Valor ECONÔMICO

16/02/2017 às 05h00

A escalada dos ataques cibernéticos

Por **Virgilio Almeida e Danilo Doneda**

Os conflitos no ciberespaço são de múltiplas naturezas e tendem somente a proliferar. Têm sido usados para atacar infraestruturas críticas, desestabilizar redes de comunicação, paralisar serviços fundamentais, expor segredos de Estado e disseminar desinformação. É difícil detectá-los. É mais difícil ainda determinar quem são os verdadeiros responsáveis pelos ataques cibernéticos.

Há vários atores envolvidos nesses conflitos: desde Estados-nações, grupos terroristas, ativistas, facções políticas até organizações criminosas. E, em um mundo cada vez mais conectado, os conflitos cibernéticos só tendem a aumentar, por demandarem estruturas muito menores e mais baratas, quando comparadas às "máquinas de guerra" de conflitos tradicionais. O custo e os riscos de se espalhar bots, agentes de software e vírus são muitos menores, por exemplo, do que o custo de se atacar "fisicamente" uma instalação como uma estação de geração ou distribuição de energia.

Os conflitos e as diferentes formas de guerras cibernéticas trazem em si vários níveis de incerteza. Não existe uma distinção precisa entre ações ofensivas e defensivas. Não existem ainda normas ou tratados internacionais que limitem as ações de guerras cibernéticas ou suas consequências, como os acordos construídos para guerras convencionais. Ações de retaliação e punição a ataques cibernéticos ainda não são claras, devido principalmente a indefinições ligadas às noções de atribuição e proporcionalidade. É nesse nebuloso cenário que se deflagram os recentes conflitos envolvendo Estados Unidos e Rússia bem como outros países como China, Coreia do Norte, Irã, França e Alemanha.

LEIA **MAIS**

Presidente eleito aceita ataques russos, diz Priebus

Reação de Trump a ataques indica nova abordagem nos EUA

Obama quer revisão de ataques cibernéticos ocorridos nas eleições

É indispensável a coordenação de esforços para a construção de uma política nacional de ciberdefesa que envolva não somente estruturas militares, mas também civis, como entes estatais e

Ataques cibernéticos e guerra de informação estão moldando novas formas de conflitos internacionais, com táticas e recursos tecnológicos que não são ainda devidamente compreendidos por políticos e autoridades de governo. Este cenário veio para ficar e demanda planos e ações consistentes para

Mensagens dos leitores

Temer

O governo Temer, após pouco mais de nove meses, pode ser avaliado à luz de dois holofotes autônomos, mas interdependentes. O primeiro diz respeito à economia. Apesar de alguns deslizes iniciais, pode-se classificar como ganhos reais a implementação de reformas que se faziam urgentes, o encaminhamento de outras e o controle do processo inflacionário. Mas as...

16/02/2017 às 05h00 - Paulo Roberto Gotaç -

Déficit público

O editorial "Governo não tem urgência em deter aumento da dívida" (**Valor**, de 15/02) não menciona o fator principal do aumento da dívida pública nas últimas décadas: a altíssima taxa de juros real acumulada (descontada a inflação), de 666%, imposta pelo BC de 1995 a 2016, contra expansão real acumulada do PIB de apenas 78% no...

16/02/2017 às 05h00 - Luiz Mariano de Campos -

Ver todas| Envie sua mensagem

privados, e que conte com a participação ativa da academia e sociedade civil proteger a sociedade e suas estruturas fundamentais contra ameaças cibernéticas.

A combinação de circunstâncias estratégicas e geopolíticas tem sido o propulsor de ações que vêm sendo caracterizadas como sinais de inevitáveis conflitos de guerra cibernética. Em 2007, a Estônia teve suas instalações de governos e serviços na internet atacados por série de ações destinadas a paralisá-las. "Stuxnet" é o nome de um malware que foi utilizado para sabotar as instalações nucleares do Irã.

Outros incidentes que mostram a face visível dos conflitos cibernéticos incluem o ataque perpetrado pela Coreia do Norte aos sistemas de computadores da Sony e o acesso às bases de dados do departamento de pessoal do governo americano ("Office of Personnel Management - OPM") em 2014.

A França recentemente tornou públicos dados que mostram que suas instalações de defesa sofreram 24 mil tentativas de ataques cibernéticos em 2016. Em 2015 um ataque destruiu parte das instalações da TV estatal francesa, que teve de sair do ar temporariamente. Os recentes ataques aos sistemas de computadores do comitê do partido democrata nos Estados Unidos mostram a extensão e o potencial disruptivo que a guerra de informação pode causar a uma sociedade democrática.

Um dos fatores que facilita a execução desses ataques é a vulnerabilidade de diversos sistemas de tratamento de dados pessoais, tornando-os alvos relativamente fáceis - uma situação que tende a ficar ainda mais crítica na perspectiva da "internet das coisas". A proteção de dados pessoais, além de garantir direitos aos indivíduos sobre seus dados, é um importante fator em um marco de cibersegurança, pois dados pessoais muitas vezes também representam informações estratégicas e fundamentais para um ataque cibernético, além do que a devassa em informações pessoais de atores-chave em qualquer sistema de segurança enfraquece o próprio sistema.

Em uma guerra de informação, onde a estratégia passa por denegrir pessoas e instituições, além de espalhar notícias falsas e gerar pânico, a proteção dos dados pessoais é certamente um fator minimizador dos efeitos desse tipo de guerra.

Neste sentido, o desenvolvimento de um marco regulatório sobre proteção de dados pessoais, com disposições sobre temas como vazamento de dados e direitos dos cidadãos sobre seus próprios dados vem sendo cada vez mais frequentemente mencionado como um dos pilares de uma política integrada de segurança cibernética. Neste ponto, em particular, o Brasil ainda não conta com um marco regulatório desenvolvido a respeito, estando, no momento, sendo consideradas no Congresso Nacional algumas propostas de lei que visam cobrir esta lacuna.

Seja no campo econômico, político ou militar, não é mais possível estabelecer uma clara separação entre o espaço cibernético e o mundo material. Ações realizadas no espaço cibernético refletem, direta ou indiretamente, no mundo físico. Para enfrentar ameaças de ataques cibernéticos, o Brasil deve buscar construir uma estratégia integrada que envolva os diversos atores que possam ser alvos de possíveis ataques.

Opinião

Últimas Lidas Comentadas Compartilhadas

Para crescer mais: infraestrutura
05h00

Há obstáculos para redução mais ousada da taxa de juros
05h00

Ceifando os diferenciais da aposentadoria não contributiva
05h00

A escalada dos ataques cibernéticos
05h00

Ver todas as notícias

Videos

Inteligência artificial será tão essencial quanto energia elétrica
06/01/2017

O grau de conectividade da sociedade brasileira, a natureza diversificada da economia do país e a gama de potenciais perpetradores tornam necessário o desenvolvimento de iniciativas para proteger estruturas que, anteriormente, pouco teriam a temer. Somente como exemplo, em virtude dos episódios de ataques a alvos associados às eleições americanas, o governo dos EUA passou a considerar o seu sistema eleitoral como parte integrante da infraestrutura crítica do país.

É preciso que o governo e a sociedade brasileira avaliem continuamente a resiliência de suas infraestruturas críticas para enfrentar diferentes tipos de ataques cibernéticos. É indispensável a coordenação de esforços para a construção de uma política nacional de ciberdefesa que envolva não somente estruturas militares, mas também civis, como entes estatais e privados, e que conte com a participação ativa da academia e sociedade civil.

Virgilio Almeida, professor Associado ao Berkman Klein Center na Universidade de Harvard, foi secretário de política de informática no Ministério da Ciência, Tecnologia e Inovação (2011-2015).

Danilo Doneda é professor da Escola de Direito da UERJ, doutor em direito civil e especialista em privacidade e proteção de dados.