

ALEXANDRE MAGALHÃES DE MATTOS  
ADVOGADO, MEMBRO DO IAB-NACIONAL, PÓSGRADUADO EM DIREITO  
INTERNACIONAL E EM DIREITO EMPRESARIAL, ANALISTA DE SISTEMAS, PERITO EM  
CRIMES NA INTERNET, PROFESSOR UNIVERSITÁRIO E DE CURSOS PREPARATÓRIOS.

# **A CIBER GUERRA CHEGOU PARA FICAR**

No dia 8 de agosto de 2008 enquanto o mundo celebrava o início dos jogos olímpicos de Pequim, tropas russas cruzavam as fronteiras da Geórgia para desferir um ataque em grande escala nas províncias separatistas da Abkázia e da Ossétia do Sul.

Por trás dessa guerra convencional acontecia o que se pode chamar de III Ciber Guerra. Longe do que possa parecer um filme de ficção, essa nova modalidade de conflito está se tornando corriqueira e estou usando o numeral romano III pois esta já é a terceira ocorrência.

A primeira guerra aconteceu logo após a primeira semana de abril de 2001 quando o avião de espionagem norte-americano modelo EP-3E colidiu com um caça Mig chinês quando sobrevoava as proximidades da província de Hainan. Após esse incidente diversos hackers chineses se uniram espontaneamente e durante um período de pouco mais de uma semana eles comprometeram cerca de 10 mil sistemas americanos. Essa re-ação não incentivada, nem propagada pelo governo chinês demonstrou que uma motivação política pode causar muitos danos a sistemas específicos de um determinado país.

Após uma primeira onda coordenada de ataques específicos, um determinado tipo de verme foi liberado, batizado de code-red, ele deixou partes importantes da internet norte-americana inoperante ou danificada. Este tipo de verme teve uma propagação muito rápida pois cada computador infectado passava a enviar o verme a demais computadores ainda não infectados e isso deixou a rede saturada. O code-red agia quando o relógio do computador marcava uma determinada data e hora e sua propagação se encerrou no dia 20 de abril de 2001. A partir dessa data o verme passou a ter outra função, espalhar uma ação de impedimento de acesso ao site da Casa Branca. Após alguns dias descobriu-se que o code-red fora criado em uma universidade chinesa e na sua última linha de código estava escrito “invadido por chineses”. A Casa Branca alterou o número do endereço do seu site mas o code-red foi um prenúncio de que uma info-guerra automatizada seria possível num futuro próximo.

A segunda guerra se iniciou quando no final de abril de 2007 o governo da Estônia decidiu retirar de uma praça em Tallin, capital do país, uma estátua de bronze de um soldado soviético, conhecida como monumento ao Exército Vermelho. A retirada da peça levou a duas noites de protestos violentos por parte de integrantes da etnia russa nas ruas de Tallin. Na opinião do governo da Estônia, a estátua era um símbolo da opressão soviética sobre o país, que integrou a ex-União Soviética.

A partir de então e, até meados de maio de 2007, a Estônia sofreu uma onda de ataques DDOS (Distributed Denial Of Service - solicitações em massa para um único site ou servidor, fazendo com que ele não suporte o tráfego e fique indisponível para outros usuários) que tiraram do ar diversos sites oficiais. O site do parlamento, de bancos, da presidência da República, dos ministérios e dos serviços de saúde e tecnologia foram afetados. Na época o ministro das relações exteriores da Estônia, Urmas Paet, acusou o Kremlin de estar por trás dos ataques mas nenhuma evidência até hoje foi capaz de comprovar o envolvimento do governo Russo no caso.

O que chamo de terceira guerra se iniciou logo após a retaliação das forças armadas russas contra a Geórgia. Vírus e vermes criados na Rússia re-direcionaram centenas de milhares de computadores no mundo fazendo com que eles sobrecarregassem os acessos aos sites georgianos, incluindo as páginas da presidência, do parlamento, agências de notícias, bancos numa primeira onda de ataque. Numa segunda onda diversos sites tiveram seus conteúdos alterados, como por exemplo o do parlamento no qual imagens do presidente Mikheil Saakashvili foram trocadas pelas de Adolf Hitler. Numa terceira onda, as invasões feitas através de micros zumbis espalhados pelo

mundo, literalmente derrubaram os servidores localizados na Geórgia, tornando inoperante a internet neste país.

Demonstrando um ataque centralizado e coordenado por profissionais, até o site do jornal russo skandaly.ru foi atacado por expressar solidariedade ao governo georgiano em um de seus editoriais.

Como a natureza e a infra-estrutura atual da internet não permite que uma resposta, ou até mesmo um contra-ataque, possa ser feito de uma forma rápida e segura, devemos ter em mente que podemos ter centenas de milhares de computadores zumbis infectados, conectados a internet e prontos para desferirem um ataque tão preciso e destruidor quanto qualquer bomba ou míssil considerado inteligente.

Também em agosto de 2008, durante a campanha presidencial norte americana, os computadores da campanha de Barack Obama foram atacados por um trojan. A empresa responsável pela segurança desses dados tomou as precauções básicas por considerar esse ataque como sendo um ataque típico de *phishing scan* e instalou anti-vírus e programas firewall. O que os especialistas não perceberam foi que o ataque fazia parte de uma sofisticada ciber-espionagem. No dia seguinte a sede da campanha de Obama foi visitada por agentes do FBI e do Serviço Secreto norte-americano que informaram a Michael Slaby, chefe de tecnologia e a David Plouffe, chefe de campanha de Obama que hackers haviam invadido os sistemas do partido e que haviam furtado documentos e dados sobre a campanha de Obama de uma forma muito rápida e precisa jamais vista. Os representantes das duas agências também informaram que os computadores da campanha e McCain haviam sido invadido dias antes.

Investigações feitas pela inteligência americana revelaram que os tipos de documentos e dados que mais foram visados durante as invasões eram os relativos as políticas externas dos dois candidatos e que as invasões que ocorreram nos computadores de Obama tiveram suas origens na Rússia e as que invadiram os computadores de McCain vieram da China, mais precisamente das agências de segurança e espionagem desses dois países.

Mais recentemente, em março de 2009, de acordo com especialistas canadenses, um computador da OTAN localizado em um quartel na cidade de Mons (Bélgica), foi invadido por uma pessoa não autorizada cujo rastreamento levou esses especialistas até um provedor na China. O que esse invasor obteve nesse computador é sigiloso e a OTAN não divulga essa informação mas, considerando que essa força atua não apenas na Europa mas também no Afeganistão, certamente não foi um simples dado corriqueiro o objetivo do invasor..

Essa ciber guerra pode ocorrer contra computadores que controlam outros computadores ou sistemas mais complexos como de organizações financeiras. Um ataque desse tipo poderia fazer com que as operações bancárias on-line fossem prejudicadas ou até mesmo validar compras não solicitadas com cartões de crédito. Em abril de 2009 ciberespões da China, Rússia e outros países invadiram a rede elétrica dos Estados Unidos e instalaram programas que poderiam ser utilizados para interromper os sistemas de distribuição de energia, segundo reportagem do Wall Street Journal.

Se um sistema desse porte pode ser invadido o que dizer então de sistemas que controlam represas, eclusas de rios, sistemas de navegação de portos e aeroportos e todo e qualquer sistema que esteja conectado a internet. Que belo roteiro hollywoodiano teríamos na vida real.

Por certo que ainda veremos, e muito, no futuro, exércitos nacionais invadindo países estrangeiros mas, ao invés da enorme quantidade de carros de combate, aeronaves, navios, bombas e mísseis, veremos exércitos nacionais e agências de segurança atacando computadores de países inimigos através da internet, destruindo seus sistemas de comunicação, sistemas financeiros e demais serviços e formas de interação com a grande rede.