GUERRA NA PAZ
AÇÕES MALICIOSAS SOBRE REDES E SISTEMAS DE INFORMAÇÕES

Frank Ned Santa Cruz de Oliveira
Pesquisador independente

Abstract

As computer networks and informational systems has become vital to institutions: academicals, commercial and governmental, becoming communication vehicles between those and the society, we became aware of the infrastructure exposure to malicious individuals. Therefore, it is necessary a deeper understanding of this phenomenon so the strategic and tactical plans of combat to these malicious actions can be established.

1. INTRODUÇÃO

Nos dias atuais, de entrechoques de civilizações num mundo globalizado e fragmentado, mais do que nunca se faz necessário interpretar os sinais da era vivida e ser capaz de reconhecer como a conjuntura internacional evoluiu. Ademais, saber quais as prováveis tendências do porvir, bem como, concomitantemente buscando determinar os interesses nacionais para definir o que e como fazer – a política e as estratégias a adotar.

Destarte, torna-se fundamental desenvolver uma visão estratégica global dos acontecimentos mundiais para ajudar na reavaliação dos meios e dos valores empregados, ao pesar as decisões tomadas, os métodos usados e as realizações obtidas.

A estratégia não deve ser uma doutrina única, mas um método de pensamento, permitindo classificar e hierarquizar acontecimentos e, depois, escolher os procedimentos mais eficazes. A cada situação corresponde uma estratégia particular; toda estratégia pode ser a melhor em uma das conjunturas possíveis e detestável em outras conjunturas.

Hodiernamente, a guerra tornou-se abertamente total, isto é, conduzida simultaneamente em todos os domínios, político, econômico, diplomático e militar.

Nesse contexto configura-se uma nova realidade com o surgimento da *netwar* que se trata do equivalente ao termo militar *cyberwar*.

Sendo assim, torna-se fundamental o desenvolvimento de ações estratégicas e táticas no sentido de atuar com respostas apropriadas, bem como o desenvolvimento de programas de cooperação entre instituições e atores deste novo cenário.

Assim o assunto abordado neste texto tem por objetivo principal tratar a *netwar* no aspécto da sociedade civil, desenvolvendo uma analogia de conceitos estratégicos empregados no universo militares e aplicáveis à segurança de redes e sistemas de informação. Com sua modesta abrangência, este trabalho pretende servir como motivação ao leitor para busca de novos conhecimentos. Não houve aqui a pretensão de esgotar o assunto, mas sim fornecer ao leitor um texto condensado, reunindo conceitos fundamentais ao entendimento dos termos relacionados, promove-los e coloca-los no centro de debate das questões estratégicas para instituições, governamentais, educacionais, privadas e por que não do Brasil. Várias obras serviram de apoio na elaboração deste material, as quais encontram-se elencadas ao final.

2. VISÃO GLOBAL DE ESTRATÉGIA

Estratégia, noção nascida da arte militar, estendendo-se atualmente a toda atividade humana.

Mas, o que é a estratégia?

Caso se parta da noção de estratégia militar, o ilustre autor, Carl Von Clausewitz definiu-a "como a arte de empregar as forças militares para atingir resultados fixados pela política". Já o general André Beaufre, resume a evolução do conceito: "a arte de promover o concurso de forças para atingir

os objetivos da política (...). É, por conseguinte, a arte da dialética de forças ou ainda, mais exatamente. A arte da dialética de vontades, empregando a força para resolver conflitos."

Tomando-se a definição de Aurélio Buarque, temos: "... 2. Arte de aplicar os meios disponíveis ou explorar condições favoráveis com vista a objetivos específicos."

Desta forma, as definições apresentada anteriormente nos ajuda a compreender a finalidade da estratégia: atingir os objetivos fixados pela política, utilizando da melhor maneira os meios de que se dispões. Esses objetivos podem ser ofensivos ou **defensivos**.

Adotando esses conceitos para segurança de redes e sistemas de informação, em uma nação que não esteja em estado de guerra, conforme definição comumente aceita, o principal objetivo é **defensivo** empregando-se uma estratégia de **dissuasão**.

O entendimento dos meios da estratégia permite melhor colocar em evidência a forma de raciocínio que lhe é própria.

Para atingir a decisão, a estratégia vai dispor de uma gama de meios materiais e morais, indo da implementação de tecnologias, estabelecimento de parcerias à divulgação de conceitos. A arte consistirá em escolher entre os meios disponíveis, e em combinar sua ação, para fazê-los convergirem para um mesmo resultado.

A escolha dos meios vai depender de uma confrontação entre as vulnerabilidades conhecidas e as possibilidades. Para fazer isso, é preciso analisar o efeito. O que se quer convencer? Em última analise, é o inimigo que se quer convencer. Para tanto deve-se definir uma ação direta ou **indireta**.

Na estratégia da ação indireta, o adversário não é derrotado, mas é vencido pela manobra, procura-se desgastá-lo progressivamente.

3. GUERRA

A guerra é uma forma de fazer política, ou pelo menos um meio de fazer política, já que, na verdade a guerra é a luta pelo poder. Guerra é o estado em que vivem aqueles que lutam. Na guerra ambos os lados buscam impor sua vontade. Destarte, a guerra é um fenômeno muito mais abrangente que o conflito armado. Guerra só existe se houver choque de vontades, tem que haver uma dialética de vontades.

Até o século XVIII, era claro como a guerra se processava: a guerra ocorria entre dois ou mais estados nacionais, representados por duas ou mais casas reais e normalmente era conduzida através de exércitos de mercenários. Hoje, não se pode prever com certeza como se dará uma guerra em um determinado espaço e em um dado tempo. Há, hoje, quatro diferentes tipos de guerra:

A guerra convencional;

A guerra de destruição em massa;

A guerra irregular; e

A guerra assimétrica.

A guerra irregular foi progressivamente tomando o lugar das guerras convencionais e caracteriza-se pela transferência dos conflitos para as ruas, cavernas, florestas e redes de computadores.

A guerra assimétrica é uma guerra irregular travada no espaço mundial e é composta, entre outras, das seguintes assimetrias:

Assimetria de poder econômico e financeiro – muitos recursos versus poucos;

Assimetria de estrutura organizacional - hierarquia versus rede;

Assimetria de objetivos – infinitos alvos versus poucos;

Assimetria de resultados – indiferença de resultados no curto e médio prazo contra a necessidade de resultados expressivos do adversário no curto prazo;

Assimetria comportamental – não sujeito a nenhuma regra, inclusive admitindo o suicídio na ação versus o adversário preso a regras e a convenções.

A guerra assimétrica, assim como a guerra irregular, é, devido a sua natureza, a guerra dos fracos contra os fortes, a guerra dos pobres contra os ricos. Ambas são fundamentalmente guerras de desgaste. Tanto a guerra assimétrica como a guerra irregular não é apenas guerra nas sombras, elas são **guerra na paz**, a guerra assimétrica é uma guerra que não se combate e, sim, se vive. A guerra assimétrica coloca-se como um tipo de guerra praticada pela estratégia de ação indireta. A guerra

irregular é a guerra do espaço amplo. A guerra assimétrica é a guerra do espaço ilimitado. Em ambas, não existem frentes de combate. A retaguarda não existe para elas. O espaço não é mantido, nem ocupado. O espaço é contaminado. São guerras de movimento.

Um dos principais movimentos é o da infiltração, que é característica central tanto operacional como tática. Podemos observar dois momentos principais: o de reunir e o de dispersar.

Sabemos que toda arma tem um alvo adequado. A guerra assimétrica não oferece alvos a um dos lados e oferece qualquer oportunidade como alvo ao outro. Em função disso, em um dos lados há muita dificuldade no emprego de determinados recursos enquanto no outro há ampla possibilidade de se empregar qualquer facilidade.

As formas de guerra assimétrica são:
Guerra psicológica;
Guerra econômica;
Guerra com armamento usual;
Guerra radiológica, nuclear ou radioativa;
Guerra biológica, bacteriológica ou virótica;
Guerra química;
Guerra cibernética, eletrônica ou informática.

Neste ponto voltamos nossa atenção para a *netwar*.

4. ASPÉCTOS DA NETWAR

A *netware* trata-se do equivalente ao termo militar *cyberwar*. *Netwar* possui uma natureza dupla, de um lado temos terroristas, criminosos e extremistas nacionalistas, já do outro lado temos o ativismo da sociedade civil. O que caracteriza a *netwar* como uma forma de conflito é a natureza da estrutura organizacional dos participantes que estão interconectados através das redes computacionais.

Trata-se de vários grupos, sem uma liderança definida, acefalarquias, que se organizam de forma extremamente rápida com o propósito de lançar ataques contra alvos /computacionais/eletrônicos de instituições comerciais, financeiras, educacionais e governamentais. Ataques estes que possuem natureza assimétrica e que não são limitados pelo átomo como os conflitos de épocas anteriores. Independente de quem sejam os protagonistas ativistas da sociedade civil ou terrorista, os ataques praticados com freqüência são bem sucedidos. Em parte o sucesso dos ataques praticados na *netwar* pode se explicado em função da novidade, ou seja, decorrente da exploração de novas vulnerabilidades para as quais não existem correções ou não houve tempo hábil para aplicar a correção, por outro lado a desinformação quanto à necessidade de mecanismos de segurança, de arquiteturas de redes seguras, procedimentos de resposta a incidentes, entre outros facilitam a ação do inimigo.

Outra característica marcante da *netware* é que além de ser uma guerra assimétrica, a origem dos ataques também é assimétrica o que dificulta em muito as ações de combate principalmente em virtude dos aspéctos legais.

Na *netwar* acontece o rompimento da mais velha convenção: a guerra como assunto exclusivo dos militares, em que se faz o emprego exclusivo de armas militares. A *netwar* não é conduzida exclusivamente por militares e não usa armamento militar. Há uma relação dialética entre a guerra assimétrica com origem assimétrica e a lei. Pois aquela pode apresentar uma manifestação de tendência revolucionária, ser ilegal, mas não necessariamente ilegítima. Não é possível ao agente operar de forma legal politicamente e de forma ilegal enquanto agente. O agente é totalmente ilegal. Acontece que o agente é ilegal perante uma legislação nacional, mas será que também o é perante a legislação internacional?

Nesta guerra os agentes constituem ou não redes, que se opõem a estruturas hierárquicas. A ligação entre agentes se dá muito mais horizontalmente em redes, pela fórmula política ou no plano das idéias, do que verticalmente, como resultado de estruturas de comando. A primazia que os agentes têm no estabelecimento de sistemas de redes sempre redunda em vantagens estratégicas e táticas. A multiplicação das redes gera do lado dos agentes, sistemas de heterarquias, panarquias e acefalarquias, todos incompatíveis com sistemas usuais de condução da guerra baseados em hierarquia. O soldado

está preso às convenções da guerra e o agente está livre de tudo, que não as regras de sua luta. Eles tornam-se neutros e desaparecem no campo de batalha.

A liberdade para operar neste tipo de guerra constrói a sua própria força. Liberdade vista aqui como liberdade sobre o espaço e sobre o tempo. Além da facilidade e velocidade que os agentes dispõem para rapidamente agruparem-se para lançar ataques. A forma de organização em redes computacionais permite a utilização de antigas formas de atividades ilícitas e lícitas. Em questões de minutos novas ferramentas de ataque são compartilhadas entre diversos grupos de forma mundial.

Na *netwar* existem cinco aspéctos que devem ser observados:

Tecnológico;

Social;

Narrativo;

Organizacional;

Doutrinário.

Embora o nível de sofisticação tecnológico faça diferença e em geral as pessoas pensem que se trata do principal aspécto, os demais níveis são de igual importância. Por exemplo, o nível social que caracteriza a cooperação entre os membros dos grupos. Embora os laços sociais sejam fortes, permitindo a construção de confiança mútua e identificação de valores, a forma de organização permite através da narrativa captar novos agentes para a causa .

A organização estrutural varia de canais diretos a estruturas de maior complexidade, como estrela dispersa por diversos paises. No passado, as ações de inteligência tinham foco em mapear a estrutura de hierarquia dos líderes na organização em rede, esta abordagem não é suficiente.

Com os avanços tecnológicos e facilidade de acesso às novas tecnologias o poder de comunicação, organização e ataque destes grupos vai aumentar de forma exponencial. Alguns exemplos são: comunicação criptografada, rede sem fio, a telefonia celular com IP (GSM), VoIP, *homing* de IP, *bluetooth*.

5. SISTEMA DE DEFESA EM CAMADAS MÚLTIPLAS

Faz-se necessária a elaboração de uma "Política de Defesa" bem como das diretrizes com a finalidade de empregarmos as estratégias e táticas adequadas. Para tanto alguns pontos fundamentais devem ser claramente explorados:

Quem são os ofensores?

Onde situam-se e com que grau de ameaça?

Quais são as vulnerabilidades?

Onde fortalecer e com que prioridade e intensidade?

Uma visão, em camadas, dos ativos a serem protegidos auxilia na elaboração das estratégias e táticas de contramedida. Uma abordagem é a segurança de perímetro alinhada com segurança em profundidade, *hardening*, tendo foco nos sistemas classificados de alta criticidade, núcleo, e vigilância dos sistemas periféricos.

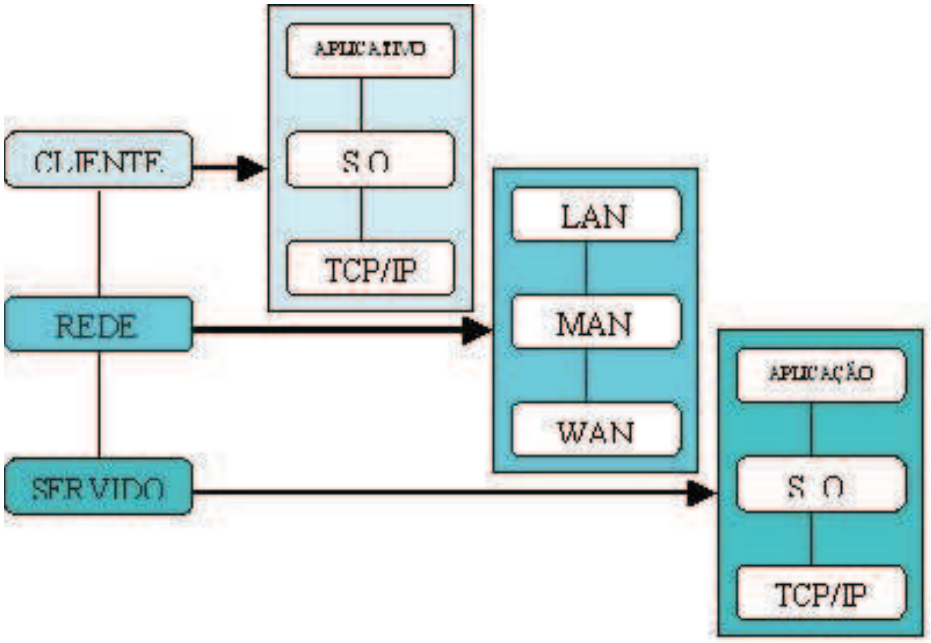

Figura 1 – Visão em camadas

Pode-se expandir o nível de detalhamento de cada uma das camadas até atingir a profundidade desejável. Por exemplo:

rede::WAN
Borda
Core
Distribuição
Acesso

Assim, tem-se uma visão em maior profundidade que auxilia a responder as questões fundamentais, no nosso exemplo:

Quem são os ofensores? *Crackers*, criminosos e vândalos.

Onde se situam e com que grau de ameaça? Situam-se externa a internamente, com diferentes graus de ameaça, conforme o ofensor.

Quais são as vulnerabilidades? Vulnerabilidades de arquitetura, sistemas operacionais, pilha TCP/IP e aplicações.

Onde fortalecer e com que prioridade e intensidade? Fortalecer os sistemas de núcleo de forma prioritária com a implantação de mecanismos de controle de conexão e segurança em profundidade.

É desejável que todos os mecanimsos possuam recursos de gerar registro dos eventos, *logs*, com o objetivo de serem centralizados e correlacionados em um Centro de Operações de Segurança, para finalidade de correlacionamento, análise forense, mineração de dados, possibilitando desta forma o efetivo acompanhamento de acordo com o C4I2 (Comando, Controle, Comunicação, Computador, Informação e Inteligência), que permite ações estratégicas, operacionais e táticas em tempo real permitindo a tomada de decisão em função da visão global dos eventos.

6. CONSIDERAÇÕES FINAIS

Sendo assim, faz-se necessária um amadurecimento perante a nova realidade, a definição de um plano estratégico de operações de "combate" que deve incluir a caracterização dos objetivos do inimigo, técnicas operacionais, recursos utilizados e agentes. Outrossim deve-se identificar as ações de combate legal e operacional, além de aparelhar os centros de gerência de segurança com tecnologia que permita a coleta e correlacionamento dos diversos eventos, permitindo desta forma uma visão global do teatro de operações e estabelecimento de parcerias com outros centros de segurança."

A defesa tem uma finalidade passiva: preservação; o ataque, uma positiva: conquista. Este aumenta nossa capacidade de condução da guerra, aquela não" (Carl Von Clausewitz)

7. REFERÊNCIAS BIBLIOGRÁFICAS

BEAUFRE, André. Introduction a la Stratégie; TRADUÇÃO DE Luiz de Alencar Araripe (Biblioteca do Exército).
CLAUSEWITZ, Carl Von. Da Guerra; TRADUÇÃO DE Maria Teresa Ramos (Martins Fontes).
CARDOSO, Alberto Mendes; Os Treze Momentos – Análise da Obra de SUN TZU (Biblioteca do Exército).
STEPHESON, Peter; Investigating Computer-Related Crime (CRC).
MACHIAVELLI, Niccolo; O Príncipe – COMENTÁRIOS DE Napoleão Bonaparte (Biblioteca do Exército).
PARET, Peter; Construtores da Estratégia Moderna (Biblioteca do Exército).
ARQUILLA, John / RONFELDT, David; In Athena´s Camp (RAND).
FERREIRA,Aurélio Buarque de Holanda. Dicionário da Língua Portuguesa.
SANTOS, Murilo; Segurança Defensica – Ideais, Disponível em: <http://www.mct.gov.br/CEE/revista/Parcerias3/seg_def.html> Acesso em: 07 mai. 2004.
COSTA, Darc;.Visualizações da Guerra Assimétrica , Disponível em: <http://www.militar.com.br> Acesso em: 07 mai. 2004.