Conflitos Cibernéticos: um *overview* sobre a participação asiática recente

Cyber Conflict: An overview about the recent Asian participation

Alexandre César Cunha Leite*
Ahmina Raiara Solsona Oliveira**

Boletim Meridiano 47 vol. 15, n. 144, jul.-ago. 2014 [p. 3 a 9]

Introdução

Ao observar atentamente os casos mais conhecidos de guerra cibernética é possível perceber a constante presença de países asiáticos, estejam estes apontados como responsáveis ou como alvos dos ataques. Neste contexto, esse artigo se propõe a apresentar um *overview* a respeito da participação asiática em guerras cibernéticas e em ataques cibernéticos e lançar luz no debate concernente aos motivos pelos quais a Ásia tem acirrado sua movimentação nessa seara.

Este trabalho está dividido em três seções: a primeira aborda os conceitos fundamentais relacionados ao tema, traçando os alicerces das discussões subsequentes, assim como trata das dificuldades que o tema apresenta; a segunda apresenta os últimos conflitos cibernéticos registrados e que tiveram, coincidentemente, seu ponto de partida e/ou destino, países da Ásia, tais como os casos Rússia *vs* Estônia e Rússia *vs* Geórgia, considerados por Nye importantes exemplos de união do uso da tecnologia da informação à guerra tradicional (NYE, 2008) Vale ressaltar que no tópico supracitado não se restringe aos dois casos citados acima, faz-se uso de uma descrição cronológica dos eventos. A terceira e última seção apresenta e discute se o histórica humilhação que afligiu países da região asiática pode ser dado como um dos fatores que impulsionaram o investimento das nações do continente em tecnologia e, neste caso, em tecnologia cibernética, como forma de contrabalancear o poderio tradicional das potências desenvolvidas.

Apesar dos efeitos nocivos causados pela Guerra-Fria e posterior descolonização dos continentes asiático e africano, estes fizeram com que alguns países da Ásia desenvolvessem a perspectiva de que o investimento em tecnologia seria o fator determinante para garantir que a humilhação sofrida no passado não se repetisse. Desta forma, o Japão (em um primeiro momento) e a China (posteriormente), seguidos de outros países da região (as duas Coréias entre outros), decidiram se modernizar (DOBSON, 2006). Essa percepção individual de desenvolvimento para independência mobilizou esforços em todo o continente asiático, justificando a existência de tantos países envoltos no desenvolvimento de programas cibernéticos de segurança, proteção

* Professor adjunto de Relações Internacionais da Universidade Estadual da Paraíba – UEPB. Coordenador do Grupo de Estudos e Pesquisa em Ásia-Pacífico (GEPAP/UEPB/CNPq).

** Membro do Programa de Pós-graduação em Relações Internacionais da Universidade Estadual da Paraíba – UEPB, bolsista e pesquisadora do Grupo de Estudos e Pesquisa sobre Ásia – Pacífico (GEPAP/UEPB/CNPq).

e, simultaneamente, invasão; enquanto em outros continentes a maioria dos países ainda está à procura do desenvolvimento desse tipo de instrumental de segurança.

Ciberguerra: conceitos e definições

Por se tratar de um tema ainda recente, há uma diversidade de definições de termos com o prefixo "ciber" (como ciberguerra, ciberterrorismo, ciberativismo, ciberpolítica, entre outros), embora tais definições ainda não tenham atingido um consenso a respeito da forma e de uma uniformização em seu uso. O que, porém, há de comum entre estes vocábulos é que seu *locus* de ação é o ciberespaço, ou seja, um ambiente metafísico.

Não obstante, depois de inúmeras tentativas, em 2008, o Pentágono definiu, segundo Friedman e Singer (2014: 13) ciberespaço como "*o domínio global dentro do ambiente de informação que consiste numa rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicação, sistemas de computador, e embutidos processadores e controladores*".

Os mesmos autores afirmam que o espaço cibernético pode ser global, mas que não é "apátrida" ou um "bem comum global", e que este é um ponto de frequente desentendimento, pois, assim como dividimos o globo em nações e os indivíduos em nacionalidades, o mesmo pode(ria) ser feito com o espaço cibernético. Este espaço depende de estrutura física e de usuários humanos que estão presos à geografia e, portanto, também estão sujeitos a noções humanas (como soberania, nacionalidade e propriedade) (FRIEDMAN e SINGER, 2014).

As divisões do ciberespaço são reais e significativas, apesar de sua característica imaginária, não palpável. Contudo, o ciberespaço, assim como toda a sorte de cenário nas relações humanas apresenta-se em constante evolução, ou seja, é um ambiente altamente dinâmico. A híbrida combinação de tecnologia e a ação humana, o primeiro o instrumento, o segundo o criador-usuário-interveniente, ambos, encontram-se em constante mudança, alterando continuamente toda a sua configuração, desde tamanho, escala e intensidade do espaço cibernético até as regras técnicas e políticas que o guiam. A geografia do ciberespaço é muito mais mutável que outros ambientes. "*Montanhas e oceanos são difíceis de mover, mas porções de espaço cibernético podem ser ligados ou desligados com o clique de um botão*" (FRIEDMAN e SINGER, 2014).

Assim, diante da complexidade de definições, o presente trabalho utiliza a ideia de guerra cibernética de Marques (2012), que a entende como uma modalidade de guerra onde o conflito ocorre no espaço cibernético através de meios eletrônicos e informáticos. Termo, da forma exposta, designa ataques, represálias ou intrusão ilícita em um computador ou rede. Ou seja, apresenta-se como uma forma menos física e tradicional de se guerrear, posto que, em geral, tem por objetivo interromper comunicação, obter e/ou destruir informações estratégicas, que não pode ser desconsideradas no atual cenário político, econômico e de segurança mundial.

O conceito de Marques (2012) não anula a possibilidade de confronto real, já que ainda trata-se de uma forma alternativa de guerra, mas minimiza o contato humano, tornando possível a prática do que Liang e Xiangsui (1999) chamaram de "*humanização contemporânea*", a saber: a despeito da ocorrência de um conflito e de um eventual ataque, tem-se como premissa manter a garantia do direito à vida.

Em decorrência desta tendência observa-se o desenvolvimento de meios para desferir ataques diretos e, especificamente, visar o centro nervoso do inimigo, sem danificar as áreas circundantes. Assim, têm-se novas opções para obtenção da vitória, desfazendo a crença de que a melhor forma de obtê-la é através de um maior exército físico, quando na verdade, pode-se obter resultado através a existência de um maior "*exercito de controle*" e não através da imposição da morte (LIANG e XIANGSUI, 1999).

Embora para Lewis (2009) a incerteza seja o aspecto mais importante de conflito cibernético, uma vez que o ciberespaço permite ataques anônimos e identidades são facilmente ocultadas ou fabricadas. Essa qualidade

permite, a título de exemplificação, uma situação na qual um oponente astuto tem plena condições para atribuir a outro(s) a responsabilidade pelo ataque lançado. Tal perspectiva levou alguns Estados a investir na tecnologia da informação e comunicação (TIC) tanto com o objetivo de criar um exército cibernético para sua defesa e segurança nacional, quanto de penetrar e obter informações secretas e privilegiadas de organizações e instituições governamentais (SOUZA, 2010). A discussão principal, porém, se dá em torno do motivo que justifique a predominância de tantos países asiáticos em tais tipos de conflitos. É com o intuito de compartilhar e melhor compreender essa primazia e participação que o tópico a seguir salienta, por meio da descrição de eventos, o caso asiático.

Conflitos Cibernéticos e a participação asiática

Para melhor compreensão da participação asiática em tais conflitos é preciso, sobretudo, apresentá-los. Tal apresentação partirá dos conflitos entre Rússia *vs*. Estônia e Rússia *vs*. Geórgia, que foram escolhidos por suas semelhanças ao envolver a mesma grande potência[1] (Rússia), por possuírem questões étnicas como princípio gerador e utilizarem a TIC para obtenção de maiores vantagens (SOUZA, 2010) e seguirá, em ordem cronológica, até os casos das Coreias, em 2013.

Os primeiros ataques aqui sucintamente descritos foram iniciados pela Rússia, em 2007, em um conflito contra a Estônia[2], e no ano seguinte, contra a Geórgia. O primeiro foi motivado por questões nacionalistas e gerado pela população russo-estoniana, que mais tarde recebeu o apoio do governo russo que, por sua vez, invadiu e atacou os *sites* do parlamento, da presidência da República e dos ministérios de saúde e tecnologia da Estônia (SOUZA, 2010, p. 48).

O segundo conflito, entre russos e georgianos, ocorreu por questões, além de étnicas, territoriais. Depois de um período de conflitos e de cessar-fogo, em 2008 a Geórgia foi vítima de ataques à sua estrutura de TIC. A Geórgia resolveu revidar pela "via tradicional" invadindo a Ossétia do Sul (motivo do período de guerra e de cessar-fogo que houve anteriormente). Deste modo, o ataque cibernético evoluiu para um conflito armado e terminou com o pedido e a posterior intervenção norte americana por meio do Conselho de Segurança da ONU. (SOUZA, 2010, p. 52-55)[3].

De acordo com Nye (2008), este conflito "*representa os primeiros ataques cibernéticos significativos acompanhados de conflito armado*". Assim, esses são exemplos de conflitos cibernéticos que findaram por unir a guerra virtual à guerra real (ou tradicional). Entretanto, recentemente, há casos do uso da tecnologia para obtenção de informação secreta e para a destruição de programas virtuais, como aconteceu com o Irã (2010), que teve seu sistema invadido pelo vírus *Stuxnet*[4] (considerada a primeira "ciberarma" de uma guerra cibernética) que danificou suas ogivas e atrasou seu programa nuclear em até dois anos. Estes ataques cada vez mais

1 Especificamente no que concerne ao quesito segurança local, regional e mundial.

2 A Estônia foi anexada pela antiga União Soviética em 1940 e invadida pela Alemanha em 1942. Em 1944 a URSS invade a Estônia novamente e em 1947 ergue a estátua de um soldado de bronze no centro da capital estoniana. Em 1991 a Estônia recupera sua independência e em 1994 o exército russo sai do território estoniano. Em 26 de Abril de 2007, ao remover a estátua de seu local de origem para um cemitério, é iniciado o conflito nacionalista por parte da população russo-estoniana. Concomitantemente ao conflito, sites do parlamento, da presidência da República e dos ministérios de saúde e tecnologia da Estônia receberam ataques virtuais, provenientes do governo russo, e que iniciaram uma onda de protestos virtuais (SOUZA, 2010, p. 49-50).

3 Recomenda-se adicionalmente a leitura de LOPES, Gills, TEIXEIRA JR, Augusto. (2010). O ***Ciberespaço é o novo front: implicações para o pensamento estratégico***. Trabalho apresentado na I Conferência Nacional da ILA (International Law Associations)-Brasil.

4 Mais informações disponíveis em: http://g1.globo.com/tecnologia/noticia/2012/06/barack-obama-acelerou-uso-do-virus-stuxnet-diz-new-york-times.html.

sofisticados foram secretamente ordenados pelo presidente Obama que decidiu acelerar os ataques iniciados no governo Bush (de codinome Jogos Olímpicos), porém de tipo e sofisticação completamente diferentes dos primeiros ataques (SINGER, 2012).

Outro caso importante é o do vírus *Flame*[5], um caso de "ciberespionagem" descoberto em maio de 2012, mas que agia há dois anos roubando dados dos governos do Irã (com o maior número de vítimas), Israel e Palestina, Sudão, Síria, Líbano, Arábia Saudita e Egito. Esse vírus se sobressai por sua capacidade de se camuflar e enganar os softwares – uma vez que não foi identificado por nenhum sistema antivírus – e sua complexa estrutura, que segundo a Kaspersky, empresa de segurança online, deve levar anos para ser analisado adequadamente (ROHR, 2012).

O caso descoberto em outubro de 2012 é o do vírus batizado de *Outubro Vermelho*[6]. Este, que existe há pelo menos cinco anos, atacou organizações em aproximadamente setenta países, incluindo o Brasil – apesar dos principais alvos serem os países do Leste Europeu, ex-repúblicas soviéticas e países da Ásia Central. A empresa Kaspersky afirma ainda que o vírus foi desenvolvido para roubar arquivos de instituições como embaixadas, centros de pesquisa nuclear e institutos ligados a setores como gás e petróleo.

As suspeitas caem sobre os chineses e russos, pois, segundo relata a Kaspersky, o código do programa inclui termos no inglês mal escrito e uma gíria russa que não é usada em nenhuma outra língua. Já os chineses estão sendo acusados de envolvimento em muitos outros ataques por possuírem um "exército" cibernético. Apesar da evidência, esta palavra pode ter sido propositadamente posta no programa para gerar suspeitas contra os russos, embora na verdade não haja nenhuma prova (KASPERSKY, 2013).

Segundo o Pentágono[7], China, Rússia e Irã já possuem sua Força de Operação Cibernética. Apesar das Coreias não fazerem parte desta lista, em março de 2013 a Coréia do Norte acusou os Estados Unidos de ter hackeado seus sites. Uma semana depois a Coreia do Sul teve derrubados os servidores de três emissoras de TV e dois grandes bancos[8]. De acordo com as autoridades, alguns computadores tiveram programas instalados e informações apagadas. Os bancos conseguiram reparar suas operações rapidamente, mas as emissoras não souberam informar quando seriam capazes de recuperar seus sistemas (BBC, 2013).

O fato, porém, provocou aumento de tensões na Ásia, uma vez que a suspeita de invasão caiu primeiro sobre a Coreia do Norte (que havia ameaçado atacar Estados Unidos e Coreia do Sul em resposta às sanções da ONU, em fevereiro de 2013) e depois sobre a China (por ter em um dos computadores o endereço de IP identificado como chinês). A situação, por fim, se estabilizou quando a Coreia do Sul reconheceu ter sido um ataque interno e se desculpou com os dois países (THE GUARDIAN, 2013).

Estes, porém, são apenas alguns exemplos da participação asiática em tais tipos de conflitos. O objetivo, entretanto, é compreender o que pode justificar tal envolvimento e desenvolvimento nesta área, que será tratado no tópico seguinte.

Um insight a respeito do porquê de a Ásia ter dado o primeiro passo

Para entender a questão que circunda a primazia asiática é importante observar que o processo histórico da região mostra que sua população passou por vários momentos de guerra e humilhação. Dobson (2006) explica

5 Mais informações disponíveis em: http://g1.globo.com/tecnologia/noticia/2012/05/por-quase-dois-anos-virus-flame-roubou-dados-sem-ser-percebido.html.

6 Mais informações disponíveis em: http://www.webdig.com.br/16429/operacao-outubro-vermelho-uma-avancada-rede-de-cyber-espionagem/ e http://www.techtudo.com.br/noticias/noticia/2013/01/brasil-e-vitima-de-virus-de-espionagem-que-existe-ha-cinco-anos.html.

7 BBC (2013).

8 Mais informações disponíveis em: http://g1.globo.com/tecnologia/noticia/2013/03/redes-de-tv-e-bancos-da-coreia-do-sul-sofrem-ciberataque.html

que durante a Guerra-Fria, quando o centro de interesse mundial se deslocou da Europa para os polos – Estados Unidos e União Soviética – as colônias africanas e asiáticas aproveitaram o momento parar reclamar suas independências. Desta forma, os poderes imperiais perderam suas colônias e, consequentemente, os recursos humanos e materiais delas provenientes, o que gerou forças políticas, sociais e ideológicas, assim como o amadurecimento dos movimentos de libertação nacional (VISENTINI, 2011).

A Guerra Fria também foi responsável por inúmeros acordos bilaterais que mantiveram a Ásia numa estrutura de insegurança e desconfiança mútua que perdura até os dias atuais. Esses acordos, construídos através da presença concreta dos Estados Unidos no continente, permitiram que algumas questões fossem congeladas no período da Guerra Fria e que estas pudessem ressurgir durante o Pós – Guerra Fria, como é o caso da redefinição dos papéis dos principais atores regionais (OLIVEIRA, 2006).

Como consequência dos movimentos de descolonização e dos acordos elaborados pelas grandes potências, em 1955, vinte e nove países afro-asiáticos se reuniram em Bandung (Indonésia) para defender a emancipação total dos territórios e repudiar as ações sofridas como consequência da Guerra-Fria, além de reivindicar apoio ao desenvolvimento econômico. Essa reunião é então conhecida como Conferência de Bandung e marcou a ascensão do Terceiro Mundo no cenário político (VISENTINI, 2011).

Outro exemplo da influência colonialista no processo asiático de descolonização é a existência de movimentos de guerrilha nas colônias europeias ocupadas pelo Japão; conflitos armados na China, Coréia, Filipinas, Birmânia[9] (atual Mianmar), nas ilhas Sakarina e no arquipélago das Kurilas; investimento americano em Taiwan, com o objetivo de contrapor e balancear o poder da China e utilização de bombas de gasolina gelatinosa e ameaça de uso de armas atômicas, ambas provenientes dos Estados Unidos durante a Guerra da Coréia (VISENTINI, 2011).

Esta, que teve como resultado a divisão do continente asiático em regimes comunistas (URSS, China, Mongólia, Coreia do Norte e Vietnã do Norte) e regimes capitalistas aliados aos Estados Unidos (Japão, Coreia do Sul, Taiwan, Filipinas, Vietnã do Sul, Malásia, e Tailândia) é o motivo pelo qual as Coreias, até então, vivem em um estado de guerra declarada e o continente de forma geral vive em um ambiente de hostilidades e desconfianças (*ibidem*), embora essa animosidade venha diminuindo depois da criação da ASEAN e de suas derivações.

Durante os momentos de conflito e de completa instabilidade que a Guerra-Fria proporcionou

> *O problema imediato, que os japoneses haviam observado muito prontamente e os chineses mais tarde, era que o atraso na ciência e na tecnologia tinha levado a dominação da Ásia pela Europa, e que a libertação estava na ciência e na tecnologia, na "modernização", mas não na ocidentalização* (DOBSON, 2006, p. 261).

Essa consciência da necessidade de investir em tecnologia para criar condições de não mais ser subjugado é, dentre outros motivos, a mola que impulsiona esses Estados e justifica o crescente investimento em aparato tecnológico, mas que também produz um ambiente de desconfianças, incertezas e eminência de ataques. Esse ambiente, porém, é responsável pela corrida tecnológica (quando ao descobrir que um Estado x investiu em tecnologia, por temor de esta ser usada para diminuir ou aniquilar suas capacidades, um Estado vizinho passa a também investir em tecnologia).

Considerações Finais

Os conflitos e ataques cibernéticos são cada vez mais discutidos e estão adensando sua presença na agenda internacional. A utilização da tecnologia da informação, seja para fins militares, econômicos ou para deter a infiltração em sua estrutura crítica (HJORTDAL, 2011) traz à tona um novo modelo de guerra, conflito e ataque,

9 Também já teve como denominação Burma.

porém regido por diretrizes que possibilitam a garantia do direito à vida, conforme afirmaram Liang e Xiangsui (1999). Este novo modelo permite a participação de países em eventos de segurança internacional que, de outra forma, não reuniriam condições de se envolver em uma guerra, tão pouco de enfrentar nações desenvolvidas, como os Estados Unidos. Esta dinâmica sugere uma facilitação de ações de ataque ao invés das ações de defesa, haja visto o caráter mais agressivo do que preventivo das ações no ciberespaço. Ainda, constata-se, pelos exemplos citados, que o uso do instrumental tecnológico/informativo, tende a favorecer o anonimato tornando as reações incertas e de maior complexidade de comprovação do fato.

Referências

BBC. UK. *South Korea blames North for bank and TV cyber-attacks*. 2013. Disponível em: http://www.bbc.co.uk/news/technology-22092051. Acessado em 10 de abril de 2013.

DOBSON, W. A. C. H. China, pasado y presente. In: *Revista Estudios de Asia y África*. China: perspectivas sobre su cultura e historias. México: El Colegio de México. Centro de Estudios de Asia y África, 2006.

FRIEDMAN, Allan e SINGER, P. W. *Cybersecurity and Cyberwar: what everyone needs to know*. Oxford University Press. UK. 2014.

HJORTDAL, Magnus. *China's Use of Ciber Warfare: Espionage Meets Strategic Deterrence.* CHINA_SEC, Centre of Military Studies, University of Copenhagen, 2011.

LEWIS, James A. *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict.* Center for Strategic and International Studies. 2009. Disponível em: http://dspace.cigilibrary.org/jspui/bitstream/123456789/26510/1/The%20Korean%20Cyber%20Attacks%20and%20Their%20Implications%20for%20Cyber%20Conflict.pdf?1 Acessado em 28 de agosto de 2013.

LIANG, Qiao; XIANGSUI, Liang. *Conjecturas sobre a Guerra e a tática na era da Globalização*. Beijing: Pla Literature and Arts Publishing House, 1999.

MARQUES, Oscar. Palestrante do tema: Guerras cibernéticas e ameaças. In: *Seminários Tecnológicos – Segurança da Informação*. Disponível em: http://assiste.serpro.gov.br/cisl/semtec.html Acessado em 18 de dezembro de 2012

NYE, Joseph S. *Cyber Insecurity*. dez. 2008. Disponível em: http://belfercenter.ksg.harvard.edu/publication/18727/cyber_insecurity.html. Acessado em 17 de janeiro de 2013.

OLIVEIRA, Henrique Altemani de. A Ásia na atual conjuntura mundial. In: OLIVEIRA, Henrique Altemani e LESSA, Antônio Carlos *Política Internacional Contemporânea: mundo em transformação*. São Paulo: Saraiva, 2006.

ROHR, Altieres. *Por quase dois anos, vírus 'Flame' roubou dados sem ser percebido*. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/por-quase-dois-anos-virus-flame-roubou-dados-sem-ser-percebido.html. Acessado em 28 de maio de 2012.

SINGER, E. David. *Obama Order Sped Up Wave of Cyberattacks Against Iran*. Disponível em: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0. Acessado em 01 de junho de 2012.

SOUZA, Gills. Lopes M. *A Cibersociedade Anárquica: análise do uso das TIC nos conflitos internacionais do século XXI à luz da escola Inglesa de RI (parte 6 e final)*. 2010. Disponível em: http://www.mundialistas.com.br/blog/index.php/a-cibersociedade-anarquica-analise-do-uso-das-tic-nos-conflitos-internacionais-do-seculo-xxi-a-luz-da-escola-inglesa-de-ri-parte-6-por-gills-lopes/ Acessado em 02 de março de 2011.

THE GUARDIAN. *South Korea says it was mistaken when it linked cyber-attacks to China*. 2013. Disponível em: http://www.theguardian.com/world/2013/mar/22/south-korea-cyberattacks-mistake. Acessado em 10 de abril de 2013.

VISENTINI, Paulo Fagundes. *As Relações diplomáticas da Ásia: articulações regionais e afirmação mundial (uma perspectiva brasileira)*. Belo Horizonte. Ed. Fino Traço, 2012.

Resumo

No pós Guerra Fria, os países asiáticos adotaram os investimentos em tecnologia da informação como uma estratégia de rompimento com o atraso e, simultaneamente, de defesa. O presente artigo procura apresentar alguns dos conflitos cibernéticos relevantes e recentes e apresentar um overview a respeito da participação asiática no desenvolvimento tecnológico e cibernético.

Abstract

In the post Cold War, the Asian countries have introduced investments in information technology as a strategy to breakup with the delay and simultaneously defense issue. This article seeks to present some of the relevant and recent cyber conflicts and provide an overview about the Asian participation in cyber and technological development.

Palavras-chave: Ásia; Guerra cibernética; Ataques cibernéticos
Key-words: Asia; Cyber war; Cyber-attack.

Recebido em: 18/02/2014
Aprovado em: 06/04/2014