ComCiência no. 131 Campinas 2011

REPORTAGEM

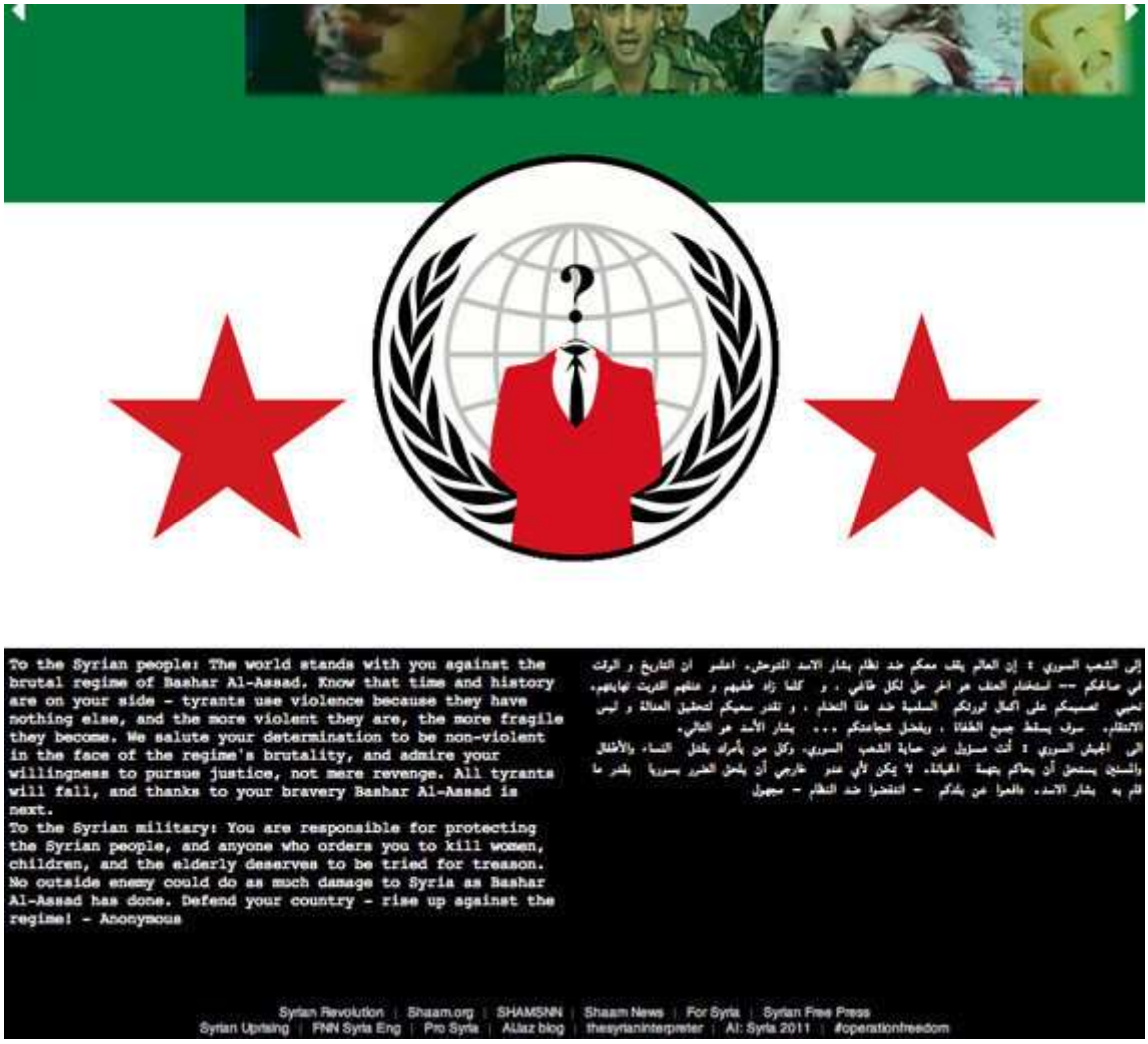
Hackativismo: crime cibernético ou legítima manifestação digital?

Por Jacqueline Lafloufa

Eles foram assunto de muitas matérias no primeiro semestre de 2011, ainda que nem todo mundo compreendesse ao certo quem eram ou por quais motivos estavam agindo. Conhecidos no meio digital pela alcunha genérica de hackers, eles se juntaram em agremiações digitais e apontaram seus canhões virtuais para os alvos que melhor lhes convinham, dando muita dor de cabeça para administradores de redes de grandes empresas e de entidades governamentais. Além disso, muita gente engajada digitalmente e com conhecimentos técnicos resolveu solucionar, com linhas de programação, os problemas que encontrava nas publicações de dados oficiais, como é o caso do grupo Transparência Hacker. Outros ativistas, com um bocado de mobilização via redes sociais, impulsionaram levantes como a Primavera Árabe, entre outros protestos.

No primeiro trimestre, o destaque ficou para o Anonymous, grupo de pessoas não identificadas que funciona de forma anárquica. Surgido no fórum 4chan, esse grupo se "identifica" com o nome genérico usado para postagens anônimas e resolveu se unir para perpetrar ações coordenadas que precisassem de um maior poder de fogo digital – são os conhecidos ataques DDoS, Distributed Denial of Service, que sobrecarregam os servidores devido ao excesso de acessos simultâneos até que eles "caiam" (se desliguem devido ao processamento acima da capacidade), levando a página a sair do ar.

Entre os ataques de maior destaque na mídia coordenados pelos Anonymous estão as "operações" Avenge Assange, cuja proposta era vingar digitalmente Julian Assange, líder do Wikileaks, atacando as instituições que se recusaram a permitir doações para a organização, como a MasterCard e o PayPal; a Payback, que mirou em sites da RIAA e da MPAA, entidades norte-americanas representantes das indústrias de música e cinema, em uma revanche aos ataques que algumas empresas da indústria fonográfica estavam fazendo a sites de *torrents* (onde são compartilhados arquivos digitais), tentando tirá-los do ar; e a Operação Sony, uma das que causou os maiores prejuízos financeiros, que aconteceu em retaliação à perseguição da Sony ao hacker George Hotz, conhecido pela alcunha GeoHot, que conseguiu desbloquear o console de games PlayStation 3 de forma a permitir a instalação de jogos. São eles também os responsáveis por algumas grafitagens digitais, ações que têm como meta invadir um determinado site para modificar sua identidade visual, muitas vezes inserindo mensagens de protesto, como foi o caso da invasão do site do Ministério de Defesa da Síria.



Grafitagem conclama os sírios a se rebelarem contra o governo (Crédito: The Huffington Post / Reprodução)

Já mais próximo do fim do primeiro semestre, outro grupo de hackers conseguiu um bocado de notoriedade na mídia: os Lulz Security, conhecidos pelo apelido LulzSec, são hackers dispostos a perpetrar invasões e ataques DDoS apenas pela diversão ("just for the lulz"). Algumas ações dos LulzSecers incluíram vencer um desafio da empresa Black & Berg Cybersecurity, que ofereceu quantias em dinheiro para quem conseguisse invadi-los – os LulzSecers recusaram o prêmio em dinheiro, afirmando que tinham feito a invasão apenas pela diversão – ; e mobilizar a Titanic Take Down Tuesday, uma terça-feira escolhida pelo grupo para a realização de ataques em massa, que derrubaram sites de jogos, uma companhia de segurança de rede e até mesmo o site da CIA e de outras instituições governamentais dos Estados Unidos. Os LulzSec chegaram a se aliar aos Anonymous para a execução da chamada Operação AntiSec, que visava trazer a público quaisquer tipos de dados confidenciais de governos e grandes empresas do mundo todo, em um protesto que militava pela liberdade de expressão e por uma maior transparência, o que nos Estados Unidos foi taxado de ciberterrorismo. No Brasil, um braço regional dos LulzSec promoveu ataques DDoS a sites do governo, deixando fora do ar os domínios brasil.gov.br e presidencia.gov.br, ambos do governo federal.

Quem acompanhou as notícias sobre os ataques digitais talvez tenha tido a impressão de que está cada vez mais fácil cometer crimes digitais, o que não é exatamente verdade. O setor de segurança de rede tem profissionais cada vez mais qualificados, e muitas empresas adotaram a

estratégia de contratar seus antigos invasores para que estes passassem a cuidar da proteção dos seus dados digitais. Outras companhias também passaram a oferecer boas oportunidades àqueles que se divertem ao tentar quebrar a segurança de sistemas, como é o caso da Google e do Facebook, que premiam com até US$ 500 quem cumprir um protocolo de denúncia de falhas, que consiste em relatar o erro e não divulgá-lo antes que uma solução já tenha sido desenvolvida pela empresa. Além disso, grande parte dos ataques consiste em bombardear o site com acessos simultâneos, de forma a tirá-lo do ar (ataques do tipo DoS), e não roubar dados sensíveis.

De acordo com Nichols Jasper, especialista em segurança da Data Security, grande parte dos chamados hackers atuais na verdade são “peões” da invasão de sites, utilizando programas automatizados para a execução de rotinas já conhecidas. "85% deles são os script kiddies, que não têm conhecimento aprofundado e apenas seguem as coordenadas dos que disponibilizam códigos de invasão; outros 10% têm uma boa noção de segurança e apenas 5% deles, ou até menos, são especialistas no assunto", revela.

Rastreando os hackers

Ainda que as empresas consigam seduzir alguns dos hackers a trabalharem a seu favor, muitos deles ainda ficam de fora, e outros não o fazem por conta de princípios pessoais. Assim, as instituições passam a tomar medidas mais drásticas para preservar seu patrimônio digital, rastreando os supostos hackers e entrando com processos legais contra eles. Esse jogo de gato e rato nunca é tão fácil assim, ainda que o rastreamento não seja algo tecnicamente complexo. Todo usuário de computador ganha um número único quando acessa a internet, o chamado IP (Internet Protocol). Esses números são distribuídos por área e, como em antigos números de telefone fixo, é possível delimitar de onde vieram os acessos baseado em determinados prefixos e, através de uma espécie de lista telefônica de IPs, descobrir qual é a operadora que oferece os serviços de internet ao computador utilizado para os ataques. Ou seja, achar o “computador culpado” não é difícil. O complicado é conseguir a autorização legal para a quebra de sigilo telefônico que revele quem é o responsável pela conta, para então dar entrada em um processo judicial. "Muitas vezes, esse tipo de solicitação de quebra de sigilo pode demorar anos", conta Jasper. E é por isso que existe cada vez mais uma preocupação sobre o anonimato na rede.

No Brasil, o Projeto de Lei 89/2003, conhecido como Lei Azeredo, tem como um de seus principais pilares obrigar os provedores de internet a manterem um arquivo com as informações de acesso de seus usuários por até três anos. Isso visa proteger as empresas que conquistam o direito de quebrar o sigilo telefônico de hackers e acabam esbarrando em questões burocráticas dos provedores, que hoje apagam esses logs de acesso quando querem – por vezes, antes que os trâmites judiciais deem um parecer, seja ele favorável ou não. Nos Estados Unidos, a ação dos hackers que invadem sites oficiais está sendo classificada pelo governo como ciberterrorismo, passível de condenação que pode levar a até dez anos de prisão. Já na China, país conhecido pela falta de liberdade de expressão, um comunicado oficial do governo divulgado no fim de agosto afirma que as pessoas que comprarem, venderem, encobrirem ou obtiverem acesso ou dados de redes de forma ilegal estarão sujeitas a punição criminal, e novas regras de elevada severidade podem vir (veja matéria sobre o assunto).

Cibercrime ou cibermobilização?

O problema do mundo digital, contudo, é que ele não tem fronteiras, enquanto que a legislação é aplicada de acordo com a localidade de realização do suposto crime cibernético. Sabendo disso, hackers de todo o mundo têm aprendido a burlar as leis, hospedando seus sites em países de legislação mais flexível, como a Eslovênia ou a Suíça, e usando artimanhas digitais para que seus acessos via IP apontem para regiões onde a punição judicial a cibercrimes seja mais difícil, com o uso de proxys, sites da web que permitem a navegação de forma supostamente anônima, ao trocar o IP que identifica o computador que realiza determinado acesso.

Atualmente, especialistas discutem se é realmente necessária a criação de uma legislação específica para a criminalização de atividades ilegais através da rede. Em alguns casos, a própria lei vigente já dá conta do recado – alguém que invada um site ou um computador para roubo financeiro pode ser condenado por estelionato, por exemplo. Para Tiago Dória, jornalista e pesquisador de mídia na pós-graduação da Fundação Getúlio Vargas (FGV), uma legislação específica é bastante desnecessária, e o que seria importante mesmo seria que o setor judiciário brasileiro entendesse melhor como funciona a internet. "Às vezes, a falta de uma cultura de internet faz o judiciário não aplicar a lei da forma correta. Um exemplo foi o caso do bloqueio do YouTube por causa do vídeo da (Daniela) Cicarelli, em 2007. Na época, era nítido que o juiz do caso não tinha o pleno conhecimento de detalhes técnicos e culturais, chegando a comparar o YouTube a um canal de TV, que supostamente teria um sinal próprio de transmissão(!)", rememora Dória.

Contudo, outras questões ainda estão abertas à discussão, em especial para a definição do que é cibercrime e o que seria considerado hackativismo – ações políticas feitas através de meios digitais. No caso dos hackers grafiteiros, como os que invadiram o site do ministério sírio, cujo objetivo é modificar o visual das páginas e inserir mensagens de protesto, eles poderiam ser considerados criminosos, ou apenas representam um levante contra o governo? A legislação de diversos países ainda não consegue definir que tipos de manifestações são ilegais ou se isso pode ser considerado uma manifestação popular legítima. "Uma tendência mais comum é os governos pararem de bloquear ou inibir o uso dos meios digitais para utilizá-los a seu favor", opina Dória, referindo-se a governos como o do Egito, que durante o levante dos seus cidadãos, na chamada Primavera Árabe, resolveu suspender o acesso à internet em todo o país. "China e Irã utilizam, cada vez mais, esse tipo de expediente de monitorar a população através da rede e usar o espaço virtual como uma ferramenta de propaganda para fortalecer os seus governos", explica.

Outro tipo de hackativismo menos opressivo é aquele que visa melhorar a usabilidade de dados públicos, como o que é feito pelo grupo brasileiro Transparência Hacker. Unidos, esses especialistas em computação têm trabalhado para transformar em modelos digitais de fácil acesso dados já disponíveis ao público mas de difícil manipulação digital, como estatísticas do governo publicadas em documentos no formato PDF, informações listadas em arquivos de texto e outras do tipo. É o que fazem, por exemplo, no projeto SACSP (Sistema de Estatísticas e Acompanhamento das Reclamações de Munícipes na Cidade de São Paulo), iniciativa que mostra em um mapa do Google as regiões da cidade que possuem uma maior incidência de reclamações, como a falta de poda de árvores, problemas com transporte público, limpeza ou buracos nas ruas. Esses dados já estão disponíveis aos cidadãos interessados, mas quando são apenas listados, não permitem a comparação nem a compreensão de quais áreas do município têm um maior número de solicitações – e, portanto, deveriam ser atendidas de forma prioritária. Esse tipo de atividade é denominado de hackativismo devido à característica do uso de programação para a exibição dos dados em outras plataformas – no caso de mostrar ocorrências em um mapa, é preciso criar todo um sistema web por trás do projeto para torná-lo viável. Iniciativas como essas claramente merecem mais o incentivo do governo do que uma possível criminalização.

Além disso, a conectividade que a internet permite também tem possibilitado outros tipos de manifestação política, através de redes sociais como o Facebook. Foi através dele que muitas mobilizações em todo o mundo foram organizadas, e até mesmo no Brasil, como o Churrascão da Gente Diferenciada, uma divertida passeata que promoveu um "churrascão" nas imediações da Avenida Angélica, em São Paulo, como forma de demonstração de apoio da população à construção de uma estação de metrô no local, o que ia contra a requisição dos moradores do bairro, que queria evitar a circulação de "gente diferenciada" na região. Será mesmo que a saída é suspender a internet, impedir a comunicação via celular e criminalizar quaisquer manifestações políticas de origem digital para evitar quebra-quebra ou o melhor seria reconhecer nessas atividades uma insatisfação da população e tentar solucioná-las dentro do

possível? A questão ainda está em aberto, e está nas mãos dos políticos encontrar uma boa saída.