São Paulo, 15 de outubro de 2012

Ciberterrorismo – um novo capítulo da nação do medo?

Por Alexandre Yokote

É uma questão interessante, abordada hoje em reportagem do jornal O Estado de São Paulo "Guerra de Dados".

Ao longo de 100 anos, passando pelos conflitos do nazismo, depois guerra fria e agora religiosa ou cultural, no atual mundo globalizado e tecnológico, o terrorismo ainda é um fator de alto risco percebido pela sociedade, mas agora, evoluído.

Uma pesquisa acadêmica em Foz do Iguaçu mostra que 22% dos entrevistados listam ataque terrorista como um risco com potencial para colapso da Usina de Itaipu. O medo de um atentado como o de 11 de setembro ainda faz parte do dia a dia dos americanos.

Segundo a reportagem, na última semana foi apresentada uma recomendação por uma comissão do Congresso americano, quanto a interrupção da aquisição de produtos de tecnologia da informação e comunicação (TIC) de duas grandes empresas fabricantes chinesas. O contexto era de que os produtos poderiam ser ferramentas de espionagem.

Medo de espionagem e terrorismo ou uma ação de Protecionismo? Seria esse evento uma forma de usar o risco percebido a favor da economia, baseando no medo da população para implantar uma medida protecionista para a economia americana em tempos de crise, sem bater de frente com a OMC?

De qualquer forma, parece que já vimos este filme.

Die Hard 4 ou a série Exterminador do Futuro, mostram uma percepção worst case para o risco cibernético. As informações rodam digitalmente, as pessoas se relacionam cada vez mais virtualmente. Em quase tudo hoje há um microprocessador ou uma dependência direta ou indireta a um microprocessamento ou sistema computacional.

Enquanto hoje nos preocupamos com invasões de povos indígenas e movimentos sociais nas hidrelétricas que poderiam gerar danos manualmente, um chip no sistema de automação da Usina ou mesmo no Controlador Nacional podem ser a fonte de um risco percebido de ciberterrorismo. Não digo que isto seja possível ou não, mas digo que no contexto, da mesma forma dos equipamentos de TIC alvo da comissão, tem gente despertando esse medo na sociedade.

A reportagem destaca dois eventos de ciberataque que realmente geram uma preocupação, primeiro o caso do "ataque de negação e serviço" em sites na Geórgia antes da invasão Russa em 2008, depois tem o caso do vírus sabotador em usina nuclear no Irã.

Sim, é preciso admitir que o mundo para com um ciberterrorismo de grande amplitude. Mesmo as pequenas vilas, afastadas do interior também no longo prazo param com o caos resultante que afetariam principalmente as metrópoles.

A dependência da TIC é grande, mas será que estamos preparados para uma "falha segura" para todos esses riscos, independente do nível de sua probabilidade?

Para os gestores de risco de "instalações de alto risco", como plataformas, refinarias, usinas nucleares, hidrelétricas, e até bancos e bolsas de valores, o ciberterrorismo hoje á uma realidade que deve ser considerada em todas as suas faces: hardware, software, rede e dados & informações.

Telefones: (11) 4620-1080 / (11) 99795-8456
Email: contato@ykrisk.com.br