Potências vão dominar ciberguerra, afirma general
Santos Guerra Neto

Fundado em 20 de fevereiro de 2009, o CCOMGEX (Centro de Comunicações e Guerra Eletrônica do Exército Brasileiro) é o orgão que zela pelo Brasil na ciberguerra. Ele é chefiado pelo general Antonino dos Santos Guerra Neto, que falou com a Folha sobre o assunto e sobre o contrato que o Exército fez com a empresa de segurança Panda, que vendeu 37,5 mil licenças à instituição.

Folha - É verdade que algumas redes do Exército já operaram sem antivírus?

Santos Guerra Neto - São centenas as organizações militares do Exército espalhadas pelo Brasil. Eventualmente alguma instalação militar pode ficar temporariamente sem solução de segurança de antivírus, devido ao fluxo do orçamento para as aquisições legais de proteção. Essas instalações ou redes não trabalham com dados que afetem minimamente a segurança do Exército.

Quais os cuidados que o Exército toma com pen drives e laptops pessoais?

Para cada tipo de rede, conforme o nível de segurança necessário, há o remédio adequado. Há redes em que o usuário não tem nenhuma possibilidade de inserir ou retirar dados, apenas um único administrador da rede o faz. Há redes em que a monitoração é por programas de gerenciamento, que registram os acessos e a extração de dados por qualquer mídia.

Que tipo de nação mais se beneficia de uma ciberguerra?

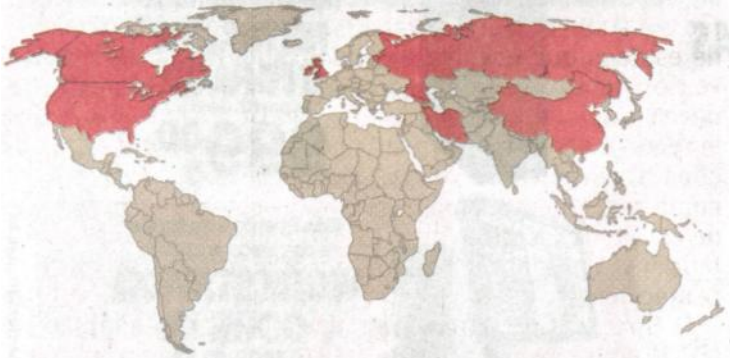
Acredito que, nesse estágio inicial, pequenos países, entidades e até mesmo indivíduos podem causar um bom estrago. Em médio prazo, a preponderância, tanto no poder ofensivo quanto na questão da proteção dos sistemas, deve ser das grandes potências.

Por que o Exército optou por soluções de proteção de uma empresa privada?

Não existe uma solução nacional pronta. O desenvolvimento disso não é uma prerrogativa do Exército. Somos clientes do mercado como qualquer outra entidade. A questão da guerra cibernética está dando uma nova dimensão a essa necessidade e possivelmente levará a soluções inovadoras e de maior independência desses produtos de prateleira.

O MAPA DA GUERRA CIBERNÉTICA

Veja alguns dos países que já atacaram e foram atacados



ATACADOS

1982 > Rússia (então União Soviética). Na Sibéria, canos de gases explodiram após um software infectado ter sido levado para o país

2003 > EUA/Canadá - O guru em segurança Bruce Schneier acredita que uma praga do tipo worm, chamada Blaster, tenha causado um apagão

2007 > Estônia - Sites do parlamento, ministérios, bancos, jornais e empresas de comunicação foram derrubados quase ao mesmo tempo

2008 > Geórgia - Vários sites do governo foram atacados, forçando o país a hospedá-los nos EUA

2008 > EUA - A maior falha da história na rede militar dos EUA foi causada por um pen drive

2010 > Irã - O Stuxnet infectou milhares de máquinas no país, e teria sido criado para sabotar o programa nuclear iraniano

AGRESSORES

1982 > EUA- O software infectado na Sibéria seria obra da CIA, que teria plantado o programa em uma empresa canadense

2007 > Rússia - O ministro das relações exteriores da Estônia acusou a Rússia pela onda de ataques aos sites do país

2008 > Russia - O governo da Geórgia também acusou a Rússia pela onda de ataques

2010 > Israel - Um trio de pesquisadores da Symantec anunciou ter encontrado indícios de que o Stuxnet tem origem israelense

> China e Grã-Bretanha - Embora não existam casos concretos contra os dois, especula-se que eles estejam entre as potências da guerra cibernética. A China, por exemplo, é acusada de roubar informações sobre o F-35, novo avião de guerra a ser usado pelos EUA

Fonte: Folha de S.Paulo, São Paulo, 20 out. 2010, Tec, p. F4.