RECONHECIMENTO ELETRÔNICO DE LONGO ALCANCE DA CHINA

Tenente-Coronel Timothy L. Thomas, Exército dos EUA, Reformado

O Congresso aprovou uma legislação esta semana que requer que o Pentágono informe sobre a capacidade crescente de guerra de computadores da China ao elaborar avaliações do poder militar chinês. A Lei de Autorização de Defesa Nacional do exercício fiscal de 2008, aprovada ontem pela Câmara dos Deputados dos EUA, contém uma disposição que exige que o relatório anual sobre o Poder Militar da República Popular da China inclua uma nova seção sobre "os esforços [de Pequim] de adquirir, desenvolver e empregar recursos de guerra cibernética" em suas avaliações da capacidade de guerra "assimétrica" da China.

—*Early Bird*, 14 de dezembro de 2007

DESDE 2005, O número de ataques cibernéticos chineses contra sistemas americanos aumentou a uma taxa alarmante. Entretanto, o termo "ataque" possui conotações indesejáveis. É mais provável que essas incursões injustificadas sejam missões de reconhecimento para coletar informações sobre os sistemas militares americanos, para identificar vulnerabilidades ou introduzir vírus ou portas dos fundos em nossos sistemas e para conferir uma vantagem imediata ao Exército de Libertação Popular (ELP) no caso de uma guerra que envolva os EUA e a China. Se as incursões fossem "ataques", os nossos sistemas estariam fora de operação e destruídos. Em vez disso, essas medidas de reconhecimento parecem obedecer a um antigo estratagema chinês: "um exército vitorioso ganha primeiro e inicia a batalha depois; um exército derrotado luta primeiro e tenta obter a vitória depois." O reconhecimento via computadores para identificar vulnerabilidades antes da primeira batalha se enquadra bem no estratagema.

Os Estados Unidos, é claro, não são o único país a acusar os chineses de incursões injustificadas. A Alemanha, Inglaterra, França, Japão, Taiwan, Austrália e outros também foram alvo da China. Ao considerar esses eventos à luz de relatos de fontes ostensivas sobre a teoria de operações de informações (Op Info) da China ao longo dos últimos anos, há um grande número de provas circunstanciais para condená-la. Evidentemente, a única prova forense real é sigilosa e situada nos órgãos de segurança dos países que sofreram invasão eletrônica da China.

O presente artigo explica o pensamento militar chinês que sustenta suas atividades de ataque cibernético. Enquanto outros trabalhos focalizam quem sofreu o ataque e quantas vezes, este artigo se concentra mais na teoria por trás dos ataques, especialmente no uso de estratagemas

O Tenente-Coronel Timothy L. Thomas, Exército dos EUA, Reformado, é analista sênior no Escritório de Estudos Militares Estrangeiros, no Forte Leavenworth, Kansas. É bacharel pela Academia Militar dos EUA e mestre pela University of Southern California.

eletrônicos por parte do ELP para suas operações de rede de computadores e no uso de substitutos como os grupos de hackers patrióticos. O artigo examina incursões chinesas desde 2005 e avaliações de fontes ostensivas, oferecidas por alguns dos principais teóricos chineses sobre a guerra da informação.

O ELP colocou a teoria em prática. As operações de redes de computadores se tornaram parte das atividades estratégicas em tempo de paz do ELP. Mais preocupante é a finalidade dessas incursões. Trata-se de reconhecimento? Ou o objetivo é colocar cavalos-de-troia, ou algum outro dispositivo, nos sistemas dos EUA ou parceiros para desativá-los ou destruí-los no caso de guerra? À medida que se lê sobre os desdobramentos da guerra da informação chinesa, fica claro que as possíveis intenções da China levantam questões.

As Unidades de Guerra da Informação e a Ofensiva Ativa

Embora se desconheça a razão exata dos ataques cibernéticos da China, pode-se seguir uma lógica de causa e efeito em textos chineses atuais. A causa da ligação da China a novas tecnologias da informação e da "informatização" de sua força é o impacto dramático que as tecnologias tiveram sobre questões militares, mais notavelmente o uso de tecnologia pelos EUA no Iraque. O efeito dessas tecnologias sobre o pensamento militar da China é a sua crença de que só vencerão os países que tomarem a iniciativa numa guerra da informação ou estabelecerem, de antemão, a superioridade e o controle da informação e de que isso exige o reconhecimento e a coleta de informações antes da primeira batalha para preparar o terreno para o uso de forças cibernéticas.

Historicamente, o ELP baseou sua filosofia estratégica na "defesa ativa", que significa que a China nunca atacaria alguém primeiro, mas estaria pronta para reagir caso fosse atacada. Essa filosofia mudou no decorrer dos últimos anos com a chegada da era cibernética. Há um fluxo contínuo de descrições ostensivas de unidades cibernéticas e de operações cibernéticas ofensivas das forças militares chinesas. O fato de o ELP reconhecer abertamente a necessidade de operações ofensivas reflete uma ruptura significativa com o pensamento militar tradicional. Além disso, o ELP declarou abertamente que a dependência dos EUA em relação a sistemas computacionais representa uma imensa vulnerabilidade, pronta para ser explorada. Se ele espera compensar a enorme vantagem dos EUA na aplicação prática da teoria de Op Info (em Kosovo, Iraque e Afeganistão), o ELP precisa explorar essa vulnerabilidade. Para entender essa mudança de operações voltadas à defesa para operações voltadas à ofensiva, é preciso primeiro examinar os acontecimentos de 1999.

1999

Quase uma década atrás, os teóricos de Op Info chineses já discutiam ações ofensivas. O livro *Information War* (Guerra da Informação, em tradução livre), de Zhu Wenguan e Chen Taiyi, publicado em 1999, contém uma seção chamada "Conducting Camouflaged Preemptive Attacks" (Conduzindo Ataques Preventivos Camuflados, em tradução livre). Os autores observam que a ofensiva ativa preventiva é necessária para desestruturar e destruir as forças ofensivas computacionais do inimigo.[1] Parece que parte dos ataques preventivos consiste na vigilância de rede, que engloba a coleta de informações sobre o desempenho, finalidade e estrutura de sistemas relacionados com os sistemas de C4I (Comando, Controle, Comunicações, Computadores e Inteligência), guerra eletrônica e armas. Os autores observam ainda que, no sentido mais amplo, a vigilância de informações computacionais faz parte do ataque de informações computacionais. Afirmam:

> Para conduzir a vigilância de computadores, podemos utilizar redes de informações computacionais estabelecidas em tempo de paz e entrar nelas como usuários diferentes para realizar a vigilância de uma área mais ampla que o campo de batalha. Podemos aproveitar a capacidade de especialistas em computação, especialmente hackers, para concluir tarefas de vigilância de computadores. . . é possível observar que a utilização de hackers para obter informações militares de redes de computadores é um método bastante eficaz. Devemos conhecer os protocolos de rede e acumular informações de rede.[2]

Os autores acrescentam que o ELP estabeleceu pequenas brigadas de forças de confronto

computacionais ofensivas e defensivas para conduzir esses ataques.[3] O treinamento ofensivo inclui como projetar e organizar invasões de vírus e como entrar nas redes de computadores do adversário. As brigadas ofensivas devem estudar e analisar o potencial do inimigo repetidas vezes. Também devem ser capazes de distinguir entre a verdade e a dissimulação, localizar os centros de controle computacional do inimigo e bloquear as rotas visadas.[4]

Em novembro de 1999, um artigo do jornal *Jiefanguin Bao* (Diário do Exército de Libertação) afirmou que a China talvez desenvolva uma força singular de guerra da informação — uma "força de rede"— para complementar o Exército, a Marinha e a Força Aérea. (Embora o artigo diga que é bem provável que isso aconteça, não há indícios que comprovem a criação de tal força singular atualmente) A tarefa dessa força seria proteger a soberania da rede e se engajar em guerra de redes. Entre os elementos da guerra de redes estão tecnologias "ofensivas e defensivas", de "varredura", de "mascaramento" (dissimulação) e de "recuperação". A tecnologia de mascaramento ajudaria alguém que quisesse se fazer passar por comandante e se apoderar de uma rede.[5]

2000

A ideia de focalizar atividades de reconhecimento e estratagema surgiu já em 2000. Um artigo do jornal *Jiefanguin Bao* observa que as unidades no escalão Exército e superiores devem concentrar seu estudo no reconhecimento e alerta antecipado, na coordenação de comando e na aplicação da estratégia.[6] Um artigo que comprova esse pensamento apareceu no jornal oficial do ELP, o *China Military Science* (de importância equivalente ao Joint Force Quarterly nos EUA). Este último artigo observa que os estratagemas devem criar oportunidades e momentos favoráveis para a liberação de vírus.[7]

...a China acredita que só vencerão os países que tomarem a iniciativa numa guerra da informação ou estabelecerem, de antemão, a superioridade e o controle da informação...

Outro artigo do *China Military Science* esclareceu a postura ofensiva descrita em 1999. Nele, o General Dai Qingmin opina que a ofensiva é no mínimo tão importante quanto a defesa ativa, observando: "Como a chave para ganhar a dianteira nas operações consiste em disputar a superioridade da informação com um inimigo de forma positiva e ativa, a China deve estabelecer a visão de Op Info como uma 'ofensiva ativa'." A seu ver, a ofensiva ativa é essencial para manter o controle da informação, ganhar a dianteira e contrabalançar a superioridade do adversário. Os métodos de informações ofensivos podem ajudar a sabotar o sistema de informações de um inimigo.[8]

Dai, que se tornou chefe do Quarto Departamento do Estado-Maior do ELP (Guerra Eletrônica), também observa que os estratagemas de Op Info podem ser formulados antes de iniciar uma guerra, para servir como uma "espada afiada", que sabota e enfraquece um inimigo superior, ao mesmo tempo em que protege ou aprimora a capacidade de combate da China. A Guerra da Informação pode servir como uma espécie de capacidade de luta invisível para evitar o combate com um inimigo mais forte.[9] Se a meta futura na Guerra da Informação é derrotar forças poderosas com forças fracas, mediante a utilização de estratagemas, esses métodos são, então, um dos meios assimétricos da China para combater a alta tecnologia americana.[10] Os estratagemas seriam, portanto, uma das "armas mágicas" que a cultura estratégica chinesa sempre enfatiza.

Finalmente, o artigo de agosto de 2000 de Dai no jornal *China Military Science* discute a utilização de dados eletrônicos como estratagemas e o desenvolvimento de uma capacidade de guerra eletrônica de rede integrada. Aliado ao conceito de ofensiva ativa, esse artigo representa um dos trabalhos mais importantes sobre Guerra da Informação escritos na China.

Outras publicações menos notáveis também discutem operações ofensivas. Em uma versão on-line de março de 2000, da publicação *Computer and Information Technology*, analistas do Instituto de Engenharia Eletrônica do ELP, em Hefei, discutem a necessidade de equipes de confronto de redes e de conduzir tanto operações

defensivas quanto ofensivas.[11] Em setembro de 2000, o jornal *Guangjiao Jing* observou que o ELP estabelecera recentemente departamentos de Guerra da Informação dentro de seus quartéis-generais.[12] Assim, a ideia de operações ofensivas não se limitava a Dai apenas.

2001

O livro *Science of Strategy* (Ciência da Estratégia, em tradução livre), publicado pela Universidade Nacional de Defesa da China em 2001, inclui uma seção sobre operações ofensivas da Guerra da Informação. Declara que a Guerra da Informação estratégica deve "empregar a ofensiva como estratégia principal, mas estar pronta tanto para a ofensiva quanto para a defensiva". Afirma ainda: "Devemos utilizar a estratégia de ataque preventivo e tomar a iniciativa. Lançar uma ofensiva de informações de modo ativo é a chave para obter a superioridade da informação e a liderança no campo de batalha."[13] Nesse sentido, o pensamento parece se aplicar primordialmente a tempos de guerra e não a ações em tempo de paz.

O livro *Science of Strategy* também descreve o tipo de guerra a ser travada contra as redes. O livro afirma que, em uma guerra de aniquilação, os nós devem ser atacados para fragmentar a rede antes de atacar os sistemas de armas. Os sistemas de informação e apoio devem ser sempre os primeiros alvos para desestabilizar o equilíbrio operacional. O *Science of Strategy* observa: "Depois de ataques para danificar a rede e de operações contínuas e enfraquecimento persistente do inimigo, lance um ataque aniquilador vigorosamente." As instalações terrestres de guerra da informação, meios de transmissão, plataformas de recepção e capacidade de fluxo de informação devem ser destruídos nessa ordem. Esse tipo de ataque permite que se "retire a lenha debaixo do caldeirão."[14] Embora pareça se aplicar apenas a condições de tempo de guerra, esse cenário também pode ser facilmente adaptado para condições em tempo de paz.

A tecnologia da informação estimulou, assim, o pensamento estratégico chinês. Os acadêmicos militares argumentam hoje que os que não lançam ataques preventivos perderão a dianteira no que pode ser uma guerra de Op Info bastante curta. Nos conflitos modernos, sugerem, é mais fácil alcançar o objetivo da guerra com uma única campanha ou batalha que em qualquer outro momento da história. Essa linha de pensamento dá ainda mais ímpeto ao ELP para conduzir atividades de reconhecimento cibernético em tempo de paz para se preparar para "conquistar a vitória".[15]

2002

Um artigo de junho de 2002 afirma que unidades do ELP estavam prontas para falsificar "informações em termos de ordem, tempo, fluxo, conteúdo e forma; excluir informações por partes para criar informações fragmentadas; e inserir informações para incluir dados irrelevantes com o intuito de confundir e enganar uma à outra."[16] O autor acrescenta que os dois lados de um confronto de computadores podem tentar invadir as redes um do outro por meio da inserção de vírus em softwares carregáveis, que possam ser ativados quando necessário para sabotar os sistemas computacionais um do outro.[17]

O General Dai Qingmin escreveu, em 2002, que uma das prioridades do ELP era adquirir equipamentos de operações de informações ofensivas e que o ELP deve tomar e manter a dianteira.[18] Outras publicações também se manifestaram quanto a essa questão.

O jornal *Jiefangjun Bao*, por exemplo, veiculou um artigo em agosto de 2002 sobre os tipos de ataque a redes, que foram classificados em "premeditados" (isto é, um vírus persistente incorporado no software), "contaminação" (dirigido à qualidade da informação), "forte" (que se refere à modulação forçada de vírus de computador por ondas eletromagnéticas), e "fissão" (forte capacidade de regeneração de um vírus).[19] Todos são passíveis de inserção em tempo de paz, com exceção talvez da variedade "forte".

2003

No 10º Congresso Nacional do Povo, em 2003, representantes do ELP revelaram que ele ativaria as primeiras unidades de guerra da informação de alta tecnologia em Pequim naquele ano. O relatório afirmava que haveria unidades em todos os exércitos do ELP um dia. As unidades de guerra da informação seriam providas de equipamentos de alta tecnologia e teriam a habilidade de conduzir a guerra de redes na Internet e a capacidade de transferir dados via satélites de sensoriamento remoto.[20] Não se sabe

como a "primeira" unidade difere das brigadas de guerra da informação discutidas no livro chinês Information War, de 1999.

O General Dai, em 2003, destacou mais uma vez a importância de executar ataques de informações.[21] Dai escreveu que a guerra da informação é "precursora" (começa antes de outras operações) e de "curso inteiro" (ocorre durante toda a operação). Talvez a ênfase atual em ganhar a iniciativa, e em guerras curtas, seja a razão principal pela qual Dai dá a impressão de que o emprego de ataques preventivos mediante a guerra da informação seja uma necessidade em guerras futuras.[22] Ele observa:

> As ações como guerra de inteligência, guerra psicológica e dissimulação de campanha antes do combate parecem ser ainda mais importantes para a implantação sem obstáculos do planejamento e execução da guerra. Por isso, a guerra da informação deve ser iniciada anteriormente a outras ações de combate, antes e durante a elaboração dos planos de guerra.[23]

Certas unidades de reserva específicas também se engajam em atividades de guerra da informação. Por exemplo, no final de 2003, o jornal mensal da Academia de Ciência Militar do ELP, Guofang, ofereceu instruções específicas sobre atividades de ataque a redes às unidades de reserva. O autor Li Mingrang diz que é preciso estabelecer tropas de assalto de informações como "primeiras forças" com talentos de comunicações locais, telecomunicações e departamentos financeiros e dos institutos de pesquisa científica e de ensino superior. Devem ser desenvolvidos estratagemas para aumentar a capacidade de sobrevivência do sistema.[24] Li acrescenta:

> Não há escassez de peritos em computação, incluindo especialistas em redes, podendo qualquer um deles se tornar um guerrilheiro de rede capaz de abrir, por si só, um campo de batalha sem pólvora ao realizar ataques à rede com a liberação de grandes volumes de dados vindos de diversas direções, concentrados em alguma estação de rede do inimigo para congestionar seu roteador de rede e paralisá-la…e uma vez que haja uma exigência militar, penetrar no sistema de rede para roubar informações ou ativar vírus, ou detonar 'bombas' para atingir o alvo de combate de destruição da rede.[25]

As forças de reserva são orientadas a trabalhar em estratégias ofensivas.

Em seu livro Deciphering Information Security (Decifrando a Segurança da Informação), de 2003, o "pai da guerra da informação" na China, o coronel reformado Shen Weiguang, escreveu sobre o desenvolvimento de uma universidade de segurança da informação com uma especialização em segurança da informação militar. Essa especialização engloba, entre vinte e poucos temas, "Estudo de Métodos de Ataque de Hackers", "Detecção de Intrusão em Rede e Defesa contra o Ataque", "Táticas de Ataque e Defesa da Informação" "Projeto e Aplicação de Programa de Vírus", "Estruturas de Sistema de Segurança de Redes" e "Varredura para Detecção de Problemas Ocultos em Redes".[26] Muitos desses tópicos se enquadrariam na definição de atividades de incursão em redes computacionais em tempo de paz do ELP.

2005

Em *Study Guide for Information Operations Theory* (Guia de Estudo da Teoria de Operações de Informações, em tradução livre), de 2005, o General Dai e co-autores definiram 400 termos relacionados a Op Info, muitos deles referentes a atividades preventivas ou de reconhecimento. Apenas a guerra de redes de computadores é descrita aqui.

> A guerra de redes é composta de reconhecimento, ataques e defesa de redes de computadores. As operações envolvem, em geral, o emprego de combatentes cibernéticos armados e equipados. O meio de operações inclui vários tipos de vírus, bombas lógicas e armas de circuitos integrados desenvolvidos a partir da tecnologia computacional. A guerra de redes atuará tanto como meio de dissuasão quanto como um meio de combate, podendo ter um grande e profundo impacto na política, economia e forças militares do inimigo. Também é um importante meio de batalha para uma força militar menos equipada contra outra com poderes formidáveis em alta tecnologia.[27]

Dai também discutiu a importância da conduta da guerra, concentrando-se na dissuasão da informação como um conceito a ser considerado e desenvolvido com maior profundidade no âmbito estratégico. Entre outros que escreveram sobre

o tópico de dissuasão da informação está Shen Weiguang. O livro *Science of Military Strategy* (Ciência de Estratégia Militar, em tradução livre) dedica um capítulo inteiro ao tema. Esta última fonte explica como a dissuasão da informação (intimidação mediante a demonstração da capacidade ou poderio da informação) pode contribuir para a consecução dos objetivos nacionais e militares. Entre os métodos de dissuasão estão a tecnologia da informação (inovações de hardware e software), armas de informação (dissimulação ou desinformação discursiva) e supressão de recursos da informação (análogo ao congestionamento). Segundo alguns autores chineses, as teorias de dissuasão de contrainformação também devem ser consideradas. Em *Warfare Strategy Theory* (2005) (Teoria de Estratégia de Guerra, em tradução livre), Yao Youzhi assevera que a estratégia se desenvolveu até o ponto em que considerações tecnológicas se tornaram dominantes e o emprego de tecnologia, estratégico. Qualquer estratégia que se distancie do foco nas armas de alta tecnologia não tem utilidade, segundo Yao. Isso também significa que a China deve desenvolver contraestratégias adequadas.[28] Afirma:

> É preciso ser proficiente na utilização da super-rodovia da informação, criando informações enganosas, espalhando a neblina da guerra e bloqueando e destruindo a consciência estratégica do inimigo, utilizando, assim, a estratégia para controlar o adversário. É necessário ser proficiente no uso de ataques simulados eletrônicos, camuflagem eletrônica, interferência eletrônica, ataques de vírus e interferência e dissimulação de satélites espaciais, levando o inimigo a tirar a conclusão errada e alcançando o objetivo de dissimulação estratégica.[29]

Embora concebidas para o emprego em tempo de guerra, várias dessas técnicas também funcionam como medidas de prevenção e antecipação em tempo de paz.

Nos comandos compartimentados do passado, uma força calculava o seu poder pela soma de todas as suas partes. Atualmente, o poder de combate de uma força é o produto de elementos operacionais, em que as tecnologias da informação são fatores de uma multiplicação potencialmente exponencial.[30]

Yao escreve que a guerra "informatizada" mudou a importância tradicional de "ataque, captura, controle e defesa", porque os ataques de precisão possibilitam a destruição de todo o sistema de guerra do inimigo. O principal alvo de ataque se tornou o sistema estratégico de informação da força inimiga. Todas as atividades hoje giram em torno de conquistar a supremacia no campo de batalha e a supremacia da informação é a sua base. A destruição direta da vontade do inimigo suplantou a aniquilação da capacidade militar dele. Esse foco na informação requer métodos completamente diferentes em guerras futuras.[31]

2007

O autor Zhang Zhibin observa, em *Jiefanguin Bao*, 13 de março de 2007, que a relação dialética entre a ofensiva e a defesa na guerra de redes deve dar igual ênfase a cada uma delas. Uma teoria de dissuasão de rede implica que as duas capacidades são necessárias: a ofensiva para assustar alguma força inimiga potencial e a defensiva para impedir algum ataque. Zhang diz:

> Somente com um bom trabalho de defesa positiva, a China poderá assegurar a conquista da liderança na guerra de redes. Assim, a China deve envidar esforços contínuos para buscar oportunidades de antecipação por meio do desenvolvimento de tecnologia e sistemas de rede e da pesquisa e implantação de operações defensivas de rede correspondentes.[32]

Outros artigos de 2007 enfatizam a necessidade de ação por parte do ELP para obter o controle de redes, incluindo o acesso, se possível. Dois livros sobre Op Info chinesas deste autor, *Dragon Bytes* (Bytes do Dragão, em tradução livre) e *Decoding the Virtual Dragon* (Decodificando o Dragão Virtual, em tradução livre), mencionam esse foco no controle.

Prováveis Ataques Computacionais Chineses contra os EUA

Ao longo dos últimos anos, a guerra da informação e os recursos de Op Info chineses se tornaram mais visíveis e preocupantes. A China utilizou esses recursos não apenas contra os EUA, mas, segundo consta, contra o Japão, Taiwan, Alemanha, Inglaterra e Austrália também. Devido ao caráter das operações

FOTO da AP, Andy Wong

Uma tela de computador que mostra um site militar é vista dentro da base do Exército em Tianjin, nas proximidades de Pequim, China, 30 de julho de 2007. Redes de computadores serviram de alvo para espiões cibernéticos que, segundo relatos da imprensa, são comandados pelas forças militares da China, mas ela nega estar por trás de tais ataques.

de rede de computadores, não se sabe o número exato de eventos chineses de reconhecimento ou ofensiva da guerra da informação ocorridos, ou o objetivo real dessas incursões. Entre os episódios que chegaram ao conhecimento público estão os relacionados a seguir:

• A espionagem realizada contra os computadores do Departamento de Defesa dos EUA, noticiada na revista Time. A matéria tratava de uma aliança ilegal de espionagem cibernética, à qual os investigadores federais deram o codinome de *Titan Rain*.[33]

• As tentativas chinesas de cegar um satélite americano, noticiadas em Defense News. A reportagem discutiu os ataques da China com laser de grande potência contra um satélite americano.[34]

• Ataque de hackers chineses contra a capacidade de rede da Escola de Guerra Naval dos EUA, noticiado em Federal Computer Week. Esse ataque, segundo consta, se originou na China e colocou sistemas fora do ar.[35]

• A destruição, pela China, de um velho satélite meteorológico chinês com um míssil antissatélite, noticiado na National Public Radio. A reportagem citou um comentarista da Universidade Popular de Pequim, que observou: "A tecnologia de destruição de satélites é lógica no desenvolvimento de mísseis e da capacidade de guerra da informação."[36]

• Um sofisticado ataque a computadores no Laboratório Nacional de Oak Ridge, em Tennessee, em outubro e novembro de 2007. O ataque foi na forma de e-mails falsos que, ao serem abertos, permitiram aos hackers penetrar a segurança dos computadores do laboratório.[37]

• Os ataques de hackers contra o Japão e o Taiwan, noticiados na imprensa dos dois países.[38] As reportagens observaram que esses ataques foram retaliações pelas interpretações de história antichinesas do Japão e pelas reivindicações de independência de Taiwan.

Em 05 de setembro de 2007, o jornal Kansas City Star veiculou um artigo em que a China negou ter realizado ataques cibernéticos contra país algum. O porta-voz do Ministério de Relações Exteriores, Jian Yu, observou: "O governo chinês sempre se opôs a crimes da Internet, incluindo a prática de hacking, reprimindo-os segundo a lei."[39] Ele repudia acusações de ataques da China contra computadores do Pentágono, classificando-os de "infundadas". Um porta-voz do Pentágono se recusou a dizer se a China havia perpetrado o crime, mas o jornal britânico Financial Times cita uma autoridade americana não identificada que disse que havia seguido a pista da fonte até o ELP.

Uma semana antes, a revista *Der Spiegel*, da Alemanha, noticiara que o ELP havia se infiltrado nos sistemas informatizados do governo alemão. Segundo a reportagem, os hackers foram localizados em Guangzhou e Lanzhou.[40] Assim, as provas circunstanciais continuam a aumentar. É difícil acreditar que a Alemanha, Austrália, Japão, Taiwan e América estão conspirando para indiciar a China e retratá-la como uma nova ameaça. De fato, por meio de operações cibernéticas não provocadas, a China parece ter se indiciado sem a ajuda de ninguém.

Uso de Substitutos pela China

Um dos estratagemas da China é "atacar com uma espada emprestada." Talvez o uso de hackers patrióticos se enquadre nesse estratagema. Um artigo recente da revista Time discutiu a utilização da iniciativa do grupo "Network Crack Program Hacker" (*NCPH*) para alcançar essa meta. O artigo disse que o ELP desenvolveu uma

competição para os hackers e que o vencedor receberia uma remuneração mensal dos militares. Observou que o grupo NCPH não apenas ganhou a competição e recebeu a remuneração, como também o ELP utilizou o NCPH para ensinar técnicas e procedimentos para outros integrantes da sua equipe de guerra cibernética. A companhia iDefense, filial americana da VeriSign, observou que o NCPH da China criou 35 programas para implantar cavalos-de-troia (que tomam controle parcial dos computadores), usados para atacar órgãos governamentais dos EUA. A iDefense da VeriSign acusou o NCPH de desviar milhares de documentos não sigilosos dos EUA. Essa atividade se enquadraria no foco em ataques preventivos do ELP.[41]

O conceito de "guerra popular" também combina com o chamado "hacking" patriótico. A "guerra popular" na era cibernética significa que os cidadãos se envolvem na realização de hacking ou ataques cibernéticos contra os sistemas de um inimigo. Atualmente, mais de 250 grupos de hackers operam na China.[42] A quantidade poderia, assim, criar uma qualidade própria com a variedade e intensidade de incursões que eles poderiam conduzir. Não seria possível ligar responsáveis diretamente ao ELP, se os grupos de hackers fossem compostos de cidadãos particulares (ou, na verdade, militares da ativa ou reserva que conduzem operações cibernéticas de suas casas). Mais uma vez, só há provas circunstanciais como base, mas elas vêm se tornando contundentes.

Conclusões

A teoria chinesa ao longo dos últimos anos indica que a China quer se tornar proficiente na ofensiva ativa, reconhecimento cibernético, estratagema cibernético e atividades de exploração computacional, caso o ELP precise ir à guerra. Se a China acha que pode ganhar a dianteira por meio da obtenção da superioridade da informação ou da prevenção de ataques cibernéticos, os próximos anos podem, então, envolver desafios desse setor. Embora seja fácil avaliar a finalidade dos desdobramentos das tropas, é mais difícil determinar o objetivo de um dado eletrônico chinês. É inserir um vírus, efetuar reconhecimento ou desabilitar um sistema? O mundo entrará em território incerto conforme as nações tentarem responder e desenvolver ações de gerenciamento de consequências para intrusões eletrônicas realmente danosas.

Os chineses observam que as táticas e técnicas de Op Info permitem mais ênfase no princípio de ofensiva do que na guerra tradicional. Uma força mais fraca, por exemplo, pode infligir muitos danos a uma força superior com um ataque de informações assimétrico devidamente programado e precisamente definido. A China normalmente se retrata como o lado mais fraco nas relações sino-americanas. Acredita que as operações de ofensiva como dissuasão da informação, bloqueio da informação, criação de poder de informação (camuflagem eletrônica, dissimulação de rede, etc.), contaminação da informação, assédio da informação, destruição nodal, paralisação de sistemas e destruição de entidades são essenciais para a vitória em um conflito contemporâneo com os EUA.

Um dos estratagemas da China é "atacar com uma espada emprestada." Talvez o uso de hackers patrióticos se enquadre nesse estratagema.

É preciso lembrar que essa análise se origina apenas de informações ostensivas e comentários públicos do ELP e que o entendimento da China quanto à interseção entre estratégia e tecnologia da informação, especialmente em relação ao conflito atual, não é ampla num sentido prático. Os chineses têm pouca experiência recente com conflitos. Suas forças não lutam em uma guerra real há décadas. De uma perspectiva teórica, porém, a China escreveu amplamente sobre a utilização de tecnologia da informação e ataques preventivos eletrônicos, levando ambos em consideração. As intrusões cibernéticas da China indicam que os chineses estão adquirindo bastante experiência prática e teórica em tempo de paz.

Os comentários ostensivos do ELP podem ser interpretados como uma tentativa de cooperar com o Ocidente ou se opor a ele vigorosamente. Talvez o ELP seja bastante aberto e transparente

quanto às suas estratégias cibernéticas, talvez mais aberto que em qualquer outra área de operações militares. (O ELP é bem mais aberto quanto ao seu pensamento sobre a guerra da informação, por exemplo, que a Rússia.) Se a intenção do ELP é se opor ao Ocidente, ele pode, de fato, estar ocultando conceitos valiosos sobre guerra da informação nos "regulamentos" do ELP (o seu equivalente à doutrina) nas diretorias de estado-maior e nos institutos de pesquisa. Os regulamentos sobre guerra da informação da China não estão disponíveis para outras nações, ao passo que a doutrina ostensiva dos EUA está à disposição de todos na Internet. O ELP mantém seus regulamentos bem escondidos. Nesse caso, a falta de transparência introduz uma ambiguidade indesejável. Os EUA e outros países sob ameaça de incursões do ELP podem reagir com severidade a alguns cenários desenvolvidos pelos chineses e, assim, sem querer, provocar um conflito.

Não está claro como e quando a China poderia usar seus conceitos de ofensiva ativa para fins além de reconhecimento, mas, como conceitos gerais, são preocupantes. Não é um bom sinal para a futura cooperação e estabilidade que os teóricos chineses acreditem realmente (como declaram abertamente) que a China só poderá contrabalançar a superioridade informática de um oponente se atacar primeiro. Sem dúvida, a China continuará a utilizar a tecnologia em conjunto com estratagemas inovadores para tentar enganar nossos sistemas de alta tecnologia ou talvez até gerar erros nos processos cognitivos dos tomadores de decisões dos EUA. Vivemos tempos interessantes.***MR***

REFERÊNCIAS

1. WENGUAN, Zhu e TAIYI, Chen. *Information War* (local e editora não declarados, 1999), cap. 5 (Computer Operations). Esse capítulo discute operações de informações computacionais ofensivas e defensivas.

2. Ibid.

3. Ibid.

4. Ibid. A certa altura da discussão, os autores afirmam: "Precisamos observar a estratégia de nossas forças militares de ofensiva ativa e assegurar que, no treinamento em conflitos computacionais, tanto a defesa quanto a ofensiva sejam parceiros principais."

5. BINGLING, Leng; YULIN, Wang; e WENXIANG, Zhao. "Bringing Internet Warfare into the Military System is of Equal Significance with Land, Sea, and Air Power", *Jiefangjun Bao* (Liberation Army Daily), 11 de novembro de 1999, 7, conforme traduzido e acessado no site de Foreign Broadcast Information Service (FBIS), 15 de novembro de 1999.

6. CHANGLONG, Fan. "Stand in the Forefront of the New Military Revolution in Deepening Troop Training through Science and Technology", *Jiefangjun Bao* (Liberation Army Daily), 4 de abril de 2000, 6, conforme traduzido e acessado no site de FBIS, 6 de abril de 2000.

7. LI, Niu; JIANGZHOU, Li; e DEHUI, Xu. "Planning and Application of Strategies of Information Operations in High-Tech Local War", *Zhongguo Junshi Kexue* (China Military Science) nº 4, 2000, 115-22, conforme traduzido e acessado no site de FBIS, 9 de novembro de 2000.

8. QINGMIN, Dai. "Innovating and Developing Views on Information Operations", Zhongguo Junshi Kexue, data não fornecida.

9. Ibid.

10. Ibid.

11. JIAN, Yang; YOUHUA, Zhang; e ZHANKUN, Lu. (sem título), *Jisuanji Yu Xinxi Jishu* (versão on-line de *Computer and Information Technology*), Anhui Computer Subscriber Association e Anhui Computer Society, 16 de março de 2000, conforme traduzido e acessado no site de FBIS, 18 de abril de 2000.

12. "China's IWCapabilities", *Guangjiao Jing*, Hong Kong, 16 de setembro de 2000.

13. *Ge Zhenfeng*, cap. 16, sec. 4, p. 366. O autor agradece o Dr. Gary Bjorge, Combat Studies Institute, Forte Leavenworth, Kansas, pela tradução de trechos do livro.

14. *Ge Zhenfeng*, cap. 24, sec. 6, p. 493.

15. PENG e YAO, pp. 418-19.

16. T'AO, Wen. "PLA Bent on Seizing 'Information Control.'" *Hong Kong Ching Pao*, 1 de junho de 2002, no 299, pp. 44-46, conforme traduzido e acessado no site de FBIS, 5 de junho de 2002.

17. Ibid.

18. QINGMIN, Dai. "On Integrating Network Warfare and Electronic Warfare", *Zhongguo Junshi Kexue* (China Military Science), February 2002, 112-17, conforme traduzido e acessado no site de FBIS, 24 de junho de 2002.

19. YONGSHENG, Fan; XINGHAN, Wu. "War on Networks: Modern 'Contradictory' Offensive, Defensive Warfare", *Jiefangjun Bao* (Liberation Army Daily), 14 de agosto de 2002, p. 11, conforme traduzido e acessado no site de FBIS, 14 de agosto de 2002.

20. "PLA to Organize First Information Warfare Units", *Mingpao News*, 12 de março de 2003, Disponível em: <http://full.mingpaonews.com/20030312>.

21. *Direct Information War*, p. 170.

22. Ibid., p. 169.

23. Ibid.

24. MINGRANG, Li. "Develop the Advantage of People's War under the Conditions of Innovation and Informatization", *Guofang*, 15 de novembro de 2003, pp. 7-8, conforme traduzido e acessado no site de FBIS.

25. Ibid.

26. WEIGUANG, Shen. *Deciphering Information Security* (Xinhua Publishing House; July 2003), pp. 127-241.

27. Ibid., 211.

28. YOUZHI, Yao. Redator-chefe, *Warfare Strategy Theory* (Liberation Army Press, 2005), pp. 475-76.

29. Ibid.

30. Ibid., pp. 346-49.

31. Ibid., pp. 99-101.

32. ZHIBIN, Zhang "Offense is Not Necessarily the Best Defense—Preliminary Study and Thinking on the Dialectical Relationship between Offense and Defense in Network Warfare", *Liberation Army Daily*, 13 March 2007, as downloaded from the Open Source Center web site, 9 April 2007.

33. THORNBURGH, Nathan. "The Invasion of the Chinese Cyberspies", *Time*, 29 August 2005, Disponível em: <www.time.com>.

34. MURADIAN, Vago "China Tried to Blind U.S. Sats with Laser", *Defense News*, 25 de setembro de 2006, p. 1.

35. ROGIN, Josh. "Network Attack Disables Naval War College", *Federal Computer Week*, 30 de novembro de 2006, Disponível em: <www.fcw.com>.

36. KUHN, Anthony. *National Public Radio*, 19 de janeiro 2007, entrevista com representante de Pequim.

37. "Oak Ridge National Lab Reports 'Sophisticated' Cyber Attack Netted Personal Data on Visitors", The Associated Press, 6 de dezembro de 2007, Disponível em: <www.iht.com/bin/printfriendly.php?id=8626732>.

38. "Chinese Hackers Attack Taiwan Military Computers", *Taipei P'ing-kuo Jih-pao* (versão on-line), 15 de maio de 2006, conforme descrito no relatório CPP20060516310002 do Centro Ostensivo.

39. JOHNSON, Tim. "China Denies Cyber-Attack", *Kansas City Star*, 5 de setembro de 2007, p. A5.

40. Ibid.

41. ELEGANT, Simon. "Enemies at the Firewall", *Time*, 19 de dezembro de 2007, Disponível em: <www.time.com/time>.

42. Conversa com Scott Henderson, cujo livro sobre hackers chineses, Dark Visitor, será publicado futuramente. Esse livro é provavelmente o melhor trabalho ostensivo sobre hackers chineses.