TEXTO PARA DISCUSSÃO

1850

Brasília, julho de 2013

SUMÁRIO EXECUTIVO

A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL E UMA REVISÃO DAS ESTRATÉGIAS DOS ESTADOS UNIDOS, RÚSSIA E ÍNDIA PARA O ESPAÇO VIRTUAL

Samuel César da Cruz Júnior
Técnico de planejamento e pesquisa da Diretoria de Estudos e Políticas Setoriais, de Inovação, Regulação e Infraestrutura (Diset) do Ipea

A sociedade moderna tem se caracterizado pela dependência da internet e dos sistemas de informação. Com isto, cresceram também as vulnerabilidades de *softwares* e de sistemas computacionais, que atingem todos os níveis e classes do ambiente virtual. Estas vulnerabilidades colocam em risco pessoas, negócios e governos, os quais dependem fortemente da segurança de suas redes.

Os eventos relacionados ao ambiente virtual ocorridos nos últimos anos mostram que os países vivem em uma guerra fria cibernética. Frequentes são as identificações de tentativas de invasões, roubo de informações, quebra de sigilo, exploração de vulnerabilidades de sistemas etc. Preparar-se para agir em situações de risco e ser capaz de se proteger quando a ameaça for identificada é uma questão de Estado e não apenas de priorização de governo.

Os Estados Unidos apresentaram, em 2011, o documento intitulado *Estratégia Internacional para o Espaço Cibernético*, em que buscam expor o posicionamento deles para o mundo nos temas relacionados ao ambiente virtual. O documento é também um convite a todos aqueles que quiserem contribuir para colocar em prática os ideais, princípios e condutas apresentados no texto.

O documento valoriza ideais como a adequada capacitação humana, abertura comercial, respeito à propriedade e privacidade, livre fluxo das informações, promoção dos direitos universais. Contudo, ao defender o direito de autodefesa, o governo deixa claro que reserva-se o direito de defender os ativos nacionais vitais da forma como julgar necessário e apropriado. Alerta que atos hostis oriundos do ciberespaço terão resposta da mesma forma como qualquer outra ameaça identificada, incluindo-se, em última instância, a força militar.

O *site* do Ministério da Defesa russo apresenta um documento que é uma prévia do que virá a ser a estratégia cibernética russa. O posicionamento do governo russo basicamente segue o padrão da estratégia norte-americana. Defende princípios como interação, cooperação internacional, inovação e reconhece a complexidade da tarefa de proteção das redes no espaço cibernético. Busca a solução pacífica e diplomática para eventuais conflitos, mas também se reserva o direito de utilizar os meios que julgar necessários para a autodefesa.

O documento indiano busca ser mais um alerta à população e ao próprio governo para a importância da proteção dos ativos da informação. Destaca a importância na capacitação de pessoas e na constituição de parcerias.

Apesar de segurança e defesa cibernéticas serem conceitos, em muitos aspectos, semelhantes, no Brasil são tratados de forma e por organismos distintos. Aqui, segurança cibernética é vista como o meio de proteção às informações e infraestruturas críticas nacionais, especialmente ligadas à Administração Pública Federal.[1] Suas ações são conduzidas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Já a defesa é voltada à salvaguarda de ativos estratégicos nacionais contra ameaças internacionais que possam vir a comprometer a soberania nacional.[2] Suas ações são conduzidas pelo Centro de Defesa Cibernética (CDCiber), instalado dentro da estrutura do Exército Brasileiro. Todavia, seria muito mais producente se o CDCiber estivesse dentro da estrutura de Estado-Maior Conjunto das Forças Armadas (EMCFA), pois envolve questões afetas às três forças. Com isso, poder-se-ia contar com militares das três forças – e por que não também civis – atuando em conjunto, coordenados e integrados.

Na prática, a defesa cibernética depende da segurança cibernética e vice-versa. Essa segregação faz com que tanto o programa de segurança quanto

1. Mandarino Junior, R. *Segurança e defesa do espaço cibernético brasileiro*. Recife: CUBZAC, 2010.
2. Brasil. *Estratégia nacional de defesa*. Brasília: MD, 18 dez. 2008. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>.

o de defesa percam força, porquanto ambos dependem da afinidade, integração e colaboração nas duas instituições. Além disso, isto favorece a existência de retrabalho, bem como a ausência de atuação por divergências quanto às responsabilidades.

O Brasil se caracteriza pela existência de redes muito vulneráveis e bastante comprometidas. Esta precariedade coloca o Brasil entre os países mais abusados por *hackers* nacionais e internacionais, abrangendo redes públicas e privadas. A administração pública federal, que deveria ser o modelo de segurança para o restante da sociedade, apenas reflete a realidade do restante do país.

Em suma, verificou-se que há muito a ser feito para melhorar a proteção no espaço cibernético em território nacional. O Brasil tem a oportunidade de se juntar a países mais ricos e desenvolvidos para buscar se nivelar a eles, especialmente na capacitação de pessoas. É uma janela de oportunidade que se abre para se equiparar, com baixo investimento, às nações mais ricas e interferir, como *stakeholder*, no processo de construção do futuro da internet.

SUMÁRIO EXECUTIVO