

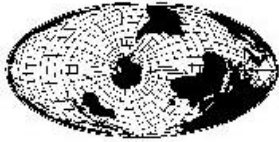
Escola Superior de Geopolítica e Estratégia
Mantenedora: Organização para Estudos Científicos (OEC)

CIBERGUERRA
GUERRA ELETRÔNICA E INFORMACIONAL
UM NOVO DESAFIO ESTRATÉGICO

Texto para Debate de 26/04/2001

Prof. Fernando G. Sampaio

Reitor da Escola Superior de Geopolítica e Estratégia
Presidente da O.E.C.
Professor de Pensamento Geopolítico e Estratégico
Cidadão Emérito de Porto Alegre.



Escola Superior de Geopolítica e Estratégia
Mantenedora: Organização para Estudos Científicos (OEC)

1. DEFINIÇÃO: O desafio que as sociedades dependentes de redes de computadores para suas atividades normais apresenta ao analista de estratégia é sua vulnerabilidade, que pode ser explorada por um inimigo, não necessariamente um país, que pode atacar as redes de comando e controle de uma imensa variedade de serviços públicos, até o ponto de criar o caos e implantar um tal grau de desmoralização, que um país, assim atacado, se desintegre, moral, psicologicamente e, até, fisicamente. A questão de definir, então, que nova modalidade de ameaça de guerra – ao mesmo tempo não-guerra – é imperiosa.

Existem os que falam na guerra eletrônica e na guerra informacional, mas preferimos abranger uma totalidade de ações dentro de duas concepções que nos parecem não só mais abrangentes, mas igualmente mais precisas. Tais conceitos são:

1- CIBERGUERRA – a idéia de Guerra Cibernética ou, mais comumente, Ciberguerra, tem suas origens na própria definição e conceito da técnica cibernética. Com efeito, a palavra tem uma origem grega, *kybernetiké* e significa a arte de controle, exercida pelo piloto sobre o navio e sua rota. Aquele que pilota é aquele que comanda e comanda exercendo o controle. Foi este o conceito que Norbert Wiener introduziu ao final da década de 40, quando lançou o famoso “Cibernética ou controle e comunicação no animal e na máquina” (1948).

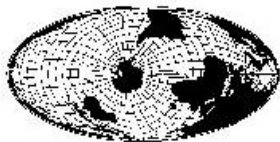
Quer nos parecer que o conceito embutido em Ciberguerra diz tudo o que tal tipo de desencadeamento de conflito pode acarretar.

De fato, Wiener afirmava:

Decidimos denominar todo o reino da teoria do comando e da transmissão de informações, quer seja em máquinas ou em seres vivos, de cibernética que tomamos da palavra grega para timoneiro.” interrogado sobre sua definição, no Simpósio sobre Cibernética do Sistema Nervoso, realizado pela Academia de Ciências da Holanda, em Amsterdã, em 1962, ele foi bem preciso sobre o que queria significar com sua teoria:

“a cibernética não se ocupa primordialmente nem de organismos nem de produtos técnicos, mas sim daquilo que é comum a ambos, ou seja, a cibernética se centraliza não na eletrotécnica, mas no conceito mais fundamental da informação, quer ela seja transmitida por meios elétricos, mecânicos ou nervosos.”

E, sendo a cibernética a arte de comandar ou controlar, sua forma primordial de



agir é pelo comando ou controle de todo o ciclo de informações.

Assim, a Ciberguerra não é apenas guerra eletrônica ou guerra de informações, mas abrange, pelo que podemos deduzir de nossas observações, as operações de guerra psicológica, a teoria da mentira, o terrorismo seletivo ou generalizado, a manipulação do sistema nervoso humano para a aplicação dosada do medo (psicologia do medo) e muitos outros campos do conhecimento humano, que podem ser utilizados para o domínio, fora das técnicas convencionais da arte da guerra, ou seja, pelo combate direto que visa a inutilização ou destruição de homens e instalações pelo emprego das forças armadas.

A Ciberguerra poderia, até, ser utilizada por forças armadas ou - como veremos - terceirizada sob direto comando do aparelho político de um Estado, sem utilização ou mobilização direta das forças armadas, ou, pelo menos, das forças armadas convencionais.

Isto nos leva a um segundo conceito, já proposto:

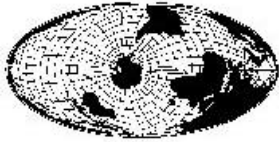
2- LEITENKRIEG - ou “guerra de controle”. Evidentemente, este conceito está baseado na idéia anterior da “Blitzkrieg”, que operava em outro tipo de guerra. Mas, essencialmente, a “blitzkrieg”, pela surpresa, ataques de aviação tática (com sirenes para semear o medo) e movimentação de tropas blindadas e mecanizadas, objetivava paralisar o adversário, penetrar em sua retaguarda e, por esta forma, adquirir o controle operacional, levando a vitória.

A Leitenkrieg, ou “guerra de controle” é o mesmo que ciberguerra, variando quanto ao uso de um vocábulo alemão.

Ambas as idéias, entretanto, estão relacionadas com um novo tipo de operação de guerra, que poderemos chamar de uma variante da “guerra total” de Liddendorff, já que se trata de atacar não só as forças armadas mas também os civis.

Talvez, até, a “ciberguerra” ou “leitenkrieg” sejam a forma de “guerra total” que pode vir a ser aplicada no século XXI, sendo que é evidente que o conceito abrange aquilo que os grandes teóricos da guerra, tanto Liddel Hart como Fuller entendiam como “paralisação estratégica”.

Podemos, pois, adiantar, que a Ciberguerra visa a paralisação de um adversário, no caso um país ou até um Bloco Econômico, ou Uma aliança militar, pela penetração



Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

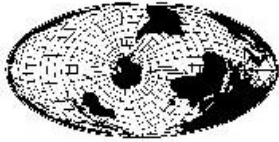
nas redes de computadores que dirigem a maioria das atividades vitais da economia, criando o caos e difundindo um estado de medo generalizado. Tal quadro permite o enfraquecimento das defesas convencionais, podendo-se, então, por técnicas de infiltração, atacar o país, bloco ou aliança, por meio de ações terroristas, boatos (difundidos por agentes infiltrados), notícias falsas veiculadas pelos meios de informação de massa e mesmo técnicas mais sofisticadas, umas em desenvolvimento, outras já utilizáveis, que destruiriam a coesão, a capacidade de resistência e levariam a um colapso total, que seria a paralisação estratégica, elevada, porém, a um potencial muito maior do que o previsto até hoje.

Colocado o ponto da definição, vejamos a questão dos alvos.

2. ALVOS DA CIBERGUERRA - naturalmente, os alvos da ciberguerra são os computadores, individualmente ou em redes. Trata-se de invadir os programas de controle de operações as mais diversas e, uma vez os mesmos penetrados, aguardar um momento propício para ativar a sabotagem.

Os alvos preferenciais para serem penetrados e desvirtuados são os programas de computadores que controlam ou gerenciam os seguintes aspectos:

- 1- comando das redes de distribuição de energia elétrica
- 2- comando das redes de distribuição de água potável
- 3- comando das redes de direção das estradas de ferro
- 4- comando das redes de direção do tráfego aéreo
- 5- comando das redes de informação de emergência:
 - a. pronto-socorro
 - b. polícia
 - c. bombeiros
- 6- comando das redes bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registrado em nome dos cidadãos (o potencial para o caos e a desmoralização de um país embutido neste tipo de ataque é por demais evidente)
- 7- comando das redes de comunicações em geral, em particular:
 - a. redes de estações de rádio



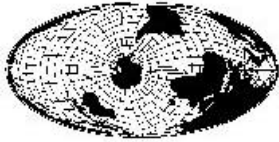
- b. redes de estações de televisão
- 8- comando dos “links” com sistemas de satélites artificiais:
 - a. fornecedores de sistemas telefônicos
 - b. fornecedores de sistemas de Sinais para TV
 - c. fornecedores de previsões de tempo
 - d. fornecedores de sistemas GPS
- 9- comandos das redes dos Ministérios da Defesa e, também:
 - a. Banco Central
 - b. Outros Ministérios Chave (Justiça, Interior)
- 10- comandos dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral

Podem existir outros alvos, que serão apontados/selecionados, pelos serviços de coleta de informações (inteligência), pelo estudo, por adidos militares, adidos de informações (outros) ou, ainda, agentes implantados no país sob outras coberturas (comércio, serviços, professorado, etc.).

As possibilidades são imensas, pois, cada vez mais, a própria complexidade e tamanho quer das atividades comerciais, dos governos e das populações, leva a uma dependência dos computadores, que armazenam informações que não estão mais disponíveis de outra forma. Muitos sistemas de comando e controle, civis, governamentais e mesmo, alguns militares já estão, inclusive, automatizados e em alguns casos, confia-se na velocidade de resposta do computador, muito acima da humana, para reagir a ataques que virão com antecipação de minutos ou até mesmo segundos, quando o homem não teria condições de dirigir o sistema de defesa. Os meios sofisticados e de alta velocidade e, mais recentemente, as técnicas ditas invisíveis (para o radar), tornam a dependência de sistemas automatizados de previsão de ataque/defesa, cada vez mais uma necessidade, o que é confiado a computadores. A penetração nestes sistemas pode inutilizar, portanto, toda uma estratégia de defesa e levar a rendição, pela total paralisia estratégica de um país, bloco ou aliança.

3. DESDOBRAMENTO DA QUESTÃO

Sabemos que a guerra de controle (leitenkrieg ou ciberwar) pode ser complementada pela utilização de ações terroristas, que podem ser:



Escola Superior de Geopolítica e Estratégia
Mantenedora: Organização para Estudos Científicos (OEC)

- 1- seletivas
- 2- generalizadas

e ainda, por ações de guerra política/psicológica, que também podem ser:

- 1- seletivas
- 2- geral

Vejamos como se desdobram estas questões, no cenário geral que estamos descrevendo:

Ações terroristas: as ações terroristas são muito antigas na história e foram utilizadas por governos com finalidade de domínio ou, pelo contrário, por grupos insatisfeitos, com a finalidade de derrubar governos. Não existe, entretanto, até agora, uma campanha organizada, de terror, com o objetivo de ganhar uma guerra, talvez, porque as condições para isto não existiam. A quantidade de terroristas que deveriam ser colocados no país-alvo seria muito grande, quase impossível atingir os alvos, pela própria organização do país. Entretanto, se desorganizarmos completamente tal país, ao nível da desmoralização e do caos, poucos terroristas, bem treinados, podem realizar estragos imensos, utilizando, para isto, as conhecidas táticas de golpes-de-estado. Assim, os alvos poderiam ser a liderança política, os principais agentes do Governo ou o que se chama de “alvos simbólicos” (por exemplo, o Palácio do Planalto foi tomado, dinamitado e está queimando). As ações terroristas poderiam, também, extrapolar e dirigir carros-bomba, por exemplo, contra filas de cidadãos que estão recebendo rações de emergência ou água potável, de unidades de serviços civis de emergência ou unidades militares. Neste caso, a própria aglomeração ou busca dos órgãos emergenciais para a situação de caos criada pelo ataque de “ciberguerra” seria inibida e os próprios mecanismos de ajuda governamental seriam totalmente ou quase anulados.

Guerra Psicológica: em casos de situações caóticas, com anulação dos serviços normais de notícias, os boatos se difundem facilmente, precisamente porque não existe mais a rede de comunicações conhecida e confiável. Poucos agentes e muitas maneiras de difusão são suficientes para fazer o caos se multiplicar a até fazer as multidões atacarem o que resta de seu próprio governo, forças de segurança e sistemas de emergência. Os casos de motins (riots) nas grandes cidades americanas, espoletados, por exemplo, pelo espancamento brutal de negros ou imigrantes (Los Angeles,



Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

recentemente) nos dão uma idéia do que seria um pânico criado por um ataque aos sistemas de comando/redes de controle gerenciadas por computadores. O próprio povo se encarregará de gerar seus próprios boatos e difundi-los, pois emergira, então, toda uma complexa teia de medos manias e estados até patológicos de indivíduos ou de grupos. Quanto maior, por exemplo, o conflito racial ou étnico, mais fácil será que explodam incontrolavelmente, nestas situações de desordem absoluta. Além disto, a guerra psicológica pode ser dirigida contra a elite, seja política, econômica, militar de um país, configurando, então, a velha técnica da “desinformação”, ou seja:

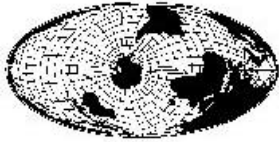
O objetivo da desinformação é levar a acreditar na veracidade da mensagem e, conseqüentemente, agir nos interesses da nação que conduz a operação de desinformação. Esta técnica pode ser utilizada através de boatos, falsificações políticas manipulatórias, agentes, de influência, organizações de fachada e outros meios. Tanto a elite governamental como não governamental podem compor o alvo.” (Desinformação,p. 185).

4. “STATUS” DO COMPUTADOR COMO ARMA - Naturalmente, tal estado de caos, que os analistas chamam de “paralisia estratégica”, vai ser obtido através do uso de computadores e de seus operadores, chamados, no jargão, hoje, de “hacker”. Embora, diga-se que os primeiros “hackers” eram aqueles considerados como peritos em computador de alta qualificação o termo é, agora, utilizado no sentido mais depreciativo e que esta de acordo com sua origem etimológica, pois, de fato “hack” significa despedaçar, cortar, estropiar e “hacker” é um sinônimo de ferramenta de corte ou, até, de machado.

Assim, temos duas questões, que já estão sendo abonadas pelos analistas de direito, com referência a este novo tipo de guerra:

- 1- podemos considerar um computador como uma “arma” ?
- 2- um “hacker” é um combatente e pode ser morto por possuir, simplesmente, tal “status” (ou aprisionado, ferido, etc)?

A primeira questão é, por um lado complexa e pelo outro lado, simples. Arma é tudo o que pode ser empregado com a finalidade de matar, ferir ou incapacitar as pessoas para o combate e/ou aquilo que danifica ou destrói objetos/propriedades. O



Escola Superior de Geopolítica e Estratégia
Mantenedora: Organização para Estudos Científicos (OEC)

computador, em si, não é, portanto, uma arma, mas o que ele pode “efetuar”, por sua possibilidade de “comunicação, comando e controle”, como diria Wiener (Cibernética) o coloca nesta categoria. E mais:

muito provavelmente e quase certamente, a ação de guerra por meio de computadores pode configurar uma utilização dos mesmos como arma de destruição de massas.

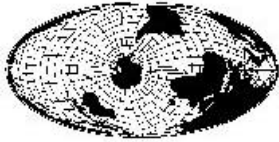
Em “Ciberdireito da IW: a questão legal da guerra de informação”, o major David J. DiCenso, da USAF comenta que “se uma nação hostil definir o ato de guerra baseada no dano causado ou no dano potencial (grifei, FGS), em vez de na natureza do instrumento usado para praticar o ato... se da operação IW (information war) resultar morte e destruição, provavelmente seria permitida uma resposta armada da nação-vítima... à luz das atuais leis de guerra e do direito internacional...” (p. 40).

E que dizer dos “hackers” ?

Na exposição sobre aspectos legais da guerra por computadores o já citado major DiCenso afirma: “se uma dessas pessoas (hacker) se envolvesse em um ato de hostilidade, esse indivíduo seria considerado um combatente ilegal e poderia ser punido pelas leis do captor. Os espões não recebem qualquer tratamento especial pelas leis da guerra e são punidos de acordo com as leis da nação que os captura” (normalmente, a morte desonrosa, FGS).

Os governos teriam que estudar, desde já, a criação de um “quadro de hackers”, comissionando soldados, sargentos ou oficiais “hackers” ou seus exércitos? Mas sendo estas atividades mais aproximadas das exercidas pelas agências de inteligência e sabotagem, que “status” concede-a eles? Forças especiais sob o comando de um órgão paralelo à estrutura militar (de comando) normal/padrão? Ou reconheceria o governo que o “hacker” é combatente regular e que, portanto, tal governo deseja realizar e está se preparando para a “leitkrieg”? Mas, isto não envolveria uma escalada? Uma resposta dos possíveis alvos/adversários e a preparação de ataques preventivos, no campo da “ciberwar” ou “leitkrieg”? Um cenário de conflito para o século XXI poderia, então, nos levar a um novo tipo de confrontação entre países, em que os primeiros disparos seriam eletrônicos?

Mas, como distinguir uma ação intencional, de ciberguerra, de um acidente, de um problema natural (manchas solares, p. ex.) ou de uma ação de um particular,



até mesmo, de um paranóico ?

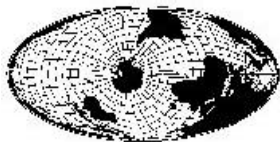
A necessidade de inteligência, monitoração e quadros altamente preparados se faz, portanto, mais do que nunca, necessários. Ainda assim, nada impedirá, no futuro, que o quadro de um acidente não sirva, se monitorado devidamente, como cobertura para o desencadeamento de ações de ciber guerra.

Marchamos, portanto, para um ambiente, de alta tecnologia e que implica em conhecer muito bem e em tempo real, tanto o comportamento do Sol, em seus ciclos explosivos, como as modas dos terroristas individuais, que atos estão praticando comumente e o que podem preparar. Assim, a infiltração contra-hackers se torna outra necessidade dos órgãos de governo, infiltração esta que deve ser autorizada por alguma medida judicial e ser centralizada em um só serviço de inteligência, sem o que de nada servirá, pela competição, dispersão e demora em reunir informações, que as diversas agências, historicamente, sempre apresentaram. A necessidade de contar com psicólogos comportamentais, sociólogos, peritos em computadores e planejadores de segurança/militares se apresenta como um impositivo imediato para os governos e a alta administração estratégico-político-militar.

Neste aspecto, países como os Estados Unidos, que contam com as instituições denominadas de “think tanks” (traduzido como “centrais de idéias”, na falta de melhor...) e com a tradição da criação de “forças tarefas interdisciplinares”, contam com imensa vantagem. Mas outros países, europeus, China, Japão, já copiaram estas idéias (ver “Centrais de idéias: a indústria e o comércio das idéias e sua enorme influência sobre os destinos humanos”, Paul Dickson, Melhoramentos, S.P. 1975).

5- DOCTRINA CHINESA EM FORMAÇÃO SOBRE LEITENKRIEG -

A recente operação militar chamada de “Guerra do Kosovo”, despertou a atenção da China para a necessidade de firmar-se na guerra de alta tecnologia, com vistas a poder concorrer com o poder americano, na área geopolítica chamada de “Anel do Pacífico”. Segundo informe do “Financial Times”, republicado pela “Gazeta Mercantil” SP, 5/5/99), o “Jornal do Exército de Libertação do Povo, em artigo bem detalhado, sugere a necessidade de uma capacitação militar de vasto alcance e enfatiza a necessidade de a China se preparar para uma guerra limitada sob condições de alta tecnologia... O artigo provavelmente representa o pensamento militar dominante e pode pressagiar uma



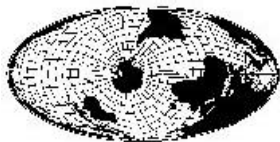
Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

mudança fundamental na estratégia. O artigo salienta que é insuficiente a pesquisa feita no campo do conflito armado contra ataques aéreos e ataques remotos de precisão lançados de uma determinada distância ou de uma distância maior... a China reconhece que pode ser atacada de forma abrangente, a partir de uma distância expressiva...”

Posteriormente, em novembro do ano passado (nov/2000), o Presidente Jiang Zemin, em reunião da APEC, precisamente a Associação de Comércio da área do Anel do Pacífico, realizada no Brunei, chamou a atenção para a necessidade da China e outros países menos desenvolvidos lutassem para superar o chamado “fosso digital” que os americanos dizem “the digital divide”). Num artigo escrito pelo Embaixador Amaury Porto de Oliveira, ex-representante brasileiro acreditado em Cingapura e publicado em Carta Internacional (Núcleo Política Internacional, USP, fev. 2001), comenta-se que a China está dando enorme ênfase ao domínio da tecnologia de fabricação dos computadores, desde os chips, fabricação de circuitos integrados e toda a parafernália ligada ao problema. Para tanto, ela abriu seu mercado para associação com firmas de alta tecnologia americanas, em especial a AT&T, Nortel, Alcatel e européias, como a Ericsson. O Ministério das Indústrias Eletrônicas criou, em associação com a IBM, uma poderosa firma, a Jitong e existem outras, que abriram a China para a Internet (estima-se que em 2002 serão 50 milhões os usuários da Internet na China. O Embaixador Oliveira chama a atenção para o fato de a China estar se adiantando para tomar a liderança no campo, em toda a Ásia, passando do Japão (pelas associações), e superando a Índia (cujo estrangulamento energético é o problema chave, o que não acontece com a China).

É interessante observar que já em 1997, dois analistas americanos, Richard Bernstein e Ross H. Munro, publicaram “The coming conflict with China” (A. Knopf. New York, 1997), onde predizem, claramente, que os dois países marcham para uma guerra, no decurso do próximo século (o atual século XXI), quando a China terá superado (por volta de 2020/2030), em Produto Bruto Interno o PIB dos EUA, a riqueza produzida na América, embora ainda se mantenha um país com imensos bolsões de pobreza e até miséria. Mas, seus nichos de excelência serão perigosos para a hegemonia americana pretendida no Anel do Pacífico, área da qual já conseguiram expulsar, como poder, a Rússia.

É em tal contexto que devemos entender o recente artigo divulgado pela nossa



Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

rede eletrônica Defesa Net, segundo a qual, a China revisa totalmente sua estratégia militar, para pode derrotar os EUA, em caso de guerra, por uma doutrina de “ciberwar”, em sua amplitude total, como vimos analisando aqui.

Segundo o livro “Guerra Irrestrita”, escrito em 1999 e de autoria dos coronéis Qiao Liang e Wang Xiangsi (versão em inglês, feita pela CIA será publicada em Defesa Net - www.defesanet.com.br), propõem uma “ guerra assimétrica”, o que é, nada mais nada menos, do que a antiga idéia da “paralisia estratégica”.

Eles dizem, em síntese que:

- 1- a guerra assimétrica não tem regras; nada é proibido
- 2- deve-se atacar as redes de computadores americanas
- 3- deve-se recorrer a sabotagem econômica, não só via redes de computadores, mas, também, por que não matar George Soros ?
- 4- deve-se financiar, secretamente, com fundos, grupos políticos nos EUA, para influenciar atitudes/opiniões
- 5- incentivar/utilizar a guerra urbana nos EUA
- 6- espalhar rumores e escândalos, que criem tumulto nos EUA
- 7- utilizar o terror puro e citam o caso do ataque com gás ao metrô de Tóquio, pela Seita Aum Shinri Kyo (agente sarin)
- 8- Pequim pode vender armas de destruição de massas para países que apoiem o terrorismo (exemplo citado o caso Bin Laden)
- 9- o livro afirma, ao final, que melhor é controlar do que matar, mas tal controle só seria obtido por uma situação em que haveria uma morte em massa de cidadãos do país atacado

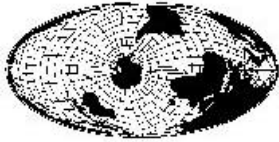
Existem muitas outras considerações, mas isto é suficiente para mostrar que a perspectiva de uma ciberguerra, pela paralisia estratégica é algo que já está em estudos e, quem sabe, em andamento.

6. O QUE É A PARALISIA ESTRATÉGICA

ESGE – Fone/FAX: 51 343-1927

E-Mail: esge@defesanet.com.br

Caixa Postal nº 8006 – Ag. Aeroporto – CEP 90.210-970



Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

O estrategista deve pensar em termos de paralisar, não destruir, ensinava Basil Lidell Hart em seu “Estratégia” (Biblioteca do Exército, Rio de Janeiro, 1966, p. 413 e seguintes).

A paralisia estratégica, como pensada originalmente, seria exercida pelo poder aéreo estratégico, que cortaria as comunicações, fornecimento de matérias primas e fábricas de componentes essenciais para a manutenção do país em estado de guerra.

Hoje, dizem os novos analistas, a ênfase passou da guerra econômica para a guerra de controle (Leitenkrieg, termo proposto no “think thank” Rand Corporation).

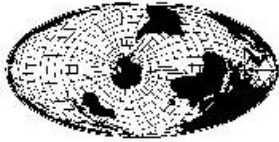
Atacar as vulnerabilidades do inimigo, ao invés de seus pontos fortes é a essência desta nova maneira de realizar a ‘paralisia estratégica’. Isto, em essência, é o que os chineses estão pregando. Resta saber se reagem a uma idéia americana ou se os americanos reagem a uma idéia chinesa. (o assunto recebeu grande tratamento em “A busca da paralisia estratégica pelo poder aéreo, T Cel. David S. Fadok, USAF, in “Aerospace Power Journal, 1º trimestre, 2001, p. 23 e seguintes)

O autor, depois de referir aos conceitos de Clausewitz, remanejados por Lidell Hart e por Fuller (ver “A conduta da guerra de 1789 aos nossos dias”, Jonh Frederick Charles Fuller, Biblioteca do Exército, Rio de Janeiro, 1966, deve-se ler várias partes, mas chamo a atenção, em especial, para a aliança União Soviética -Estados Unidos, para enfrentar a China, no futuro... ver p.320), trata da guerra aérea atual, com “armas inteligentes”.

O ponto central da paralisia estratégica consiste em reconhecer claramente que a força física de um exército está em sua organização, que é controlada pelo seu centro cerebral. Paralisando tal centro, paralisa-se o funcionamento do todo. O exército, a defesa, torna-se inarticulada e não cumpre sua finalidade, ainda que não tenha sido destruída.

O mesmo se aplicaria, na questão da ciberguerra, quanto ao problema do ataque às redes de computadores e seus programas, que seriam subvertidos ou anulados.

Um país inteiro e não só a defesa deixaria de funcionar. Para tanto, os autores da aproximação pela paralisia estratégica desenvolvem um esquema em que se visualiza um país como um alvo, que denominam de cinco anéis estratégicos de Warden (coronel John Warden, planejador estratégico da Guerra do Golfo). Deve-se atacar a liderança, os elementos orgânicos essenciais, a infra-estrutura e a população e, finalmente, as forças



Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

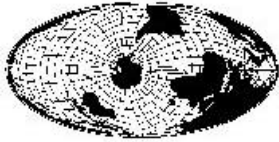
militares desdobradas.

Deve-se procurar atacar, sempre, o centro em cada anel de poder estratégico, isto é, por exemplo, diretamente o Quartel Geral de Comando, os Centros principais de comunicações, etc. O objetivo é mostrar uma superioridade tal que a mente da liderança inimiga veja que a resistência inútil e então, se dando a paralisia total ou parcial, a leve a uma mudança em seu sistema, que é o que desejamos, ao atacar. Já outro coronel e estrategista, John Boyd, faz uma análise bem mais complexa, com seu esquema dito OODA (observação, orientação, decisão, ação) e diz que os ataques devem ser de tal intensidade que o inimigo não poderá acompanhar a velocidade da ação do atacante, não podendo reagir com a precisão e o tempo necessários, acabará paralisado. Ele sustenta que a finalidade da destruição é atingir os centros de comando, visando a mente do comando inimigo, até que este entre em um estado de “stress”, o que provocará uma paralisia mental e, com isto se leve ao colapso moral e, assim, ao objetivo político desejado pelo atacante.

Ambos os esquemas, como podemos apreciar, se ajustam, perfeitamente ao ataque de ciberguerra, principalmente, se tal ataque seguir a estratégia preconizada pelos chineses, que é causar a maior desorganização possível, pelos ataques lançados contra as redes de computadores e, utilizando a confusão, atacar por formas de “não-guerra”, isto é, terrorismo, guerrilha urbana incentivada, sabotagens, boatos e desinformação em geral e, até mesmo, assassinatos políticos seletivos.

Os chineses utilizam, aqui, os ensinamentos de Sun Tzu (A arte da guerra, Publicações Europa-América, Lisboa, 1967... v. p. 61 – “dominar o inimigo sem o combater, isso, sim, é o cúmulo da habilidade”, Sun Tzu quer aqui dizer, sem travar batalhas e os chineses querem dizer, sem travar uma guerra convencional, atualmente).

Invocam, os coronéis chineses, também, os ensinamentos de Mao Tsé-tung, que em seu “Escritos Militares Seleccionados” (Edições em Língua Estrangeira, versão em inglês, Pequim, 1963, p. 187 e seguintes) propõe, em maio de 1938 a “guerra prolongada”, isto é, voltada para dentro ou, ainda, fazendo os golpes do adversário voltarem-se contra si próprio. Diz Mao Tsé-tung; “o inimigo é forte e nós somos fracos e o perigo da derrota reside aí (na fraqueza). Mas, em outros aspectos o inimigo tem limitações e nós temos vantagens. As vantagens inimigas podem ser reduzidas e suas limitações agravadas pelos nossos esforços. Por outro lado, nossas vantagens podem



ser melhoradas e nossas desvantagens remediadas pelos nossos esforços. Assim nos podemos caminhar para uma vitória final... quando o inimigo será derrotado por não poder segurar o colapso da totalidade de seu sistema imperialista” (p.208).

Observamos que Sun Tzu confiava nos espões e nas ações de guerra psicológica e Mao Tsé-tung confiava em desequilibrar o adversário, travando batalha quando ele era fraco e os chineses fortes, visando, com isto, uma desmoralização crescente do poder Imperial Japonês. Ambos jogavam, portanto, com o fator guerra psicológica, em abordagens diversas. Este é o ponto central da ciberguerra, como veremos.

7. GUERRA PSICOLÓGICA – A guerra de controle (Leitenkrieg) ou ciberwar, pelas suas ações, e uma modalidade de guerra total, como preconizada por Lundenorff, em seu “Guerra Total” (Berlim, 1935, referida em “Ludendorff”, D.J. Goodspeed, Biblioteca do Exército, Rio de Janeiro, 1968, p. 328) e tem o seu quê de insano. Lundenorff dizia “a guerra é a mais alta expressão da vontade de viver de uma nacionalidade e por isso a política deve ser belicista”.

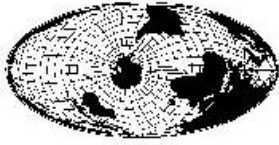
Ora, ao atacarem as engrenagens civis-administrativas-políticas e financeiras de uma nação, os contendores levam a guerra a sua mais alta expressão não só da vontade de viver, mas também de aniquilar, completamente o adversário.

O medo é o que vai se instalar no país atacado pela guerra de controle e como seria isto?

Em primeiro seria algo generalizado, mas depois iria até o pânico total. Basta imaginar o que seria chegar ao caixa do banco e ser informado que não existe nenhum dinheiro em seu nome. Aliás, nem o seu nome consta mais como depositário... O que fariam as multidões?

A “Psicologia do medo” (Mario Gonçalves Viana, Editorial D. Barreira, Porto, sem data) já nos ensina que o fenômeno pode ser dividido em várias gradações:

- 1 - susto
- 2 - temor
- 3 - receio
- MEDO 4 - pavor
- 5 - terror
- 6 - terror pânico



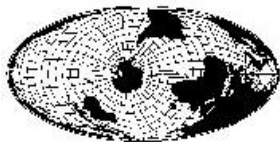
- 1 - o susto é um medo com sobressalto, oriundo do qualquer perigo ou ameaça imprevista, que logo desaparece;
- 2 - o temor já é uma predisposição para o receio, uma espécie de medo constante, que deixa a pessoa apreensiva;
- 3 - o receio já chega ao estado de dúvida, gerando incerteza, quanto ao melhor rumo a seguir ou um sentimento de perplexidade sobre as conseqüências de um fato
- 4 - no caso do pavor já temos uma combinação de temor com espanto e sobressalto, mas tem, ainda, uma duração limitada ao tempo em que os fatos determinantes ocorrem;
- 5 - finalmente, se chega ao terror que é um estado muito mais intenso que o pavor e de duração muito prolongada, não desaparecendo facilmente e podendo provocar paralisia e até morte;
- 6 - finalmente, o terror pânico é aplicado mais aos problemas que atingem toda uma população, que reage de forma desordenada, irracional e tende aos motins generalizados, com saques, linchamentos, estupros, assassinatos sem causa (boatos, desconfiança, preconceitos)!

É um estado lamentável que se quer ver chegar o povo de um país atacado por ciberguerra. Até o ponto do descontrole total, aquele chamado da “descarga”: “fala-se, freqüentemente, a respeito do impulso para a destruição da massa; esta é a primeira de suas características, que salta aos olhos, em todos os países e dentro das mais variadas culturas. Apesar de se tratar de uma realidade comprovável e geralmente desaprovada, ela jamais chega a ser satisfatoriamente explicada... a destruição de casas e coisas... a descarga se consumou através deste ato... (Elias Canetti, Massa e Poder, Melhoramentos, SP, 1983, p. 16 e seguintes: “impulso de destruição”).

É bom chamar a atenção para tais aspectos, ou seja, que a forma mais moderna, hiper-moderna, sofisticada, eletrônica, em tempo real, via satélites, pode reduzir as sociedades a bandos ou multidões se matando, chacinando, destruindo.

Em tais condições como reagir? Que governo resistiria? Mas ele não poderia revidar, enviando mísseis com armas nucleares contra o país atacante?

8. A CIBER-CRIMINALIDADE – Alguns teóricos e os chineses estão nesta categoria,



Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

preconizam utilizar redes de ciber-criminosos, ou seja, “hackers” que podem estar, já, trabalhando para o crime internacional organizado, seja no tráfico de drogas, de armas, de prostituição, de elementos proibidos (urânio, plutônio, princípios ativos venenosos para gases, material sensível como vírus, bactérias, etc). Neste caso, a guerra de domínio seria “terceirizada”, isto é, mesmo o melhor rastreamento não levaria ao país que, realmente, deu a ordem de ataque.

A entrada de motins de rua, a exploração de fricções raciais ou étnicas dentro da sociedade, pela exploração por agentes plantados, boatos e desinformação, levaria o caos urbano (guerrilha urbana), mas os elementos em luta seriam locais e seria difícil dizer que a ordem veio de fora.

Por isto mesmo, durante a Reunião do G-8 realizada em Paris, em maio de 2000 abordou a questão: “pela primeira vez numa instância multilateral, os representantes dos países desenvolvidos, juntamente com as indústrias mais importantes do setor, abordaram este problema, tendo como pano de fundo projetos de luta contra a ciber-criminalidade, sendo que a França está fazendo adaptações em seu direito penal para enquadrar o crime cibernético. Foi acrescentada às prioridades da União Europeia a chamada “e-Europa” e Paris se ofereceu para sediar um “Escritório Central” para combater a ciber-criminalidade” (Label France, out/2000, p. 19 – revista de informação da Embaixada Francesa)

Na ciberguerra não há linha de frente, não há definições precisas e o próprio conceito de guerra adquire um significado totalmente distinto.

Que fariam os Estados Unidos, se a ciberwar contra eles fosse terceirizada?

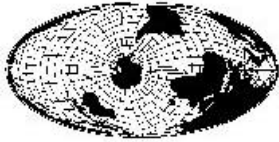
Atacariam todos os países suspeitos?

Acima de tudo, como controlariam sua própria população?

É evidente que esta situação levaria ao caos, ou seja, aquele ponto crítico, na teoria do caos, em que um sistema ordenado entra em colapso e a ordem desaparece, para restar um estado que podemos chamar de anomia. É este o ambiente do que se chama guerra de informação estratégica ou, mais abrangentemente, Leitenkrieg ou Ciberwar.

9. COMO AFETARIA ISTO O BRASIL?

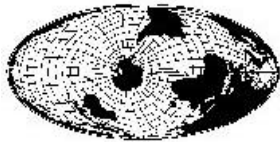
Quero propor aqui, antes de finalizar, uma reflexão-chave, algo que me parece



Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

essencial, diante deste quadro assustador. Se participarmos da ALCA, terminaremos por ser sócios e aliados preferenciais dos Estados Unidos, peça essencial no comando e integração das Américas. O Brasil, sem dúvida, será o líder e terá o papel básico de estabilidade na América do Sul, à frente dos demais Estados Associados da América do Sul. Não seríamos considerados uma espécie do calcanhar de Aquiles ou alvo prioritário para uma guerra periférica, numa linha de Ação Estratégica Indireta? Isto, não poderiam os inimigos dos Estados Unidos, para se verem livres de uma retaliação (até enlouquecida!) capazes de atacar o Brasil? Não seria criar dificuldades objetivas para os EUA, no quadro da ALCA, que deve estar terminado em 2021, atacar por ciberguerra o Brasil? O futuro pode nos reservar ainda maior vulnerabilidade, por associação ou aliança com os americanos. Nossa posição simplesmente como parceiros dos americanos (e o principal nas Américas com função vital), dentro da Área de Livre Comércio, pode acarretar um ataque desta natureza que acabe paralisando o funcionamento, pelo menos parcial, de toda a ALCA. Isto abre novas perspectivas para a análise estratégica, inclusive quanto a nossa percepção de quem podem ser nossos futuros adversários, numa guerra planetária. Nos diz, também, quais devem ser nossas ações defensivas: no plano territorial, evitar penetrações, em especial por organizações terroristas-guerrilheiras e narcotraficantes. No plano internacional, revisar a questão do Estado-Nação e das Multinacionais. Até que ponto o interesse estatal norte-americano pode ser, também o nosso interesse? Ou seja, as medidas de defesa dos sistemas de comando por computador de programas financeiros, redes energéticas, etc, que estão sendo poderosamente desenvolvidas pelos americanos devem ser algo prioritário para nos. Não temos a tecnologia nem os recursos, mas como no caso da 2ª Guerra, quando a liderança política decidiu que estava acima do interesse empresarial dotar o Brasil de uma usina de aço, nós muito bem podemos estar ao limiar de uma conjuntura similar. Até que ponto é do interesse, então, dos Estados Unidos, como Governo, pressionar na formação da ALCA para baixar a capacidade estratégica, tecnológica e de comando e controle do Brasil, sobre as nossas necessidades vitais e até que ponto tal enfraquecimento não se voltará, no futuro, contra a própria segurança, não só dos Estados Unidos, mas hemisférica?

Temos, assim, um novo cenário, em que os interesses do capital, em especial das grandes corporações multinacionais (mas com bandeira de origem norte-americana), podem estar pressionando, por seus grupos organizados de pressão, por



Escola Superior de Geopolítica e Estratégia
Mantenedora: Organização para Estudos Científicos (OEC)

obter vantagens que se revelarão, em futuro não muito distantes, verdadeiras armadilhas, pontos frágeis, no próprio sistema inter-americano (ALCA) que se quer organizar. Teremos que pensar em como nos dotarmos de maior autonomia estratégica, uma vez dentro da ALCA, pois isto nos tornaria, possivelmente, alvo, por ação indireta, de quem desejar desestabilizar os Estados Unidos.

Cabe perguntar, a quem a ALCA vai privilegiar? As Nações-Estados e seus governos e sua estabilidade, em caso de conflito futuro ou as Multinacionais e ao capital financeiro internacional, que não obedecem a nenhum governo, mas detém enorme poder de pressão sobre o governo dos Estados Unidos?

Devemos recordar, aqui, um exemplo histórico bem ilustrativo:

quando o Brasil assinou os Acordos de Washington, em Março de 1942, sobre a participação definitiva na guerra, os americanos, através do sua Diretoria de Bem-Estar Econômico (BEW) enviaram uma missão técnica para estudar nossa economia e fazer sugestões para alcançarmos os seguintes pontos:

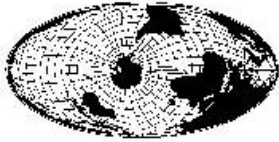
1 – substituir as commodities americanas que eram importadas dos EUA por produtos brasileiros, de modo a poupar espaço de carga na marinha mercante americana que nos abastecia e liberar este espaço para outros usos estratégicos, em outras partes do mundo;

2 – reduzir a dependência da indústria brasileira de matérias-primas importadas pelo desenvolvimento do que era possível obter no próprio território brasileiro, com isto, aliviando as necessidades globais de fornecimento de matérias-primas industriais;

3 – ajudar a conservar e aperfeiçoar o sistema de transporte nacional (especialmente terrestre);

4 – proporcionar ao Brasil a base para um crescimento industrial a longo prazo (Usina de Volta Redonda, etc).

Um capítulo com análise sobre esta missão, chefiada pelo Dr. Morris Llewellyn Cooke, antigo diretor da Rural Electrification Administration, está em “Aliança Brasil-Estados Unidos: 1937/1945” de Frank D. McCann, Jr, Biblioteca do Exército, Rio de Janeiro, 1995. E os desdobramentos sobre a introdução do planejamento do Brasil, pelas missões subseqüentes americanas desde o histórico Plano SALTE, podem ser lidas em Jorge Gustavo da Costa, Planejamento Governamental: a experiência brasileira,



Escola Superior de Geopolítica e Estratégia
Mantenedora: Organização para Estudos Científicos (OEC)

Fundação Getúlio Vargas, Rio de Janeiro, 1971.

Coloco estas considerações finais, pela simples razão de que os Estados Unidos estão preparando profundas mudanças em sua política de defesa.

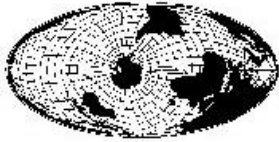
10 – REFORMULAÇÃO DOS CONCEITOS DE DEFESA NOS EUA

O documento “US Security in the 21st Century, US Department of State, issued, January, 31, 2001, afirma, em seu início: nós não achamos que segurança nacional é igual a defesa. Surpreendente!

Dizem mais: nós recomendamos a criação de uma nova agência independente, que será a Agência Nacional de Segurança do Homeland (ou seja, do interior do território), a NNSA, com a finalidade de planejar, coordenar, integrar os vários departamentos... deve integrar, já, a Guarda Costeira, o Serviço de Alfândegas e as Patrulhas de Fronteira. A NNSA deve poder proteger a infra-estrutura crítica da Nação, incluindo a tecnologia de informação. O Diretor da NNSA deve ter o status de membro do gabinete (isto é, Ministro). Ele deve zelar pela garantia das liberdades civis e, em caso de emergência nacional, interagir com o Departamento de Justiça. Propomos a criação de um novo gabinete para Assistente Secretário for Homeland Security (dentro do DOD). Todas as Guardas Nacionais devem ser reorganizadas, treinadas e equipadas to undertake that mission...

A nossa comissão (são conclusões de um painel interdisciplinar) verificou que o nosso sistema educacional e de pesquisa são inadequados e constituem uma grande ameaça para a segurança dos Estados Unidos. A liderança política deve entender que estas deficiências são desafios/perigos para a segurança nacional.

Nós recomendamos dobrar as verbas para pesquisa federal. Se não investirmos pesadamente em reconstruir a educação e pesquisa, America will be incapable of maintaining its global position long into the 21st century. Nossa comunidade de intelligence (informações, contra-informações) deve sofrer reajuste, para se adequar a Era pós-guerra fria. Economia e política devem ser mais monitorados, etc. Segurança da homeland, contra-terrorismo e ciência e tecnologia devem ser incluídos nas atividades de intelligence. Nós recomendamos a criação de cinco novas subsecretarias de Estado para monitoração das seguintes áreas: África, Ásia, Europa, Inter-América, Oriente Médio/Sudeste Asiático. Redefinir as atribuições do Subsecretário para Assuntos Globais. Reduzir de 10% a 15% os efetivos do Secretário da Defesa; Chefes de EM;



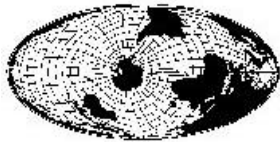
Escola Superior de Geopolítica e Estratégia Mantenedora: Organização para Estudos Científicos (OEC)

Serviços Militares em geral] e todos os Comandos Regionais. O DOD deve reduzir seus custos em 20% a 25% até pela privatização de muitos de seus serviços. Os ciclos do armamentos devem ser acelerados. São hoje 9 anos, quando as novidades na indústria civil se dão a cada 18 meses. É preciso fechar este 'gap'. Devemos acelerar nossa modificação do DOD para cinco grandes comandos/forças:

- 1 - forças estratégicas nucleares
- 2 - homeland security forces
- 3 - forças convencionais
- 4 - forças expedicionárias
- 5 - forças para ações humanitárias e de polícia (constabulary)

Nota: todas devem ter as mesmas capacidades de tecnologia superior, desenvolvimento no terreno, sobrevivência e poder de destrutibilidade, ao mesmo nível das atuais forças expedicionárias enviadas para o Exterior. Uma dimensão crítica é manter o acesso ao espaço exterior, para uso militar e comercial pelos Estados Unidos. Recomendamos o estabelecimento do Interagency Working Group on Space (IWGS), isto incluirá a coordenação da NASA, da Administração Nacional dos Oceanos e Atmosfera (NOAA), Departamento do Comércio, Departamento do Estado e de Defesa e outros ramos governamentais.

Precisamos aumentar nossa capacidade de conhecer, coletar e analisar dados econômicos, de ciência, de tecnologia que concernem aos nossos assuntos de defesa. Assim, recomendamos que o Congresso aumente significativamente o atual National Foreign Intelligence Program (NFIP). Também recomendamos a ampliação do Ato Nacional de 1991 "Security Education" (NSEA), aumentando o apoio para ciências sociais, humanidades, línguas estrangeiras e intercâmbio entre serviços civis e militares internacional. Observamos queda da qualidade de 25% dos novos funcionários do Departamento de Estado, recomendamos reexaminar o processo de seleção e aumentar dramaticamente o nível da educação profissional. No Serviço Civil recomendamos o estabelecimento do National Security Service Corps (NSSC), que deve lidar com questões de segurança nacional. Recomendamos que o Congresso aprove, igualmente, mais verbas para mais viagens para o exterior para estudos, maior participação em "wargames", etc, etc...



Escola Superior de Geopolítica e Estratégia
Mantenedora: Organização para Estudos Científicos (OEC)

Encerra.