As Estratégias Eletrônicas da China

Tenente-Coronel (Res) Timothy L. Thomas, Exército dos EUA

O *MAJOR GENERAL* DAI QINGMIN, diretor do Departamento de Comunicações do Estado-Maior Geral do Exército de Libertação Popular da China (*People's Liberation Army — PLA*), responsável pela guerra de informação (G Info) e pelas operações de informações, escreveu, recentemente, que "as novas tecnologias provavelmente encontrarão expressão material nas armas e equipamentos dotados de tecnologia da informação que, em conjunto com sistemas de informação, o som, a luz, a eletrônica, o magnetismo, o calor, e outros meios afins, tornar-se-ão um transportador de estratégias".[1] As estratégias chinesas dependem do emprego de elétrons em formas imprevistas para realizar tais estratagemas como "matar com uma espada emprestada" ou "esgotar o inimigo na entrada, e atacá-lo com calma".

Uma superioridade de estratégias, segundo a crença chinesa, pode ajudá-los a superar suas dificuldades tecnológicas. Uma comparação equivalente deste conceito teórico na arte militar seria um grupo virtual de manobra operacional russo composto de forças de elétrons ou um grupo de batalha ar-terra de elétrons dos Estados Unidos.

O artigo de Dai é um importante marco na filosofia militar do Exército de Libertação Popular por várias razões. Em primeiro lugar, o autor é considerado uma pessoa honesta e responsável. Antes de assumir sua posição atual, o Gen Dai foi comandante do Centro de Guerra de Informação do Exército de Libertação Popular em Wuhan. Segundo, ele define a guerra de informação e as operações de informações (Op Info) com caraterísticas chinesas que são diferentes das definições norte-americanas. Terceiro, o Gen Dai rompeu com a tradição quando defendeu a condução de um ataque antecipado para conquistar a iniciativa e alcançar superioridade no âmbito das informações. A ênfase desta ofensiva se contradiz com a estratégia militar da China que tradicionalmente se baseia na defesa ativa. Ainda enfatizou que operações de informações conjuntas e integradas permitem estender o alcance da guerra popular e afiançar o apoio da população. O seu artigo também indica que a China, sem dúvida alguma, já se encontra desenvolvendo estratégias adequadas para implementar a guerra de informação com características chinesas. Outros escritores também defendem o mesmo ponto de vista levando em consideração suas próprias abordagens à guerra de informação no nível estratégico.

O relatório sobre a China preparado pelo Secretário de Defesa dos EUA para o Congresso no ano fiscal de 2000 (compulsório segundo a Ata de Autorização da Defesa Nacional) indicava avanços tanto nas teorias quanto na capacidade chinesa. Este relatório salientava que desde o bombardeio inadvertido da Embaixada da China em Belgrado pelas forças da OTAN, no dia 7 de maio de 1999, os chineses vêm acelerando o processo de modernização das Forças Armadas, dedicando-se, concomitantemente, a iniciar negociações de cooperação estratégica com a Rússia e incrementar suas atividades contra a proliferação. A China concentrou-se no combate aos adversários que possuam tecnologias de informação avançadas e armas de precisão de grande alcance. A doutrina de "defesa ativa" focaliza a "guerra popular sob condições modernas", denominada segundo o relatório do Secretário de Defesa de "guerras locais sob condições de alta tecnologia".[2] O Papel Branco sobre a Defesa Chinesa, disseminado em 16 de outubro de 2000, também enfatizou a tradição da guerra popular chinesa, ênfase esta que surpreendeu muitos peritos ocidentais em assuntos da China, que estavam convencidos de que tal idéia havia perdido importância na era da informação. Na realidade, sua importância aumentou.

Em setembro de 2000, duas semanas antes de que o Papel Branco fosse publicado, o jornal *PLA Daily*, divulgou um artigo a respeito da evolução de telecomunicações

O relatório sobre a China preparado pelo Secretário de Defesa dos EUA para o Congresso no ano fiscal de 2000 (compulsório segundo a Ata de Autorização da Defesa Nacional) indicava avanços tanto nas teorias quanto na capacidade chinesa. Este relatório salientava que desde o bombardeio inadvertido da Embaixada da China em Belgrado pelas forças da OTAN, no dia 7 de maio de 1999, os chineses vêm acelerando o processo de modernização das Forças Armadas, dedicando-se, concomitantemente, a iniciar negociações de cooperação estratégica com a Rússia e incrementar suas atividades contra a proliferação. A China concentrou-se no combate aos adversários que possuam tecnologias de informação avançadas e armas de precisão de grande alcance. A doutrina de "defesa ativa" focaliza a "guerra popular sob condições modernas", denominada segundo o relatório do Secretário de Defesa de "guerras locais sob condições de alta tecnologia".

militares da China. O artigo divulgava que em 1991 o Presidente Jiang Zemin instou que fossem estabelecidos sistemas de telecomunicações para uso militar e civil que satisfizessem as necessidades da população chinesa tanto em tempo de paz quanto de guerra.[3] Somente desta forma as telecomunicações militares conseguiriam equiparar-se com a indústria de comunicações civil. Para que isto fosse conseguido seriam criadas forças da reserva (um componente-chave que unisse setores civis e militares em uma guerra popular) com missões de telecomunicações e de guerra/operações de informações. No Papel Branco encontrava-se a seguinte informação: "Organizamos a estrutura de uma força de telecomunicações da reserva com um regimento de telecomunicações da reserva como se fosse a espinha dorsal da estrutura com um departamento de informações industriais como base… organizamos um contingente de reserva formado por pessoal altamente qualificado nos âmbitos das telecomunicações e transmissões, cuja força principal está composta por pessoal especializado em telecomunicações por satélite, rádio digital, telegráfica (telefone), e por fibra óptica como a principal força…contando com o apoio indispensável de um contingente de pessoal altamente qualificado em computadores, especialistas em monitorização de redes e unidades de telecomunicações por rádio", servindo como a espinha dorsal.[4]

As forças de reserva da China estão agora preparadas para missões de guerra/operações de informações, transformando-se no elo que vincula a alta tecnologia com a teoria da guerra popular desta nação. No passado, o papel das forças de reserva era apoiar as forças do Exército de Libertação Popular em operações de defesa contra qualquer intervenção estrangeira. Hoje em dia, as forças de reserva podem realizar algumas façanhas que por muitos anos ficava fora do alcance do Exército de Libertação Nacional: empregar armas eletrônicas e de informação para alcançar um adversário em outro continente. Ataques eletrônicos podem ser tão devastadores à economia de uma nação quanto os danos causados por um míssil intercontinental.

Segundo o falecido líder chinês Deng Xiaoping a indústria de defesa da China está atrasada no desenvolvimento de equipamento de alta tecnologia e, por esta razão, deve procurar "focos seletivos de excelência". Um destes focos parece ser as telecomunicações internas. No relatório do Secretário de Defesa consta que as redes de comunicações civis e militares podem ser conectadas para auxiliar a China em uma situação de crise. O relatório publicado no número de setembro do jornal *PLA Daily* indica que é mais provável a criação de um sistema de telecomunicações cívico-militares. O sistema militar de comunicações faz uso de múltiplas linhas de transmissão para maximizar a sua sobrevivência, segurança, flexibilidade, mobilidade e resistência a ataques eletrônicos, ficando menos vulnerável à exploração e à destruição. Supostamente, a rede automatizada de dados do comando pode apoiar um limitado número de ataques convencionais pré-planejados ao longo da periferia da China.[5]

Tanto quanto se sabe, as forças de reserva chinesas possuem suas próprias páginas *web* e centros de simulações. De acordo com um relatório a China conta agora com 400 *websites* militares.[6] Em 7 de janeiro de 2001 várias companhias não identificadas concretizaram a formação da China C — Rede de Aliança Estratégica, a qual é uma de rede de segunda geração similar à Internet para os setores do governo e da indústria do país. Porém, ainda não foram determinadas as datas para iniciar ou completar a sua construção. A Agência de Notícias de Xinhua divulgou que "a Internet atualmente em uso apresenta muitos problemas e não satisfaz as necessidades nem do Governo nem das indústrias chinesas, à medida que adentram na era digital. Todavia, não está claro se os estrangeiros terão acesso à rede, ou se esta será compatível com a rede existente".[7]

A cooperação e integração cívico-militares estão aumentando na China da era da informação, da mesma forma como nos Estados Unidos. O presidente Kiang Zemin (3º à esquerda) defende a construção de um sistema comum de telecomunicações para satisfazer as necessidades civis e militares nesta área. Uma forma de se conseguir isto é através da criação de forças de reserva — um componente-chave que unifica os setores civil e militar em uma guerra popular — com missões de telecomunicações, guerra de informação e operações de informações.

As forças de reserva da China estão agora preparadas para missões de guerra/operações de informações, transformando-se no elo que vincula a alta tecnologia com a teoria da guerra popular desta nação. . . . Hoje em dia, as forças de reserva podem realizar algumas façanhas que por muitos anos ficava fora do alcance do Exército de Libertação Nacional: empregar armas eletrônicas e de informação para alcançar um adversário em outro continente. Ataques eletrônicos podem ser tão devastadores à economia de uma nação quanto os danos causados por um míssil intercontinental.

Estratégia de G Info/Op Info na revista *China Military Science*

A revista *China Military Science*, publicada trimestralmente, serviu no ano passado como um foro limitado para a disseminação de artigos relativos à guerra de informação e às operações de informações. No entanto, a edição de abril de 2000 foi uma exceção, porquanto publicou três artigos importantes sobre o tema de guerra de informação e operações de informações. Um dos artigos, intitulado *The Current Revolution in Military Affairs and Its Impact on Asia-Pacific Security* (A atual Revolução em Assuntos Militares e seu Impacto na Segurança da Ásia e do Pacífico), foi escrito pelo Coronel Wang Baocun, respeitado autor na área de operações de informações, que trabalha no Departamento de Estudos Militares Estrangeiros da Academia de Ciências Militares, organização encarregada da publicação da referida revista. Seu artigo é o único escrito em inglês e reflete o ponto de vista ocidental da guerra de informação e da revolução em assuntos militares. Wang define guerra de informação como "uma forma de ações de combate que ataca a informação e os sistemas de informações do inimigo protegendo, ao mesmo tempo, os seus. A guerra de informação compreende a segurança militar, a dissimulação militar, o ataque físico, a guerra eletrônica, a guerra psicológica e a guerra cibernética, com o objetivo básico de conquistar e manter o domínio da informação".[8]

Wang propôs uma definição muito diferente sobre guerra de informação quando escreveu outro artigo para a mesma revista em 1997. Sua descrição de guerra de informação continha elementos da ciência militar soviética/russa, relativos à natureza, às formas, aos níveis, às

diferenças, às características e aos princípios da guerra de informação. Considerou como formas da guerra de informação o tempo de paz, as crises e o período da guerra; sua natureza se reflete nas operações ofensivas e defensivas; os níveis da G Info são o nacional, o estratégico, o tático e o do teatro; e as outras diferenças da G Info se encontram no âmbito do comando e controle, da inteligência, das operações eletrônicas-psicológicas, do espaço sideral, das atividades dos *hackers*, da realidade virtual, dos aspectos econômicos, da estratégia e da precisão. Enumerou as seguintes características da G Info: complexidade, objetivos limitados, curta duração, menos danos físicos, maior espaço de combate (em todas as suas dimensões) e menor densidade de tropas, transparência, intensa luta pela superioridade de informação, maior integração, maiores exigências para os comandantes, novos aspectos da concentração de forças e o fato de que o efetivo inimigo talvez não seja o objetivo principal. Determinou que os princípios da guerra de informação incluem a decapitação, ações cegantes, a transparência, a resposta rápida e a sobrevivência.[9]

As duas definições propostas por Wang refletem as duas possíveis percepções da G Info na China. A primeira definição baseia-se no prisma da teoria ocidental, e a segunda observa-se através da óptica da ciência militar soviética/russa, que foi empregada extensamente desde a década de 50 até o início dos anos 90. Em suas mais recentes conferências, Wang fala sobre "guerra de informatização", conceito muito empregado por Dai no seu artigo.[10]

O artigo *On Information Warfare Strategies* (Das estratégias da Guerra de Informação), escrito pelos *Major General* Niu Li, Coronel Li Jiangzhou e Major Xu Dehui do Instituto de Comando e Comunicações, foi publicado no mesmo número de abril 2000. Os autores definem estratagemas de G Info como "truques e métodos arquitetados e empregados por comandantes e órgãos de comando para conquistar e manter a supremacia da informação por meio do emprego de métodos engenhosos a fim de prevalecer a um custo relativamente baixo na G Info".[11] Os líderes chineses acreditam que é possível elaborar estratégias que permitam superar a sua inferioridade tecnológica mediante a combinação adequada do pensamento qualitativo do ser humano com os cálculos quantitativos facilitados por computadores. Os autores recomendam o planejamento de estratagemas baseados tanto no conhecimento humano como na tecnologia (isto é, aquisição e processamento de informação).

A combinação de estratagemas com tecnologia é vista de forma diferente por asiáticos e ocidentais. Os autores do referido artigo esclarecem que "Tradicionalmente, os povos orientais dão ênfase aos estratagemas enquanto os ocidentais enfatizam a tecnologia… Soldados ocidentais procuram uma solução tecnológica diante de um problema, enquanto os orientais pretendem conceber estratagemas para superar as suas deficiências tecnológicas sem mudar as condições tecnológicas imperantes. O tradicional pensamento oriental não é conducente ao desenvolvimento tecnológico, mas pode servir como um meio eficaz para descobrir uma forma de sobreviver em uma situação perigosa".[12] Estratagemas de G Info podem:

- Guiar o pensamento dos comandantes e forçá-los a cometer erros ao atacar os sistemas cognitivos e de crenças.
- Gerar intensa pressão psicológica pelo uso da intimidação para indicar a vitória inevitável diante da concentração das forças e a coordenação das redes de informação.
- Intimidar através da demonstração de suas capacidades.
- Adotar medidas ativas e eficazes para gerar surpresa, e empregar equipamento técnico e meios de guerra de informação decisivos.
- Desenvolver e ocultar "armas letais" de guerra de informação.
- Ocultar a realidade mediante a criação de uma realidade fictícia.
- Empregar fintas consecutiva ou simultaneamente.
- Empregar todos os meios da G Info para manter a supremacia.
- Pretender estar em conformidade com o inimigo.
- Dispersar vírus de computadores para contaminar o fluxo de informações.
- Controlar os elementos de tempo mediante a condução de iniciativas no âmbito da informação que tendam a "induzir", "dissimular", "encobrir", e "conter".[13]

Estas estratégias são planejadas para forçar o inimigo a cometer erros cognitivos e obrigá-lo a enfrentar uma ameaça multidimensional.

Estratégias nas Op Info e a Guerra Popular

No seu terceiro artigo publicado no número de abril de 2000 da referida revista — *Inovating and Developing Views on Information Operations* (Inovando e Desenvolvendo Visões das Operações de Informações) — Dai define uma operação de informações como uma "série de operações realizadas no ambiente de informações como condição básica do campo de batalha, com a informação militar e os sistemas de informações como objetivos operacionais diretos, e com a guerra eletrônica e as redes de computadores como meios principais".[14] Em virtude dessas operações colocarem à prova as aptidões dos partidos envolvidos, focalizando seus conhecimentos e estratégias, Dai recomenda "um enfoque nas estratégias".

Os avanços científicos e tecnológicos, têm dado às estratégias um novo campo de jogo. A estratégia pode ter diferentes conteúdos sob diferentes condições tecnológicas, cedendo ainda lugar para as estratégias

tradicionais e para as novas oriundas dos novos recursos tecnológicos. Entre as opções encontram-se novas estratégias de informações/enfrentamento, acrescentando aspectos estratégicos à tecnologia existente ou empregando estratégias que permitam aproveitar a tecnologia.[15] Se esta se manifesta em armas e equipamentos, então os sistemas de informações e até mesmo os elétrons podem chegar a ser um veículo para as estratégias. Uma boa estratégia pode "servir como um tipo de poder de combate invisível; pode substituir, até certo ponto, a insuficiência de materiais; pode diminuir uma disparidade tecnológica ou material entre um exército e seu inimigo; pode compensar ou a escassez de informação e de forças de combate ou uma inferioridade de meios para a condução das operações de informações".[16] Algumas dessas estratégias incluem:

- Interferir ou sabotar a informação ou o sistema de informações inimigo.
- Sabotar a estrutura do inimigo para a condução de operações de informações.
- Debilitar a capacidade de combate de informação inimiga.
- Dispersar as forças, armas e fogos do inimigo, concentrando-se ao mesmo tempo nas forças, armas e fogos de suas próprias unidades.
- Confundir e desviar o inimigo e criar para si uma excelente oportunidade de combate.
- Desviar as atividades de reconhecimento do inimigo e preparar-se adequadamente para o seu próprio reconhecimento.
- Transmitir ao inimigo uma falsa impressão enquanto lança um ataque de informação de surpresa contra ele.
- Cegar ou ensurdecer o inimigo por meio de falsas impressões.
- Confundir ou desorganizar o pensamento inimigo.
- Fazer o inimigo acreditar de que o verdadeiro é falso e vice-versa.
- Induzir o inimigo a tomar uma decisão errada ou realizar uma ação equivocada.[17]
- Futuras operações, segundo Dai, devem ser integradas. Por exemplo, deverão integrar-se os elementos civis e militares. Dai acredita que os sistemas de informações oferecem maiores oportunidades para aumentar a quantidade de pessoas participantes nas operações de informações para servirem como uma importante força auxiliar de combate de informação em uma futura guerra de informação.[18] Integrar especialistas civis e militares revitalizará a teoria da guerra popular elaborada pelo General Mão Zedong. Especialista em guerra de

informação, o General Wang Pufeng observou pela primeira vez estas condições em 1955.[19]

Composta por 1.5 milhão de soldados, a força de reserva da China passou a ser um campo fértil para a idéia de unir a guerra popular com a G Info. Várias forças de reserva já foram formadas nas cidades de Datong, Xiamen, Shanghai, Echeng e Xian, sendo que cada uma está aperfeiçoando a sua própria especialidade. Por exemplo, as forças de reserva em Shanghai concentram seu trabalho em redes de telecomunicações sem fio e senhas criptografadas duplas.

O artigo* On Information Warfare Strategies *(Das estratégias da Guerra de Informação), escrito pelos* Major General *Niu Li, Coronel Li Jiangzhou e Major Xu Dehui do Instituto de Comando e Comunicações [explicam que] . . . A combinação de estratagemas com tecnologia é vista de forma diferente por asiáticos e ocidentais. Os autores do referido artigo esclarecem que "Tradicionalmente, os povos orientais dão ênfase aos estratagemas enquanto os ocidentais enfatizam a tecnologia…Soldados ocidentais procuram uma solução tecnológica diante de um problema, enquanto os orientais pretendem conceber estratagemas para superar as suas deficiências tecnológicas sem mudar as condições tecnológicas imperantes. O tradicional pensamento oriental não é conducente ao desenvolvimento tecnológico, mas pode servir como um meio eficaz para descobrir uma forma de sobreviver em uma situação perigosa".

Em Xian, o Departamento das Forças Armadas Populares supostamente está formulando várias estratégias baseadas na idéia de Dai, para transformar a luz, o som e os meios eletrônicos em ferramentas estratégicas. Em um exercício realizado no distrito militar na província de Jilin (Região Militar de Shenyang) foram empregadas algumas *Feuduis* (divisões) especializadas em guerra eletrônica em função da força adversária. Desta experiência foram derivados dez métodos para a condução das Op Info, os quais também podem ser considerados como estratégias eletrônicas, a saber:

- Lançar minas de informações.
- Conduzir reconhecimento de informações.
- Mudar os dados na rede.
- Lançar "bombas" de informação.
- Inundar o inimigo com informações inúteis.
- Disseminar propaganda.
- Realizar dissimulação de informação.
- Divulgar informação redundante.
- Organizar a defesa da informação.
- Estabelecer redes de estações de espionagem.[20]

Não se sabe ao certo, hoje em dia, se estas estratégias são empregadas ou não no reconhecimento externo dos sistemas de operações estrangeiros.

Um terceiro e significante meio de como a era da informação afetou a atitude da China em relação à guerra é que os seus 36 estratagemas podem encontrar novos significados e aplicações. Cerca de 300 anos atrás um desconhecido estudioso decidiu coletar e registrar os estratagemas chineses. Sua obra, *The Thirty-Six Stratagems: The Secret Art of War* (Os 36 Estratagemas: A Arte Secreta da Guerra) enfatiza a importância da dissimulação como arte militar capaz de atingir os objetivos militares.[21] Na atual era da informação, caracterizada por ataques anônimos e pela incerteza, o estratagema talvez seja revitalizado como uma tática capaz de facilitar aos próprios elementos como enganar ou infligir danos à percepção inimiga. A era da informação está se transformando na era do persuasor anônimo.

Também existem aqueles que discordam, argüindo que no mundo de alta tecnologia de hoje, esses antiquados estratagemas não mais são aplicáveis. Entretanto, apenas uma olhada aos primeiros cinco estratagemas é o sufuciente para concluir-se o contrário. O primeiro estratagema é "engane o imperador para poder atravessar o mar".[22] Fazer com que o inimigo diminua a sua vigilância deve ser um ato aberto, ocultando as verdadeiras intenções sob a aparência das atividades cotidianas. Uma aplicação da guerra eletrônica implicaria, por exemplo, no emprego dos serviços regulares de e-mail e de diversos elos na Internet para disfarçar a inserção de códigos maldosos ou de vírus. O segundo estratagema "sitiar Wei para resgatar Zhao", sugere que, quando o inimigo não pode ser vencido em um ataque direto, ataque alguma coisa de grande valor para ele. Na atualidade, guerra de informação significa que quando não é possível atacar um adversário com armas nucleares devido aos efeitos catastróficos que poderia causar à própria nação, então ataque com elétrons os servidores e as redes responsáveis por manter a estabilidade dos sistemas financeiros, elétricos e políticos do Ocidente. O terceiro estratagema "mate com uma espada emprestada" quer dizer: na ausência de meios para atacar o inimigo de forma direta, ataque empregando os recursos de outra potência. A aplicação da guerra de informação é simples, envie vírus ou

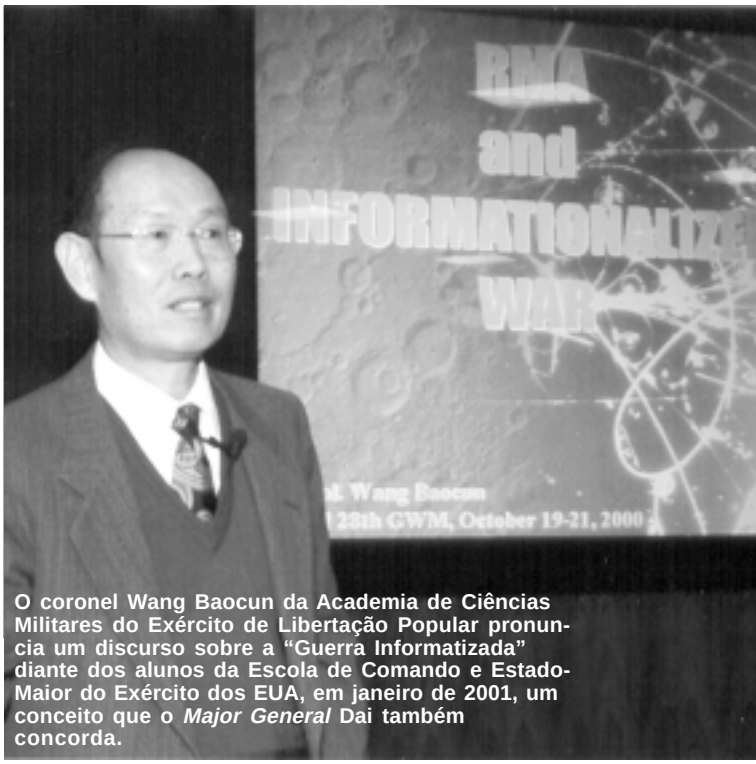
códigos nocivos através dos sistemas de computadores de outro partido ou de outro país.

O quarto estratagema diz: "espere com calma pelo inimigo exausto", a escolha do lugar e da hora para a batalha é uma vantagem. Induza o inimigo a gastar sua energia em buscas inúteis, enquanto conserva sua força. Quando o adversário estiver exausto e confuso ataque com toda a sua energia e resolução. Neste sentido, o emprego da guerra eletrônica gira em torno do emprego da teoria da guerra popular, isto é, realizar múltiplos ataques, guardando o ataque principal para o momento em que todas as equipes de resposta em caso de emergência dos computadores do Ocidente estejam engajadas. Finalmente, o quinto estratagema aconselha "roube uma casa em chamas": significando que quando um país está tumultuado por conflitos internos, não terá condições de atender as ameaças externas. Neste caso, o papel da guerra de informação é colocar *hackers* nos países ocidentais, disfarçados de alunos ou comerciantes com a missão de atacar desde o próprio país. Enquanto predomina o caos, estas pessoas deverão saquear os meios de informação.

A integração significa também o emprego da rede. O artigo publicado no jornal das FA chinesas de agosto de 2000, *PRC Army Pays Attention to the Role of Network Warfare* (O Exército da República Popular da China Presta atenção ao Papel da Guerra em Rede", uma guerra popular recebeu tanta atenção quanto a manipulação das redes eletrônicas. O autor afirmou que o jornal das Forças Armadas chinesas *Jiefangjun Bao* insiste sobre a necessidade de formular normas e regulamentos adequados para a mobilização e preparação para uma "guerra popular moderna", bem como a coleta e o processamento da informação; ações ofensivas e defensivas na Internet; e pesquisas e intercâmbios de tecnologia por meio de rede a fim de estabelecer normas para preparar e construir uma "guerra popular na rede".[23]

Obter superioridade de informação (Dai usa 32 vezes este termo, e se refere ao conceito "controle de informação" 11 vezes neste artigo) é crucial para empregar essas estratégias em uma guerra popular e implica em várias etapas. Primeiro, Dai afirma que forças profissionais (possivelmente o Exército de Libertação Popular) teriam de obter, transmitir e processar a informação sobre a guerra, interferindo ou sabotando simultaneamente a informação ou sistemas de informações inimigos. Forças não profissionais (talvez as da reserva) protegem alvos específicos dificultando a eficácia do poder de combate do adversário. Segundo, os meios de guerra eletrônica (desenhados para sabotar a capacidade de coleta e a transmissão de informação) e os meios de guerra das redes eletrônicas (desenhados para sabotar o processamento e o emprego da informação) devem ser combinados. Terceiro, os termos "suaves e duros" devem descrever tanto as forças como as operações ofensivas e defensivas.[24] A ofensiva inclui eletrônica, redes e outras unidades para destruir os sistemas eletrônicos inimigos; a defesa consiste em unidades de telecomunicações, reconhecimento técnico, de radar e outras. Quarto, operações integradas, conjuntas e multidimensionais devem cobrir terra, ar e espaço.[25]

Dai afirma que para competir pela superioridade de informação é necessário ver as operações de informações como uma "ofensiva ativa". Este ponto de vista parece contradizer a perspectiva apresentada subseqüentemente pelo



O coronel Wang Baocun da Academia de Ciências Militares do Exército de Libertação Popular pronuncia um discurso sobre a "Guerra Informatizada" diante dos alunos da Escola de Comando e Estado-Maior do Exército dos EUA, em janeiro de 2001, um conceito que o *Major General* Dai também concorda.

Os autores definem estratagemas de G Info como "truques e métodos arquitetados e empregados por comandantes e órgãos de comando para conquistar e manter a supremacia da informação por meio do emprego de métodos engenhosos a fim de prevalecer a um custo relativamente baixo na G Info". Os líderes chineses acreditam que é possível elaborar estratégias que permitam superar a sua inferioridade tecnológica mediante a combinação adequada do pensamento qualitativo do ser humano com os cálculos quantitativos facilitados por computadores.

White Paper da China que enfatizava a aderência chinesa a uma postura de defesa ativa. No entanto, Dai esclarece que para uma defesa ser positiva, tem de ser uma "defesa baseada em uma ofensiva ativa", enquanto uma defesa baseada na informação negativa será passiva.

A principal conclusão retirada de uma análise sobre os estratagemas de guerra de informação chinesa é que a estratégia, a arte militar e a ciência da condução de campanhas em uma ampla escala, têm passado por um processo de transformação. As concentrações de forças serão substituídas pela eficácia de assaltos lançados com informação e energia, ao mesmo tempo que as linhas de frente e da retaguarda serão indistintas. As operações deixarão de enfatizar o poder de fogo para destacar as atividades de detecção, encobrimento, busca e fuga, fazendo que o combate de grande alcance substitua o combate corpo a corpo. Um aspecto central será o combate pela supremacia das redes eletrônicas, a qual será indispensável para vencer concomitantemente nos níveis estratégico e tático.

Este jogo de palavras parece ser feito para manter uma ofensiva de informação ativa de acordo com o *White Paper*.[26] Neste sentido Dai recomenda o modelo de resposta ativa empregado pelos sérvios em Kosovo, em vez do modelo iraquiano, usado durante a Guerra do Golfo, que aguardava passivamente o próximo passo da coalizão.

Outras Estratégias de Informação

Um artigo publicado em 1966 menciona que a tecnologia da informação é o cerne e o fundamento da revolução militar. Informação e conhecimento mudaram o método anteriormente empregado para medir a potência militar, que anteriormente era calculada após a contagem de divisões blindadas, esquadrilhas da força aérea e os grupos de porta-aviões. Forças invisíveis devem ser incluídas no cálculo da correlação de forças na atualidade. Estas incluem:

- Capacidade de computação, incluindo rendimento total.
- Volume/capacidade de comunicações.
- Confiabilidade do sistema.
- Capacidade dos sistemas de reconhecimento.[27]
- Cada elemento pode afetar a estratégia de informação empregada pelos ou contra os adversários. Estas estratégias também possuem alcance global, são capazes de transmitir dados à velocidade da luz e conseguem a completa integração dos meios.

Conhecimento e fatores psicológicos também devem ser avaliados como componentes da correlação das forças. A guerra de conhecimento acarreta calcular as mudanças significativas das populações, armas e dos sistemas militares. O impacto de uma disparidade de conhecimento foi óbvio entre os soldados norte-americanos e os iraquianos da Guerra do Golfo Pérsico. O sistema de armas da mais alta tecnologia empregado pela Coalizão teria sido praticamente inútil para os soldados iraquianos, muitos dos quais eram analfabetos. A guerra do futuro, caracterizada por uma competição do estilo jogo de xadrez e pelo conhecimento de alta tecnologia integrados nos circuitos de armas, será "dirigida por oficiais possuidores de mestrado, comandada por alunos universitários e conduzidos por peritos". Além disso, a transformação do conhecimento em sistemas de armas irá ocorrer com mais rapidez. Ocorrerão melhoras quanto à capacidade no emprego de redes, à automatização e sistemas que funcionem em tempo real empregados em operações de alerta, controle e orientação, reconhecimento e ataque, capacitando os sistemas de armas a identificar, diferenciar e analisar automaticamente os alvos. Sistemas militares irão substituir quantidade e escala por qualidade e eficácia.[28] Guerra de conhecimento inclui também o desenvolvimento de estratégias superiores baseadas em um conhecimento superior.

A principal conclusão retirada de uma análise sobre os estratagemas de guerra de informação chinesa é que a estratégia, a arte militar e a ciência da condução de campanhas em uma ampla escala, têm passado por um processo de transformação. As concentrações de forças serão substituídas pela eficácia de assaltos lançados com informação e energia, ao mesmo tempo que as linhas de frente e da retaguarda serão indistintas. As operações deixarão de enfatizar o poder de fogo para destacar as atividades de detecção, encobrimento, busca e fuga, fazendo que o combate de grande alcance substitua o combate corpo a corpo. Um aspecto central será o combate pela supremacia das redes eletrônicas, a qual será indispensável para vencer concomitantemente nos níveis estratégico e tático.

Em um avanço revolucionário, será possível desdobrar "nuvens" de elétrons para incapacitar e destruir países inteiros (normalmente mediante a destruição econômica, mas também por meio de ataques de informação/psicológicos), em lugar de comprometer as grandes forças antes requeridas para alcançar o mesmo fim. Os elé-

trons e as tecnologias da informação são as novas formações das forças armadas do século XXI na China e em outros países. Os elétrons em combate exigem um enfoque na eficácia operacional no lugar de uma concentração da potência militar. Segundo alguns analistas de assuntos chineses, o desenvolvimento de sistemas capazes de efetuar a destruição "suave" do inimigo (por meio da finta ou da interrupção de sinais) assumirá tanta importância como o poder de fogo. O Ocidente deverá estudar o Oriente para explicar esses estratagemas. Assim como observam os próprios chineses, eles dedicam mais tempo que seus homólogos ocidentais ao pensamento estratégico.

Poucas áreas de destaque apóiam estas estratégias. Elas incluem novos critérios para calcular a correlação de forças e a nova ênfase nos fatores cognitivos, especialmente psicológicos. Para a China, a revolução no campo da informação revitalizou uma estratégia antiga porém oportuna: a guerra popular. O país pode unificar-se em torno deste conceito, incluindo suas forças de reserva e qualquer pessoa que possua um computador portátil. Para os observadores ocidentais, já é hora de estudar minuciosamente estas mudanças e resolver adaptar algumas para nossa forma de conduzir a guerra de informação. ***MR***

REFERÊNCIAS

1. Qingmin Dai, "Innovating and Developing Views on Information Operations," Beijing *Zhongguo Junshi Kexue*, (20 de agosto de 2000) pp. 72-77. Traduzido e obtido do *Foreign Broadcast Information Service —FBIS —* (Serviço de Informação e Transmissões Estrangeiras), 9 de novembro de 2000,
http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm

2. O Relatório ao Congresso Conforme a Ata de Autorização da Defesa Nacional do Ano Fiscal 2000, www.defenselink.mil/news/Jun2000/china06222000.htm.

3. Zhang Fuyou, "With Joint Efforts Made by Army and People, Military Telecommunications Makes Leap Forward," *Beijing Jiefangjun Bao*, 9 de setembro de 2000. Traduzido e *downloaded* do Serviço de Informação de Transmissões Estrangeiras, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm

4. *Ibid.*

5. Relatório ao Congresso.

6. Wei Kaqing, "On the Sudden Emergence of Military Websites," Beijing *Zhongguo Guofang Bao*, 6 de novembro de 2000, p. 4. Traduzido e *downloaded* do Serviço de Informação de Transmissões Estrangeiras (14 de dezembro de 2000) http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

7. Beijing, *The Associated Press*, 8 de janeiro de 2001.

8. Wang Baocun, "The Current Revolution in Military Affairs and its Impact on Asia-Pacific Security," *China Military Science*, abril de 2000, p. 139.

9. Baocun, "A Preliminary Analysis of IW," Beijing *Zhongguo Junshi Kexue*, 20 de novembro de 1997, pp. 102-11. Traduzido e *downloaded* do Serviço de Informação de Transmissões Estrangeiras, http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

10. *Ibid.*

11. Niu Li, Li Jiangzhou, and Xu Dehui, "On Information Warfare Stratagems," Beijing *Zhongguo Junshi Kexue*, 12 de janeiro de 2001, pp. 115-22. Traduzido e *downloaded* do Serviço de Informação de Transmissões Estrangeiras http://sun3.lib/uci.Edu/~slca/microform/resources/f-g /f_049.htm.

12. *Ibid.*

13. *Ibid.*

14. Dai, "Innovating and Developing Views on Information Operations."

15. *Ibid.*

16. *Ibid.*

17. *Ibid.*

18. *Ibid.*

19. Wang Pufeng, "Meeting the Challenge of Information Warfare," *Zhongguo Junshi Kexue* (*China Military Science*), 20 de fevereiro de 1995, pp. 8-18. Traduzido e disseminado no Serviço de Informação de Transmissões Estrangeiras, FBIS-CHI-95-129, 6 de julho de 1995, pp. 29 30.

20. *Xianjin Bao*, 10 de dezembro de 1999, enviado por e-mail para o autor pelo Sr. William Belk.

21. Wang Xuanming, *The Thirty-Six Strategems: The Secret Art of War* (China Books and Periodicals, dezembro de 1992).

22. Estas estratégias e seu significado foram obtidas no endereço http://www.chinastrategies.com; a interpretação desde a perspectiva da era da informação é do autor.

23. "PRC Army Pays Attention to the Role of Network Warfare," Hong Kong *Zhongguo Tonnxun She*, 6 de agosto de 2000, traduzido e obtido do Serviço de Informação de Transmissões Estrangeiras http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

24. Dai. "Suave" significa sabotagem ou destruição temporária, empregando técnicas tais como a interferência eletrônica, ataques de vírus, infiltração nas redes, bombas de fibras carbonizadas, ataques da realidade virtual e ataques psicológicos. "Duro" se refere às ações de sabotagem permanente, debilitamento da capacidade de luta total de um adversário e inclui armas convencionais, ataques com forças para sabotar, ataques com pulsos eletromagnéticos e ataques com armas inteligentes.

25. *Ibid.*

26. *Ibid.*

27. Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," *Kuang Chiao Ching*, 16 de janeiro de 1996, pp. 22, 23. Traduzido e *downloaded* do Serviço de Informação de Transmissões Estrangeiras FBIS-CHI-96-035, 21 de fevereiro de 1996, pp. 33, 34.

28. Jia Xi and Shi Hongju, "Analysis on Key Elements of Knowledge Warfare," Beijing *Jiefangjun Bao*, 18 de setembro de 2000. Traduzido e *downloaded* do Serviço de Informação de Transmissões Estrangeiras http://sun3.lib/uci.edu/~slca/microform/resources/f-g/f_049.htm.

O Tenente-Coronel (Res) Timothy L. Thomas é analista no Escritório de Estudos Militares Estrangeiros, no Forte Leavenworth, em Kansas, servindo também como professor adjunto no Instituto Europeu-Asiático do Exército dos EUA, localizado em Garmisch, Alemanha. Recebeu o título de Bacharel em Ciências pela Academia Militar do Exército dos EUA, em West Point; o de Mestre em Artes pela University of Southern California*, e é graduado da Escola de Comando e Estado-Maior do Exército dos EUA e do Instituto Russo do Exército norte-americano. Serviu em várias posições de comando e estado-maior no território continental dos EUA e na Europa. Dentre elas foi Diretor do Departamento de Estudos Soviéticos do Instituto Russo do Exército dos EUA, em Garmisch; inspetor das operações táticas soviéticas na Conferência de Segurança de Cooperação na Europa, no Instituto Europeu-Asiático em Garmisch, Alemanha; e S2 da 2ª Bda e comandante da Companhia C, 313º Batalhão de Inteligência Militar, 82ª Divisão de Pára-quedistas, Forte Bragg, Carolina do Norte. É editor assistente da revista* European Security*. Seu artigo "Grozny 2000: Urban Combat Lessons Learned" foi publicado no número de julho-agosto de 2000 da* Military Review*, edição em inglês.*