Estados Unidos, poder cibernético e a "guerra cibernética": Do *Worm Stuxnet* ao *Malware Flame/Skywiper* – e além

United States, cyberpower and "cyber warfare": From *worm stuxnet* to *Malware Flame/Skywiper* – and beyond

Bernardo Wahl G. de Araújo Jorge*

Boletim Meridiano 47 vol. 13, n. 131, mai.-jun. 2012 [p. 43 a 48]

Introdução

O presente artigo tratará de um tema emergente nas relações internacionais: os conflitos cibernéticos – enfocando o poder cibernético e as "guerras cibernéticas". Tal matéria será abordada a partir de um recorte específico: através da política externa dos Estados Unidos, particularmente nos governos de George W. Bush e Barack Obama. A hipótese apresentada é a seguinte: nestas duas administrações, o uso do "poder cibernético" pelos EUA, para atingir objetivos de política externa, possui duas dimensões.

A primeira dimensão é aberta e está no rol das relações públicas e das operações psicológicas, singularizada na figura de Richard Clarke. Ator oriundo do *establishment* de segurança nacional norte-americana, Clarke tem chamado a atenção para a questão da segurança cibernética, especialmente através do seu livro *Cyberwar* (2010), mostrando que os Estados Unidos – o país mais dependente de sistemas computadorizados para o funcionamento da sua sociedade – estão vulneráveis à ataques cibernéticos, e apontando que os Estados Unidos são os menos interessados em uma "guerra cibernética". Mas esta dimensão aparentemente objetiva desviar a atenção do público de uma segunda faceta, bem diferente e reveladora.

Esta outra dimensão é mais reservada e discreta. Trata-se do uso de "guerras cibernéticas", ou de "armas cibernéticas", para alcançar fins de política externa, os quais dificilmente seriam conquistados por outros meios. Trata-se do caso de "atrasar" o programa nuclear iraniano, país visto como ameaça por Washington. Conforme será mostrado neste escrito, retardar os avanços iranianos no campo da energia nuclear através de uma guerra aberta seria uma opção muito arriscada. Assim, alternativamente, é usada uma combinação de vários outros instrumentos: diplomacia, sanções econômicas e operações encobertas.

As operações encobertas envolveriam o assassinato de cientistas nucleares iranianos (embora não seja possível atribuir estes assassinatos com certeza a nenhum país, pois não há provas) e ataques cibernéticos. Até pouco tempo, desconfiava-se que as investidas contra o Irã pelo ciberespaço, particularmente por meio dos vírus de computador *Stuxnet* e *Flame*, eram trabalho dos Estados Unidos e de Israel. Só que a suspeita está caminhando para uma certeza

* Mestre em Relações Internacionais pelo programa San Tiago Dantas da Universidade Estadual Paulista – UNESP, Universidade Estadual de Campinas – UNICAMP e Pontifícia Universidade Católica de São Paulo – PUC-SP. Professor de Relações Internacionais das Faculdades Metropolitanas Unidas de São Paulo – FMU-SP e da Fundação Escola de Sociologia e Política de São Paulo – FESPSP (bernardowahl@gmail.com).

(embora ainda seja cedo para afirmar isso plenamente), pelo menos com as revelações feitas pelo jornalista David E. Sanger no livro *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (2012).

Para iluminar as duas facetas do uso do "poder cibernético" pelos EUA, este artigo está dividido em seis partes: (1) Introdução; (2) Contextualização – sobre como a "guerra cibernética" emergiu para a condição de um instrumento estratégico de política externa dos EUA nos últimos onze anos; (3) Do *Stuxnet* ao *Flame* – seção dedicada a examinar dois importantes vírus de computador, as "armas cibernéticas" da "guerra cibernética" norte-americana; (4) Política Externa Norte-Americana, o Poder Cibernético e a "Guerra Cibernética" – mostra a transição dos governos Bush (filho) a Obama, a metamorfose das ameaças percebidas por Washington e os meios para combatê-las – das guerras abertas às operações encobertas, especificamente os ataques cibernéticos; (5) Considerações Finais e; (6) Referências Bibliográficas. Uma observação: são usadas aspas quando se refere às "guerras cibernéticas" pois se trata de uma definição ainda em processo de elaboração.

Contextualização

O evento determinante para a política externa dos Estados Unidos sob George W. Bush (2001-2009) foram os ataques perpetrados pela al-Qaeda no onze de setembro de 2001, a partir dos quais declarou-se uma "guerra global ao terror", caracterizada por duas guerras abertas – uma no Afeganistão e a outra no Iraque – e por uma série de iniciativas diplomáticas, assim como por um conjunto de operações encobertas de contra-terrorismo pelo mundo afora – quer dizer, uma série de medidas ofensivas para prevenir, dissuadir e responder ao fenômeno do terrorismo.

Um efeito talvez inesperado da "guerra ao terror" foi a ascensão do Irã como potência regional no Golfo Pérsico: seus dois principais inimigos, o Talebã a leste e Saddam Hussein a oeste, foram retirados do poder pelos Estados Unidos, facilitando assim o caminho de Teerã rumo ao seu principal objetivo de política externa: a condição de força motriz na região. Nos últimos anos, de Bush (filho) à Obama, embora isso venha oscilando desde a revolução de 1979, o Irã cresceu na condição de ameaça percebida por Washington. E por que? Basicamente por causa da desconfiança de alguns países ocidentais em relação ao programa nuclear iraniano, o qual não seria apenas para fins pacíficos.

Desde Bush (filho) a questão iraniana vem sendo tratada com muito cuidado. Em 2008, por exemplo, o governo norte-americano não autorizou a venda de bombas anti-bunker ao seu aliado Israel, com as quais possivelmente seria lançado um ataque contra as instalações nucleares subterrâneas de Natanz, no Irã. As estimativas de inteligência dos EUA, apesar de oscilações, tenderam a apontar que o governo iraniano ainda não havia tomado a decisão política de enriquecer urânio a um nível que permitisse a elaboração de armas nucleares.

Na administração de Barack Obama (2009 até o presente), os conflitos com o Irã ficaram mais visíveis, chegando próximos ou até mesmo à condição de uma crise. Atualmente há uma série de sanções econômicas que tentam convencer o governo iraniano a "cooperar". Também haveria uma "guerra de inteligência" entre Washington e Teerã. Embora tal guerra não possa ser comprovada, alguns indícios apontam para ela: o assassinato de cientistas nucleares iranianos e as acusações, por parte dos EUA, de um complô iraniano para assassinar o embaixador da Arábia Saudita em Washington, entre outros acontecimentos.

Quer seja com George W. Bush ou Barack Obama, a opção dos EUA em impor a sua vontade sobre o governo iraniano através de uma guerra aberta foi e continua sendo vista como muito arriscada, por diversas razões: atacar o Irã abertamente poderia levar a um contra-ataque iraniano perigoso, que teria como objetivos desde alvos regionais – como tropas estadunidenses no Afeganistão e no Iraque, assim como retaliações a Israel – à alvos no nível global: embaixadas, consulados ou quaisquer interesses norte-americanos ou israelenses além-mar. Este quadro ajuda a entender o programa secreto "Jogos Olímpicos" (*Olympic Games*).

"Jogos Olímpicos" é o nome de um plano iniciado em 2006, quando George W. Bush percebeu que tinha poucas opções para lidar com Teerã. Naquela época, os aliados europeus dos EUA estavam divididos em relação às sanções ao Irã, pois estas poderiam afetar as próprias economias européias. Depois do engano das armas de destruição em massa no Iraque, Bush (filho) tinha pouca credibilidade para discutir publicamente as ambições nucleares do Irã. Mas uma solução apareceu. O General James E. Cartwright, que havia criado um núcleo de operações cibernéticas no Comando Estratégico (responsável pelas armas nucleares dos Estados Unidos), juntou-se a funcionários da área de inteligência para apresentar uma "idéia nova e radical" (SANGER, 2012) ao presidente George W. Bush, concepção esta a qual envolvia uma arma cibernética muito mais sofisticada daquilo que se tinha pensado até então. Trata-se da gênese dos "Jogos Olímpicos".

Com o apoio israelense, os EUA teriam desenvolvido um complexo vírus de computador, inicialmente chamado de "the bug" ("o inseto", ou "a falha/erro" – caso seja usado vocabulário da área de informática), recebendo, depois – quando parte dos "Jogos Olímpicos" vazaram publicamente – a denominação Stuxnet, considerado o primeiro ataque de maiores proporções no qual uma investida cibernética foi usada para causar destruição física – no caso, as centrífugas enriquecedoras de urânio do Irã. O Stuxnet é considerado a arma cibernética mais sofisticada já empregada.

Do Stuxnet ao Flame: Compreendendo as "Guerras Cibernéticas" Além dos Seus Aspectos Técnicos

Stuxnet é o nome dado a um "verme" (do inglês *worm* – um tipo de vírus) de computador que começou a se espalhar em meados de 2009. Deve ser entendido à luz dos desentendimentos entre o ocidente e o Irã em torno do programa nuclear iraniano. Apareceu em programas industriais ao redor do mundo. Mas especialistas que o dissecaram rapidamente determinaram que o verme foi precisamente calibrado de uma maneira que deixasse centrífugas nucleares de enriquecimento de urânio fora de controle, daí vindo a suspeita de que o verme foi criado para sabotar o programa nuclear iraniano. Aparentemente danificou cerca de 1/5 das centrífugas nucleares do Irã e ajudou a atrasar, mas não a destruir, a habilidade de Teerã construir suas primeiras armas nucleares, embora não haja nenhuma informação que comprove que o Irã esteja de fato seguindo este caminho.

Após a disseminação do Stuxnet, funcionários de agências de inteligência começaram a falar de retrocessos no programa nuclear iraniano que poderiam atrasar o dia no qual Teerã estaria capacitada a produzir uma arma nuclear, objetivo este que o Irã nega. Em janeiro de 2011, Meir Dagan, chefe da inteligência estrangeira israelense (Mossad), prestes a se aposentar, e a Secretária de Estado norte-americana Hillary Clinton, anunciaram, separadamente, acreditar que os esforços nucleares do Irã tinham sido atrasados por vários anos. H. Clinton falou das sanções encabeçadas pelos EUA, as quais teriam ferido a habilidade do Irã em comprar componentes e fazer negócios pelo mundo afora. Já Dagan falou ao parlamento israelense que o Irã estava passando por dificuldades tecnológicas que poderiam atrasar a construção de uma eventual bomba atômica até 2015. Aparentemente o maior fator singular a atrasar os esforços nucleares iranianos foi o Stuxnet.

A "guerra cibernética" pode ser entendida como um grupo de ações conduzidas por Estados-nação para penetrar computadores ou redes de computadores de outros países, com o objetivo de causar algum dano (CLARKE; KNAKE, 2010). Seguindo esta definição, o uso do Stuxnet teria sido uma ação de "guerra cibernética", pois causou dano físico às centrífugas iranianas.

Apesar de admirável, o Stuxnet foi apenas o primeiro *worm* ("verme") de computador neste emergente cenário de conflitos cibernéticos. Como mencionado acima, "o Stuxnet é considerado a arma cibernética mais sofisticada já empregada". Entretanto, embora o Stuxnet tenha sido surpreendente, não era impossível pensar que haveria outros

malwares depois dele. E isso se confirmou no fim de maio de 2012, quando começaram a ser veiculadas notícias sobre a descoberta, feita pela União Internacional de Telecomunicações (UIT) e os Laboratórios Kaspersky (empresa fabricante de programas antivírus), de um novo vírus, que recebeu nomes variados: *Flame*, *Skywiper*, *Flamer* e *Worm.Win32.Flame*.

Ao contrário do Stuxnet, o *Flame* não causa dano físico, então, em tese, seu uso não pode ser considerado um ato de "guerra cibernética". Todavia, no espaço cibernético, guerra, espionagem e crime se confundem, então o *Flame* acaba se enquadrando no espectro mais amplo dos conflitos cibernéticos. O vírus em questão possui cerca de 20MB de código (é cerca de 20 vezes maior do que o Stuxnet) e é usado para espionagem (interceptação e captura de tráfego de rede, tira fotos da tela do computador, grava conversas de áudio pelo microfone etc). Analistas do Laboratório de Criptografia e Segurança do Sistema (*CrySys*), do Departamento de Telecomunicações da Universidade de Tecnologia e Economia de Budapeste, na Hungria, afirmam que o *Skywiper* é o *malware* mais sofisticado já encontrado (SKYWIPER ANALYSIS TEAM, 2012).

Política Externa Norte-Americana, o Poder Cibernético e a "Guerra Cibernética"

A política externa dos Estados Unidos, de George W. Bush à Barack Obama, foi marcada por uma transição de enfoques. Enquanto Bush (filho) caracterizou a sua ação externa através de duas guerras abertas, no Afeganistão e no Iraque, e por uma série de ações encobertas de contra-terrorismo pelo mundo afora, Obama deixou de usar a designação "guerra ao terror", que tanto marcou a administração anterior, e enfatizou o desengajamento, pelo menos de suas Forças Armadas, das duas frentes abertas de batalha já referidas, enfatizando as operações encobertas. A eliminação de Osama bin Laden em maio de 2011 é resultado disso. No contexto destes dois governos, e da transição de uma administração para outra, que emergiu publicamente o debate em torno das chamadas "guerras cibernéticas".

Quem chamou a atenção para a vulnerabilidade dos Estados Unidos em relação às ameaças cibernéticas foi, basicamente, Richard Alan Clarke. No governo de George W. Bush, Clarke atuou, além do cargo de conselheiro de contra-terrorismo do Conselho de Segurança Nacional (*National Security Council*), na função de assessor especial do presidente para a segurança cibernética. Clarke, porém, ficou pouco tempo nos quadros deste último governo, saindo em 2003, aparentemente por causa de divergências em relação à maneira como a administração Bush (filho) vinha lidando com as questões de segurança cibernética, assim como pela pouca atenção que os neoconservadores deram aos primeiros sinais de um ataque iminente da al-Qaeda. A saída de Clarke não foi discreta, chamou a atenção para a sua dissidência ao governo, podendo esta retirada ser associada ao início do programa "Jogos Olímpicos" alguns anos depois, em 2006. Esta associação entre Clarke e os "Jogos Olímpicos" será examinada mais detalhadamente à frente. Porém, antes, serão inseridos no raciocínio os conceitos de "difusão de poder" e de "poder cibernético".

A transição de poder de um Estado dominante para outro é um evento histórico relativamente habitual, o que Paul Kennedy chamou de "ascensão e queda das grandes potências" (1989), mas o fenômeno da "difusão do poder" é um processo mais novo. A questão para todos os Estados na atual era da informação de nível global é que mais eventos estão ocorrendo fora do controle dos Estados, inclusive dos países mais poderosos. A nova revolução da informação está mudando a natureza do poder e aumentando a sua "difusão". O Estado continuará sendo o ator dominante no cenário mundial, mas a cena internacional estará mais movimentada e difícil de controlar. Uma porção muito maior da população, tanto internamente quanto entre os Estados, tem acesso ao poder que vem da informação (NYE, 2010). O "poder cibernético" deve ser visto no quadro da "difusão do poder". O "poder cibernético" pode ser definido como a habilidade em usar o espaço cibernético para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder (KUEHL apud NYE, 2010: 4).

Inseridos os conceitos de "difusão do poder" e de "poder cibernético", é possível retomar as "guerras cibernéticas". Conforme Clarke aponta em diversos trechos de *Cyberwar* (2010), (1) a guerra cibernética não dá nenhuma vantagem aos Estados Unidos, mas o coloca em perigo; (2) a guerra cibernética coloca os EUA em uma posição desvantajosa; (3) haveria um desbalanço estratégico no qual os EUA estariam em desvantagem; (4) os EUA têm desvantagens assimétricas na guerra cibernética (CLARKE; KNAKE, 2010). Porém, quase ao mesmo tempo, o governo George W. Bush deu início ao programa "Jogos Olímpicos", sofisticados ataques cibernéticos aos sistemas computadorizados que gerenciam as instalações de enriquecimento de urânio iranianas, programa este posteriormente intensificado por Barack Obama (SANGER, 2012). Então, se as colocações de Clarke forem associadas aos "Jogos Olímpicos", é verossímil perceber uma certa discrepância. Tal disparidade pode levar a pensar que Clarke assumiu o papel de dissidente justamente para desviar a atenção dos ataques cibernéticos que os EUA lançariam contra o Irã através dos "Jogos Olímpicos". Mas isto é apenas uma conjectura.

Considerações Finais

Tendo como pano de fundo um tema emergente nas relações internacionais – os conflitos cibernéticos – este artigo buscou mostrar como os Estados Unidos têm se utilizado de uma nova dimensão do poder – o "poder cibernético" – e de novas formas de guerra e espionagem – a "guerra cibernética" e a espionagem cibernética – como instrumentos para alcançar objetivos de política externa.

Nas gestões de George W. Bush e Barack Obama, ou pelo menos na transição entre ambas, o uso do poder cibernético teve duas dimensões. Uma aberta, encabeçada por Richard Clarke (mesmo não trabalhando com Obama, Clarke não deixa de transmitir uma visão do *establishment* de segurança nacional dos EUA). A outra fechada, embora esteja sendo revelada aos poucos (SANGER, 2012). A dimensão aberta objetivava mostrar que a "guerra cibernética" não interessava aos EUA, desviando a atenção da dimensão fechada, que utilizou da "guerra cibernética" e espionagem cibernética para alcançar fins de política externa: atrasar o programa nuclear do Irã, e possivelmente outros objetivos que ainda não vieram à público.

Clarke (2011), assim como muitos outros analistas (ver, por exemplo, MCCONNELL *et. all*. 2012) tem acusado a China de um "assalto cibernético" aos Estados Unidos, através do roubo de propriedade intelectual por meio de espionagem cibernética. Isso pode de fato estar acontecendo, mas os EUA, todavia, também se utilizam desta ferramenta, embora longe do olhar público.

Referências bibliográficas

CLARKE, Richard. "China's Cyberassault on America". *The Wall Street Journal*, June 15, 2011. Disponível em: <http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html>. Acesso 03 jun. 2012.

CLARKE, Richard A.; KNAKE, Robert K. *Cyberwar*: The Next Threat to National Security and What to Do About It. HarperCollins e-books, 2010.

KENNEDY, Paul. *Ascensão e Queda das Grandes Potências*: transformação econômica e conflito militar de 1500 a 2000. Rio de Janeiro: Campus, 1989.

MCCONNELL, Mike; CHERTOFF, Michael; LYNN, William. "China's Cyber Thievery is National Policy – And Must be Challenged". *The Wall Street Journal*, January 27, 2012. Disponível em: <http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html>. Acesso 03 jun. 2012.

NYE JR., Joseph S. *Cyber Power*. Harvard Kennedy School, Belfer Center for Science and International Affairs, May

2010. Disponível em: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>. Acesso 19 mai. 2012.

SANGER, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran". *The New York Times*, June 1, 2012. Disponível em: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of--cyberattacks-against-iran.html>. Acesso 02 jun. 2012.

SKYWIPER ANALYSIS TEAM. "sKyWIper: A complex malware for targeted attacks". *Technical Report* by Laboratory of Cryptography and System Security (CrySys Lab), v1.03 (May 28, 2012). Budapest University of technology and Economics, Department of Telecommunications. Disponível em: <http://www.crysys.hu/skywiper/skywiper.pdf>. Acesso 03 jun. 2012.

Resumo

Inserido no contexto de um tema emergente nas relações internacionais, os conflitos cibernéticos, este artigo objetiva mostrar como os Estados Unidos, nos governos Bush (filho) e Barack Obama, têm usado o poder cibernético, mais especificamente a "guerra cibernética" e a espionagem cibernética, para alcançar alguns objetivos de sua política externa.

Abstract

Inserted in the context of an emerging theme in international relations, cyber conflicts, this article aims to show how the United States, in the Bush (son) and Barack Obama governments, have used the cyberpower, specifically "cyberwar" and cyber espionage, to achieve some goals of its foreign policy.

Palavras-chave: Estados Unidos; Poder Cibernético; Guerra Cibernética
Keywords: United States; Cyberpower; Cyber Warfare

Recebido em 03/06/2012
Aprovado em 10/06/2012