários políticos, ao invés de ameaças reais à segurança nacional", diz o professor Peter Gill.

Privacidade, preocupação crescente em todo o mundo

A privacidade é um direito fundamental de qualquer cidadão, consagrado na Declaração Universal dos Direitos Humanos, aprovada pela Organização das Nações Unidas (ONU) em 1948. Não é difícil imaginar por quê. Só livre da constante fiscalização do Estado e dos poderosos o cidadão pode exercer a liberdade de expressão e de organização, enunciadas em um texto ainda mais antigo, a Declaração dos Direitos do Homem e do Cidadão, documento culminante da Revolução Francesa (1789) e que serviu de inspiração para a publicação da ONU.

Antes mesmo da declaração francesa, leis de direitos civis na Inglaterra do século 17 já proibiam a Coroa de interceptar cartas ou invadir domicílios sem autorização judicial. Na época, o que se queria proibir era a violação das casas por coletores de impostos. Garantir esse direito, em última instância, é zelar pela democracia, à qual a privacidade está intimamente ligada.

Nos últimos anos, o advento

SUSAN MELKISETHIAN

Protestos contra vigilância também ocorreram em cidades norte-americanas, como Washington: "Espionagem é censura"

PETE SOUZA/THE WHITE HOUSE

Obama em reunião na Casa Branca: espionagem tem sido criticada pela imprensa e opinião pública dos EUA

da internet ampliou a liberdade de expressão e o acesso de direitos civis, como a cultura e a educação, a tal ponto que a ONU declarou, em 2011, o acesso à rede como direito fundamental do ser humano. Paralelamente, porém, a preocupação da comunidade internacional com a garantia à privacidade na internet é crescente.

Ao aceitar serviços gratuitos de e-mails e redes sociais, por exemplo, a pessoa implicitamente — e até por contrato — abre mão de parte da própria privacidade. Mensagens e postagens são analisadas automaticamente pelos sites para identificar hábitos de consumo, círculos sociais e até preferências políticas.

Isso, porém, é muito diferente da espionagem cibernética, na qual há uma invasão não autorizada. Essa violação é crime fora da internet e dentro dela, mas as leis, superadas pela velocidade das mudanças tecnológicas, precisam ser atualizadas para melhor atender as necessidades das pessoas e dos Estados.

A reação contra a espionagem norte-americana não partiu apenas de fora do país. As medidas autorizadas pela Lei Patriótica (Patriot Act) têm sido alvo constante de críticas por expressiva parte da imprensa e da opinião pública dos Estados Unidos. O próprio Conselho de Supervisão de Liberdades Civis e Privacidade, uma agência governamental independente, divulgou relatório logo após as denúncias de Edward Snowden afirmando que a grande quantidade de registros telefônicos reunidos pela NSA representa "um benefício mínimo no combate ao terrorismo, é algo ilegal e deve terminar".

"Não identificamos uma única instância envolvendo uma ameaça aos EUA na qual o programa de registros telefônicos fez uma diferença concreta nos resultados de uma investigação antiterrorismo", disse o órgão, formado por cinco conselheiros.

Ficção antecipa vigilância

Desde 1949, quando o britânico George Orwell publicou o clássico livro *1984* — que retratava um estado totalitário e onipresente, representado pela figura do Big Brother —, a literatura, o cinema e a TV têm imaginado cenários muito semelhantes à espionagem cibernética que se tornou realidade nos anos recentes. Impactados pelas ditaduras nos moldes comunistas do século 20, e nos anos recentes pelo ataque terrorista às Torres Gêmeas, vários autores criaram cenários em que os cidadãos são inteiramente desprovidos de qualquer privacidade.

No futuro descrito em *Fahrenheit 451* (1953), de Ray Bradbury, todos os livros são proibidos, opiniões próprias são consideradas antissociais e hedonistas e o pensamento crítico é suprimido. No filme *Inimigo do Estado* (1998), de Tony Scott, um advogado se torna o alvo de agentes corruptos da NSA que usam os recursos de espionagem da agência para caçá-lo mundo afora.

Em 2008, a BBC produziu a minissérie *The Last Enemy (O Último Inimigo)*, em que o governo do Reino Unido implanta um sistema capaz de centralizar todas as informações e atividades de qualquer cidadão, espionando por meio de câmeras de segurança, violação de e-mails e escutas telefônicas.

Glossário

Abin: a Agência Brasileira de Inteligência é o serviço de inteligência civil do país, tendo como função principal investigar ameaças reais e potenciais, bem como identificar oportunidades de interesse da sociedade e do Estado. Atua nas frentes de inteligência e contrainteligência.

Ataque: qualquer tentativa de acesso ou uso não autorizado de um serviço, computador ou rede. Ver intrusão e invasão.

Boundless Informant: programa de vigilância utilizado para análise de megadados e visualização dos dados coletados pela Agência de Segurança Nacional (NSA).

CIA: a Agência Central de Inteligência do governo dos EUA é responsável por investigar e fornecer informações de segurança nacional. Também se engaja em atividades secretas, a pedido do presidente dos Estados Unidos.

Espionagem cibernética: ato pelo qual se obtém na internet informação pessoal, classificada, de propriedade ou sensível, sem permissão do proprietário, com o uso de programas, hackers, trojans...

Five Eyes: apelido dado a um acordo que estabelece a aliança de cinco países para compartilhar informações secretas (EUA, Reino Unido, Austrália, Canadá e Nova Zelândia).

Globalização: nome dado aos processos de aprofundamento da integração econômica, social, cultural e política internacional, a partir do final do século passado.

Inteligência de sinais: termo usado para descrever a atividade da coleta de informações ou inteligência através da interceptação de sinais de comunicação entre pessoas ou máquinas.

Icann: a Corporação da Internet para Atribuição de Nomes e Números é uma entidade subordinada ao governo dos EUA, responsável pela alocação do espaço de endereços, pela atribuição de identificadores de protocolo e pela administração do sistema de nomes de domínio da internet.

Invasão: Ataque bem-sucedido que resulta no acesso, manipulação ou destruição de informações em um computador.

Intrusão: Quando um hacker acessa um sistema sem autorização com o objetivo de controlar a máquina ou roubar informações confidenciais, aproveitando alguma vulnerabilidade do sistema.

IGF: O Fórum de Governança da Internet foi criado pela ONU em 2006 e reúne a sociedade civil, empresas, comunidade técnica e governos para discutir questões relacionadas a políticas e regulação da Internet.

NSA: a Agência de Segurança Nacional dos EUA, criada em 4 de novembro de 1952, com funções relacionadas a Inteligência de sinais, incluindo interceptação e criptoanálise.

Prism e XKeyscore: programas do sistema de vigilância global da NSA. Permitem coletar e fazer pesquisas em imensos bancos de dados, onde estão informações de usuários da Internet, incluindo navegação na rede, e-mails, arquivos, chamadas de voz e vídeo, detalhes de redes sociais etc.

Patriot Act: legislação em vigor desde outubro de 2001 que permite, entre outras medidas, que órgãos de segurança e de inteligência dos EUA interceptem ligações telefônicas e e-mails de organizações e pessoas supostamente envolvidas com o terrorismo, sem necessidade de qualquer autorização da Justiça, sejam elas estrangeiras ou americanas.

WSis: a Cúpula Mundial sobre a Sociedade da Informação foram encontros patrocinados pela ONU em 2003 e 2005, tendo como uma de suas metas principais diminuir a chamada exclusão digital global que separa países ricos e pobres.

WikiLeaks: organização transnacional sem fins lucrativos, sediada na Suécia, que publica em sua página, de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas.

Falta maior integração

Diretor do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional (GSI) da Presidência da República, Raphael Mandarino Junior credita boa parte dos incidentes de segurança nas redes públicas brasileiras a falhas humanas e garante: o Brasil está em um "bom nível" de entendimento e de preparo para a segurança e a defesa cibernéticas.

O mais recente relatório do Tribunal de Contas da União (TCU) mostrou que 73% das 337 instituições públicas federais pesquisadas não classificam a informação, 90% não fazem análise de riscos e 55% não possuem política de segurança da informação. O que está sendo feito para mudar rapidamente esse cenário?
Pela Lei de Acesso à Informação, as informações produzidas ou custeadas pelos poderes públicos deverão estar disponíveis a todos os cidadãos. Assim, o acesso passa a ser a regra e o sigilo, a exceção. Dessa forma, uma instituição pública somente poderá classificar suas informações nas hipóteses de sigilo legalmente estabelecidas ou cuja divulgação possa trazer riscos à sociedade ou ao Estado brasileiro, tornando irrelevante o índice de 73%. O GSI articula e promove um conjunto de normas visando assegurar a segurança da informação e comunicações no governo. Incentiva debates e troca de experiências com centros de tratamento de incidentes de segurança em rede de órgãos e entidades públicas e privadas nacionais e internacionais e assina acordos bilaterais de preservação do espaço cibernético com nações estrangeiras, além de credenciar gestores de segurança para troca de informações classificadas. [Já foram] formados mais de 200 especialistas em gestão de segurança da informação e comunicações na administração pública federal, em parceria com a Universidade de Brasília, e capacitados mais de 50 mil servidores públicos.

Há cinco anos, o senhor escreveu que o Brasil recebia 2 mil ataques por hora nas "grandes redes" e que esses seriam apenas tentativas de invasão para roubar dados, sem considerar vírus e spams. Não estamos muito vulneráveis a invasões e captura de informações sigilosas?
Boa parte dos incidentes de redes decorre de falhas humanas. O servidor público, ao abrir e-mail desconhecido ou acessar sítios via redes sociais, pode, de alguma forma, estar contribuindo para fragilizar e criar vulnerabilidades nas redes de governo. Participamos como convidados de diversos fóruns internacionais e pudemos constatar que o Brasil está em um bom nível de entendimento e de preparo para a segurança e defesa cibernética e que nossas ações são semelhantes às de outras nações. A verdade é que nenhuma nação está 100% preparada para enfrentar as diversidades no ambiente digital. Todas precisam evoluir e inovar continuadamente, principalmente nos quesitos disseminação de cultura interna de proteção, aprimoramento do marco legal de SIC [Serviço de Informação ao Cidadão] — nacional e internacionalmente — e cooperação intergovernamental, intragovernamental e internacional.

Diversos senadores, durante a CPI, lembraram que muitas empresas de tecnologia da informação que prestam serviços ao governo são americanas e também trabalham para o Departamento de Defesa dos EUA. Esse não seria um risco adicional à nossa segurança cibernética?
Enquanto o Brasil não desenvolver sua pesquisa e inovação tecnológica, criando seus próprios equipamentos e sistemas, essa dependência técnica continuará trazendo risco a toda a sociedade brasileira. O risco não está em comprar equipamentos de um ou outro país, está em não ter tecnologia própria ou metodologia de aquisição e uso voltadas a mitigar os riscos.

Segurança e defesa cibernética são tratadas no Brasil por diversos organismos governamentais. A primeira fica a cargo do órgão que o senhor chefia. Já a segunda é atribuição do Exército, por meio do Centro de Defesa Cibernética. Essa configuração não tende a fragilizar a proteção nacional, na medida em que passa a depender da afinidade, integração e colaboração dos dirigentes de tais instituições?
O que falta, na verdade, é a institucionalização da integração e colaboração das diversas instituições que atuam nessa área. A tendência mundial vem priorizando a segurança cibernética e o estabelecimento formal de órgão que centralize as competências básicas relacionadas ao tema, visando integrar esforços isolados e propiciar macrocoordenação no nível da nação, a exemplo das experiências americana, inglesa, australiana, coreana e colombiana, entre outras. Assim, como visão de futuro, é de vital importância o estabelecimento de órgão que assuma, no Brasil, a governança do tema como um todo, coordenando-o estrategicamente, buscando articular e harmonizar ações dos diversos atores nos três níveis de governo e da sociedade e otimizando investimentos, orçamento e atribuições.

DIVULGAÇÃO

Em busca da GOVERNANÇA GLOBAL

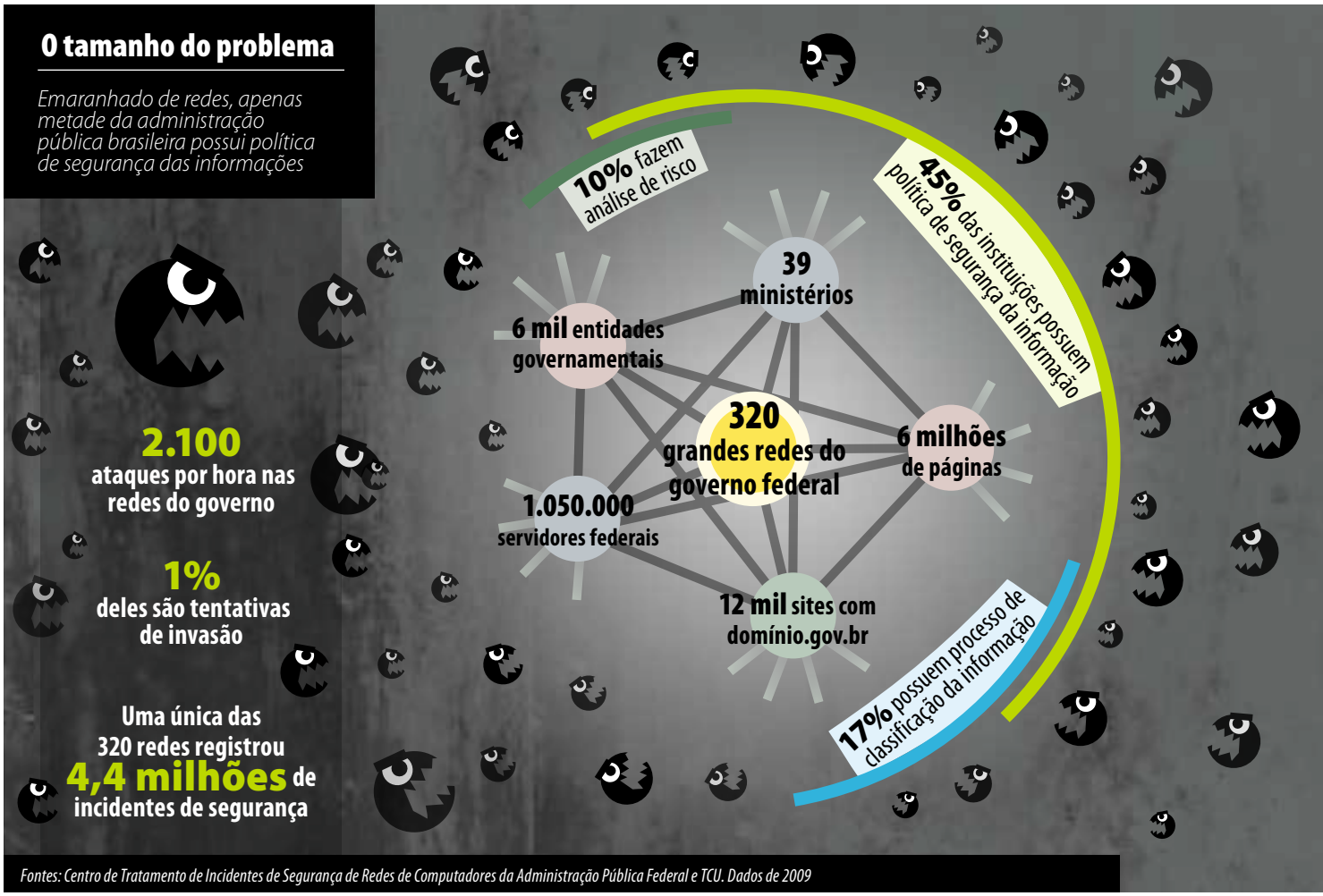
estudiosos discordam sobre praticamente tudo quando o tema é globalização, mas são unânimes em reconhecer que a revolução nos meios de comunicação e a velocidade no fluxo de informações que vivemos hoje foram poderosas ferramentas no que se define como "crescente internacionalização dos interesses nacionais".

"Se fosse verdade que a globalização inelutavelmente acarreta o encolhimento das soberanias e a superação do Estado-nação, em nenhum lugar essas tendências deveriam ser tão evidentes como nos EUA, inventor e centro da globalização e Estado mais globalizado do planeta. Ora, é o inverso que ocorre. Nunca a soberania americana dispôs de tantos instrumentos de poder e nunca os utilizou com tamanha desenvoltura, para afirmar-se como faz hoje", constatou, há 11 anos, o ex-ministro e embaixador Rubens Ricupero, em seu livro *O Brasil e o Dilema da Globalização*.

O episódio das denúncias de Edward Snowden mobilizou parte da opinião pública internacional em torno da necessidade, urgente, de estabelecer uma governança global para a internet, o que poderia servir como um freio à expansão da espionagem cibernética como prática de Estado. Para se ter ideia, a organização do NETmundial, encontro realizado em 23 e 24 de abril em São Paulo, recebeu 188 propostas de temas centrais, vindas de 46 países, na maioria relacionadas à segurança na rede, proteção à privacidade, garantia da liberdade de expressão e papel dos governos na governança da internet.

Depois de três anos de debates, o Congresso Nacional aprovou, em abril, a proposta de Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para internautas e provedores de rede *(leia mais na seção Propostas, a partir da pág. 50)*.

Em março deste ano, o governo de Barack Obama anunciou a decisão de transferir para a comunidade global o controle que exerce sobre um elemento-chave do ecossistema da inter-



REPRODUÇÃO

Encontro da Icann em Cingapura: entidade subordinada aos EUA responde por atividades centrais na administração da internet

net: a Corporação da Internet para Atribuição de Nomes e Números (Icann, na sigla em inglês), entidade que responde pela alocação do espaço de endereços, atribuição de IPs (protocolos de internet) e administração do sistema de nomes de domínio, atividades centrais no gerenciamento da rede.

"A internet está se expandindo em um ritmo explosivo. Mas, enquanto cresce, devemos assegurar que continue a promover a livre escolha e a competitividade, a buscar a inovação e a estimular o desenvolvimento em todo o globo. A internet é um recurso global e todos os participantes têm direito a voz em sua governança", resumiu Fadi Chehadé, presidente da Icann.

Washington definiu claramente os patamares da discussão, cuja premissa é a de que "os EUA não cederão o controle de tais funções para qualquer entidade governamental ou intergovernamental", disse Chehadé. Sob o impacto do escândalo de 2013, a União Europeia fez declaração pública de apoio a um modelo compartilhado de gestão *(leia mais na pág. 36)*.

O Brasil defende a governança global, como destacou a própria presidente Dilma Rousseff em discurso na ONU. "A internet está muito concentrada nos Estados Unidos, os servidores estão todos no Hemisfério Norte", declarou o ministro das Comunicações, Paulo Bernardo, em abril deste ano. A governança é considerada essencial também para estabelecer regras claras e um campo nivelado de disputa naquele que é um dos mais promissores setores econômicos do planeta.

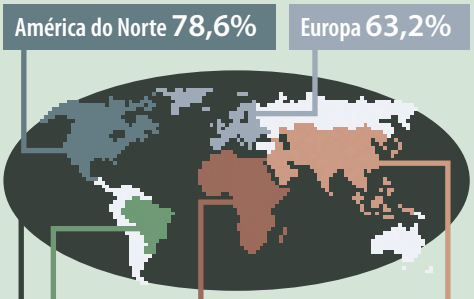
Para o senador Ferraço, a implementação de marco legislativo no âmbito do direito internacional ainda está por ser feita. "É preciso regulamentar os espaços de intromissão excepcional dos Estados na privacidade dos cidadãos em um mundo globalizado, bem como os mecanismos multilaterais de controle dessa eventual intromissão", explicou.

Com mais de 3 bilhões de usuários no mundo, a internet é considerada hoje "elemento básico e essencial na vida de quase todos os cidadãos e um componente-chave na economia e nos governos dos países", escreveu Virgilio Almeida, secretário de Política de Informática do Ministério da Ciência, Tecnologia e Inovação e coordenador do Comitê Gestor da Internet no Brasil (CGI.br).

Há dois anos, a consultoria Boston Consulting Group previu que, em 2016, a internet contribuiria com US$ 4,2 trilhões para o total de riquezas gerado pelas 20 maiores economias do mundo. "É fundamental que, para lidar com a espionagem internacional, o Brasil desenvolva mecanismos de proteção do conhecimento e de segurança cibernética, além de investimentos em inteligência e, sobretudo, em contrainteligência, com ênfase no desenvolvimento de tecnologias próprias e nacionais e de quadros capacitados para o tema", concluiu a presidente da CPI, Vanessa Grazziotin.

Acesso desigual

Um terço da humanidade já se conecta à internet. Mas a distribuição é muito irregular



Perfil do brasileiro

- 45,6% dos brasileiros têm acesso à rede (metade deles vive na Região Sudeste)
- 77% dos jovens entre 15 e 17 anos acessam a internet
- 21% dos acima de 50 anos usam a rede
- 88% dos que acessam a internet a usam para se comunicar
- Brasileiro navega, em média, quase 17 horas por mês, à frente dos EUA, França e Japão

No mundo, 50% usam o telefone celular como primeira fonte de acesso à rede

A cada 60 segundos na rede...

- 70 novos domínios registrados
- 695 mil buscas pelo Google
- 775 mil posts no Facebook
- 168 milhões de e-mails enviados

Fontes: Internet World Stats e IBGE. Dados de 2012

Origem dos sistemas explica fragilidade

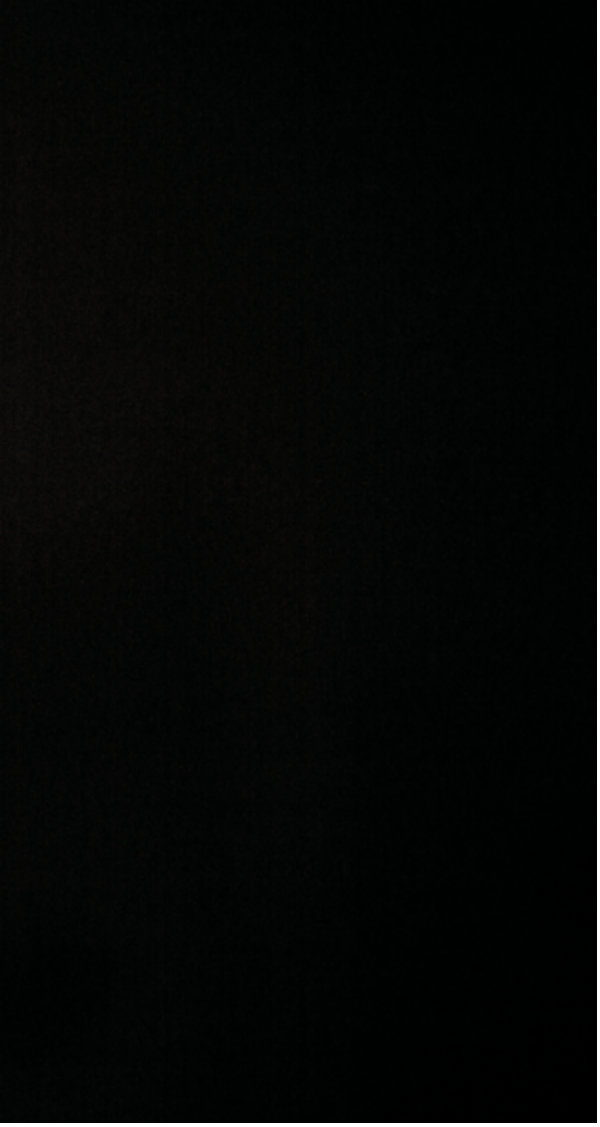
O avanço das chamadas tecnologias de informação e comunicação (TICs) trouxe enormes benefícios, mas, ao mesmo tempo, fez surgir um novo tipo de prática: os ataques cibernéticos, que crescem em velocidade impressionante, a julgar pelas estatísticas das empresas do setor, e já representam um dos maiores desafios do século em termos de segurança, tanto para as empresas quanto para as nações.

A espionagem é facilitada, principalmente, pela vulnerabilidade dos sistemas de segurança cibernética (que inclui a proteção de dados de instituições governamentais, privadas e de cidadãos em geral), cada vez mais estratégica e essencial à manutenção e preservação das infraestruturas críticas de um país, como saúde, energia, defesa, transporte, telecomunicações, a própria informação.

"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", escreveram Claudia Canongia e Raphael Mandarino Junior, no artigo "Segurança cibernética: o desafio da nova sociedade da informação", de 2009.

A segurança cibernética inclui, segundo o Departamento de Segurança Interna dos Estados Unidos, a prevenção aos danos causados pelo uso não autorizado da informação eletrônica e de sistemas de comunicações e a respectiva informação neles contida, visando assegurar a confidencialidade, integridade e disponibilidade.

O Departamento de Segurança Interna trabalha na esfera civil para proteger o território, dentro e fora das fronteiras, enquanto o Departamento de Defesa está encarregado de ações militares no exterior.



DENNIS SKLEY

Na raiz da fragilidade dos sistemas está a própria estrutura com que foram concebidos e são operados os sistemas de telefonia e de internet em escala local, regional e global. Se alguém no Brasil deseja telefonar para a Austrália, por exemplo, a conexão não será feita de modo direto. Não há um cabo telefônico submarino interligando os dois países. A chamada será recebida por uma central, nesse caso localizada nos Estados Unidos, e, de lá, redirecionada para o país de destino.

Portas de entrada

Esses pontos físicos de concentração são paisagem ideal para a ação dos espiões cibernéticos. O mesmo ocorre com as comunicações por satélites, cuja estrutura é intrinsecamente aberta. A única saída é usar de criptografia para transmitir e receber dados, mas, ainda assim, não é 100% seguro.

"As informações que passam por lá são 'bisbilhotáveis'. Não existe uma deficiência técnica que gere monitoramento — se houver uma deficiência, é uma deficiência ética ou política de quem faz o monitoramento. Da mesma forma, quando você se comunica através da internet, o seu provedor tem acesso a tudo que passa por lá e ele é que deveria tomar providências para não invadir esse conteúdo", explica o diretor do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e membro do Comitê Gestor da Internet no Brasil (CGI.br), Demi Getschko, em entrevista ao site do Núcleo de Direito, Internet e Sociedade da Faculdade de Direito da Universidade de São Paulo (USP).

Outro caminho comumente usado pelos invasores são as chamadas *backdoors* (portas dos fundos), em geral criadas por desenvolvedores de programas de computador sob o argumento de que o fabricante precisa reunir estatísticas para avaliar o desempenho do software e atuar para corrigir defeitos. Por essas portas, não apenas podem sair tais dados como entrar pequenos programas invasores, incumbidos de fazer a "bisbilhotagem".

Getschko cita dois exemplos bem recentes. "O contrato de uso da versão 8 do Windows tem uma disposição que reserva à Microsoft o direito de monitorar o que acontece no seu computador para ter informações sobre o funcionamento técnico do software — claro que essa prerrogativa existe sob o argumento de que seja útil para 'resolver problemas' mas, evidentemente, essas informações podem ser utilizadas para outros fins. Já o XKeyscore [usado pela Agência de Segurança Nacional dos Estados Unidos, segundo as denúncias de Edward Snowden] é um software de monitoramento que infecta a máquina do usuário para monitorar o que você teclava. Em suma, a gente vive imerso em um mundo em que somos vulneráveis", resume o especialista.

História da internet

Em menos de meio século, rede criada nos EUA revoluciona o mundo e conecta mais de 3 bilhões de pessoas

1969 — Conexão
Desenvolvida pelo Departamento de Defesa dos EUA, a rede Arpanet é criada para interligar os computadores das bases militares e os departamentos de pesquisa do governo.

1972 — E-mail
Ray Tomlinson cria o correio eletrônico, escolhendo o símbolo @ (*at*, em inglês).

1974 — TCP
Vint Cerf e Robert Kahn desenvolvem a técnica de comunicações TCP, permitindo que as múltiplas redes se compreendessem, criando a verdadeira internet.

1983 — DNS
A Domain Name System é proposta. A criação dos sufixos, como .com e .gov, chega um ano depois.

1989 — http e www
Tim Berners-Lee cria a World Wide Web e inventa o hipertexto.

1993 — Mosaic
Marc Andreessen e colegas da Universidade de Illinois (EUA) criam o Mosaic, o primeiro navegador que combina gráfico e texto numa só página.

1997 — SixDegrees
A primeira rede social, bisavó do Facebook, chega à rede.

1998 — Google
Período de crescimento dos sites de busca culmina com a criação do Google, por Sergey Brin e Larry Page.

1999 — Napster
Serviço Napster populariza o compartilhamento de arquivos de música. Ele, e seus sucessores, mudaram permanentemente a indústria da música e a relação com as gravadoras.

2002 — Meio bilhão
Usuários da internet superam a barreira dos 500 milhões de pessoas.

2004 — Facebook
Aluno de Harvard, Mark Zuckerberg lança o Facebook.

2005 — Youtube
Lançado o site de compartilhamento de vídeos do Youtube.

2006 — 1 bilhão
A barreira de 1 bilhão de usuários é ultrapassada.

2014 — 3 bilhões
A internet tem 3 bilhões de usuários e 1 milhão de sites. O acesso a ela é considerado direito fundamental do ser humano.

O que foi dito

Assim que as revelações de Edward Snowden vieram a público, os senadores reagiram ao que interpretaram como violação da soberania nacional. Veja o que foi dito no Plenário do Senado e por lideranças de todo o mundo:

"Não é uma questão de privacidade, é uma questão de liberdade."

Edward Snowden, ex-técnico de segurança da NSA

MARCOS OLIVEIRA/ AGÊNCIA SENADO

"É muito provável que a espionagem tenha recolhido informações estratégicas sobre esse campo [de Libra, no pré-sal] que outras de todo o mundo não têm e que apenas as empresas americanas teriam."

Rodrigo Rollemberg (PSB-DF)

"A atitude abusiva do governo americano foge completamente ao padrão de confiança esperado de uma parceria estratégica, como a que tradicionalmente o Brasil desenvolve e mantém com os Estados Unidos."

Eduardo Braga (PMDB-AM)

"Os direitos de todos os brasileiros foram agredidos mediante interferência brutal e continuada."

Ângela Portela (PT-RR)

WALDEMIR BARRETO/ AGÊNCIA SENADO

"Você não pode 100% de segurança, 100% de privacidade e 0% de inconveniência."

Barack Obama, presidente dos Estados Unidos

"Se o nosso governo tivesse as mesmas possibilidades norte-americanas, ele, provavelmente, estaria sendo acusado também de espionagem em relação a tantos outros países."

Álvaro Dias (PSDB-PR)

WALDEMIR BARRETO/ AGÊNCIA SENADO

"Não adianta ficar esperneando, porque eles vão continuar fazendo. E não vão adiantar leis, porque a espionagem é secreta, exatamente para que a lei não a toque."

Cristovam Buarque (PDT-DF)

"Ficaram mais claros e patentes os interesses econômicos da espionagem americana em território nacional."

Randolfe Rodrigues (PSOL-AP)

“Assim como a guerra nuclear era a guerra estratégica da era industrial, a ciberguerra é a guerra estratégica da era da informação; e esta se tornou uma forma de batalha massivamente destrutiva, que diz respeito à vida e morte de nações.”

Generais Ye Zheng e Zhao Baoxian, do Exército chinês

WALDEMIR BARRETO/AGÊNCIA SENADO

“Oposição e situação estão no mesmo lado, que é a defesa do interesse brasileiro diante de uma invasão à privacidade, que é um direito inalienável que está nos termos da Constituição brasileira.”

Ana Amélia (PP-RS)

“É preciso dar ao mundo digital um quadro jurídico, uma ordem subjacente, e estamos apenas no início desse processo. As leis nacionais, por si só, não serão suficientes para continuar a regular um mercado cada vez mais globalizado.”

Angela Merkel, primeira-ministra da Alemanha

REPRODUÇÃO

MÁRCIA KALUME/AGÊNCIA SENADO

“É mais um caso de violação intolerável à soberania nacional e aos direitos de pessoas e empresas.”

Anibal Diniz (PT-AC)

“O governo americano deveria ser o defensor da internet, não uma ameaça. Eles precisam ser mais transparentes sobre o que está acontecendo, se não as pessoas só vão esperar o pior.”

Mark Zuckerberg, fundador do Facebook

“Nas Nações Unidas, o objetivo é buscar uma definição sobre normas claras de comportamento para os países quanto à privacidade das comunicações dos cidadãos e a preservação da soberania dos demais Estados. Na UIT [União Internacional de Telecomunicações], a ideia é tentar o aperfeiçoamento de regras multilaterais sobre segurança das telecomunicações.”

Antonio Patriota, ex-ministro das Relações Exteriores

LIA DE PAULA/AGÊNCIA SENADO

“Se não houver uma política de um organismo multilateral como a ONU estabelecendo os limites e pondo freio às ações de empresas privadas, o mundo vai colecionar episódios como esse [de espionagem].”

Jorge Viana (PT-AC)

“É inadmissível que outros países possam usar o nosso território para bisbilhotar a vida dos brasileiros.”

Inácio Arruda (PCdoB-CE)

O mundo perplexo diante do big brother

Denúncias de espionagem americana sobre líderes e cidadãos comuns instalam clima de desconfiança até entre os mais fortes aliados dos EUA, os países do bloco europeu

À medida que os meios de comunicação repercutiam, no ano passado, as denúncias de Edward Snowden, os cidadãos foram se dando conta do alcance da atuação da Agência de Segurança Nacional (NSA) dos Estados Unidos. Governos e empresas, diante da exposição pública, tiveram que se manifestar. Muitos já sabiam, se não no todo pelo menos em parte, e até colaboravam para a espionagem dos seus cidadãos sob a justificativa de proteção contra o terrorismo.

Vários países convocaram os embaixadores dos EUA para dar explicações, enquanto outros pediram esclarecimentos diretamente ao governo norte-americano e a grandes empresas, como Google e Facebook. Além da diplomacia, o tema contaminou setores sensíveis, inclusive acordos de cooperação econômica. Uma das maiores preocupações dos governos em relação à espionagem em larga escala é o risco que correm as negociações para a assinatura de acordos comerciais e os segredos industriais e estratégicos dos países e de suas empresas.

Depois de declarações fortes, porém, as reações foram diminuindo e se mostraram praticamente inócuas. As crises internas em que diversos países estão imersos por conta das dificuldades econômicas que o mundo atravessa desde 2008 também arrefeceram a temperatura da tensão entre os

ACFI PRESS

Reunião da Comissão Europeia, órgão executivo da UE: reações inicialmente fortes perderam força diante da difícil agenda econômica

países, muitos dos quais parceiros.

Analistas de segurança e veículos de comunicação de todo o mundo trouxeram à tona questões preocupantes, que deixaram dúvidas sobre o que estariam fazendo as agências de espionagem e contraespionagem de países como Israel, Irã, Rússia e China.

Acordo ameaçado

A União Europeia (UE) já havia exigido explicações dos Estados Unidos no fim de junho de 2013 quando, em outubro, a revista alemã *Der Spiegel* apontou o Velho Continente como um dos principais alvos dos programas de espionagem dos EUA. O presidente do Parlamento Europeu, Martin Schulz, exigiu que os Estados Unidos esclarecessem se espionaram a União Europeia.

"Estou profundamente preocupado e surpreendido", reconheceu Schulz num comunicado, no qual afirmou que, "se as acusações forem verdadeiras, constitui um assunto muito grave que terá um grave impacto nas relações União Europeia-Estados Unidos".

Num momento em que Europa e Estados Unidos negociam o fim das barreiras alfandegárias para promover o livre-comércio no Atlântico Norte, a comissária europeia da Justiça, Viviane Reding, admitiu que as notícias podem prejudicar as negociações, ao declarar que "entre parceiros não há espionagem".

Por sua vez, a ministra alemã da Justiça, Sabine Leutheusser-Schnarrenberger, disse que a União Europeia deve punir a espionagem por serviços secretos estrangeiros. "As empresas americanas que não respeitem essas medidas devem ser excluídas do mercado europeu", afirmou.

Reação chinesa

Com um cotidiano de acusações mútuas de espionagem com os EUA, a China inicialmente reagiu com discrição às revelações de Snowden. No entanto, em março deste ano, os chineses romperam o silêncio. Em entrevista à Rádio Internacional da China, o porta-voz do Ministério da Defesa, Geng Yansheng, condenou os EUA

Manifestantes diante da sede da Comissão Europeia, em Bruxelas: denúncias puseram em risco acordos comerciais entre a UE e os EUA

pela espionagem a órgãos governamentais, empresas e indivíduos e prometeu que seu país tomaria medidas efetivas para reforçar a segurança na internet.

E a coisa piorou depois que a *Der Spiegel* divulgou, ainda em março, que a NSA teria infiltrado servidores na sede da Huawei, a gigante chinesa das telecomunicações. O presidente chinês, Xi Jinping, levantou a questão em encontro com o colega americano, Barack Obama, à margem de reunião de cúpula do G7 sobre segurança nuclear em Haia, Holanda, e ouviu a explicação de que "os Estados Unidos não espionam com intenção de obter vantagem comercial", como disse o vice-conselheiro de Segurança Nacional da Casa Branca, Ben Rhodes.

Na Alemanha, o governo encontrou provas de que até o celular da chanceler Angela Merkel foi monitorado pela NSA. Segundo a *Der Spiegel*, 35 líderes mundiais foram monitorados de perto. Em junho, Sabine Leutheusser-Schnarrenberger exigiu explicações de Washington. "Excede tudo o que é imaginável os nossos amigos dos Estados Unidos olharem para os europeus como inimigos", afirmou a ministra alemã.

Desdobramentos da crise chegaram à reunião de cúpula da UE em Bruxelas, em outubro de 2013, quando Merkel exigiu que os EUA assinassem um acordo de "não espionagem" com Alemanha, França e Grã-Bretanha.

Em janeiro deste ano, em sua mais dura reação, a chanceler disse ao Parlamento alemão que os americanos colocaram em xeque sua posição no mundo ao violarem a liberdade dos indivíduos. Mas Merkel afirmou que isso não deve interferir nas negociações para uma zona de livre-comércio entre os EUA e a UE: "A Alemanha não pode desejar melhor parceiro que os Estados Unidos".

EUROPEAN PARLIAMENT

Versões contraditórias

França e México também reagiram fortemente às denúncias. Paris convocou o embaixador americano — na linguagem diplomática, uma das mais duras reações de um país — para explicar porque mais de 70 milhões de comunicações francesas foram bisbilhotadas pelo serviço secreto americano, de acordo com reportagem do diário *Le Monde*.

Já o governo mexicano determinou uma investigação sobre a revelação feita pela *Der Spiegel* de que a conta de e-mail do ex-presidente Felipe Calderón (2006-2012) foi invadida pela NSA enquanto ele ocupava o cargo. Antes, já havia sido revelado que os EUA espionaram o então candidato e atual presidente do México, Enrique Peña Nieto.

MONIKA FLUECKIGER

Revista revelou que e-mail do ex-presidente mexicano Felipe Calderón foi invadido pela NSA enquanto ele ocupava o cargo

A Espanha também convocou o embaixador dos EUA para esclarecer as acusações de espionagem contra cidadãos do país e disse que, se comprovado, esse é um comportamento inaceitável entre países aliados. O jornal espanhol *El Mundo* afirmou que a NSA rastreou mais de 60 milhões de telefonemas na Espanha no espaço de um mês, citando um documento fornecido por Edward Snowden.

No entanto, segundo o diário americano *Wall Street Journal*, a espionagem a milhões de cidadãos na França e na Espanha foi realizada pelos serviços de inteligência dos próprios países, que compartilharam as informações com a NSA.

Já na Itália, uma nota divulgada pela ministra das Relações Exteriores, Emma Bonino, foi mais branda: "Pedimos as explicações necessárias sobre esse caso espinhoso" e os Estados Unidos "nos garantiram que esclarecerão o assunto com a União Europeia e com seus Estados-membros". A nota afirma ainda que a Itália "acredita no espírito de colaboração e amizade" entre os dois países.

ONU aprovou resolução proposta por Brasil e Alemanha

A repercussão das revelações de Edward Snowden levou quase 200 países a aprovarem uma resolução contra a espionagem sugerida pelos governos alemão e brasileiro na Assembleia Geral da ONU, em dezembro do ano passado.

A iniciativa representa a primeira resposta internacional de peso às revelações sobre a espionagem praticada pela inteligência americana.

O texto pede aos países que revejam seus procedimentos e legislação relacionados a programas de vigilância e que protejam a privacidade dos usuários da internet e de outras formas de comunicação eletrônica.

Também faz um apelo para que sejam criados ou mantidos mecanismos de controle independentes e efetivos, capazes de assegurar transparência e prestação de contas sobre os programas que interceptam dados pessoais.

Ao longo dos 11 artigos da proposta, os governos alemão e brasileiro reafirmam o direito humano do indivíduo "à privacidade e a não ser submetido a ingerências arbitrárias ou ilegais em sua vida privada. Bem como o direito à proteção da lei contra tais ingerências ou ofensas, reconhecendo que o exercício do direito à privacidade constitui requisito essencial à realização do direito à liberdade de opinião e de expressão sem ingerências e um dos pilares de uma sociedade democrática".

A resolução insta os países a "respeitar e proteger o direito à privacidade, incluindo o contexto das comunicações digitais", com base na doutrina de que os direitos humanos devem ser preservados também on-line.

Privacidade

O documento afirma que, embora preocupações com a segurança pública possam justificar a coleta e a proteção de certas informações sensíveis, os estados devem assegurar o total cumprimento de suas obrigações sob a lei internacional de direitos humanos.

O texto também solicita que

ROBERTO STUCKERT FILHO/PLANALTO

Texto apoiado por Dilma e Angela Merkel vincula o cumprimento de obrigações pelos países-membros da ONU à lei internacional de direitos humanos

a alta comissária das Nações Unidas para os Direitos Humanos, Navi Pillay, apresente um relatório à 69ª Assembleia Geral, que acontece este ano.

Esse deve ser um dos primeiros resultados práticos da medida, trazendo recomendações e análises sobre a proteção do direito à privacidade no contexto da vigilância nacional e extraterritorial das comunicações, interceptação e coleta de dados pessoais.

A resolução não especifica qualquer país como alvo das recomendações, mas foi claramente uma resposta direta às notícias sobre o monitoramento de Angela Merkel e Dilma Rousseff pela NSA.

Em nota emitida pelo Itamaraty, o governo brasileiro comemorou a aprovação da proposta como um "reconhecimento, pela comunidade internacional, de princípios universais defendidos pelo Brasil, como a proteção do direito à privacidade e à liberdade de expressão, especialmente contra ações extraterritoriais de Estados em matéria de coleta de dados, monitoramento e interceptação de comunicações".

A medida, no entanto, não obriga os países a cumprir as determinações — as resoluções da Assembléia Geral, ao contrário das do Conselho de Segurança da ONU, não são vinculantes, apenas fazem recomendações. Já no Conselho de Segurança, os Estados Unidos têm poder de veto — ou seja, impor obrigações ao país, na prática, é muito difícil pelos atuais instrumentos da ONU.

Asinda assim, a iniciativa conseguiu o apoio de 193 países, incluindo os Estados Unidos, tornando-se um importante instrumento político e com peso moral.

Especialmente no momento em que a administração Barack Obama está sendo pressionada não apenas para mudar seus programas de espionagem, mas também para abrir mão da gestão unilateral da internet.

Unasul planeja rede própria de comunicação

Sem citar diretamente os Estados Unidos, a União das Nações Sul-Americanas (Unasul) emitiu declaração em agosto de 2013 condenando a espionagem das comunicações. Assinado em Lima, no Peru, durante a terceira reunião de ministros das Comunicações dos países-membros, o texto condena "qualquer ação de interceptação" das comunicações sem a autorização das autoridades competentes e considera que essa atividade viola o princípio da não intervenção nos assuntos internos dos Estados estabelecido na Carta das Nações Unidas e os tratados e convenções internacionais e os direitos humanos fundamentais.

O documento adverte que os países sul-americanos precisam "elaborar uma agenda conjunta sobre o desenvolvimento tecnológico" para "reduzir a vulnerabilidade das comunicações". Também destaca a importância de "fortalecer e ampliar a participação governamental em foros de governança da internet". A Unasul insiste na criação de "ambientes de discussão multilateral sobre esse tema mais adequados à participação governamental", reforçando a proposta do governo brasileiro de centralizar a governança da internet em um órgão multinacional, como a União Internacional de Telecomunicações (UIT), agência das Nações Unidas dedicada ao tema.

Os ministros defenderam a construção de uma rede de comunicações sul-americana, com "pontos de troca de tráfego regional", para "minimizar a dependência de enlaces internacionais". Eles analisaram uma proposta de convênio entre a Unasul e o Banco Interamericano de Desenvolvimento (BID) para financiar a implantação dessa rede em cada país e recomendaram que o bloco assinasse o acordo.

Reduzir dependência

Segundo o ministro das Comunicações do Brasil, Paulo Bernardo, o projeto de interconexão vai ser importante para evitar que informações enviadas a um país vizinho tenham de cruzar o continente até chegar ao destino. "Além disso, a medida vai baratear os custos de conexão aos provedores e, consequentemente, ao consumidor. Então, mais pessoas poderão ter acesso à internet", acrescentou.

MARCELLO CASAL JR/ABR

O ministro das Comunicações, Paulo Bernardo, representou o Brasil na reunião da Unasul de agosto de 2013

Além disso, o grupo de trabalho de telecomunicações do Conselho Sul-Americano de Infraestrutura e Planejamento (Cosiplan) vai trabalhar para fortalecer a segurança das comunicações dos países da América do Sul e reduzir a dependência tecnológica de outras regiões, contando, inclusive, com auxílio do Conselho de Defesa Sul-Americano.

Também o Mercosul, reunido em Montevidéu, condenou a indiscriminada espionagem norte-americana. Brasil, Argentina, Uruguai e Venezuela insistiram na "necessidade prioritária de promover nas instâncias multilaterais pertinentes um debate profundo sobre normas, com o objetivo de garantir parâmetros adequados de segurança nas comunicações". O bloco solicitou à Argentina — que ocupa um assento temporário no Conselho de Segurança da ONU — que submeta o assunto ao órgão.

Parlasul

Por sua vez, os congressistas que compõem o Parlamento do Mercosul (Parlasul) endossaram em setembro uma moção de repúdio à espionagem dos Estados Unidos, apresentada pelo presidente da Representação Brasileira, deputado Newton Lima (PT-SP), e assinada também pelo senador Roberto Requião (PMDB-PR) e por representares dos outros quatro países do bloco: Argentina, Venezuelam, Uruguai e Paraguai.

No texto, eles manifestam o "veemente repúdio" às atividades de espionagem da Agência de Segurança Nacional (NSA) e de outras agências de inteligência norte-americanas. O documento faz referência, especialmente, à espionagem sofrida pelo Brasil e pela presidente Dilma Rousseff.

"Na moção também prestamos solidariedade à presidenta e total apoio à sua decisão de levar o assunto para a ONU", explicou Lima. O texto ressalta também que o princípio do respeito à vida privada, presente na Declaração Universal dos Direitos Humanos, vem sendo descumprido pelos Estados Unidos.

Europeus querem internet global, aberta e democrática

Na sequência da divulgação das ações de vigilância e espionagem em larga escala e da consequente diminuição da confiança na internet, a Comissão Europeia propôs, em abril passado, uma completa reforma na governança da rede, baseada em mais transparência e responsabilidade. Para os europeus, a internet deve servir às liberdades fundamentais e aos direitos humanos, que são inegociáveis e devem ser protegidos on-line.

No comunicado *Política e Governança da Internet: o papel da Europa na definição do futuro da internet*, a vice-presidente da Comissão Europeia, Neelie Kroes, afirmou que "os próximos dois anos serão críticos. A Europa precisa contribuir para um avanço confiável na governança global da internet".

Os europeus defendem ainda que os grupos sociais e econômicos de todas as partes do mundo tenham sua voz ouvida de uma maneira justa e construtiva. Ao mesmo tempo, isso não significa que os governos e outras autoridades devam renunciar ao seu papel na gestão da rede mundial.

A proposta deixa claro que a comissão apoia um "modelo multissetorial, abrangente, multinível" de governança da internet, baseado no envolvimento total de todos os atores e organizações relevantes. "Alguns pedem que a União Internacional das Telecomunicações [agência da ONU] assuma o controle das funções principais da internet. Concordo que os governos

GREGOR FISCHER

Neelie Kroes, da União Europeia, diz que o bloco precisa contribuir para "um avanço confiável na governança global da internet"

DHODI WIRASA

Países europeus defendem o fortalecimento do Fórum de Governança da Internet (IGF)

têm uma função crucial a desempenhar, mas as abordagens de cima para baixo não são a resposta certa. Devemos fortalecer o modelo multissetorial, de maneira a preservar a internet como motor rápido de inovação", declarou Kroes.

Detalhes

A proposta sugere um cronograma para que a Icann, hoje sediada nos EUA e sujeita às leis americanas, seja globalizada, salvaguardando a estabilidade e a segurança do sistema de nomes de domínio. A Europa defende também o lançamento de uma plataforma on-line transparente para o desenvolvimento técnico para a rede, chamado de Observatório Global da Política da Internet, que permita a "participação antecipada e verdadeiramente inclusiva" nas decisões técnicas.

"Dado o modelo centrado nos EUA de gestão da web, é necessário uma transição suave a um modelo mais global, mas que ao mesmo tempo proteja os valores de uma governança aberta", declarou a Comissão Europeia, que sugere ainda que uma nova Icann assuma três compromissos permanentes:

- Aprimoramento da transparência, responsabilidade e inclusão dos processos multissetoriais *(multistakeholders)* e daqueles que deles participam.
- Criação de um conjunto de princípios de governança da internet que salvaguardem a natureza aberta e não fragmentada da rede.
- Globalização do processo decisório (por exemplo, a coordenação dos nomes de domínio e dos endereços de protocolo) para salvaguardar a estabilidade, a segurança e a resiliência da internet. O fortalecimento do Fórum de Governança da Internet (IGF, na sigla em inglês) e a construção de um arcabouço legal global que solucione conflitos entre legislações ou jurisdições nacionais completariam a reforma defendida pelos europeus.

A Comissão Europeia quer ainda garantir o desenvolvimento de uma economia europeia na internet, alinhada ao fortalecimento de um verdadeiro mercado único digital, promovendo a neutralidade da rede, a partir de um quadro jurídico global, especialmente para o *e-commerce*, regulação com base na igualdade de oportunidades, governança e mercados abertos à concorrência, proteção dos consumidores, comunicações, audiovisual, comércio eletrônico, privacidade e proteção de dados pessoais.

Kroes informou também que, embora o documento ainda deva ser aperfeiçoado em conjunto pela comissão, pelo Parlamento Europeu e pelo Conselho da União Europeia, ele já é o alicerce da Europa nas negociações globais, como na Reunião de Alto Nível da Icann, em maio passado, e no Fórum de Governança da Internet, marcado para o final de agosto de 2014, na Austrália.

Obama promete parar de espionar líderes aliados

Presidente garantiu fim da vigilância sobre amigos e aliados, mas se recusou a pedir desculpas

A primeira reação norte-americana às denúncias foi tentar reaver o material vazado e repatriar o próprio Snowden. Porém, depois de enfrentar as críticas das nações vítimas da coleta ilegal de dados eletrônicos, que clamaram por uma ampla mobilização mundial em defesa do direito à privacidade, a Casa Branca admitiu que a NSA foi longe demais em relação aos países aliados.

Em 17 de janeiro de 2014, Barack Obama anunciou a disposição de rever o funcionamento da agência. Ele prometeu colocar um fim à espionagem de dirigentes de nações aliadas. "Fui muito claro para os serviços de informação: a menos que a segurança nacional esteja em jogo, não iremos espionar as comunicações dos líderes dos países aliados mais próximos e nossos amigos".

O presidente norte-americano também ressaltou mais de uma vez que não monitora e-mails ou ligações de cidadãos comuns. Ele esclareceu que a coleta de metadados — informações sobre ligações telefônicas — não incluía a identidade de quem fazia a ligação ou mesmo o conteúdo dela. De acordo com Obama, as informações coletadas eram sobre os números, hora e duração das chamadas, o que, segundo ele, poderia ser consultado apenas no caso de suspeitas de ligação com organizações terroristas. Essas informações, disse o presidente, são essenciais na luta contra o terrorismo. "Poder examinar os contatos telefônicos para estabelecer a existência de uma rede é essencial", declarou.

Sem desculpas

Obama fez questão de afirmar que não se desculpará por fazer "o que serviços de inteligência de qualquer outra nação fazem". "Nós não vamos nos desculpar simplesmente porque nossos serviços podem ser mais eficazes. Mas chefes de Estado e governo com quem trabalhamos, e de cuja cooperação dependemos, podem se sentir confiantes de que estamos tratando-os como verdadeiros parceiros."

A partir de então, anunciou o presidente dos EUA, a NSA terá de pedir autorização — com base em uma suspeita "razoável" — da corte secreta de segurança nacional (Fisc, na sigla em inglês) para espionar dados telefônicos, com redução do escopo das buscas individuais.

Ainda como consequência das revelações de Snowden, a Câmara dos Deputados dos Estados Unidos aprovou, em maio de 2014, o projeto de lei USA Freedom, segundo o qual a polícia federal americana (FBI) e a NSA não poderão forçar as operadoras nacionais a fornecer integralmente os metadados (datas, duração, números) de chamadas telefônicas feitas em suas redes nos Estados Unidos sem autorização do Fisc.

As empresas do Vale do Silício e ONGs ligadas ao tema criticaram a ambiguidade do texto, argumentando que a reforma impede na prática a coleta de dados eletrônicos dos americanos, mas nada impedirá a espionagem em massa pela NSA de grupos de pessoas, potencialmente milhões.

"A versão mais recente cria uma lacuna inaceitável que poderia permitir a coleta em massa de dados dos internautas", considerou em um comunicado a coalizão Reform Government Surveillance, que inclui AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter e Yahoo!.

Traidor

O presidente americano também voltou a criticar Snowden, que, segundo ele, colocou a segurança nacional em risco. "A maneira sensacionalista como essas revelações vieram à tona foi, no fundo, mais espetacular do que significativa. Elas revelaram a nossos adversários métodos que podem ter consequências em nossas operações, que talvez só compreenderemos em muitos anos", disse.

PETE SOUZA/THE WHITE HOUSE

Five Eyes: espionagem moderna começou há quase um século

A modernização do negócio da espionagem tem um marco inicial definido: a assinatura, em março de 1946, do Tratado de Segurança entre os Estados Unidos e o Reino Unido. O acordo formalizou a Carta do Atlântico, assinada em 1941, antes da entrada americana na 2ª Guerra Mundial, para a decodificação de mensagens alemãs e japonesas e a partilha de informações secretas entre os Estados Unidos e o Reino Unido. Restrito inicialmente aos dois países, o sistema posteriormente agregou Canadá, Austrália e Nova Zelândia — formando os Cinco Olhos ou Five Eyes —, unidos pela língua inglesa e pelo objetivo de antecipar os movimentos dos inimigos.

As organizações de cada país que participam do sistema, sob o comando da NSA, são o GCHQ (Government Communications Headquarters), do Reino Unido, o CSEC (Communications Security Establishment Canada), do Canadá, o ASD (Australian Signals Directorate), da Austrália, e o GCSB (Government Communications Security Bureau), da Nova Zelândia. Juntos, eles criaram o Echelon, uma rede de vigilância global e de espionagem.

Como em tudo que diz respeito à espionagem, à exceção das revelações de Snowden, baseadas em documentos subtraídos da NSA, há poucos indícios concretos e documentados da atuação dos Five Eyes. Segundo investigação feita pelo Parlamento Europeu em 2001, por exemplo, o Echelon foi usado pelos EUA para colaborar com a empresa americana Raytheon na concorrência lançada pelo governo brasileiro por serviços e equipamentos para o Sistema de Vigilância da Amazônia, o Sivam. Os americanos venceram a disputa.

Em março de 2014, a revista *Der Spiegel* publicou documentos mostrando que, por meio do CGHQ, e sob o comando da NSA, os sistemas de satélite da Alemanha se tornaram alvo de espionagem. Segundo o presidente da Cloud Security Alliance Brasil (CSA Brasil), Paulo Pagliusi, ouvido pela CPI da Espionagem, os Five Eyes monitoram chamadas telefônicas e de fax, transmissões de rádio e os acessos à internet em todo o mundo.

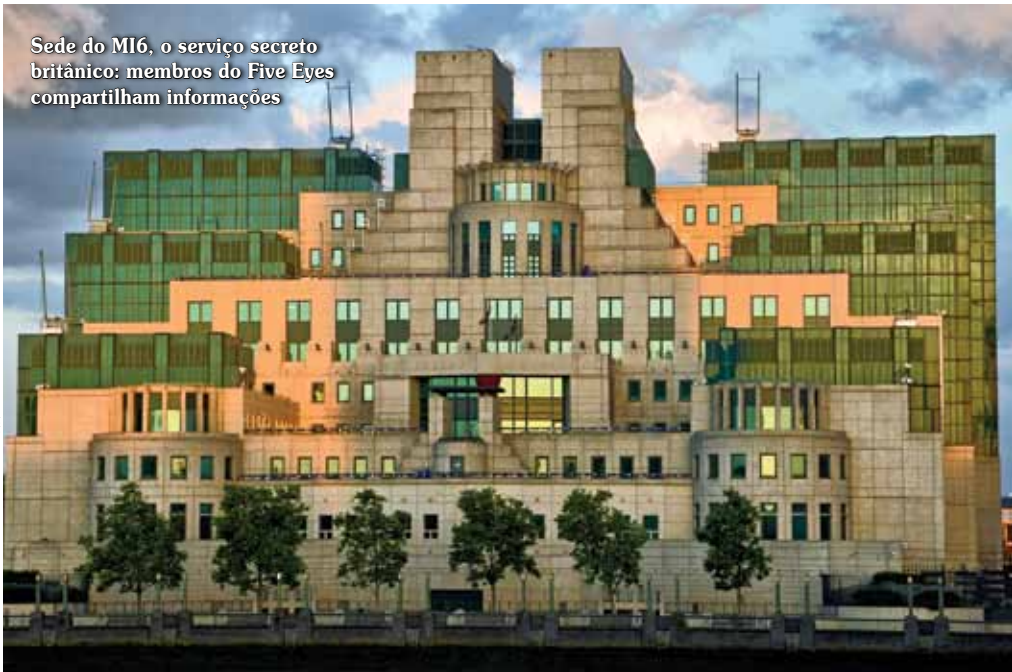
DIVULGAÇÃO

A espionagem cibernética cresce no pós-guerra e se impõe até na ficção: que seria de James Bond *(D)* sem Q, o hacker do MI6?

Mercado

Atentados foram evitados; terroristas, localizados e presos; e inúmeros outros objetivos dos Five Eyes, alcançados como resultado de sua associação, afirmam ex-agentes secretos, muitos deles sob anonimato, ouvidos por grandes veículos da mídia mundial. Para eles, as informações dos Estados Unidos são tão valiosas que não há indignação, reação ou argumentos em favor do direito à privacidade que convençam britânicos, canadenses, australianos e neozelandeses a renunciarem à parceria com os EUA.

"Informações são como ouro. Se você não as tem, não há como sobreviver", disse à agência Associated Press o ex-chefe da agência de espionagem estrangeira da Nova Zelândia Bruce Ferguson. Nesse "mercado", a informação é a moeda, e a confiança recíproca, a despeito de eventuais desconfianças mútuas, deve ser o contrato.



DUNCAN HARRIS

Sede do MI6, o serviço secreto britânico: membros do Five Eyes compartilham informações

PAÍSES VULNERÁVEIS A ATAQUES

As revelações de Edward Snowden trouxeram a questão da segurança em tecnologia da informação de volta ao topo das agendas das nações, fazendo com que muitas dessem prioridade à atualização das estratégias nacionais. Apesar de muitas delas serem recentes, nenhuma, mesmo com as revisões propostas, garante as condições para segurança total dos sistemas.

A França, por exemplo, vem se concentrando, desde 2011, em fortalecer os sistemas de informação para resistir a ataques que possam comprometer a disponibilidade, a integridade e a confidencialidade dos dados. A estratégia francesa enfatiza tanto o aperfeiçoamento tecnológico da segurança dos sistemas de informação quanto a luta contra o crime na rede e a criação de ciberdefesas.

A Alemanha privilegia, em estratégia definida em 2011, a prevenção e a repressão de ataques cibernéticos e também a prevenção de falhas de TI, especialmente em relação a suas infraestruturas críticas. Funções básicas de segurança são certificadas pelo Estado alemão. Agora, as autoridades do país acham que há necessidade de estabelecer novos poderes para garantir a manutenção da disponibilidade e confiabilidade dos seus sistemas.

Liberdade fundamental

Já a estratégia do Reino Unido, do mesmo ano, relaciona entre os objetivos do país tornar-se a maior economia em inovação, investimento e qualidade de tecnologia da informação, para ser capaz de explorar plenamente o potencial e os benefícios da rede mundial. Eles estão focados ainda em reduzir os riscos do ciberespaço, sejam eles a atuação de criminosos, ataques terroristas ou a espionagem por parte de outros Estados.

Para a Holanda e a República Tcheca, o principal objetivo é garantir a segurança, a confiabilidade e a disponibilidade dos seus sistemas, prevenindo abusos e interrupções em larga escala. Mas a estratégia holandesa reconhece a necessidade de proteger a liberdade da internet, ainda que defenda a confidencialidade das informações armazenadas e a necessidade de evitar quaisquer danos à integridade das informações.

Segurança também é o foco de Estônia, Finlândia e Eslováquia, sendo que, para os dois últimos, o papel da internet no desenvolvimento econômico é considerado essencial. A Estônia privilegia ainda a regulamentação, a educação dos usuários e a cooperação entre os setores público e privado.

Fragilidades

Segundo pesquisa da Security & Defence Agenda (SDA), um centro de estudos de Bruxelas dedicado à segurança cibernética, as estratégias dos países, no entanto, estão longe de materializarem-se em efetiva segurança quando se trata de espionagem ou ciberataques.

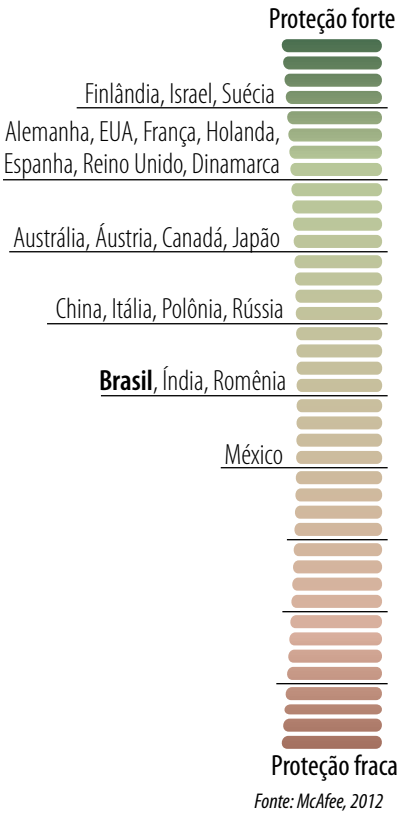
O relatório analisou 23 países e nenhum recebeu a nota máxima. "Nenhum país está à frente de ciberatacantes", disse Phyllis Schneck, então chefe do setor de tecnologia da SDA. Segundo ela, os maus vão "mais rápido" do que os mocinhos.

"A questão é que os cibercriminosos não têm de lutar com questões legais e políticas e podem compartilhar livremente informações uns com os outros sem se preocupar com questões de concorrência", disse ela. "Nós estamos enfrentando um adversário que não tem limites e temos que ir a reuniões e escrever relatórios", acrescentou Phyllis, que hoje ocupa um cargo no Departamento de Segurança Interna dos EUA. "Estamos em uma enorme desvantagem."

A pedido da gigante americana de segurança McAfee, a SDA entrevistou 330 especialistas para elaborar o relatório. Os que disseram acreditar que uma corrida armamentista cibernética está acontecendo chegaram a 57%, enquanto 36% afirmaram que a segurança cibernética é mais importante do que uma defesa antimísseis. Quase a metade, 45%, disse que a cibersegurança é tão importante quanto a segurança na fronteira. Nesse quesito, as fronteiras da maioria dos países estão desguarnecidas, à exceção de Israel, Finlândia e Suécia, considerados os mais bem preparados.

Estamos todos muito expostos

Pesquisa de 2012 revela que mesmo países que mais investiram em segurança não estão livres de ataques



Fonte: McAfee, 2012

V. MARTIN/UIT

Sede da UIT, em Genebra: Brasil defende aperfeiçoamento das regras multilaterais sobre segurança das telecomunicações

Entidade pode ter papel regulador

A indignação geral com a exposição do alcance da espionagem norte-americana não demorou a chamar a atenção dos usuários da internet para a falta de regras que protejam pessoas, empresas e países da onipresente ameaça de desrespeito à privacidade das comunicações. Consequência da exacerbação dessa percepção foi a avalanche de propostas e medidas mundo afora — ainda que a maioria tenha sido inócua.

A Alemanha, por exemplo, anunciou que a Deutsche Telekom — da qual o governo detém 32% das ações — passaria a exigir que as parceiras locais blindassem o tráfego em suas redes contra a ação de serviços de inteligência estrangeiros. Críticos da medida, no entanto, afirmam que ela não terá resultados práticos quando os alemães estiverem navegando em sites hospedados em servidores no exterior.

Isolamento

Pior, avaliam que o avanço da rede mundial em território alemão pode ser desestimulado, na medida em que a exigência implica que as empresas deverão revelar o caminho percorrido pelos dados que transportam, considerado um dos segredos do negócio.

Os estudiosos do tema, ONGs e associações civis alertam para o risco de que um aumento da regulamentação nos países, além de restringir a liberdade de expressão na rede, crie dificuldades para sua expansão e aperfeiçoamento e até provoque retrocesso, com o aparecimento de redes isoladas e estanques, fadadas a serem mais pobres em informações e em inovação tecnológica. Exemplos como Irã e China — que instalam barreiras de alcance nacional e bloqueiam sites como Facebook e Twitter —, embora extremos, são apresentados como sinais de que não se pode abrir mão da liberdade na rede.

Também para Rafael Moreira, secretário-adjunto de Política de Informática do Ministério da Ciência e Tecnologia, confinar o tráfego de dados ao território nacional é complicado. Na apresentação aos senadores da CPI da Espionagem, ele afirmou que a medida poderia, até mesmo, inviabilizar o trânsito de dados em caso de problemas nas redes.

Por outro lado, as próprias história e estrutura da internet — que nasceu e prosperou nos Estados Unidos, tornando-se em pouco tempo um novo fator de crescimento econômico para todo o mundo e cujo tráfego passa de rede em rede, pago ou não, sem qualquer relação com as fronteiras nacionais — dificultam uma regulamentação. Isso sem contar que os EUA se opõem fortemente à regulação. Sem apoio dos norte-americanos, qualquer iniciativa com relação à internet tem grandes chances de fracassar.

Normatização

Essa posição, porém, vem perdendo apoio e credibilidade a cada revelação de Snowden. Embora a Constituição dos EUA obrigue o governo a apresentar motivos plausíveis para vigiar as comunicações de cidadãos norte-americanos dentro do país e outras nações tenham regulamentações parecidas, na arena internacional praticamente não há regras.

Se nas fronteiras nacionais a regulação da internet parece impossível, a União Internacional de Telecomunicações (UIT) está sendo pressionada a assumir papel regulatório sobre a rede. Fundada em 1865, em Paris, para padronizar ondas de rádio, a agência das Nações Unidas (com representantes de 193 países e mais de 700 organizações dos setores privado e acadêmico) é essencialmente técnica, mas tem sido cada vez mais instada a se tornar um órgão regulador da internet.

O Brasil e a Unasul também defendem a normatização. Em junho do ano passado, o então ministro das Relações Exteriores, Antonio Patriota, declarou que o Brasil pretendia "promover no âmbito da UIT o aperfeiçoamento de regras multilaterais sobre segurança das telecomunicações".

A própria CPI argumenta, no relatório, que "a única maneira de regulamentar a economia global e o mundo globalizado é desenvolver a eficiência da lei internacional, tanto no seu conteúdo quanto na sua estrutura legal".

CONNIE ZHOU/GOOGLE

Unidades de resfriamento dos servidores do Google, nos EUA: americanos têm domínio operacional e técnico da rede

NOVA governança esbarra nos EUA

Diante da espionagem em larga escala patrocinada pelos Estados Unidos, por que os demais países não propõem uma nova governança para a internet que permita equilibrar o poderio norte-americano? Se a pergunta parece simples, a resposta também é: porque a infraestrutura da rede — cabos submarinos, hardware, softwares e regras — e seus maiores atores — Amazon, Google, eBay, Facebook, Priceline, Yahoo, Twitter, Netflix, de quem todos dependem, até voluntariamente —, além de uma pujante indústria em tecnologia da informação, continuam de posse daqueles que criaram a internet e a trouxeram ao estágio atual. E que hoje a consideram um recurso crítico para sua segurança e liderança global.

Esse domínio é tão extenso que estima-se que grande parte dos acessos à internet e das comunicações via web no mundo transitem pelos servidores americanos. Segundo Ari Sergio Perri Falarini, diretor de Operações da Telefônica Vivo, o tráfego de clientes da empresa do Brasil para o exterior está em torno de 386 gigabits por segundo (Gbps), dos quais 229 Gbps, ou quase 60%, seguem diretamente para os EUA. Mesmo quando o destino original não são os Estados Unidos, trafegar pelas redes do país pode ficar bem mais barato, justamente porque, com uma infraestrutura maior, essa opção de tráfego acaba ficando mais em conta.

Em pesquisa de pós-doutorado para a Universidade de Barcelona, o professor Hindenburgo Francisco Pires, do Instituto de Geografia da Universidade do Estado do Rio de Janeiro (Uerj), afirma que, para entender a hegemonia americana na internet, é preciso retroceder e perceber que, durante o pós-guerra e a Guerra Fria, o poderio do país se estruturou em dois grandes pilares: a expansão econômica e a acumulação militar.

Concentração

Concebida como peça integrante desse poderio militar, a internet logo revelou sua vocação comercial, mas, ao mesmo tempo em que os EUA perceberam o

enorme potencial econômico da rede, também se deram conta de suas vulnerabilidades. "O ciberespaço continua sendo, na atualidade, um terreno estratégico de interesses econômicos e militares dos EUA e também um campo virtual de guerra, sobre o qual esses interesses devem manter um sistema militar permanente de segurança, de vigilância e de proteção de suas redes", explica Pires.

Para o professor, a concentração de servidores nos EUA — em especial os da chamada zona-raiz, que está na base de todo o funcionamento da rede (dos 13 servidores-raiz, 10 estão no país) — "é um fenômeno historicamente estabelecido desde a constituição da internet como uma rede militar, que posteriormente se tornou uma rede acadêmica e comercial. Os parâmetros do sistema hierarquizado de concessão de nomes de domínios permitem a articulação e o mapeamento geográfico dos servidores regionais interconectados no ciberespaço, fortalecendo e reforçando o controle geopolítico e a concentração dos servidores da zona-raiz pelos EUA".

Ainda segundo Pires, o domínio tecnológico e jurídico facilita o domínio comercial, e questões como soberania dos demais países, segurança, educação, direito à privacidade, liberdade de expressão e democracia ficam a reboque dos interesses norte-americanos, prejudicando a visão da rede mundial como um serviço público e um fomento à democracia.

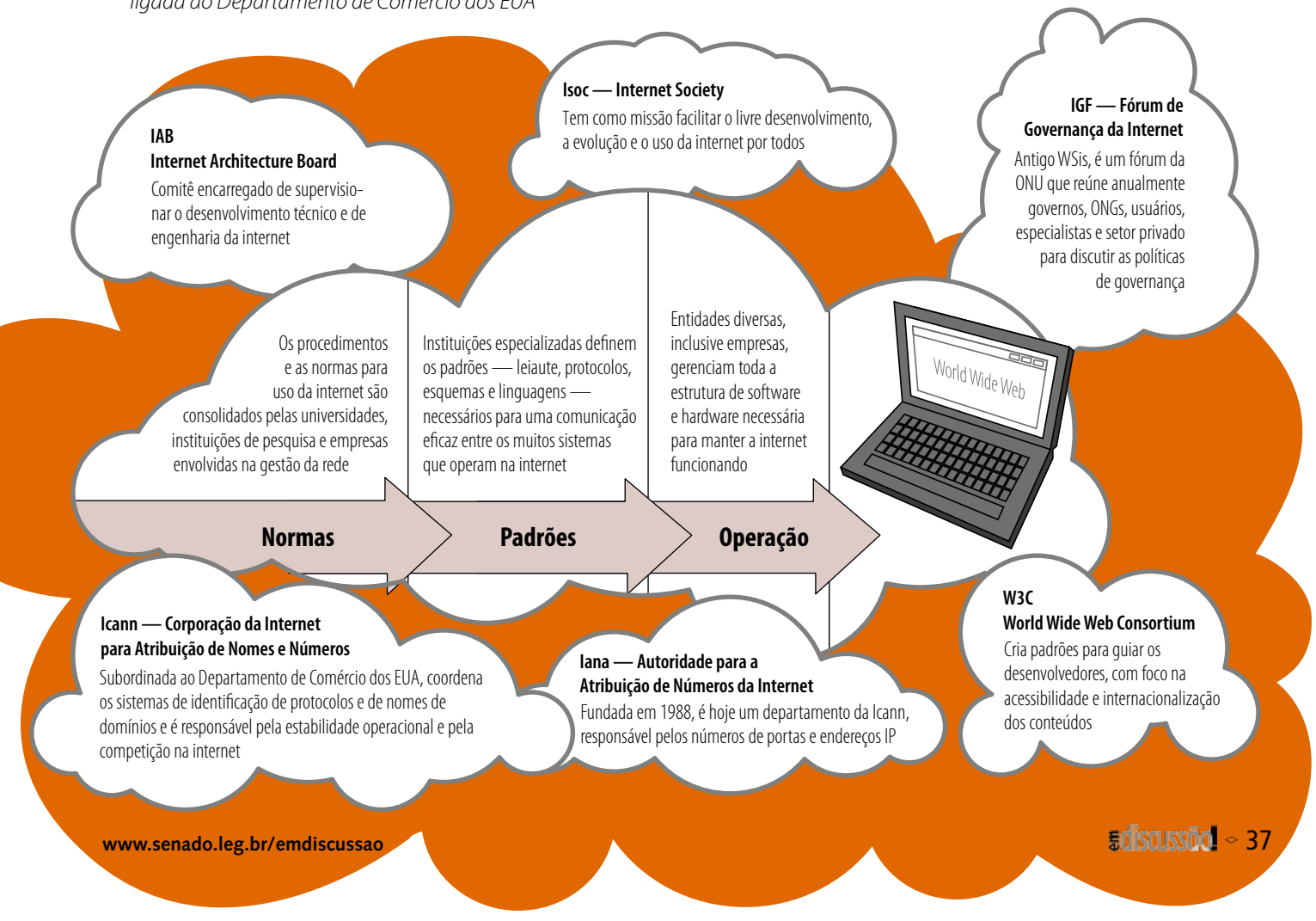
Estrutura

O atual modelo de governança da internet foi consolidado em 1998 e é integrado pelos Departamentos de Comércio e de Defesa dos Estados Unidos, pela Icann (sigla em inglês para Corporação da Internet para Atribuição de Nomes e Números) e pela Verisign, empresa de segurança prestadora de serviços ao governo norte-americano. "Nesse sentido, o Departamento de Defesa manteve o controle militar do ciberespaço e a Icann, juntamente com a Verisign, ficou com o controle comercial. Por isso, eles vêm sendo os organismos formais responsáveis e exclusivos pela atribuição de parâmetros de protocolo da internet, pela regulação do sistema de nome de domínio, pela alocação de blocos de números de endereços IP e pela gestão do servidor-raiz do sistema... Um negócio altamente lucrativo", explica em sua pesquisa o professor da Uerj.

A despeito das várias iniciativas de 2003 até 2011 para reformar o modelo atual de governança da internet, com a realização de oito fóruns promovidos pela ONU (Internet Governance Forum — IGF), os Departamentos de Segurança Doméstica e de Defesa e a Casa Branca publicaram, no mesmo período, quatro importantes documentos de estratégias políticas de manutenção do controle da internet, informa Hindenburgo.

Gestão descentralizada

Nascida para ser uma rede militar, a internet só depois se revelou um importantíssimo fator econômico global. Em função desse histórico, sua gestão segue um padrão descentralizado, tendo à frente a Icann, ligada ao Departamento de Comércio dos EUA



SEM CULTURA DE INTELIGÊNCIA

ELZA FIÚZA/ABR

Sala de monitoramento da Abin, em Brasília: órgão central da inteligência não tem poder de coordenação no setor

Terceiro do mundo em número de usuários da internet, Brasil apresenta baixos níveis de segurança e defesa cibernética, tanto no setor público quanto no privado. Sistema de inteligência é complicado, muito fracionado e carece de coordenação

O Brasil é o terceiro país do mundo em número de usuários ativos da internet. Segundo dados do Ibope, foram 52,5 milhões de brasileiros conectados em 2013, atrás apenas dos Estados Unidos, 198 milhões, e do Japão, 60 milhões. Quando se considera o número de cidadãos com acesso à internet, a quantidade sobe para 105 milhões de pessoas, praticamente metade da população do país.

Apesar da significativa presença da internet na vida do brasileiro, o país é apontado como um dos mais vulneráveis a ataques cibernéticos. As denúncias de espionagem do técnico da Agência de Segurança Nacional (NSA) dos EUA Edward Snowden não foram surpresa para os especialistas. Em 2012, o centro de pesquisas belga Security & Defence Agenda (SDA) e a empresa McAfee divulgaram estudo no qual o Brasil figura como um dos menos preparados para se defender de ataques virtuais entre 23 países, com nota 2,5, ao lado de Índia e Romênia, à frente apenas do México. Os mais bem-colocados no ranking foram Israel, Finlândia e Suécia, com nota 4,5.

O estudo levou em consideração a adoção de medidas básicas como *firewalls* (barreiras contra invasões) adequados, proteção antivírus e outras mais sofisticadas, além de variáveis como a cultura de segurança geral e o grau de proteção dado às informações de governo.

Em setembro do ano passado, em discurso na Assembleia Geral das Nações Unidas, a presidente da República, Dilma Rousseff, repudiou a espionagem eletrônica levada a cabo pelos Estados Unidos. Segundo ela, a prática afeta a comunidade internacional e pode transformar as tecnologias de informação e comunicação em um novo campo de batalha entre os Estados. A presidente, seus assessores e a Petrobras tiveram e-mails invadidos pelo serviço secreto norte-americano em busca de vantagens comerciais. Mesmo assim, Dilma Rousseff negou a vulnerabilidade. "O Brasil sabe se proteger", sentenciou a presidente.

Mas essa não foi a conclusão da Comissão Parlamentar

de Inquérito da Espionagem do Senado. De acordo com o relator, senador Ricardo Ferraço (PMDB-ES), há falta de cultura de inteligência no Brasil. "Pouco se conhece e pouco se discute sobre os serviços secretos e seu trabalho", diagnosticou o senador. Como consequência, constata-se o despreparo dos brasileiros para fazer frente a ameaças reais como espionagem, atuação de organizações criminosas e grupos terroristas.

"Incursões como as que supostamente ocorreram contra autoridades e instituições brasileiras continuarão a ocorrer e passarão despercebidas, caso não se desenvolva, com urgência, aparato de contrainteligência e de mecanismos de proteção ao conhecimento para fazer frente a essas ameaças", afirmou Ferraço.

De fato, não foi preciso esperar muito tempo para ver uma nova incursão. Em maio, o Brasil sofreu um novo ataque. Dessa vez, o Ministério das Relações Exteriores foi alvo do grupo de hackers Anonymous, que invadiu o sistema de e-mails do serviço diplomático e teve acesso a cerca de 300 documentos, alguns deles classificados como secretos.

De acordo com a CPI, a implementação de uma política de segurança e defesa cibernética *(veja quadro na página ao lado)* exige mudanças profundas na tecnologia e nos processos utilizados, bem como no comportamento das pessoas e nas instituições que os utilizam. São mudanças essenciais para fazer frente às ameaças crescentes.

Sistema

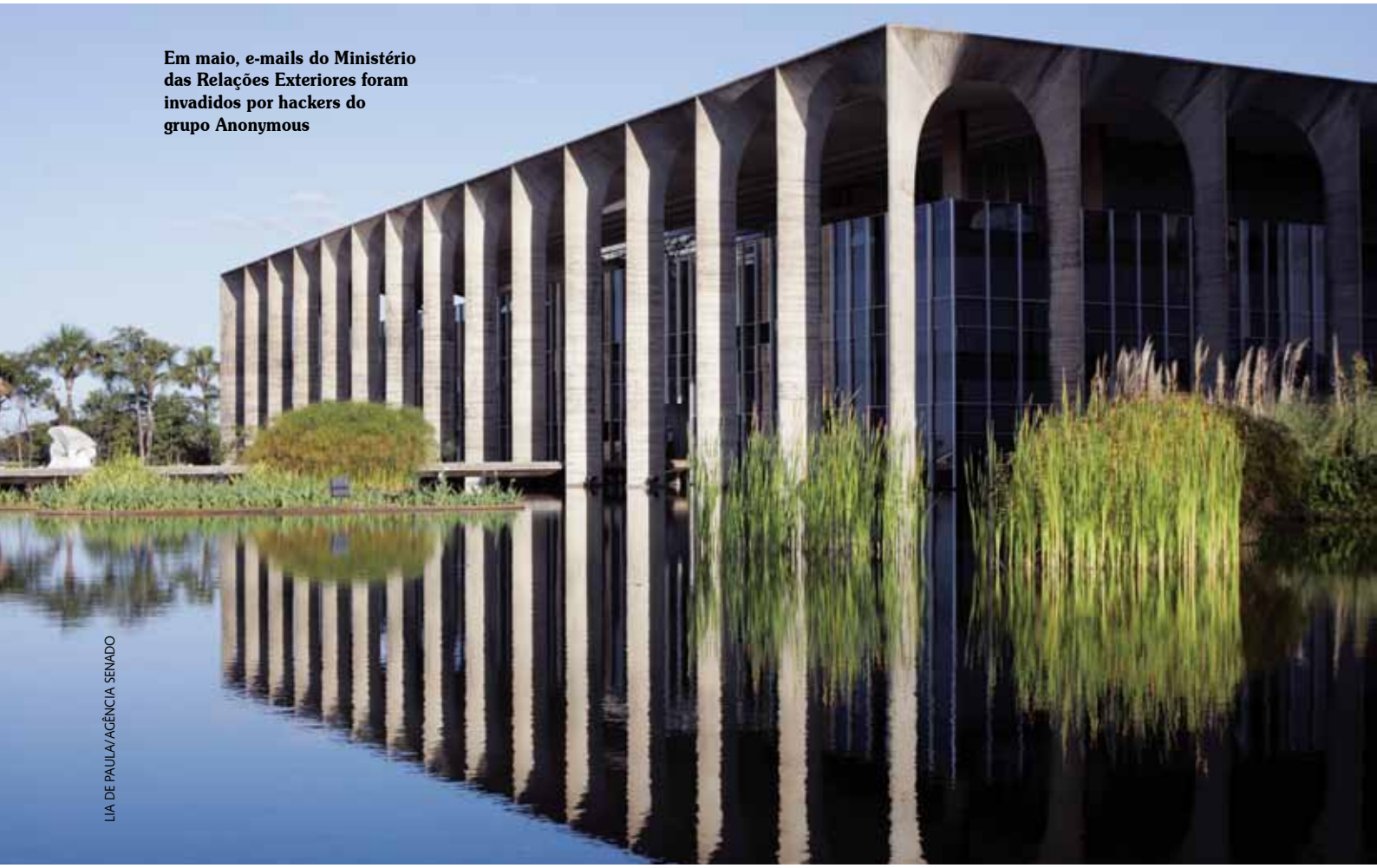
Mas a quem cabe proteger o Brasil desse tipo de ameaça? Espionagem e contraespionagem, de forma geral, são responsabilidade do Sistema Brasileiro de Inteligência (Sisbin), criado em 1999 pela Lei 9.883. O sistema é composto de várias instituições e subsistemas que, juntos, formam a "comunidade de inteligência", da qual a Agência Brasileira de Inteligência (Abin) é o órgão central.

Esse sistema enfrenta vários problemas, como dificuldade de integração entre os muitos órgãos que o compõem, pouca clareza na definição das atribuições e orçamento baixo.

Uma das deficiências que mais atrapalham o bom andamento das atividades é a falta de compartilhamento de informações entre as diversas instituições que constituem a comunidade.

De acordo com a lei, cabe à Abin "planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência no país". Na prática, isso não acontece. Embora seja responsável por coordenar as ações de inteligência, a Abin não tem qualquer ingerência sobre as outras instituições que integram o sistema.

A tarefa de coordenar a comunidade de inteligência não é fácil, dada a quantidade de entes envolvidos. Além da Abin, outras 18 instituições públicas fazem parte do Sisbin, entre elas a Casa Civil e o Gabinete de Segurança Institucional da Presidência da República, a Controladoria-



Em maio, e-mails do Ministério das Relações Exteriores foram invadidos por hackers do grupo Anonymous

LIA DE PAULA/AGÊNCIA SENADO

LIA DE PAULA/AGÊNCIA SENADO

Senadores Pedro Taques, Vanessa Grazziotin e Ricardo Ferraço durante sessão que instalou a CPI no Senado

-Geral da União (CGU) e vários ministérios, como os da Fazenda, do Trabalho, da Saúde, da Integração Nacional e das Comunicações.

Subsistemas

Os estados podem integrar o Sisbin, desde que firmem convênio com o governo federal. Mas, até agora, nenhum foi firmado, de acordo com o relatório da CPI.

Na última década, foram desenvolvidos subsistemas regionais e estaduais de inteligência de segurança pública, que reúnem a comunidade de inteligência local, entes das administrações direta e indireta e segmentos do setor privado.

Além do Sisbin, foram criados no âmbito federal o Subsistema de Inteligência de Segurança Pública (Sisp), em 2000, e o Sistema de Inteligência de Defesa (Sinde), em 2002. Do primeiro, fazem parte os Ministérios da Justiça, da Fazenda, da Defesa e da Integração Nacional, além do Gabinete de Segurança Institucional da Presidência. O órgão central do Sisp é a Secretaria Nacional de Segurança Pública (Senasp) do Ministério da Justiça.

Segundo a CPI, esse subsistema tem sido de extrema importância para integrar os órgãos de inteligência na área de segurança pública, particularmente no que concerne ao desenvolvimento de doutrina e metodologia para o combate ao crime organizado. Já o Sinde é voltado para a área militar. Assessora o Ministério da Defesa em ações de inteligência e reúne órgãos de inteligência da pasta e dos comandos das três Forças Armadas (Exército, Marinha e Aeronáutica).

Superposição

O consultor do Senado Joanisval Brito Gonçalves destacou, no artigo "O que fazer com nossos espiões? Considerações sobre a atividade de inteligência no Brasil", que uma das prioridades para melhorar o sistema é aperfeiçoar as competências legais, hoje vagas, dos órgãos envolvidos com inteligência. "Falta legislação que estabeleça mandato claro para cada órgão da comunidade de inteligência, bem como as competências e áreas de atuação de cada um e, sobretudo, os limites para a execução das atividades dessas agências", escreve.

Segundo ele, as lacunas legais geram superposição de tarefas e choque entre órgãos do sistema.

"A quem compete acompanhar o crime organizado, somente à Polícia Federal ou a Abin também pode fazê-lo? Qual o papel do serviço de inteligência das Forças Armadas, como no caso das fronteiras, onde elas têm poder de polícia?", pergunta o consultor.

Entre as soluções recomendadas pela CPI, de maneira geral, estão a reestruturação do Sistema Brasileiro de Inteligência, o estabelecimento de atribuições claras para os muitos órgãos que compõem a comunidade de inteligência e a criação de centros de integração nos principais órgãos.

A CPI também sugere a criação de uma única escola de formação de profissionais de inteligência ou o estabelecimento de uma estreita parceria entre as escolas existentes.

Segurança e defesa, conceitos distintos

Segurança cibernética compreende aspectos e atitudes tanto de prevenção quanto de repressão. É "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".

Já a **defesa cibernética** diz respeito ao conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente.

Fontes: Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro *(Raphael Mandarino Júnior, 2009)* e Desafios Estratégicos para a Segurança e Defesa Cibernética *(SAE, 2011)*

Por uma política nacional de segurança cibernética

A CPI da Espionagem ressaltou que, embora o tema da segurança na rede já figurasse como prioridade na Estratégia Nacional de Defesa, em 2008, o sistema de defesa cibernética do país se encontra em estágio inicial. As instituições que lidam com inteligência e a administração pública, de modo geral, ainda não se prepararam para enfrentar os problemas da realidade virtual, segundo o técnico do Instituto de Pesquisa Econômica Aplicada (Ipea) Samuel Cruz.

A defesa cibernética costuma sofrer dos mesmos problemas da área de inteligência, diz ele. Há grande diversidade de atores e pouca coordenação entre eles. Os principais órgãos que atuam na área são Gabinete de Segurança Institucional da Presidência da República (GSI), Abin, Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR. Gov), Ministérios das Relações Exteriores, da Justiça e da Defesa, Polícia Federal, Marinha, Exército e Aeronáutica.

O *Livro Verde da Segurança Cibernética*, elaborado pelo GSI em 2010, elenca entre os desafios a serem solucionados a superposição de missões institucionais entre os atores governamentais e a deficiência de governança. Destacam-se ainda a carência de senso comum e de arcabouço conceitual de segurança cibernética e o pequeno fluxo e intercâmbio de informação entre as equipes de tratamento de incidentes em redes computacionais do governo e as redes de inteligência de governo.

A proposta do GSI para resolver os problemas é criar a Política Nacional de Segurança Cibernética, que deve "viabilizar o exercício da macrocoordenação do tema e propiciar a congruência dos esforços e iniciativas entre os diferentes atores da rede, apoiada no senso comum e suas derivações".

Samuel Cruz concorda em dar prioridade à criação da política: "O Brasil ainda não possui um documento que estabeleça as diretrizes próprias de uma estratégia nacional para a defesa cibernética. Ou seja, ainda não há um plano integrado de metas, objetivos e responsáveis para a melhoria da segurança e defesa cibernética a médio e longo prazo", argumentou.

Essa proposta ganhou apoio entre os senadores da CPI. Ricardo Ferraço defendeu que, em um país com dimensões continentais como o Brasil, a proteção do ciberespaço deve ser encarada de forma estratégica pelo Estado, pois desempenha papel essencial, tanto para a segurança e soberania quanto para a integração cultural e o desenvolvimento econômico. "O país deve discutir e elaborar uma política nacional de segurança cibernética, com a participação de todos os órgãos envolvidos, de todas as esferas de poder", completou.

Defesa militar

A Estratégia Nacional de Defesa definiu três setores estratégicos: o nuclear, o espacial

Centro de Defesa Cibernética, localizado no quartel-general do Exército em Brasília, é um dos responsáveis pela área

e o cibernético, que devem ser gerenciados pela Marinha, Aeronáutica e Exército, respectivamente. Como responsável pela proteção do ambiente virtual, o Exército criou, em 2010, o Centro de Defesa Cibernética (CDCiber), que já está em operação.

Entre os objetivos do centro, estão a criação de um simulador de guerra cibernética, de um antivírus nacional e de um sistema de criptografia, além da capacitação de militares para situações críticas. O órgão já forneceu segurança e defesa virtual para a conferência internacional de meio ambiente Rio+20, em 2012.

Naquele ano, o Ministério da Defesa aprovou a Política Cibernética de Defesa, coordenada pelo Estado Maior Conjunto das Forças Armadas. O objetivo é orientar as atividades de defesa cibernética, no nível estratégico, e de guerra cibernética, nos níveis operacional e tático. A medida foi aprovada visando à segurança dos grandes eventos — Copa das Confederações, em 2013, Copa do Mundo neste ano e Jogos Olímpicos de 2016. Há previsão ainda de criar o Sistema Militar de Defesa Cibernética (SMDC), que contará com a participação de civis e militares.

Além do setor público, existem empresas privadas dedicadas à segurança na rede, proteção de dados, sistemas de criptografia, antivírus, entre outros.

FOTOS: EXÉRCITO BRASILEIRO

Criado há quatro anos, o Centro de Defesa Cibernética do Exército desenvolve um simulador de guerra cibernética

De acordo com o pesquisador do Ipea Samuel Cruz, esse setor é mais forte e eficiente em termos operacionais e produtivos do que o setor público. "Percebendo isso, o Exército tem se utilizado da capacidade da indústria para desenvolver ferramentas estratégicas para o programa de segurança. Contudo, a quantidade de empresas nacionais ainda é muito reduzida frente aos desafios do futuro. Atualmente, há cerca de 35 empresas de desenvolvimento e fornecimento de soluções robustas em segurança cibernética localizadas no país", esclareceu. Na avaliação dele, o setor público jamais conseguirá atingir níveis desejados de segurança ou defesa sem parcerias com o setor privado.

De espiões na Guerra Fria a arapongas na ditadura

O primeiro serviço de inteligência brasileiro foi criado em 1927, pelo então presidente da República, Washington Luís. Ao Conselho de Defesa Nacional cabia, entre outras funções, assessorar o presidente em assuntos de inteligência e contrainteligência.

Após o término da 2ª Guerra Mundial, em 1946, o presidente Eurico Gaspar Dutra organizou o Serviço Federal de Informações e Contrainformações, que se transformou no principal ator da área de inteligência no país. Em 1949, foi aprovado o Regulamento para a Salvaguarda das Informações que Interessam à Segurança Nacional, primeiro instrumento legal de proteção das informações sigilosas. A partir de 1958, com o recrudescimento da Guerra Fria, o serviço passou a cooperar com Estados Unidos e Europa Ocidental.

Mas a atividade de inteligência cresceu em importância com o golpe militar de 1964, mesmo ano em que foi criado o Serviço Nacional de Informações (SNI) e o Sistema Nacional de Informações (Sisni). De acordo com a lei, o chefe do SNI teria a nomeação sujeita à aprovação prévia do Senado e prerrogativas de ministro.

Vinculado diretamente à Presidência, o serviço secreto tinha grande influência no governo. Para mensurar o peso da atividade de inteligência, Emílio Garrastazu Médici (1969–1974) e João Baptista Figueiredo (1979–1985) foram chefes do SNI que trocaram o cargo pela Presidência, por eleição indireta. Esse vínculo com o regime autoritário plantou na sociedade um sentimento negativo e uma forte desconfiança em relação à atividade de inteligência, que perdura quase 30 anos depois do fim da ditadura.

O SNI foi extinto em 1990, pelo então presidente Fernando Collor de Mello, mas a medida, embora bem-intencionada ao extinguir o órgão que era símbolo máximo do regime autoritário, teve consequências negativas. "A comunidade de informações foi desmantelada, servidores civis foram redistribuídos, aposentados ou demitidos, os militares que trabalhavam nos órgãos de inteligência reconduzidos às respectivas Forças. Muitos arquivos foram perdidos ou destruídos e houve uma ruptura na memória organizacional de muitos serviços secretos que dificilmente poderia ser recuperada", escreve Joanisval Brito Gonçalves no artigo "O que fazer com nossos espiões".

Ele avalia que esse cenário só começou a mudar a partir de meados da década de 90, com a proposta do governo Fernando Henrique Cardoso de criar uma agência de inteligência e de um sistema de inteligência que operassem de acordo com o regime democrático, em defesa do Estado e da sociedade e em estrito cumprimento da lei. A proposta deu origem à Lei 9.883, promulgada em 1999, que criou a Abin e o Sisbin.

General João Figueiredo toma posse, em 1979: foi o segundo chefe do SNI a chegar à Presidência

SENADO FEDERAL

DESAFIO é implantar mudança profunda

Para a CPI da Espionagem, a implementação de uma política de segurança e defesa cibernética exige mudanças profundas na tecnologia e nos processos utilizados. É preciso também mudar o comportamento das pessoas, dos servidores públicos e das instituições que os utilizam. "São mudanças essenciais para fazer frente às ameaças crescentes em número e gravidade", defende o senador Ferraço.

O consultor do Senado Joanisval Gonçalves considera que, entre as consequências da falta de cultura de inteligência no Brasil, está o despreparo dos brasileiros, tanto no setor público quanto no privado, para fazer frente a ameaças reais como a espionagem e a atuação de organizações criminosas. "A vulnerabilidade do Brasil diante desse tipo de ameaça é enorme", alertou Gonçalves.

Levantamento junto a 337 instituições federais, feito pelo Tribunal de Contas da União (TCU) em 2012, mostrou que houve melhora no tratamento da segurança da informação em relação a 2010. Mesmo assim, alguns índices continuam muito baixos. Os percentuais relacionados à designação de equipe para gerenciamento da segurança da informação e à formalização de política de segurança da informação tiveram crescimento razoável, 11% e 12%, respectivamente.

O número de instituições que possuem processo de classificação das informações aumentou 6%. Mas o TCU considerou esse crescimento pequeno, tendo em vista a Lei de Acesso à Informação, promulgada em 2011. "A ausência de classificação pode implicar tratamento inadequado da informação, como a divulgação ostensiva de dados não públicos", avalia o tribunal.

Por outro lado, alguns itens de segurança sofreram retrocesso: inventário de ativos de informação, análise de riscos e gestão de incidentes. "Causa preocupação especial o baixo percentual de instituições que realizam análise de risco, o qual caiu de 17% para 10%. Ou seja, 90% das instituições públicas federais ainda não realizam esse tipo de análise", alerta o TCU.

Infraestrutura

Mas o problema não se resume à capacitação de pessoal e gerenciamento. Falta também infraestrutura não só na administração pública, mas no país de modo geral, para ter uma navegação segura na internet.

Pesquisa feita pela Agência Nacional de Telecomunicações (Anatel), à qual a CPI teve acesso, mostrou que todos os pontos da rede são vulneráveis, mas os setores mais críticos estão nas duas pontas do processo de navegação: a rede local, onde se encontram os usuários domésticos ou corporativos, e a rede global, na qual se dá o tráfego internacional de informações.

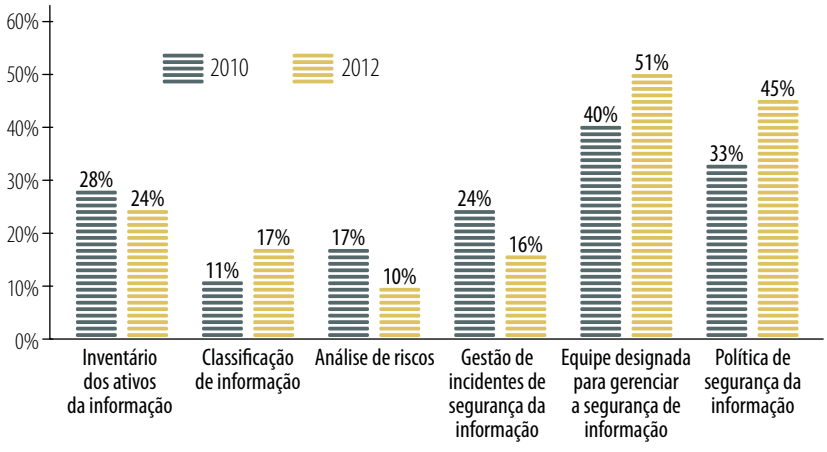
No primeiro caso, o ambiente é inseguro porque os usuários não tomam as precauções necessárias. Já em relação à rede global, a Anatel estima que 70% dos dados gerados por brasileiros circulem fora do Brasil, já que a maior parte dos servidores que fornecem serviços à rede de computadores, como correio eletrônico, está alojada no exterior. É o caso, por exemplo, dos gigantes Google, Facebook e Yahoo, que estão sediados nos Estados Unidos e obedecem às leis desse país. A pesquisa ressalta que uma interceptação das comunicações para fins de espionagem, além de extremamente fácil, pode ser absolutamente legal.

As redes de acesso à internet, por sua vez, pertencem, em geral, a grandes empresas como Oi, NET e GVT. De acordo com a CPI, são mais de 4 mil provedoras de acesso no país, com os mais diversos portes. É grande a variedade de meios de transmissão, métodos de acesso e de tecnologias empregados. Apesar de contarem com administração mais profissional, são vulneráveis também. No Brasil, o setor público utiliza extensivamente as redes das operadoras privadas, o que dificulta a adoção de medidas de segurança.

É o caso, por exemplo, do Serviço Federal de Processamento de Dados (Serpro), vinculado ao Ministério da Fazenda e considerado uma das maiores organizações públicas de tecnologia da informação do mundo. Entre os trabalhos do Serpro, destacam-se o gerencia-

Ambiente público inseguro

Pesquisa feita pelo TCU com 337 instituições federais mostra que, em dois anos, país avançou pouco — e até regrediu — no quesito segurança da informação



Fonte: TCU, 2012

GUERRIC

Projeto de implantação de cabo submarino brasileiro ainda depende da adesão de investidores nacionais

mento de informações do Orçamento da União, a declaração do Imposto de Renda via internet (ReceitaNet) e os sistemas que controlam e facilitam o comércio exterior brasileiro (Siscomex).

Cabos e satélites

De acordo com o presidente da instituição, Marcos Vinícius Mazoni, o Serpro utiliza redes fora de seu ambiente. Os grandes *backbones* (principal rede de transporte de dados da internet) são contratados de operadoras privadas, como BrasilTelecom, Telecom Italia, Telefônica, Embratel e Global Crossing, pois a rede pública não tem capacidade de atender, via Telebras, a necessidade do Serpro.

O relatório da CPI aponta, entre os possíveis locais para espionagem, os cabos submarinos e os satélites geoestacionários, de propriedade estrangeira, utilizados pelo Brasil para tráfego das comunicações telefônicas e telemáticas. O presidente da Anatel, João Batista de Rezende, explicou que, para realizar chamadas telefônicas internacionais ou utilizar *roaming*, são necessários acordos entre empresas brasileiras e de outros países.

No momento da interconexão, há troca de informações entre as operadoras, incluindo número de origem, número de destino, duração e horário da chamada. Esses dados saem do país por cabos submarinos ou por satélites geoestacionários. Como as principais empresas da internet são dos Estados Unidos, há concentração de tráfego e das receitas naquele país. "O desequilíbrio do tráfego aumenta a vulnerabilidade das comunicações de brasileiros", acredita Rezende.

Para ligações telefônicas e comunicações telemáticas, o Brasil utiliza cabos submarinos das empresas Brasil Telecom Cabos Submarinos, AT&T Global Network Services Brasil e Latin America Nautilus Brasil.

Além dos cabos, oito satélites geoestacionários de comunicação possuem autorização para operar no Brasil: seis deles são explorados pela empresa Star One, pertencente à Embratel; um pela Telesat Brasil; e outro pela Hispamar. Os satélites são usados para serviços como TV por assinatura, TV aberta, telefonia, rastreamento e internet em banda larga, além de atividades militares.

REPRODUÇÃO

Brasil usa oito satélites geoestacionários estrangeiros, situação classificada como "incômoda" pelo ministro da Defesa

O ministro da Defesa, Celso Amorim, já se referiu a essa situação como um "incômodo absoluto". "Todas as comunicações brasileiras, inclusive as de defesa, são feitas por satélite alugado, o satélite não é nosso", revelou.

Por causa disso, a CPI recomendou o investimento em satélites e cabos submarinos de comunicação próprios, conforme já determina a Estratégia Nacional de Defesa. Em janeiro, a Telebras anunciou que vai investir na construção de um cabo submarino ligando o Brasil à Europa, por questões comerciais e estratégicas. O projeto já conta com a parceria da espanhola Isla-Link Submarine Cables. A Telebras ainda negocia investidores brasileiros para formação de um conglomerado de empresas com capital majoritário nacional.

Em novembro passado, a Telebras e a Visiona Tecnologia Espacial formalizaram contrato para executar o projeto do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC). O contrato, no valor de R$ 1,3 bilhão, prevê a entrega do sistema no final de 2016.

Entre outras sugestões, a CPI também propõe que o Brasil desenvolva mecanismos de proteção do conhecimento e de segurança cibernética. "Investimentos em inteligência e, sobretudo, em contrainteligência, com ênfase no desenvolvimento de tecnologias próprias e nacionais e de quadros capacitados para o tema. A valorização dos profissionais de inteligência e a percepção de que esses atuam em prol do Estado e da sociedade é aspecto fundamental para o fomento da atividade de inteligência no Brasil", diz o relatório.

PORTAL EBC

Relatório da CPI diz que, sem recursos, Brasil seguirá vulnerável a todo tipo de espionagem física ou virtual

CPI considera "pífio" orçamento para o setor

No campo de inteligência e de defesa cibernética, os investimentos ainda têm sido mínimos. Como revela o relatório da CPI, a Lei Orçamentária Anual (LOA) de 2013 alocou R$ 520,4 milhões para a Agência Brasileira de Inteligência (Abin), dos quais quase 90% eram para pagar pessoal e encargos sociais. Só restaram R$ 55,9 milhões para investimentos em "ações de inteligência".

Ainda que seja difícil estabelecer parâmetros para comparar orçamentos de países com necessidades de segurança bastante diferentes, os recursos destinados à comunidade de inteligência dos Estados Unidos para o ano fiscal de 2013 foram de US$ 52,6 bilhões, segundo divulgado por Edward Snowden. O diretor-geral da Abin, Wilson Roberto Trezza, revelou, em reunião da Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional (CCAI), que o orçamento para a área de inteligência no Brasil é menor que o da Argentina e do México.

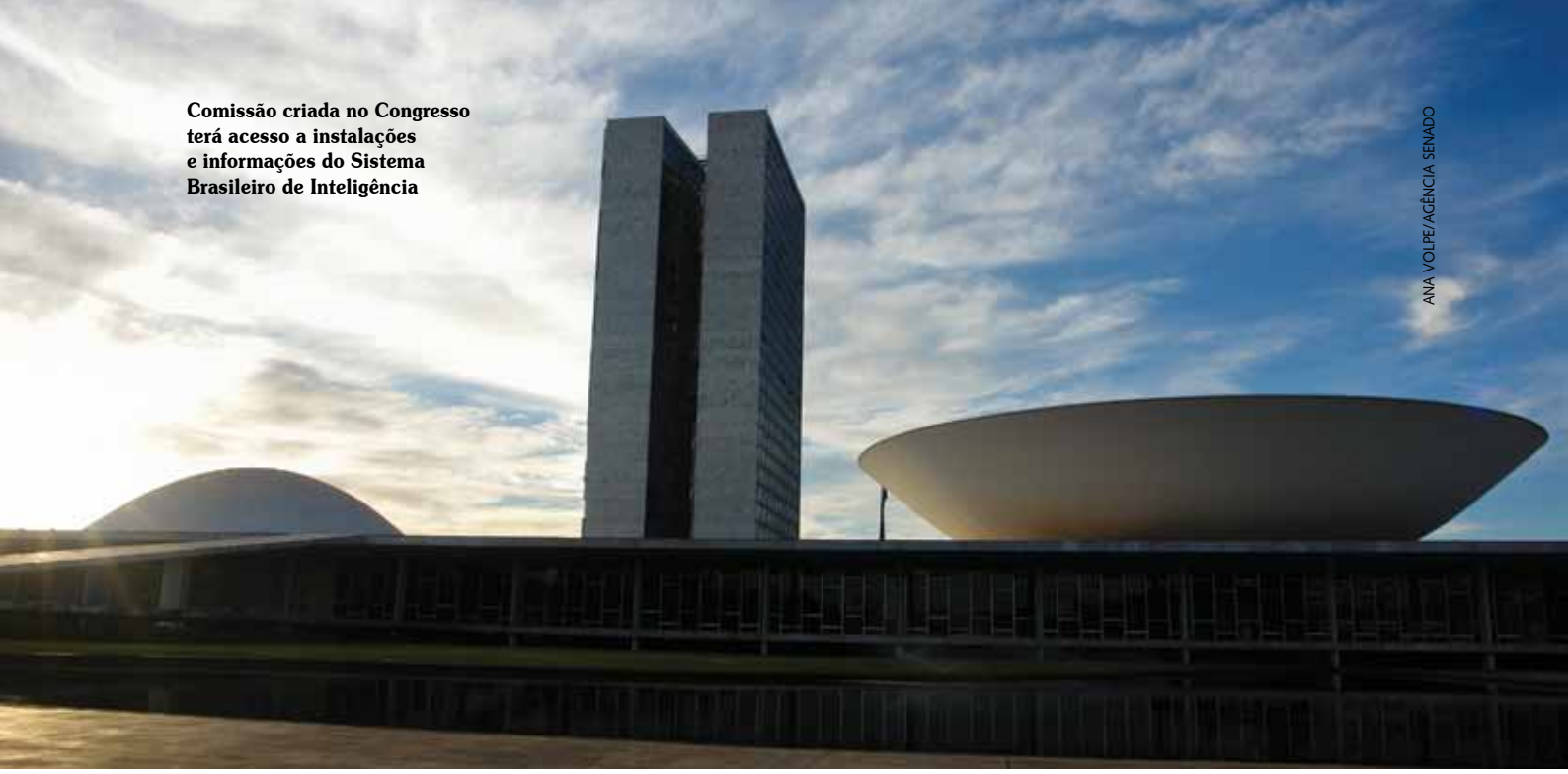
JOSÉ CRUZ/AGÊNCIA SENADO

Wilson Trezza, da Abin, disse que orçamento para inteligência no Brasil é menor que os de argentinos ou mexicanos

O chefe do Centro de Defesa Cibernética do Exército brasileiro (CDCiber), general José Carlos dos Santos, confirmou as dificuldades orçamentárias do setor. "Para fazermos progredir alguns programas que acelerem a implantação da defesa cibernética no âmbito do ministério, nós teríamos que dobrar o orçamento inicialmente previsto. Os recursos para implantação do setor cibernético no Exército foram de R$ 400 milhões. Em 2012, dos R$ 81,5 milhões iniciais, foram alocados R$ 61 milhões. Em 2013, estavam previstos R$ 110 milhões, que acabaram reduzidos para R$ 90 milhões."

Os parlamentares da CPI pediram mais recursos para a comunidade de inteligência. "Enquanto permanecer pífia a alocação orçamentária para a Abin e outras organizações responsáveis pela atividade de inteligência, só se pode esperar que o Brasil permaneça vulnerável a toda forma de espionagem, tanto no meio físico quanto no ambiente virtual. Daí a necessidade de maior dotação orçamentária para o setor de inteligência", recomenda o relatório.

Na opinião do general Santos, apesar do orçamento restrito, já é possível pensar em um modelo para a área de segurança cibernética a ser adotado no país, em termos de ações concretas, a partir da experiência conquistada especialmente com a organização de grandes eventos. "A sistemática de trabalho do Ministério da Defesa está baseada no tripé governo, instituições acadêmicas e indústria nacional e tem sido bem-sucedida", afirmou. Entre as ações realizadas, estão o desenvolvimento de softwares nacionais e a criação de laboratório no Instituto Militar de Engenharia voltado à inteligência artificial, análise de *malware*, criptografia e computação.



Comissão criada no Congresso terá acesso a instalações e informações do Sistema Brasileiro de Inteligência

ANA VOLPE/AGÊNCIA SENADO

Congresso deve fiscalizar ações do serviço secreto

A Lei 9.883/1999, que criou a Abin, responsabilizou o Poder Legislativo pelo controle e pela fiscalização externos da atividade de inteligência. No ano seguinte, o Congresso Nacional criou a Comissão Mista de Controle das Atividades de Inteligência (CCAI), que conta com a participação dos líderes da Maioria e da Minoria na Câmara dos Deputados e no Senado Federal e dos presidentes das Comissões de Relações Exteriores e Defesa Nacional de ambas as Casas legislativas. Atualmente, a comissão é presidida pelo senador Ricardo Ferraço.

MOREIRA MARIZ/AGÊNCIA SENADO

Consultor Joanisval Gonçalves: Congresso é principal instância de controle externo da administração

Na avaliação da CPI, no entanto, a CCAI passou por problemas de inoperância e seu controle tem sido pouco efetivo. De acordo com Ferraço, a situação começou a ser resolvida com a aprovação do Regimento Interno da CCAI, em novembro passado, que define possibilidades de atuação da comissão.

As novas regras para o funcionamento da CCAI foram aprovadas com o objetivo de fortalecer o órgão e aprimorar as formas de fiscalização e controle da atividade de inteligência e contrainteligência. A comissão terá acesso a informações e instalações dos órgãos do Sistema Brasileiro de Inteligência (Sisbin), independentemente do grau de sigilo. Esse acesso, no entanto, deverá ser acordado previamente com os órgãos, de modo a preservar a segurança de locais e documentos.

A comissão poderá solicitar às Mesas do Senado ou da Câmara que enviem pedido de informações a ministro de Estado ou titular de órgão diretamente subordinado à Presidência. Além disso, também é de competência da CCAI emitir parecer sobre proposições legislativas relativas à atividade de inteligência e contrainteligência e receber e apurar denúncias sobre violações de direitos e garantias fundamentais praticadas por órgãos e entidades públicos em razão de atividades de inteligência e contrainteligência.

O consultor do Senado Joanisval Brito Gonçalves lembra que o Parlamento constitui a principal instância de controle externo da administração pública e dos serviços secretos em particular. Além da atribuição de elaborar as leis, a competência fiscalizadora e de controle é da essência do Poder Legislativo, ressalta Joanisval.

O presidente da CCAI defende que uma iniciativa importante para tornar mais efetivo o controle é dar à atividade de inteligência status constitucional. "Não há referência na Carta de 1988 à atividade de inteligência, aos serviços secretos e a seus mecanismos de controle", reclama Ferraço. Já tramita uma proposta de emenda à Constituição com essa intenção (PEC 67/2012), de autoria do senador Fernando Collor (PTB-AL).

INQUÉRITO não identifica **AUTORES**

Em julho de 2013, a Polícia Federal instaurou inquérito para identificar a autoria dos crimes de espionagem praticados contra a presidente Dilma Rousseff e a Petrobras e apurar se houve interceptação ilegal de comunicações em território nacional, conforme as denúncias de Edward Snowden.

Ao longo de um ano de investigações, os policiais federais já ouviram os principais envolvidos do ponto de vista técnico, mas a expectativa é de que dificilmente o inquérito chegue a uma conclusão definitiva.

Em princípio, a hipótese da Polícia Federal é de que as informações obtidas clandestinamente pela NSA foram interceptadas de cabos submarinos e satélites geoestacionários utilizados pelo Brasil para o tráfego de comunicações telefônicas e telemáticas e também de empresas de telecomunicações e de internet que atuam em território nacional.

Em depoimento à polícia, o jornalista Glenn Greenwald, do diário inglês *The Guardian*, que divulgou as denúncias de Snowden, disse que as empresas Google, Facebook, Skype, Microsoft e Apple teriam um acordo com NSA que dá ao governo norte-americano acesso às informações de seus clientes.

Ao prestar esclarecimentos à PF, os representantes dessas empresas deixaram a questão em aberto. Eles alegaram que suas estruturas de armazenamento de dados *(data centers)* ficam nos Estados Unidos e que, em tese, o governo norte-americano pode requisitar informações guardadas por eles referentes a cidadãos de qualquer parte do mundo. O fundamento legal para isso é a Legislação sobre Vigilância de Inteligência Estrangeira (Fisa, na sigla em inglês), combinada com o Patriot Act, decreto editado logo após o ataque das Torres Gêmeas em 11 de setembro de 2001, que permitiu o acesso do serviço de inteligência norte-americano a e-mails e ligações telefônicas de modo irrestrito.

Em relação às ligações telefônicas, a Anatel esclareceu à polícia que as empresas Embratel, Telefônica e TIM têm acordos operacionais com a norte-americana AT&T para complementação de chamadas internacionais. Esses acordos contêm cláusulas de segurança e confidencialidade. No entanto, a Anatel admitiu que é possível haver interceptação clandestina das comunicações telefônicas sem o consentimento das operadoras brasileiras.

Durante os trabalhos da CPI da Espionagem, também ficou evidente a impossibilidade de indiciar possíveis responsáveis pelas ações de espionagem denunciadas por Snowden. A comissão se propôs, então, a ter como principal responsabilidade elencar possíveis vulnerabilidades das redes de comunicações do país e levantar opções para eventual alteração legislativa, modificação de processos e atualização tecnológica necessárias para a construção de um país apto a enfrentar os crescentes desafios do meio cibernético em que vivemos.

CONNIE ZHOU/GOOGLE

Funcionário em sala de controle de *data center* do Google: informações expostas à espionagem americana

Senadores querem inteligência forte

Muito além de indiciar responsáveis pela espionagem internacional, CPI encerrada em abril se preocupou em estruturar sistema que garanta segurança de informações para os usuários e para o governo

MARCOS OLIVEIRA/AGÊNCIA SENADO

A CPI da Espionagem não teve foco no indiciamento de pessoas nem o apelo midiático de outras agitadas comissões de inquérito do Congresso. Os senadores concentraram esforços no diagnóstico e no aperfeiçoamento do serviço de inteligência e segurança da informação de usuários de internet e de instituições públicas do país. "O objetivo nunca foi apontar eventuais culpados", ressaltou o relator, senador Ricardo Ferraço (PMDB-ES), ciente da impossibilidade prática de comprovar delitos e autores.

Em sintonia com a visão do relator, os demais senadores da comissão se empenharam em "propor um reforço do sistema de defesa da comunicação oficial brasileira", como resumiu o senador Roberto Requião (PMDB-PR). Vice-presidente da CPI, o senador Pedro Taques (PDT-MT) explicou que, muito além de "quebrar sigilo bancário, sigilo fiscal", o trabalho do colegiado foi levantar a estratégia de inteligência de outros países, fazendo comparações para elaborar as contribuições do relatório final. Segundo Eduardo Suplicy (PT-SP),

MARCOS OLIVEIRA/AGÊNCIA SENADO

JOSÉ CRUZ/AGÊNCIA SENADO

Requião diz que empenho foi em propor reforço do sistema de defesa da comunicação. Suplicy destacou esforço em aprender com experiências de outros países

Parceria entre Congresso *(E)* e Planalto será necessária para implementar algumas das sugestões feitas pela CPI da Espionagem

isso foi feito levando em conta os depoimentos de todos os especialistas ouvidos pela CPI nas 12 reuniões realizadas.

O relatório final da comissão traz sugestões que só podem ser implantadas pelo Executivo, um projeto de lei e a recomendação de aprovação da Proposta de Emenda Constitucional (PEC) 67/2012. O esforço para aumentar a segurança dos dados privados e de interesse do governo passa ainda por emendas não aprovadas durante a análise do projeto de lei do Marco Civil da Internet (PLC 21/2014) no Senado, que apenas ratificou o texto que veio da Câmara, descartando alterações. Presidente da CPI, Vanessa Grazziotin (PCdoB-AM) anunciou que várias delas serão reapresentadas como projeto de lei, com destaque para as que tratam da privacidade e do armazenamento de dados e registros de conexão.

Fragilidades

A comissão contou, de início, com as contribuições do jornalista Glenn Greenwald, do jornal britânico *The Guardian*. Foi ele quem revelou ao mundo no ano passado as denúncias sobre espionagem, com base em documentos obtidos pelo ex-técnico da Agência de Segurança Nacional (NSA) dos Estados Unidos, Edward Snowden, sua principal fonte de informação.

Greenwald advertiu que os Estados Unidos e seus aliados (Inglaterra, Canadá, Austrália e Nova Zelândia) receberam muito mal as reportagens, acusando os jornalistas investigativos, como ele, de estarem a serviço de nações antidemocráticas. Ele pediu que o Brasil e outros países que vêm sendo alvo de espionagem tenham um programa de proteção aos jornalistas e suas fontes. "Isso dará mais segurança e liberdade para que repórteres possam investigar os fatos relacionados à espionagem americana", explicou.

Diretor do setor de Inteligência da Polícia Federal (PF), José Alberto de Freitas Iegas afirmou que a quebra do sigilo das comunicações brasileiras constatou a necessidade de aprimorar o sistema de comunicação do governo federal e a legislação da área de inteligência. O diretor disse que a maioria das empresas do setor colabora com as investigações da PF, mas algumas, especialmente o Google, impõem obstáculos. A alegação é de que a matriz da empresa está nos Estados Unidos e que seria necessária a obtenção de ordem da Justiça norte-americana para a colaboração.

Outra autoridade entre os mais de dez especialistas ouvidos pela CPI, o general José Carlos dos Santos, chefe do Centro de Defesa Cibernética do Exército, elencou fragilidades do país: dependência tecnológica, carência de especialistas na área de segurança cibernética, orçamento para o setor muito inferior ao de potências mundiais e indefinição de um arcabouço legal.

Melhorar a situação do país frente a esses desafios foi a grande missão da CPI. Nas próximas páginas, veja alguns dos remédios prescritos pela comissão para que o Brasil não continue à mercê da cobiça de outros países por informações nacionais sigilosas e preciosas.


LIA DE PAULA/AGÊNCIA SENADO

Jornalista Glenn Greenwald sugeriu que país garanta proteção a quem denuncia espionagem


PEDRO FRANÇA/AGÊNCIA SENADO

José Iegas, da Polícia Federal: algumas empresas dificultam as investigações

LIA DE PAULA/AGÊNCIA SENADO

Dependência tecnológica é uma das principais fragilidades do país, advertiu o general Santos

SHEYLA LEAL/AGÊNCIA SENADO

Comissão do Congresso vem cobrando do governo a publicação do decreto que regulamentará o setor

Comissão cobra publicação de decreto

Há 15 anos o Brasil espera por uma efetiva Política Nacional de Inteligência (PNI). Prevista na Lei 9.883 de 1999, que criou o Sistema Brasileiro de Inteligência (Sisbin) e a Agência Brasileira de Inteligência (Abin), a PNI poderia melhorar a organização dos serviços, integrar os diversos órgãos e prever investimentos necessários para sustentar o setor.

Somente dez anos depois de aprovada a lei, a PNI foi elaborada pelo governo. A iniciativa das leis e das políticas do setor é prerrogativa do Executivo, que pede sugestões ao Legislativo. Enviado ao Congresso em 2009, o texto voltou ao Planalto no final do ano seguinte, mas até hoje não foi confirmado por decreto presidencial.

O relator da CPI da Espionagem, senador Ricardo Ferraço (PMDB-ES), cobrou da Presidência da República que publique, quanto antes, o decreto que formalizaria a proposta de PNI, segundo ele, "esquecida nos escaninhos do Palácio do Planalto há mais de três anos depois de apreciada pelo Congresso". Para Ferraço, a omissão é injustificável.

Correndo riscos

Ferraço avalia que, sem uma política nacional "corre-se sempre o risco de ver os órgãos de inteligência extrapolando suas funções, cometendo eventuais arbitrariedades e trabalhando em prol de governos e não do Estado e da sociedade".

Na ausência da PNI, é a própria Lei 9.883/1999 que vem regulando a atividade de inteligência no país. Porém, a CPI acha que o texto já não é suficiente para o contexto de espionagem cibernética e para orientar investimentos adequados para o aparelhamento do setor.

Presidente da Comissão de Relações Exteriores (CRE), Ferraço também está à frente da Comissão de Controle das

Atividades de Inteligência (CCAI), do Congresso Nacional, criada em 2000 pela Lei 9.883/1999. A CCAI vem cobrando da Casa Civil da Presidência que a política se transforme em decreto.

Para a CPI da Espionagem, a atividade de inteligência precisa ainda ter status constitucional no país. Para isso, o relatório final pede a aprovação da Proposta de Emenda Constitucional (PEC) 67/2012. A proposta insere um novo capítulo na parte que trata da defesa do Estado e das instituições democráticas, organizando-o em atividade de inteligência, Sistema Brasileiro de Inteligência e controle da atividade de inteligência.

A PEC também visa criar o Conselho Nacional de Controle da Atividade de Inteligência, órgão auxiliar do Congresso, composto por especialistas da área.

"Passo importante"

A PEC, iniciativa do senador Fernando Collor (PTB-AL), foi apresentada 2012 e tem como relator na Comissão de Constituição, Justiça e Cidadania (CCJ) o senador Walter Pinheiro (PT-BA).

Para Collor, a proposição é um passo importante para o aprimoramento da legislação de inteligência no país.

"Embora tremendamente abrangente, dispondo sobre os mais diferentes assuntos, a Constituição brasileira não faz referência alguma à atividade de inteligência. Como tema tão importante passou ao largo do texto constitucional por mais de duas décadas?", questiona Collor, que era presidente da CRE quando apresentou a proposta.

Para ele, serviços secretos têm ainda mais importância em um país que pretende ocupar posição de destaque no cenário internacional.

Para Ferraço, a PEC também deve prever que a CCAI seja mencionada na Constituição, para que seja consolidada como mecanismo de controle externo da atividade no Brasil.

O senador considera que a comissão deve promover as reformas na legislação de inteligência e fomentar a atividade dentro dos preceitos democráticos e o controle constante.

LIA DE PAULA/AGÊNCIA SENADO

SHEYLA LEAL/AGÊNCIA SENADO

Walter Pinheiro *(E)* é relator na CCJ da proposta de emenda à Constituição apresentada pelo senador Fernando Collor

Dados de brasileiros, só com autorização da Justiça

Numa tentativa de reforçar a segurança nas comunicações do país, seguindo as normas de tratados internacionais e a Constituição, a CPI da Espionagem propôs uma lei para tratar do fornecimento de dados de cidadãos e empresas brasileiros a organismos estrangeiros. A proposta (PLS 131/2014) determina que o Judiciário controle as requisições de dados por autoridades governamentais e tribunais estrangeiros. Para ter acesso a essas informações, será preciso um requerimento bem fundamentado, com indícios de ato ilícito, justificando a necessidade dos dados para investigação.

O projeto da comissão ainda prevê que todos os pedidos de governos e de tribunais estrangeiros — e o fornecimento dos dados — sejam publicados semestralmente pelo Judiciário.

O direito à inviolabilidade e ao sigilo das pessoas naturais e jurídicas, nesse caso, compete com a necessidade de garantir o fluxo de informações para investigar crimes, onde quer que eles ocorram.

CPI propõe criação de agência cibernética

Diante da tendência seguida por diversos países que decidiram estabelecer estruturas fortes no campo cibernético, a criação da Agência Brasileira de Inteligência de Sinais é uma das recomendações mais importantes no relatório final da CPI da Espionagem.

Os senadores afirmam que o órgão deverá operar no ambiente virtual na busca de dados de interesse do Brasil e na proteção dos ativos nacionais nessa área. No entanto, a proposta de criação desse órgão deve ser uma iniciativa do Poder Executivo, e não do Congresso, segundo determina a Constituição federal.

De acordo com os parlamentares, estabelecer o órgão, que faria parte do Sistema Brasileiro de Inteligência, requer ainda a estruturação de um aparato que permita ao país obter dados e informações de interesse nacional por meio de mecanismos tecnológicos de ponta.

No relatório, são apresentadas agências de inteligência de sinais pelo mundo e um aspecto destacado é o fato de que todas exercem atividades de inteligência — reunião de dados, inclusive protegidos, para produção de conhecimento — e contrainteligência — proteção contra a inteligência de outros países.

Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia já investem na inteligência de sinais há pelo menos três décadas, com cooperação entre eles, na aliança conhecida como Five Eyes. Segundo os especialistas Philipe Moura e Ricardo Tavares, da Tech Polis Consultoria, na Alemanha foi criado, em 2011, o Centro Nacional de Resposta Cibernética, com o principal objetivo de coordenar as várias agências governamentais de inteligência.

Em alguns países, a atividade de inteligência de sinais associa-se à guerra eletrônica, absorvida em estruturas de defesa cibernética, geralmente no setor militar. Em outras nações, existem agências civis próprias para esse tipo de serviço. Uma terceira realidade são órgãos civis e militares de inteligência e defesa cibernética que convivem em uma mesma comunidade e se mesclam em certas missões, sendo organizações geralmente das mais secretas da comunidade de inteligência, o que dificulta a obtenção de mais informações.

Senadores Pedro Taques *(E)*, Vanessa Grazziotin e Ricardo Ferraço em reunião da CPI: exemplos vêm dos países mais desenvolvidos

LIA DE PAULA/AGÊNCIA SENADO

JONAS PEREIRA/AGÊNCIA SENADO

Marco civil, celebrado em Plenário, ainda esbarra na estrutura mundial para ter a eficácia assegurada

MARCO CIVIL, resposta à ESPIONAGEM

Aprovado pelo Senado em 22 de abril, após quase três anos de debate na Câmara dos Deputados, o Marco Civil da Internet (Lei 12.965/2014) foi também fruto de sugestões da sociedade por consulta pública do Ministério da Justiça e, nas palavras da presidente Dilma Rousseff, "é uma resposta do Brasil à espionagem".

MOREIRA MARIZ/AGÊNCIA SENADO

Empenhado na agilidade do Senado para aprovar o marco civil, Renan destaca expectativa da sociedade

Em meio às denúncias do segundo semestre de 2013, Dilma pediu aos parlamentares urgência para a análise da proposta, considerada uma espécie de Constituição para o uso da rede mundial de computadores no país.

O presidente do Senado, Renan Calheiros, empenhou-se para garantir rapidez à análise do projeto do marco civil junto aos presidentes das comissões. "A sociedade brasileira esperava uma solução para isso", afirmou ele na aprovação da proposta.

Analisada simultaneamente por três comissões, a proposta também foi discutida em duas audiências públicas com especialistas e representantes de órgãos públicos, privados e da sociedade civil.

Presidente da Comissão de Constituição, Justiça e Cidadania (CCJ) e também um dos relatores da proposta, Vital do Rêgo (PMDB-PB) avalia que o marco civil está à altura da necessidade de regulamentação jurídica que a era cibernética reivindica.

"A proteção da intimidade foi devidamente contemplada em vários dispositivos, garantindo o sigilo dos dados pessoais dos nossos brasileiros com as flexibilizações já admitidas em outras situações no ordenamento jurídico, como nos casos de investigação criminal", observou.

Para o senador Walter Pinheiro (PT-BA), a nova lei é um conjunto de diretrizes que aponta para o ordenamento do uso da internet. "Aperfeiçoamentos podem ocorrer futuramente", ressaltou.

A sanção do projeto pela presidente Dilma aconteceu um dia após a aprovação no Senado, durante a abertura do Encontro Multissetorial Global sobre o Futuro da Governança da Internet — NETmundial, que reuniu representantes de mais de 80 países em São Paulo, e ganhou

GERALDO MAGELA/AGÊNCIA SENADO

Nova lei está à altura da necessidade de regulamentação jurídica que a era cibernética reivindica, considera Vital

repercussão positiva em várias partes do mundo. O jornal francês *Le Monde*, por exemplo, destacou a nova lei na manchete principal afirmando que o Brasil "lidera a revolta contra a hegemonia americana sobre a internet".

A nova lei determina os direitos e deveres dos usuários e também dos provedores de conexão — empresas de telecomunicação que disponibilizam o meio físico para o usuário — e de serviços, no caso, sites e aplicativos da internet, na grande maioria.

O texto estipula regras e punições sobre guarda de dados que já podem ser aplicadas sem necessidade de regulamentação ou decreto. Aí estão incluídas advertência, com indicação de prazo para adoção de medidas corretivas, e multa de até 10% do faturamento anual da empresa.

Outras sanções são a suspensão temporária e a proibição de exercício das atividades que envolvam coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações.

Mas algumas ambições para garantir a segurança e a privacidade das informações esbarram na infraestrutura da internet, conforme alertou o presidente da Agência Nacional de Telecomunicações (Anatel), João Batista de Rezende, ouvido pela CPI.

Ele ressaltou que a atual topologia da internet faz com que grande parte do tráfego mundial de dados passe pelos Estados Unidos. "Tanto poder facilita os atos de espionagem sobre informações estratégicas, o que se tornou um problema para o Brasil e outros países", avalia Rezende.

Rafael Moreira, secretário-adjunto de Política de Informática do Ministério da Ciência e Tecnologia e conselheiro do Comitê Gestor da Internet (CGI), sugeriu, ao comparecer à CPI, o armazenamento obrigatório de determinados tipos de dados no Brasil.

Segundo Moreira, na Coreia do Sul, por exemplo, dados financeiros devem ser armazenados em *data centers* localizados no país. Já Paulo Pagliusi, presidente da Cloud Security Alliance Brasil (CSA Brasil), defendeu o investimento em satélites e cabos submarinos de comunicação próprios.

Uma das emendas não aprovadas na análise do projeto no Senado tentava impedir esse acesso facilitado: a senadora Vanessa Grazziotin (PCdoB-AM) defendia a utilização exclusiva de estruturas localizadas em território nacional para armazenar, gerenciar e disseminar dados do poder público em todas as esferas.

Em uma reação às denúncias de espionagem, o Executivo determinou rede própria do governo para garantir a proteção das informações da administração pública federal (Decreto 8.135/2013). A intenção da senadora, que deve apresentar projeto de lei, é "blindar" também as informações públicas municipais e estaduais.

Desafios

Na análise do consultor legislativo do Senado Marcus Martins, o marco civil ampliou a proteção ao usuário da internet, mas, para ter pleno alcance, é preciso regulamentar alguns trechos da lei.

Ele cita a forma e os padrões em que as medidas de segurança e de sigilo devem ser informadas pelos provedores de conteúdo (sites e aplicativos) aos usuários. Pendente também, nesse caso de decreto, está o modo como serão apuradas as infrações nas operações de dados entre os provedores de conexão e de conteúdo (ou serviços) e os usuários. A manutenção dos registros de conexão e de acesso a aplicações — por um ano e seis meses, respectivamente — também aguarda regulamentação.

Para ele, um dos desafios é caracterizar a oferta de serviço ao público brasileiro por provedores que não têm representação no país. "Site em português não é o bastante para exigir que empresas que usam a internet se submetam à legislação brasileira", diz.

MARCOS OLIVEIRA/AGÊNCIA SENADO

João Rezende, presidente da Anatel: concentração de tráfego nos EUA é risco à segurança das informações

PEDRO FRANÇA/AGÊNCIA SENADO

Rafael Moreira, do Comitê Gestor da Internet, defende armazenamento obrigatório no país de certos dados

Investir em capacitação tecnológica é essencial

O incentivo à capacitação e à criação de uma cultura de inteligência é uma das recomendações do relatório final da CPI da Espionagem. Ao defender o investimento em contrainteligência, o documento ressalta a necessidade de mais verbas para os serviços secretos, a aquisição e o desenvolvimento de equipamentos e a capacitação de recursos humanos. Os senadores sugerem também que, na promoção da cultura de segurança digital, seja criada uma iniciativa nacional de informação para o público em geral, com cursos de capacitação em diferentes níveis para agentes públicos e privados.

O relatório, com base em estudo do Tribunal de Contas da União (TCU), também recomenda a instituições governamentais e empresas brasileiras que ampliem a oferta de ações de capacitação em planejamento e gestão de contratos de tecnologia da informação.

Convidados que estiveram na CPI também mencionaram a capacitação como questão fundamental para o desenvolvimento do setor de inteligência e segurança da informação. O general José Carlos dos Santos, chefe do Centro de Defesa Cibernética do Exército, disse que a segurança cibernética depende da educação como vetor central que a estruture, responsabilizando-se pela capacitação da mão de obra especializada, que hoje, conforme ressaltou, "está em quantitativo inferior à demanda".

José Alberto de Freitas Iegas, diretor de Inteligência da Polícia Federal, também disse que o país precisa fazer investimentos constantes, capacitação e aprimoramento permanente na área de tecnologia e segurança.

A senadora Vanessa Grazziotin (PCdoB-AM), presidente da CPI, trouxe, de um encontro em São Paulo com empresas que formam a Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (Abimde), recomendações na área de tecnologia que se somam às do relatório final. O desenvolvimento de hardwares nacionais de comunicação, com o estímulo da indústria para atingir nível de maturidade tecnológica de padrão internacional, é uma das propostas da comissão. A ideia é buscar competitividade em qualidade, custo e compatibilidade tecnológica com outras redes de comunicações internacionais.

Os senadores também defendem um investimento na produção e comercialização de softwares brasileiros, em especial antivírus e para troca de mensagens. Eles argumentam que é preciso o fomento da indústria e das universidades para desenvolver softwares nacionais de forma independente dos grandes centros produtores mundiais de tecnologia.

Entre as medidas que a Abimde aponta para viabilizar o desenvolvimento da indústria nacional, estão a atualização da Política de Ciência, Tecnologia e Inovação para a Defesa Nacional e a garantia de recursos mínimos para investimentos e aquisições pelo governo federal.

Centro de Estudos e Sistemas Avançados do Recife: segurança cibernética tem educação como vetor central

LÉO CALDAS/TITULAR FOTOGRÁFIA

GEORG KROEMER

Sede do Serviço Federal de Informações, na Alemanha: foco na prevenção e repressão aos ataques

Segurança cibernética requer estratégia nacional

Realidade em 14 países da União Europeia e outras dez nações, uma estratégia nacional de segurança cibernética foi defendida de forma unânime pelos convidados da CPI da Espionagem. A ação, segundo o relatório final, precisa trazer as principais medidas de segurança cibernética para o Brasil e englobar iniciativas coordenadas entre os setores público e privado. Ainda que o Ministério da Defesa já tenha publicado a Política Cibernética de Defesa, caberá ao governo brasileiro elaborar essa estratégia, pois o documento ministerial restringe ações de domínio cibernético ao setor militar.

Os senadores reivindicam que sejam definidos claramente o âmbito, os objetivos da estratégia e os requisitos para a segurança cibernética. Outra condição é assegurar a participação de entidades reguladoras nacionais e outros organismos públicos para que as preocupações sejam ouvidas e levadas em consideração, além de garantir a participação de representantes da indústria, universidades e cidadãos na elaboração da estratégia. A colaboração com outros países, sobretudo os do Mercosul e da União de Nações Sul-Americanas (Unasul), para assegurar a cooperação transfronteiriça também foi um requisito ressaltado.

A constante evolução do ciberespaço deve fazer a estratégia ser dotada de flexibilidade e mudança, recomenda o relatório. É preciso ainda lembrar que tal evolução não significa apenas ameaças emergentes e novos riscos, mas também oportunidades para melhorar e aumentar o uso das tecnologias da informação e comunicação para o governo, a indústria e os cidadãos.

Subsídios

O retrabalho foi motivo de alerta dos senadores, para que não sejam perdidas todas as iniciativas feitas até agora em busca da melhoria do nível de segurança nacional. Dessa forma, deve ser evitada a duplicação de esforços e estimulada a concentração em novos desafios do setor.

As ações adotadas por outros países em documento da Agência Europeia para a Segurança das Redes e da Informação (Enisa), de 2012, podem ajudar o Brasil a elaborar as próprias diretrizes. Divulgada em 2011, a estratégia nacional francesa se concentra na capacitação de sistemas de informação para resistir a eventos no ciberespaço que poderiam comprometer a disponibilidade, a integridade e a confidencialidade dos dados.

Do mesmo ano é a estratégia da Alemanha, que tem foco na prevenção e repressão de ataques cibernéticos e também na prevenção de falhas de tecnologia da informação. Também de 2011, a abordagem da estratégia do Reino Unido está concentrada em fazer da região a maior economia de inovação, de investimento e de qualidade no domínio das tecnologias da informação e comunicação.

ATRÁS DA CRIPTOGRAFIA

Uma das recomendações em relação à segurança das comunicações que o relatório final da CPI da Espionagem traz são ações no universo das tecnologias que desenvolvam algoritmos nacionais de criptografia. Os senadores cobram do governo políticas específicas para incentivo e investimento nesse objetivo, que garante "confidencialidade, integridade, autenticação e irretratabilidade sobre mensagens trocadas".

PEDRO FRANÇA/AGÊNCIA SENADO

Paulo Pagliusi, especialista em segurança da informação, lembra supremacia americana e defende a criação do e-mail nacional para assegurar privacidade

Nas reuniões da comissão com especialistas no tema, enfatizou-se que os programas de criptografia nacionais precisam ser capazes de atender os requisitos de proteção dos órgãos do governo, das empresas estatais e das maiores empresas privadas brasileiras. "Tais programas devem garantir a interoperabilidade entre os sistemas e evitar o isolamento digital", especifica o documento.

Ouvido pela CPI, Paulo Pagliusi, presidente da Cloud Security Alliance Brasil (CSA Brasil), relatou que, desde a década de 1990, a Marinha brasileira vem desenvolvendo os próprios recursos de criptografia, mas é a Agência de Segurança Nacional (NSA) dos Estados Unidos que, atualmente, está à frente nas pesquisas sobre o assunto.

Os norte-americanos, disse Pagliusi, lidam com supercomputadores pelo menos dez anos mais avançados que as tecnologias hoje conhecidas. "As instalações da NSA em Utah contam com um *data center* avaliado em

Yottabyte

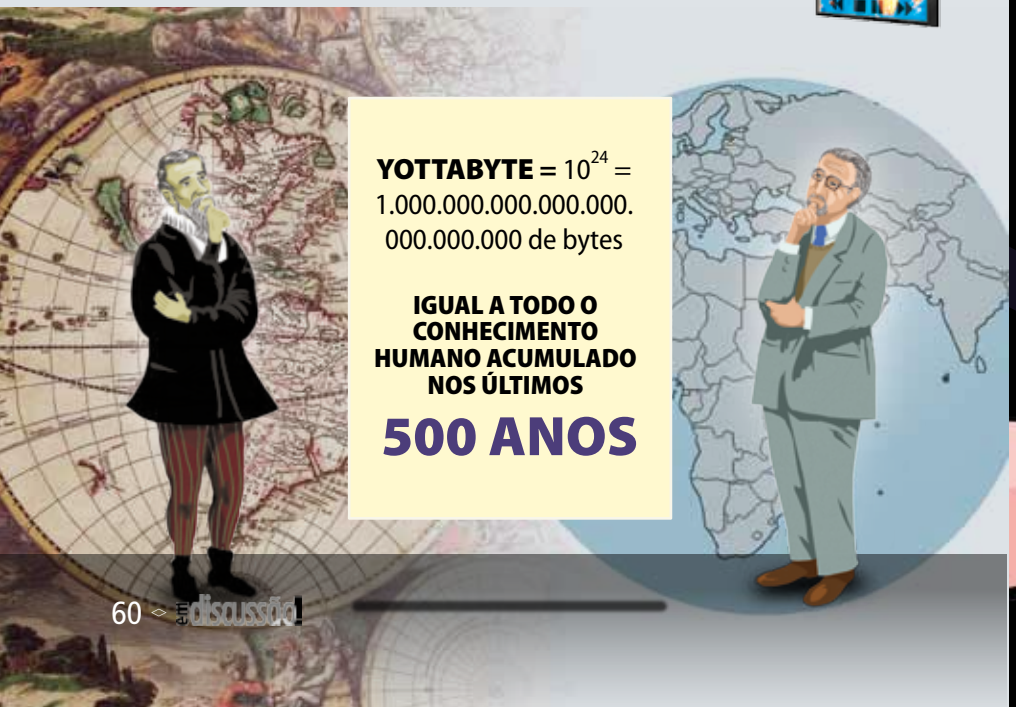
Data center *da NSA em Utah, avaliado em US$ 2 bilhões, teria capacidade gigantesca de armazenar informações*

byte = 8 bits = 1 caractere *A*

kilobyte = 10^3 = 1.000 bytes = **1 página de texto**

megabyte = 10^6 = 1.000.000 de bytes = **1 foto**

gigabite = 10^9 = 1.000.000.000 de bytes = **1 filme**



YOTTABYTE = 10^{24} = 1.000.000.000.000.000.000.000.000 de bytes

IGUAL A TODO O CONHECIMENTO HUMANO ACUMULADO NOS ÚLTIMOS

500 ANOS

Se empilhássemos **1 yottabyte** em cartões de **256 gigabytes** — com aproximadamente **1mm** de espessura cada um —, daria para percorrer a **distância entre a Terra e a Lua**

10 vezes

US$ 2 bilhões, capaz de armazenar um yottabyte, medida que comporta toda a informação produzida pelo ser humano nos últimos 500 anos", explicou.

Entre as ações que Pagliusi considera importantes no combate aos atos de espionagem contra o Brasil, está o desenvolvimento de um sistema de correio eletrônico brasileiro para uso da administração pública e, no futuro, da população. "A ferramenta pode assegurar a privacidade das comunicações e, acima disso, a liberdade de expressão, essencial para a vida em democracia. O Brasil conta com gente capacitada para desenvolver esse projeto", opinou. Ele também sugeriu a criação de um sistema nacional de criptografia de e-mails, já em desenvolvimento pelo Serviço Federal de Processamento de Dados (Serpro).

Segundo o diretor-presidente do Serpro, Marcos Vinícius Ferreira Mazoni, o objetivo é livrar o governo da espionagem estrangeira. Ele explicou que o recurso de criptografia, quando utilizado, destina-se ao chaveamento do caminho das mensagens, mas não do conteúdo delas. "Hoje os algoritmos de criptografia e os equipamentos criptográficos são criados ou controlados por países estrangeiros. Além do mais, é preciso cuidado com a construção de chaves criptográficas fracas, a depender dos algoritmos empregados nelas. A solução para esses problemas passa pelo investimento em projetos de formação e pesquisa em criptografia", argumentou.

PEDRO FRANÇA/AGÊNCIA SENADO

Para o professor Rodrigo Assad, o Brasil precisa proteger e incentivar as 87 empresas nacionais que lidam com segurança da informação e criptografia

Parcerias

Mazoni afirmou ainda que o uso de criptografia deve ser associado ao desenvolvimento nacional de hardware e o uso de software livre para deixar os ambientes virtuais mais protegidos contra ataques cibernéticos. "O Serpro mantém, em parceria com a Universidade de São Paulo (USP) e a Universidade Federal de Santa Catarina (UFSC), um projeto de formação de técnicos na área criptográfica e o hardware é nacional, desenvolvido em conjunto com a Universidade Estadual de Campinas (Unicamp) e produzido por uma empresa no Centro de Tecnologia da Unicamp", informou.

De acordo com Rafael Moreira, secretário-adjunto de Política de Informática do Ministério de Ciência, Tecnologia e Inovação, que esteve na CPI, o Brasil ainda não dispõe de produtos de criptografia prontos, mas um estudo de mercado revelou a existência de 87 empresas nacionais na área de segurança da informação e criptografia. "Com estímulo governamental, essas empresas teriam condições de desenvolver soluções nas áreas de segurança e defesa cibernética", considerou Moreira.

Professor da Universidade Federal de Pernambuco (UFPE) e integrante de um grupo de trabalho colaborativo focado em criar soluções para empresas de tecnologia de informação, o Assert Lab, Rodrigo Elia Assad lembrou que as grandes empresas americanas investem muito na contratação de profissionais qualificados de outros países, "perpetuando seu poder sobre as mais recentes inovações tecnológicas". Na avaliação de Assad, "o Brasil deve buscar estratégias para preservar as 87 empresas nacionais que lidam com segurança da informação e criptografia".

ELZA FIUZA/ABR

Marcos Manzoni, do Serpro, crê que o Brasil precisa investir muito em projetos de formação e pesquisa em criptografia

Congresso já propôs reformulação do Sisbin

Publicado pelo Senado em 2010, o livro *Agenda Legislativa para o Desenvolvimento Nacional*, entre os diversos temas de que trata, sugeriu a reestruturação do Sistema Brasileiro de Inteligência (Sisbin). A ideia era "permitir cooperação e integração mais eficazes entre os membros do Sisbin".

As propostas foram feitas durante a discussão da Política Nacional de Inteligência, enviada pelo governo ao Congresso em 2009. Durante os debates, os parlamentares recomendaram a criação de subsistemas de inteligência voltados para a defesa nacional, a segurança pública, a inteligência econômico-financeira e a inteligência estratégica.

Também foi proposto um mandato claro para os mais de 20 órgãos da comunidade de inteligência da administração pública federal. A *Agenda Legislativa*, organizada pelo consultor legislativo do Senado Fernando Meneguin, diz que "o estabelecimento de subsistemas pressupõe maior especialização entre os órgãos do Sisbin e, para isso, é fundamental que sejam estabelecidos o âmbito de atuação e os limites dos órgãos".

O documento explica que a especialização dos órgãos de inteligência "só seria possível se a ela estivessem associados mecanismos de cooperação e regras claras para integração do conhecimento produzido pelos distintos setores".

Forças-tarefa

A *Agenda Legislativa* também traz como propostas a criação de forças-tarefa, a instituição de salas de crise ou centros de integração nos principais órgãos e o estabelecimento de escola única de formação da comunidade de inteligência ou de estreita cooperação entre as existentes, como a Escola Superior de Inteligência (Esint), a Escola de Inteligência Militar do Exército (EsIMEx) e a Academia Nacional de Polícia (ANP).

Os profissionais de inteligência também receberam atenção nas recomendações legislativas. A publicação diz que eles "necessitam de normas claras que lhes deem respaldo para o exercício regular de suas atribuições, que protejam sua identidade e garantam o sigilo profissional de seus atos". Os parlamentares ressaltaram que os profissionais dos serviços secretos têm poucas garantias para atuar, "sobretudo aqueles de operações, o que os põe em situação tremendamente delicada de exposição".

Foi ainda destacada a necessidade de reforma da legislação sobre salvaguarda de assuntos sigilosos. Segundo a análise trazida pelo documento, a Lei de Acesso à Informação (12.527/2011) não distingue as informações recebidas, produzidas e custodiadas pelos setores de inteligência daquelas de outros órgãos da administração. A recomendação que está na *Agenda Legislativa* é para que "os serviços secretos tenham legislação específica referente às suas previsões e alocações orçamentárias, sendo esse um tema que merece maior discussão no Parlamento".

Academia Nacional de Polícia, em Brasília: estudo do Senado defende criação de instituição única para formar comunidade de inteligência

WILSON DIAS/AGÊNCIA BRASIL

Sala de controle do sistema elétrico brasileiro: agência de segurança cibernética protegeria integridade de setores essenciais

ONS

De olho nas infraestruturas de comunicação

A interrupção de sistemas tecnológicos que prestam serviços ao país, seja por ataques cibernéticos ou panes, pode levar a impactos econômicos, sociais e na segurança devastadores. O alerta é do professor Jorge Henrique Cabral Fernandes, doutor em Ciência da Computação e diretor do Centro de Informática da Universidade de Brasília (UnB).

Entre os setores críticos do país que têm o funcionamento controlado por sistemas informatizados, estão telecomunicações, transportes, energia, mercado financeiro e radiodifusão. Esses setores estão hoje, na grande maioria, nas mãos da iniciativa privada, por meio de concessões públicas.

Diante disso, os senadores da CPI recomendaram a criação de uma agência para segurança cibernética dentro da administração pública federal a fim de centralizar ações que garantam a integridade das infraestruturas críticas. O relatório final cita Estados Unidos, Alemanha, Coreia do Sul e Japão como países que já adotaram comandos unificados para a segurança cibernética.

"Seus modelos devem ser extensamente analisados pelo Estado brasileiro", sugere o relatório. Atualmente é o Gabinete de Segurança Institucional da Presidência da República que coordena a ação estratégica de diversos órgãos públicos envolvendo a segurança das estruturas críticas do país.

Papel fundamental

A dependência de softwares e de redes de computadores operados por empresas privadas merece, segundo o professor da UnB, fiscalização intensa. Para ele, a sociedade precisa conscientizar-se sobre o papel das agências reguladoras na supervisão dos serviços prestados pelas concessionárias, os interesses econômicos e o planejamento de ações.

"As agências têm papel fundamental e o público deve estar atento ao fato de que o Estado é responsável pela segurança da sociedade e deve ser cobrado para que as regras de concessão sejam atualizadas e ofereçam garantias de bom funcionamento. A população deve participar, dessa forma, da defesa nacional, hoje ligada ao setor militar", avalia Fernandes, que coordena o curso de especialização em Gestão da Segurança da Informação e Comunicações.

DIVULGAÇÃO

Dependência de programas e redes operadas por empresas privadas merece fiscalização intensa, alerta o professor Jorge Henrique Fernandes

O professor acrescenta que, quanto mais industrializado e organizado é o país, maior é a preocupação com as infraestruturas críticas. "Os países identificam e mapeiam as estruturas, atentos às vulnerabilidades dos sistemas", explica.

RAIMUNDO VALENTIM/DIÁRIO DO AMAZONAS

Edição 13, novembro de 2012

Inmetro usou padrões internacionais para definir durabilidade, resistência e eficiência das peças de reposição

Exigências para salvar vidas

Portaria do Inmetro obriga motos importadas e nacionais a terem peças que atendam normas básicas de segurança

No Brasil, nenhum tipo de transporte mata mais que a motocicleta. É verdade que, em parte, isso se explica pelo número de motos, que, entre 1998 e 2012, aumentou quase 500%, passando de menos de 3 milhões para quase 20 milhões. Porém, no mesmo período, o número de vítimas fatais subiu mais que 600%, passando de cerca de 2 mil para mais de 15 mil mortos.

Os números podem ser vistos na edição 13 da revista **Em Discussão!**, de novembro de 2012, juntamente com um alerta: muitas das motos importadas, especialmente da China, representam alto risco para quem as pilota.

"É preciso um olhar mais atento para empresas que importam motocicletas. Uma delas pode ter uma pane elétrica, quebra de quadro, de chassi numa rodovia e o motociclista acabar morto, e a população acabar acusando-o de imprudência. Outro problema são as peças de reposição, de péssima qualidade. Há problemas de qualidade do farol, da frenagem da motocicleta", alertou o presidente da Associação Brasileira de Motociclistas (Abram) e membro da Câmara Temática de Educação para o Trânsito e Cidadania do Conselho Nacional de Trânsito (Contran), Lucas Pimentel. Segundo ele, os pneus originais de algumas marcas não são adequados para pista molhada, sem que os compradores sejam avisados.

Diante dessa constatação, o Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro) publicou, em março passado, portaria que estabelece padrões mínimos para as peças de reposição de motocicletas, motonetas, ciclomotores, triciclos e quadriciclos no mercado nacional. Escapamentos, correntes de transmissão, coroas e pinhões, por exemplo, devem seguir normas básicas de segurança para os motociclistas.

A portaria determina que, a partir de março de 2016, fabricantes e importadores não poderão mais vender componentes que não atendam as especificações do Inmetro. E, um ano mais tarde, as lojas só poderão comercializar as peças certificadas pelo órgão. As multas para quem descumprir as determinações variam entre R$ 100 mil e R$ 1,5 milhão.

O Inmetro se baseou em padrões internacionais e em regras da Associação Brasileira de Normas Técnicas (ABNT) para especificar a durabilidade, a resistência e a eficiência necessárias para as peças.

Atraso no fim dos lixões

Maioria dos estados e dos municípios ainda não atende determinações da Política Nacional de Resíduos Solídos, em vigor há quatro anos. Senado busca solução para problema

MARCOS OLIVEIRA/AGÊNCIA SENADO

Para Cícero Lucena, presidente da subcomissão, os pequenos municípios precisam de maior apoio para dar destino correto ao lixo

Séria ameaça ao equilíbrio ambiental e à saúde pública, os depósitos de lixo a céu aberto eram o destino, até o final da década passada, de metade de todos os resíduos sólidos produzidos no Brasil, segundo estatísticas coletadas pelo IBGE. Poucas cidades dispõem dos chamados aterros sanitários, que oferecem cuidados fundamentais como solo impermeabilizado, coleta de gás, tratamento de chorume (líquido que sai do lixo) e equipamentos para compactar e aterrar os rejeitos (tipo de lixo que demora para se decompor e que não pode ser reciclado).

Com a entrada em vigor da Lei 12.305/2010, que instituiu a Política Nacional de Resíduos Sólidos, em 2010, a tolerância com a existência dos lixões ganhou data para terminar: em agosto próximo vence o prazo de quatro anos dado pela lei para que governos estaduais e as prefeituras elaborem planos de gestão de resíduos sólidos, passo essencial para o fim dos depósitos a céu aberto.

Porém, até março passado, somente 3 das 27 unidades da Federação e menos de 10% dos 5.570 municípios haviam atendido à exigência. A situação chamou a atenção do Senado, que criou naquele mesmo mês a Subcomissão Temporária de Resíduos Sólidos, que funciona na Comissão de Meio Ambiente, Defesa do Consumidor e Fiscalização e Controle (CMA). O objetivo da subcomissão é propor formas de fazer valer o que diz a lei.

Assinado pela senadora Vanessa Grazziotin (PCdoB-AM), o relatório final da subcomissão será votado no mesmo mês em que vence o prazo oficial, mas já há intensa pressão para que prefeitos e governadores ganhem mais tempo. A Confederação Nacional de Municípios (CNM), por exemplo, defende a prorrogação por mais um ano para elaboração dos planos e de mais três anos para a desativação dos lixões.

Outro problema levantado durante as seis audiências públicas, que atraíram 20 especialistas do governo e do setor privado, foi o baixo índice de reciclagem do país. Das cerca de 65 milhões de toneladas de resíduos sólidos produzidas pelas cidades brasileiras a cada ano, apenas 4% são recicladas. Na avaliação dos senadores, também faltou empenho para cumprir a política criada em lei, que prevê aumento das iniciativas de coleta seletiva e a profissionalização das cooperativas de catadores.

O senador Cícero Lucena (PSDB-PB), presidente da subcomissão, lembrou que apenas os grandes municípios, que respondem pela maioria do lixo produzido, reúnem condições financeiras e técnicas para eliminar os lixões e adotar sistemas adequados de gestão de resíduos sólidos.

GERALDO MAGELA/AGÊNCIA SENADO

Saiba mais

Apresentações na CPI

- Magda Chambriard, diretora-geral da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP). http://bit.ly/1phq2gw
- Graça Foster, presidente da Petrobras. http://bit.ly/1xFATDl
- Pedro Rezende, professor da Universidade de Brasília. http://bit.ly/UrUJmC
- General José Carlos dos Santos, chefe do Centro de Defesa Cibernética do Exército. http://bit.ly/1pD4VTK
- João Batista de Rezende, presidente da Agência Nacional de Telecomunicações (Anatel). http://bit.ly/SLGffY
- Paulo Sergio Pagliusi, presidente da Cloud Security Alliance Brasil (CSA Brasil). http://bit.ly/1hGajp1
- Rodrigo Elia Assad, professor da Universidade Federal de Pernambuco (UFPE). http://bit.ly/1kjFIbt
- Rafael Moreira, secretário-adjunto de Política de Informática do Ministério de Ciência, Tecnologia e Inovação. http://bit.ly/1jj1D2W
- Ivan Campagnolli, diretor de Redes e Engenharia da Claro S.A. http://bit.ly/1kYQMR6
- Nelson de Sá, diretor de Segurança da Informação da TIM. http://bit.ly/1kjFJMA
- Ari Sergio Perri Falarini, diretor de Operações da Telefônica Vivo. http://bit.ly/1kNlpIh
- Marcos Augusto Mesquita Coelho, diretor de Relações Institucionais da Oi. http://bit.ly/1s3RxMR

Publicações nacionais

- *80 anos da Atividade de Inteligência no Brasil*, Abin (2007). http://bit.ly/1phmMlz
- *Agenda Legislativa para o Desenvolvimento Nacional*, Senado Federal (2011). http://bit.ly/SLErDD
- *A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual*, de Samuel César da Cruz Júnior, Ipea (2013). http://bit.ly/SLEwHG
- *Aspectos Principais da Lei Nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica*, de Carlos Eduardo Elias de Oliveira, Senado Federal (2014). http://bit.ly/1q1D2qM
- *Desafios Estratégicos para Segurança e Defesa Cibernética*, SAE (2011). http://bit.ly/SLEy2g
- *Estados Nacionais, Soberania e Regulação da Internet*, de Hindenburgo Francisco Pires, UFRJ (2012). http://bit.ly/1kPgW7V
- *Levantamento do Perfil da Governança de TI na Administração Pública Federal*, TCU (2012). http://bit.ly/1mExBrB
- *Livro Verde: segurança cibernética no Brasil*, Raphael Mandarino Júnior e Claudia Canongia (orgs.), GSI (2010). http://bit.ly/1l5AtRt
- *Segurança Cibernética: o desafio da nova sociedade da informação*, de Claudia Canongia e Raphael Mandarino Junior, em *Parcerias Estratégicas,* vol. 14, nº 29 (2009). http://bit.ly/1u2YhGg

Publicações internacionais

- *Cyber Readiness Index 1.0*, Melissa Hathaway (2013). http://bit.ly/1l5Zpn9
- *Cyber-Security: the vexed question of global rules*, Security & Defence Agenda (2013). http://bit.ly/1kNjHXu
- *Guidelines for the Security of Information Systems and Networks: towards a culture of security*, Organização para a Cooperação e Desenvolvimento Econômico — OCDE (2002). http://bit.ly/1oKxnn0
- *Report on the Telephone Records Program*, Privacy And Civil Liberties Oversight Board — USA (2014). http://bit.ly/1obl0CT
- *Strategy for Operating in Cyberspace*, Departamento de Defesa dos EUA (2011). http://1.usa.gov/1l5ZpUa
- *Tracking GhostNet: investigating a cyber espionage network*, Information Warfare Monitor (2009). http://bit.ly/1s3PGYi
- *The Role of the 2002 Security Guidelines: towards cybersecurity for an open and interconnected economy*, OCDE (2012). http://bit.ly/1l5AvIZ
- *Where cyber-security is heading*, Security & Defence Agenda (2012). http://bit.ly/1q1CVLS

ESPIONAGEM CIBERNÉTICA

Grandes temas nacionais

em discussão

A cada edição, a cobertura completa de um assunto debatido no Senado Federal que afeta a vida de milhões de brasileiros. Leia esta e as demais edições também em www.senado.leg.br/emdiscussao

COPA DO MUNDO

FINANCIAMENTO DA SAÚDE

MOBILIDADE URBANA

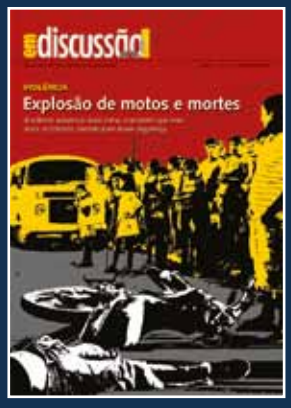
TERRAS-RARAS

DÍVIDA PÚBLICA

ADOÇÃO

EDUCAÇÃO PÚBLICA

TRÂNSITO DE MOTOS



INOVAÇÃO TECNOLÓGICA

RIO+20

DEFESA NACIONAL

NOVO CÓDIGO FLORESTAL

Se eu fosse Senador...

Participe do Concurso de Redação e seja um Jovem Senador

Se você é estudante do ensino médio de escola pública estadual ou do DF, escreva uma redação com o tema: **Se eu fosse Senador...** O vencedor do concurso de cada estado e do DF participará do **Projeto Jovem Senador 2014**, em Brasília.

senado.leg.br/jovemsenador

Jovem Senador | 2014

Jovemsenador

@jovemsenador

Jovem Senador

Alô Senado: 0800-612211

Parceria:

Ministério da Educação

Governo Federal BRASIL País rico é país sem pobreza

Realização:

Senado Federal

Senado Federal | Secom | Criação e Marketing