

Guerra cibernética: guerra fria ou ameaça iminente?

Os especialistas condenam as iniciativas norte-americanas de criar uma divisão para desenvolver defesas e armas para ataques cibernéticos.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) divulgou um relatório no qual dois especialistas analisam os riscos e ameaças impostos por uma eventual guerra cibernética.

De autoria de dois especialistas ingleses, o relatório se divide entre alertar para ameaças reais e desencorajar a criação de "forças armadas cibernéticas".

Forças armadas cibernéticas

Os especialistas condenam as iniciativas norte-americanas de criar uma divisão para desenvolver defesas e armas para ataques cibernéticos, assim como a proposta de um "desligamento preventivo" da internet no caso de uma ameaça. Ideias como essa seriam exageradas e não teriam efeitos práticos, uma vez que consideram a internet como se ela fosse um equipamento, cujo plugue pudesse ser simplesmente puxado da tomada.

"É improvável que ocorra uma verdadeira guerra cibernética," ressalta o documento, baseando-se nas proteções já existentes da maioria dos sistemas críticos, o que exigiria que as ciberarmas sejam projetadas para cada nova falha descoberta - e perderiam sua eficácia tão logo as defesas fossem levantadas.

Outra razão apontada é que é difícil prever os efeitos de um ciberataque: "de um lado eles podem ser menos potentes do que se espera mas, por outro lado, também podem ocorrer danos mais extensos em decorrência da interconectividade dos sistemas, resultando em danos não desejados para os atacantes e seus aliados."

Guerra cibernética real

Entretanto, os autores admitem que os "armamentos cibernéticos" já estão sendo largamente usados e em uma grande variedade de circunstâncias e é previsível que essas ciberarmas serão largamente usadas no futuro, em conjunto com os armamentos convencionais: "não há uma razão estratégica pela qual qualquer agressor irá se limitar a uma única classe de armamentos."

Embora **vírus**, **worms** e **trojans** sejam catalogados como ciberarmas, a primeira "verdadeira ciberarma" parece ter sido o vírus Stuxnet, que atacou equipamentos de uma usina nuclear do Irã.

Segundo o Jornal New York Times, em reportagem publicada no último dia 15/01, o Stuxnet foi criado em conjunto pelas forças armadas dos Estados Unidos e de Israel e foi testado na usina nuclear israelense de Dimona.

Apesar das tensões, não há uma guerra declarada entre esses países.

Convenção de Genebra digital

É exatamente isso o que preocupa Randall Dipert, da Universidade de Buffalo, nos Estados Unidos, especialista em ética militar.

"Ao contrário da guerra convencional, não há nada remotamente próximo da Convenção de Genebra para uma guerra cibernética. Não existem limites estabelecidos e nenhum protocolo que coloque padrões nas leis internacionais sobre como essas guerras podem e não podem ser travadas," diz Dipert.

Ataques podem surgir de qualquer lugar, a qualquer momento, sejam motivados por governos ou por indivíduos tentando impor suas próprias verdades.

Contudo, segundo o relatório da OCDE, chamar isso de guerra cibernética é um exagero: "A ciberespionagem não está apenas a algumas 'tecladas' atrás de uma ciberguerra."

Peter Sommer, um dos autores do estudo, está por trás do pseudônimo Hugo Cornwall, sob qual ele publicou, em 1985, o polêmico livro Guia do Hacker, uma ideia mais tarde copiada em larga escala no mercado editorial, com vários sucessos de vendagem. Hoje ele é professor da London School of Economics.

O outro autor do relatório é Ian Brown, do Oxford Internet Institute.

Bibliografia:

Reducing Systemic Cybersecurity Risk

Peter Sommer, Ian Brown

OECD/IFP Project on "Future Global Shocks"

January 2011

<http://www.oecd.org/dataoecd/57/44/46889922.pdf>

Redação do Site Inovação Tecnológica - 18/01/2011

QUESTÕES

1. *Explique com suas palavras por que os especialistas condenam as iniciativas norte-americanas de criar uma divisão para desenvolver defesas e armas para ataques cibernéticos.*

2. *Especialistas analisam os riscos e ameaças impostos por uma eventual guerra cibernética. Cite.*

3. *Vírus, worms e trojans são catalogados como ciberarmas? Qual foi a primeira verdadeira ciberarma?*

4. *Pesquise o significado de vírus, worms, trojans, spyware, adware e malware.*

5. *Segundo o Jornal New York Times, por quem foi criado o Stuxnet e onde foi testado?*

6. *"Ao contrário da guerra convencional, não há nada remotamente próximo da Convenção de Genebra para uma guerra cibernética". É exatamente isso o que preocupa Randall Dipert, da Universidade de Buffalo, nos Estados Unidos, especialista em ética militar, por quê?*

7. Ataques podem surgir de qualquer lugar, a qualquer momento, motivados por quem?

8. Escreva quais ferramentas e comandos do programa Flash você utilizou para realizar em aula a atividade *Pergunta e Resposta*. Não se esqueça de escrever cada comando e ação utilizada para cada objeto inserido. Se preferir pode desenhar suas telas e explicá-las.

9. Ao utilizar um botão da biblioteca do flash, quais são as ações inseridas para avançar um quadro? E quais são as ações inseridas para mudar de cena?

10. Faça uma síntese sobre o tema Cyberbullying desenvolvido em aula.