FOLHA DE S.PAULO

Pior do que Hiroshima

10/11/2015 02h50

O mundo interconectado, como um organismo, é ao mesmo tempo muito resistente e muito sensível a infecções. A mesma rede que promove uma evolução sem precedentes pode ser usada para interferir, sabotar ou destruir estruturas no mundo que teimamos em chamar de "real". Um bom exemplo está na Stuxnet, bomba digital criada por uma ação conjunta dos governos dos EUA e Israel para desmontar o programa atômico iraniano.

O ataque foi o primeiro caso de violação do espaço soberano de uma nação por outra que não estivesse em guerra declarada, o que abre um precedente para ataques futuros contra serviços de infraestrutura pelo mundo, sem que ocorra uma discussão pública a respeito de suas consequências.

Aonde vão os EUA, o resto do mundo tende a seguir. Vários países já declararam desenvolver seus programas bélicos digitais, entre eles China, Rússia, Reino Unido, França, Alemanha, Irã e Coreia do Norte. Outros têm suas operações digitais camufladas, por medo de alguma represália comercial ou diplomática.

Uma das poucas vantagens de uma guerra é que até hoje o seu custo e os horrores causados por ela são tão grandes que normalmente boa parte dos países opta pela diplomacia em vez da batalha. O ataque digital, ao eliminar boa parte desses custos e camuflar eventuais consequências, pode ser muito mais tentador.

A questão tem preocupado a comunidade científica. Kennette Benedict, diretora do Bulletin of the Atomic Scientists, identificou em um editorial diversos paralelos entre os ataques promovidos por EUA e Israel e as primeiras bombas atômicas lançadas sobre Hiroshima e Nagasaki. Entre eles está a falta de cuidado com que a tecnologia foi desenvolvida.

Em ambos os casos, líderes do governo e da comunidade científica correram para desenvolver suas armas "antes que o outro lado o fizesse" e ignoraram eventuais consequências não só com relação aos danos causados como também com relação à corrida armamentista que surgiria.

A arma digital está deixando de lado seus dias de inocência, em que poderia ser desenvolvida por um adolescente em seu quarto e cujos efeitos mais daninhos poderiam ser a interrupção de algum serviço digital, o furto de informações ou algum dano financeiro.

Hoje um ataque digital pode transformar qualquer coisa em arma, rompendo barragens, incendiando torres de transmissão ou queimando usinas. Desde que os atentados de 11 de Setembro de 2001 nos EUA mostraram que um avião comercial pode ser transformado em míssil, não é preciso detalhar a gravidade de tais eventos.

Como agentes químicos ou biológicos, armas digitais podem ser difíceis de identificar, determinar a origem e, principalmente, controlar. Elas não podem ser recolhidas, seus efeitos dificilmente são precisos e poucas têm a capacidade de

autodestruição.

Stuxnet tinha uma instrução que impedia sua propagação depois de três anos de infecção. Isso era uma característica de seu projeto, não um requisito para seu funcionamento. Outras armas podem simplesmente ignorá-la. O que aconteceria se saíssem do controle?

Para piorar, cada arma digital carrega em seu código a estrutura para que novas armas sejam construídas a partir dela. Depois que um dos componentes do programa americano e israelense foi descoberto em 2011, novos ataques explorando a mesma vulnerabilidade apareceram em diversos kits vendidos no mercado negro. Em um ano, essa era a principal porta de entrada usada por criminosos para instalar malware e roubar dados bancários.

O alvo de um ataque digital ou de seu efeito colateral pode ir muito além do projetado. Sistemas logísticos, indústrias, redes de telecomunicações, fornecimento de água, saneamento básico, transações financeiras e parte considerável da Internet podem ser facilmente inutilizados. Sua recuperação, se possível, tende a ser muito lenta. Não há mais áreas isoladas ou protegidas. Todos são igualmente vulneráveis.

A ameaça de um eventual holocausto eletrônico ainda está em seus primeiros dias. Neste estágio, ainda é muito difícil antever o tamanho do dano que poderá ser causado em uma sociedade vítima de suas armas. Se elas não causam os horrores imediatos de Hiroshima e Nagasaki, o caos que podem criar pode ser mais duradouro ou até mais daninho, sobretudo pela dificuldade maior de identificá-lo.

É preciso chamar a atenção para os perigos dos ataques bélicos que utilizem a Internet, e criar uma rede de cooperação internacional que estabeleça instituições para legitimar, controlar e atribuir responsabilidades a determinadas tecnologias e seus usos, prevenindo danos antes que seja tarde demais. Como em todas as outras revoluções digitais, a guerra eletrônica poderá criar uma nova escala de destruição que ofuscará o que foi feito anteriormente.

Chega a ser irônico pensar que o primeiro uso reconhecidamente militar de ataque cibernético tenha sido usado para impedir o avanço no desenvolvimento de armas atômicas, abrindo caminho para uma nova era de destruição em massa sem precedentes.

Endereço da página:

http://www1.folha.uol.com.br/colunas/luliradfahrer/2015/11/1704184-pior-do-que-hiroshima.shtml

---

Copyright Folha de S. Paulo. Todos os direitos reservados. É proibida a reprodução do conteúdo desta página em qualquer meio de comunicaçao, eletrônico ou impresso, sem autorização escrita da Folha de S. Paulo.