Conjuntura Austral

DESDOBRAMENTOS RECENTES DA SEGURANÇA CIBERNÉTICA E AS SUAS IMPLICAÇÕES PARA AS RELAÇÕES INTERNACIONAIS: *STRATFOR VERSUS ANONYMOUS.*

Recent developments of Cybersecurity and its implications to international relations: Stratfor versus Anonymous.

Bernardo Wahl Gonçalves de Araújo Jorge [1]

Em dezembro de 2011, o "movimento *hacker*" *Anonymous* reivindicou o roubo de dados pessoais, incluindo números de cartões de crédito, de cerca de 860.000 clientes da empresa de consultoria e análise de inteligência *Stratfor* – sigla de *Strategic Forecasting*, ou "previsão estratégica" (DILANIAN, 2012). George Friedman, proprietário da empresa, afirmou que o ataque foi designado para "silenciar a Stratfor", através da destruição dos seus dados e website (FRIEDMAN, 2012). Nos próximos parágrafos será esboçado um breve panorama das relações internacionais nos últimos anos, para que então o tema possa ser devidamente enquadrado.

Em 2002, Joseph S. Nye descreveu a distribuição do poderio entre as nações como um "complexo jogo de xadrez tridimensional" (NYE, 2002: 80). O tabuleiro de cima representava o poderio militar, o qual era preponderantemente unipolar, isto é, estava concentrado em um único polo; no caso, os Estados Unidos. O tabuleiro do meio representava o poderio econômico, o qual era multipolar, quer dizer, distribuido entre

[1] Mestre em Estudos de Paz, Defesa e Segurança Internacional ("Pró-Defesa" - iniciativa do Ministério da Defesa e da CAPES) pelo Programa de Pós-Graduação em Relações Internacionais da UNESP, UNICAMP e PUC-SP ("San Tiago Dantas" - iniciativa da CAPES). Professor convidado da disciplina de Segurança Internacional do curso de Pós-Graduação lato sensu Política e Relações Internacionais da Fundação Escola de Sociologia e Política de São Paulo (FESPSP). Docente do Curso de Relações Internacionais das Faculdades Metropolitanas Unidas (FMU). E-mail: bernardowahl@gmail.com
.

diversos polos de poder: os Estados Unidos, a Europa e o Japão – com uma probabilidade grande da China se transformar em um ator principal, o que de fato aconteceu. O tabuleiro de baixo representava o domínio das relações transnacionais, as quais ultrapassavam as fronteiras nacionais e fugiam do controle governamental. Este último tabuleiro incluia atores não-estatais dos mais diversos tipos: de banqueiros a *hackers*, passando por "terroristas".

Mais recentemente, o estudioso supracitado atualizou suas reflexões sobre o poder no livro *The Future of Power* (2011). Entre outras idéias apresentadas, Nye identifica duas mudanças em seu objeto de estudo, alterações que estão acontecendo neste século XXI: a transição do poder – no caso, para a Ásia – e a difusão do poder – mais especificamente, o "poder cibernético", que se difunde para atores outros que o Estado-nação. A primeira modificação é um evento histórico já conhecido (isto é, houve outras transições de poder, do Reino Unido aos Estados Unidos, por exemplo), mas a segunda transformação é um processo novo. A dificuldade para todos os Estados na atual era da informação global é que muitos eventos estão acontecendo fora do controle estatal, inclusive dos Estados mais poderosos (NYE, 2011: 113).

Dessa forma, agora talvez seja a ocasião adequada para atualizar o "complexo jogo de xadrez tridimensional" mencionado anteriormente. Cabe aqui apresentarmos o conceito de guerra cibernética, definida como "uma ação hostil no ciberespaço, cujos efeitos ampliam ou são equivalentes a uma enorme violência física" (NYE, 2012). A mudança mais marcante se dá no âmbito do terceiro nível. Muito embora as dimensões militar, econômica e transnacional continuem, a revolução da informação vem deixando o cenário mais complexo. O espaço cibernético é cada vez mais relevante, e isto traz implicações à política internacional. Refletindo sobre a segurança cibernética, Misha Glenny pensa o ciberespaço como uma "partida de xadrez heptadimensional", na qual nunca pode se ter certeza de quem é o oponente (GLENNY, 2011: 19). Do tabuleiro de xadrez tridimensional para o tabuleiro heptadimensional, nota-se que as relações internacionais ficaram mais intricadas, em grande parte devido ao ciberespaço.

Este é o momento para retomarmos o caso do *Stratfor* e o *Anonymous*. O que cada um destes atores representa e quais as possíveis implicações do incidente em

questão para as relações internacionais contemporâneas? Com o fim da Guerra Fria e o início do fenômeno da globalização, através da multiplicação da democracia liberal, a capacidade de inteligência dos Estados, antes voltada a outras ameaças estatais, as ameaças tradicionais – no conflito entre capitalismo e socialismo – passou a ser direcionada à inteligência econômica. A *Stratfor* deve ser vista neste quadro. É possível afirmar que a empresa inovou, ao levar a alguns internautas, através dos boletins informativos gratuitos, um tipo de conhecimento antes reservado apenas ao Estado ou a grandes organizações: o conhecimento e os *insights* decorrentes da análise de inteligência.

O *Anonymous*, por sua vez, pode ser visto como uma idéia, acoplada a um conjunto de práticas sociais e técnicas. É algo difuso e sem uma liderança central, um movimento de protesto que inspira ação dentro e fora da internet, contestando o abuso de poder dos governos e das corporações, buscando promover a transparência na política e nos negócios. Muitas vezes, porém, o *Anonymous* pode ultrapassar as fronteiras do protesto legítimo, o que acaba levando a percepções ligeiramente distorcidas sobre o fenômeno. Uma delas é a do governo dos Estados Unidos, mais especificamente na figura do general Keith Alexander, reponsável pela direção da *National Security Agency* (NSA) e pela chefia do Comando Cibernético (o órgão militar norte-americano encarregado das operações no ciberespaço), o qual passou a perceber o *Anonymous* como uma ameaça à segurança nacional norte-americana (BENKLER, 2012).

E, afinal, o que está em disputa? Trata-se de uma versão atualizada do "grande jogo" das relações internacionais, agora no ciberespaço, e não necessariamente envolvendo Estados de forma direta. Nesses termos, o "grande jogo" compreende novos atores – entre eles *Stratfor* e *Anonymous* – que não são grandes como Estados, mas podem gerar algum impacto nas relações internacionais, pelo menos no domínio cibernético. A *Stratfor* tem uma linha de raciocínio específica, um tipo de pensamento que visa a formar opiniões e influenciar decisões. Porém, os dados pessoais de seus clientes não estavam criptografados, o mínimo que se esperava de uma empresa que atua na área de segurança. O *Anonymous*, astuto como todo *hacker*, aproveitou-se desta

falha. Glenny afirma que são três as principais ameaças da internet, sendo que cada uma delas se manifesta de diferentes maneiras. A primeira ameaça é o crime cibernético; a segunda, a espionagem industrial eletrônica e; a terceira, a guerra cibernética (GLENNY, 2011: 234). Dois "atores" sempre estão presentes em todo este espectro de ameaças: o espião (ou, de maneira mais abrangente, a agência de inteligência, e aqui, a *Stratfor*) e o *hacker* (no caso descrito, o *Anonymous*).

Cabe mais uma vez retomar Nye para elucidar a questão. No mundo real, vencer a geografia, projetar poder por terra, mar, ar e espaço cósmico exige capacidade de projeção estratégica que apenas os Estados têm. No mundo virtual, entretanto, é tudo mais fácil, quer dizer, é muito mais econômico e breve conduzir bits e bytes através das redes de computadores do que mover porta-aviões pelos oceanos ou aviões de bombardeio pelos ares. A problemática é a seguinte: os impedimentos para se acessar o espaço cibernético são muito pequenos. Dessa forma, grupamentos não estatais e Estados menores têm a possibilidade de assumir um papel relevante, a um custo extremamente baixo. Já os Estados mais desenvolvidos, por dependerem de sistemas cibernéticos complexos para as suas ações militares e econômicas (vale lembrar da "guerra centrada em rede" – *network-centric warfare*), encontram-se mais vulneráveis. O espaço cibernético, além de um manancial de recursos, acaba se transformando também em uma fonte de insegurança para os países ricos (NYE, 2012).

Após os eventos de onze de setembro de 2001, Thomas Barnett (2003) ofereceu uma explicação sobre a ligação entre a globalização e o fenômeno do terrorismo. Conforme defendeu Barnett, os atentados contra os Estados Unidos desvendaram a nova realidade geopolítica emergente na época, o chamado "novo mapa do Pentágono", no qual a principal linha divisória internacional era aquela que separava o mundo em um "núcleo funcional" (composto por países desenvolvidos e conectados à globalização, os quais acreditavam na "modernidade") e em uma "lacuna não integrativa" (formada por países que rejeitavam a globalização, desconectados, em grande parte os chamados "Estados fracassados" ou "falidos"). Então, naquele momento, as ameaças viriam dos "desconectados". Atualmente, conforme os Estados menos desenvolvidos "se conectam", as ameaças cibernéticas podem aumentar, pois os computadores dos países

menos desenvolvidos estariam mais suscetíveis à vírus, *malwares* e à se tornarem escravos de *botnets* (*robot networks*) para, por exemplo, ataques distribuidos de negação de serviço (DDOS).

Em suma observa-se, basicamente, dois fenômenos. O primeiro fenômeno é o poder que grupos não-estatais e pequenos Estados podem obter no espaço cibernético, e a relativa insegurança dos países desenvolvidos, cujas infra-estruturas dependem do ciberespaço. O segundo fenômeno é o processo de "conexão" à internet dos países antes não conectados, processo este que, em vez de trazer mais segurança (tomando como ponto de partida a *rationale* de Barnett), paradoxalmente pode trazer ainda mais insegurança, pelo menos na percepção dos Estados mais desenvolvidos.

Finalmente, é possível ligar um fenômeno ao outro: a "conexão" dos países menos desenvolvidos poderia dar mais capacidade de poder cibernético aos pequenos Estados e aos grupos não-estatais. No mundo real, os Estados possuem quase que o monopólio sobre o uso legítimo da força. No mundo virtual, não necessariamente, e daí a importância do exame mais refletido sobre o incidente entre *Stratfor* e *Anonymous* e o processo de conexão à internet de Estados antes desconectados. Todos eles são pequenos atores que podem gerar impacto considerável nas relações internacionais.

REFERÊNCIAS

BARNETT, Thomas P. M. "The Pentagon's New Map". *Esquire*, March 1, 2003. Disponível em: <http://www.esquire.com/features/ESQ0303-MAR_WARPRIMER>. Acesso em 22 abr. 2012.

BENKLER, Yochai. "Hacks of Valor: Why Anonymous is not a Threat to National Security". *Foreign Affairs*, April 4, 2012. Disponível em: <http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor>. Acesso em 22 abr. 2012.

DILANIAN, Ken. “Hackers reveal personal data of 860,000 Stratfor subscribers”. *Los Angeles Times*, January 4, 2012. Disponível em: <http://articles.latimes.com/2012/jan/04/nation/la-na-cyber-theft-20120104>. Acesso em 22 abr. 2012.

FRIEDMAN, George. “The Hack on Stratfor”. *Stratfor Geopolitical Weekly*, January 11, 2012. Disponível em: <http://www.stratfor.com/weekly/hack-stratfor>. Acesso em 22 abr. 2012.

GLENNY, Misha. *Mercado Sombrio*: O Cibercrime e Você. São Paulo: Companhia das Letras, 2011.

NYE, Joseph. “Guerra e paz no ciberespaço”. *O Estado de S. Paulo*, 15 abr. 2012, Internacional, p. A22. Disponível em: <http://www.estadao.com.br/noticias/impresso,guerra-e-paz--no-ciberespaco-,861242,0.htm>. Acesso em 22 abr. 2012.

_____. *The Future of Power*. New York: Public Affairs, 2011.

_____. *O Paradoxo do Poder Americano*. Por que a única superpotência do mundo não pode prosseguir isolada. São Paulo: Editora UNESP, 2002.

Artigo recebido dia 22 de abril de 2012. Aprovado em 15 de junho de 2012.

RESUMO

Este texto trata do incidente envolvendo a empresa *Stratfor* e o grupo hacker *Anonymous*, um episódio de segurança cibernética, tendo como objetivo refletir sobre as implicações do espaço cibernético para as relações internacionais.

PALAVRAS-CHAVE

Segurança cibernética, relações internacionais, poder.

ABSTRACT

This paper deals with the incident involving the company Stratfor and the hacker group Anonymous, an episode of cybersecurity, aiming to reflect on the implications of cyberspace for international relations.

KEYWORDS

Cybersecurity, international relations, power.