

By MIGUEL CABEZAS (Netmind)

Nas últimas semanas, as denominadas "ciber guerras" voltaram a ser notícia. [As recentes negociações secretas](#) entre os governos norte-americano e russo, na tentativa de "conter" o crescente número de ataques a sistemas de informação em todo o mundo, **é um claro sintoma da gravidade da situação**.

Chama a atenção o nível tecnológico atingido pela Rússia em termos de software, especialmente software de segurança, o que contrasta com o antigo descaso em termos de tecnologia da informação da era soviética (uma das chaves para entender a sua derrocada na guerra fria). Outra grande potência em termos de tecnologia de segurança e técnicas de invasão é a China.

Assim, muitos dos recentes ataques as agências governamentais americanas, sempre à procura de informação classificada, têm como origem a China e a Rússia. Numa realidade em que praticamente toda a informação está digitalizada, parece que alguns 007 foram substituídos por mercenários digitais como método de espionagem mais efetivo e econômico.

Vende-se em alguns jornais a idéia de uma próxima ciber guerra mundial de hackers. Eu discordo. Não sou especialista em segurança, porém, tenho claro que **o paralelismo ou associação entre guerra e técnicas de invasão de sistemas de informação tem um viés sensacionalista.**

Em primeiro lugar, isto não é nada novo. As invasões a sistemas de informação são crescentes e constantes desde a explosão da Internet nos anos 90 até hoje.

Em segundo lugar, **os serviços secretos das grandes potências sempre contaram com quadros de especialistas de seguridad informática** como parte da sua estrutura. A diferença está em que agora este tipo de especialista também forma parte de organizações privadas, tanto lícitas como ilícitas.

Não se trata, pois, de "ciber guerras". Uma guerra tem início e fim, sempre com enormes perdas em vidas humanas, enquanto que muitas das denominadas ciber guerras são constantes tentativas de invasão e controle de sistemas de informação por parte de corporações, máfias, serviços secretos de governos, partidos políticos e até ONGs, entre outros, com as mais diversas e obscuras finalidades.

Como qualificar de guerra algo que é constante no tempo? O termo *ciber ataque* parece-me mais apropriado de utilizar para definir uma invasão sobre um sistema de TI (tecnologia da informação).

Dependendo do nível de agressividade do ataque, pode-se falar em terrorismo digital. Por exemplo, o ciber ataque a Estônia em 2007, pode ser qualificado como uma ação ciber terrorista aos sistemas de informação do país.

Na minha opinião o termo *ciber guerra* só é aplicável como componente dentro de uma guerra de verdade.

Ou seja, como a confrontação entre os elementos tecnológicos dos sistemas de informação dos beligerantes, tanto nos níveis estratégico (conhecimento), tático (software de segurança, infraestrutura tecnológica de informação) e operacional (técnicas de hackeo). Sem guerra real só temos ciber ataques (de distinto grau e natureza) ou ciber terrorismo. Outra coisa, seria falar na possibilidade de uma nova guerra fria, coisa que não pode ser resumida numa ciber guerra.

Muitas vezes também ouvimos falar de "ataques de hackers". Aqui cabe uma observação importante. A ética hacker não permite um uso abusivo do "poder do conhecimento", menos ainda usar esse poder para silenciar a voz de uma pessoa ou grupo de pessoas na Internet. Uma ação como a dos pretendidos "hackers" russos à Estônia ou, mais recentemente, [os ataques ao Twitter e ao Facebook](#), para silenciar um blogueiro Georgiano, não podem qualificar-se como uma "ação hacker" mas como ciber terrorismo procedente de quadros técnicos que dominam técnicas de invasão de

Ciber Guerras, Ciber Ataques e Ciber Terrorismo

Escrito por Fuente indicada en la materia

Viernes, 08 de Enero de 2010 11:22 - Actualizado Viernes, 08 de Enero de 2010 11:39

sistemas de informação.

Se alguém difunde uma mentira ou libelo na Internet, a solução do hacker não é, nem nunca será, silenciá-lo, mas mostrar o caminho, para todo o mundo, da informação verdadeira e contrastada.

A invasão dos sistemas, para um hacker, é a marca de um vigilante da liberdade de expressão e da livre circulação da informação, principalmente para mostrar o que quer ser encoberto.

`<link rel="canonical"`

`href="http://blogdonetmind.com/seguranca/ciberguerras-ciberataques-e-ciberterrorismo/?lang=pt" />`