



Sem milagres para a guerra cibernética

Potência bélica:

Com uma política agressiva, EUA encaixam lista de países com investimentos em cyber defense.

Por Washington Novaes*

Seria prazeroso escrever sobre ipês rosa floridos prenunciando a primavera, que chega em setembro. Ou sobre o comovente trabalho de músicos que criam orquestras de jovens em favelas. Mas que fazer? Jornais estão povoados de notícias sobre ameaças de uma guerra cibernética que pode levar a uma catástrofe nuclear planetária. Sobre robôs que podem, por conta própria, disparar um míssil atômico. Sobre hackers capazes de paralisar sistemas financeiros, de transporte, de saúde, de comunicação, em escala planetária.

Nesta mesma página, o embaixador Rubens Barbosa já escreveu sobre o tema (20/6). O ex-economista-chefe do Fundo Monetário Internacional, Kenneth Rogoff, também tratou da

vulnerabilidade da economia global a ataques cibernéticos, com terríveis consequências (6/7). Nestes tempos em que já estamos confrontados por tantos limites inultrapassáveis - crises de finitude de recursos naturais, da água, de terras, de alimentos, etc. -, que se fará para enfrentar a ameaça de “armagedon cibernético” mencionada pelo professor da universidade canadense de Toronto, Don Tapscott (Folha de S.Paulo, 22/7)?

Lembra o embaixador Rubens Barbosa o pensamento de Von Clausewitz, que já na primeira metade do século 19 escrevia que a guerra é a continuação da política por outros meios - tal como já começa a ocorrer nos dias de hoje, com a cibernética e o uso de instrumentos eletrônicos cada vez mais sofisticados. Estados

Unidos e Israel já os teriam utilizado para interferir no programa iraniano de enriquecimento de urânio, desativando 5 mil centrífugas. China e Estados Unidos trabalham com programas capazes de invadir sistemas sofisticados e desenvolvem comandos cibernéticos, programas de segurança nacional para informações, formatos de impedir a escalada de ataques cibernéticos.

Que pensa fazer o Brasil nesse quadro?

Já o professor Kenneth Rogoff pergunta o que acontecerá com o uso de vírus cibernéticos comandados por anarquistas e terroristas, ou com catástrofes naturais causadas por interferências em programações, ou por satélites assim danificados, paralisando redes elé-

tricas, bancos de dados do sistema financeiro, indústrias de tecnologia. E medita: se governos desenvolvem vírus com esse poder destruidor, que se fará? Confiar na sorte?

O panorama é assombroso. A instituição Royal Pingdom, citada pelo jornal The New York Times (Estado, 12/7), calculou para 2010 um número de 107 trilhões de mensagens eletrônicas circulando pelo mundo, onde no ano passado já havia 3,1 bilhões de contas de e-mail. Que acontecerá no mundo, pergunta Don Tapscott, se a nova geração usuária desse meio tem mais de 50% de seus membros desempregados?

Eugene Kaspersky, ex-funcionário do Ministério de Defesa da antiga URSS, hoje diretor da maior empresa de antivírus do mundo, propõe a criação de uma organização internacional de segurança cibernética para impedir que prossiga a guerra em que já estão envolvidos Estados Unidos, China, Grã-Bretanha, Índia, Alemanha, França, as duas Coreias e mais países, que têm unidades de guerra cibernética, de criação de supervírus, naves de guerra não tripuladas e outras armas. Segundo ele, “estamos sentados num barril de pólvora e serrando o galho que sustenta a internet” (Folha, 29/7). As hostilidades podem implicar perda de informações de Forças Armadas, perda de propriedade intelectual de empresas, etc.

Kennette Benedict, editora do Bulletin of the Atomic Scientists, diz na revista New Scientist (30/6) não ter dúvida de que os Estados Unidos “estavam por trás” do ciberataque ao Irã, com o objetivo de impedir o desenvolvimento de sistema de enriquecimento de urânio. Segundo ela, “estamos numa nova era bélica, de fortes ligações com a corrida secreta para construir bombas atômicas”. O ataque ao Irã baseou-



se no sistema de software Stuxnet, desenvolvido por Estados Unidos e Israel. Ele continha malwares (códigos agressivos) que tinham como alvo sistemas específicos de controle industrial, do tipo que controla centrífugas utilizadas para enriquecer urânio.

Faz lembrar o final da 2.^a Guerra Mundial, quando cientistas alertaram o governo norte-americano sobre as consequências dramáticas que teria atirar bombas nucleares sobre o Japão - inclusive uma corrida nuclear entre Estados Unidos e URSS -, diz Kennette Benedict. Mas outros cientistas e autoridades temiam que a Alemanha pudesse chegar antes ao domínio da tecnologia nuclear. Não vingou, assim, a tese de que a energia nuclear deveria ser posta sob controle internacional, talvez mesmo na ONU, que estava sendo criada.

A situação atual seria semelhante, por falta de controle internacional no campo cibernético. Para a editora, é “irônico que o primeiro uso conhecido da cibernética para a guerra seja exatamente para impedir a proliferação de armas nucleares: uma nova era de destruição em

massa pode começar num esforço para encerrar um capítulo da primeira era de destruição em massa”.

Se a política internacional não consegue avançar nesse terreno da cibernética e da respectiva guerra, que se fará? Acreditar em milagres? Na mesma edição da New Scientist, ao lado do texto de Kennette Benedict - coincidência ou não -, o líder da Associação Racionalista Indiana, Sanal Edamarku, conta haver sido convidado para desvendar um suposto milagre numa igreja em Mumbai, onde água brotava de uma imagem e atraía multidões. Pesquisou até descobrir que se tratava de água das instalações sanitárias, canalizada por um sistema de drenagem que passava sob a base da imagem, mas estava bloqueado. Por capilaridade, diz ele, a água infiltrou-se nas paredes adjacentes à estátua e, por um orifício, corria para os pés da imagem.

É possível que haja milagres. Mas a política internacional terá de se desdobrar na nova guerra, que já está no nosso cotidiano.

*Matéria publicada no jornal O Estado de São Paulo em 10.08.2012.