Preocupado com o surgimento da chamada guerra cibernética, na qual agressores usam computadores para infligir severíssimos danos aos inimigos, o Exército brasileiro faz acordo com empresa de segurança virtual e começa a treinar seus primeiros "ciberdefensores"

Nada de barricadas, minas, explosões ou lançamentos de mísseis. A estrela das batalhas do século 21 será invisível, capaz de desestabilizar inimigos a milhares de quilômetros de distância. E, na trincheira, um exército de homens e mulheres altamente capacitados para invadir sistemas e provocar o caos em países inteiros com apenas um clique. Nos próximos anos, o mundo deve se preparar para a nova arma, a chamada guerra cibernética, ainda sem qualquer controle por leis internacionais.

A guerra, hoje e desde sempre, é vencida por quem consegue fazer com que o inimigo sofra com a escassez: de recursos bélicos e de soldados, obviamente, mas também de estratégias de comunicação, de comida, de infraestrutura e por aí vai. Por exemplo, na Guerra do Golfo, no início dos anos 1990, os iraquianos explodiram poços de petróleo do Kuweit, pois eram a principal fonte de riqueza do país. Para combater o então presidente Saddam Hussein, kuweitianos e nações aliadas gastaram US$ 61 bilhões. Mais de 200 mil pessoas morreram, dos dois lados da disputa.

Agora, imagine como seria se o ataque fosse feito diretamente ao sistema nervoso central de cada nação. O que aconteceria se, em vez de bombas, vírus entrassem em cena? Esses dispositivos poderiam, por exemplo, atacar sistemas de usinas hidrelétricas, de abastecimento de água ou de uma plataforma de petróleo. “A guerra cibernética é a mais limpa e barata que existe. Eu sou civil, mas consigo imaginar qual o custo de lançar um míssil”, afirma Eduardo D’Antona, diretor corporativo e de tecnologia da informação da Panda Security. A empresa assinou, em setembro, um acordo com o Exército brasileiro para treinar militares para a ciberguerra.

Nos próximos dois anos, técnicos da Panda vão capacitar oficiais no uso de tecnologias forenses. “Vamos preparar a nata do Exército para entender ataques virtuais e identificar a autoria”, explica Eduardo. Até agora, 350 militares receberam o treinamento, e a ideia é atingir, pelo menos, 600. A instituição também adquiriu 37,5 mil licenças de antivírus para manter os sistemas a salvo. “O país ou a empresa que não atribuir importância à questão da segurança cibernética sofrerá enormes danos no futuro. Os efeitos serão tão danosos quanto uma invasão territorial”, diz o general Santos Guerra, comandante de Comunicações e Guerra Eletrônica do Exército.

E isso está longe de ser exagero tupiniquim. Nos últimos meses, governos de diversos países anunciaram sua preocupação com as ameaças virtuais. Iain Lobban, diretor do Government Communications Headquarters (o serviço britânico de espionagem), afirmou na semana passada que os sistemas ingleses sofrem mil tentativas mensais de ataque. “Hoje, é muito mais fácil se deparar com um software espião em uma máquina do que ver um satélite fotografando a movimentação de um quartel”, observa Eduardo D’Antona.

O primeiro

O alerta das nações ficou mais intenso depois que o Stuxnet, o vírus mais sofisticado de todos os tempos, se infiltrou em usinas nucleares do Irã. As linhas de código desse programa atacante conseguiriam inclusive mudar o sistema das máquinas invadidas, não simplesmente fazê-las parar de funcionar. O vírus poderia “mandar” o computador invadido fazer virtualmente qualquer coisa e sabotar a instituição à qual pertence. Em setembro, o governo de Mahmud Ahmadinejad reconheceu publicamente que o códigos maliciosos haviam infectado 30 mil computadores do país. “Esse tipo de vírus afeta o sistema que controla as máquinas. Ele poderia, até mesmo, parar uma turbina”, diz André Carraretto, gerente de engenharia de sistemas da Symantec. Ainda não se sabe de onde veio o vírus, mas especialistas em segurança acreditam que ele foi programado por pessoas altamente qualificadas e com um objetivo político.

Essa é, inclusive, a grande preocupação dos analistas dos setor: a dificuldade de saber quem está por trás dos ataques virtuais. “Hoje, tudo que é divulgado sobre o Stuxnet é pura especulação”, afirma Anchises De Paula, analista de inteligência e segurança da empresa iDefense. Muitas notícias associaram a criação do código a uma ação do governo israelense, mas nada foi comprovado, até porque o criador do vírus fez questão de camuflar a origem. “O Stuxnet ataca sistemas fabris presentes em outras indústrias. Eu poderia muito bem supor que isso foi uma ideia louca de um hacker argentino tentando derrubar a hidrelétrica de Itaipu”, pondera Anchises.

Os especialistas em segurança acreditam que a infecção pelo Stuxnet ocorreu por meio de um pen drive. “Na maioria das grandes indústrias, os sistemas são internos, não é possível acessá-los pela internet”, explica o analista de inteligência da iDefense. Como o pen drive teria chegado nas usinas do Irã também vira especulação — pode haver algum espião infiltrado no local ou até algo mais bobo, como a possibilidade de o dispositivo infectado ter sido um brinde para algum funcionário da empresa.

Máscaras

Outro grande problema de ataques cibernéticos tem a ver com a quantidade de efeitos colaterais que podem ser gerados. No caso do Stuxnet, mais de 50 mil computadores foram infectados. “Quem programou o vírus queria derrubar apenas um sistema, mas acabou provocando danos para uma série de pessoas”, comenta Anchises de Paula. “Qualquer tipo de ação na internet sai do controle muito rápido”, reforça o especialista. Além disso, as diversas formas de camuflar a origem da ameaça complicam as investigações. O mundo tem milhares de computadores zumbis (máquinas usadas pelos hackers para enviar vírus) e elas podem estar em qualquer lugar, no seu trabalho, na sua casa, na casa da sua avó.

A insegurança e o risco iminente de invasões virtuais fizeram com que muitos países desenvolvessem estratégias de emergência para futuros conflitos. Os Estados Unidos, por exemplo, nomearam Keith Alexander, então diretor da Agência de Segurança Nacional, para cuidar exclusivamente de um cibercomando. “Na Inglaterra, o governo liberou mais de 1 bilhão de libras em investimentos nessa área e nos setores de infraestrutura de energia elétrica, água e esgoto”, conta o analista da iDefese.

Essa movimentação indica que, mesmo parecendo mais inofensiva, a ciberguerra é tão cruel quanto o conflito tradicional. “Destruir um computador pode não matar ninguém, mas é muito romantismo acreditar que as coisas serão mais leves por causa disso”, reconhece o diretor corporativo da Panda Security, Eduardo D’Antona. Para Anchises de Paula, a ciberguerra será

apenas mais uma ferramenta da guerra comum. “Na década de 1980, as nações discutiam se haveria guerra no espaço, assim como já ocorria na terra, no mar e no ar. Penso que a internet vai se tornar mais um domínio para os conflitos, assim aconteceu com o espaço”, opina.

Fonte: Correio Braziliense = Carolina Vicentin