Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto

André Melo Carvalhais Dutra
Instituto Tecnológico da Aeronáutica – Praça Marechal Eduardo Gomes, 50 – Vila das Acácias. CEP 12228-900 – São José dos Campos – SP

***Resumo* — Este artigo analisa alguns dos principais conceitos envolvidos no estudo de Guerra Cibernética, e aponta para a necessidade de uma maior especialização nacional na área. É evidenciado como a constante evolução tecnológica conduziu a uma nova forma de enfrentamento entre nações. Uma definição do termo "Guerra Cibernética" é apresentada, e a seguir fazemos sua interpretação, direcionando-a para o contexto militar. São abordados alguns princípios, algumas de suas repercussões nos planos civil e militar, e a identificação de vulnerabilidades, e medidas de ataque e defesa em Guerra Cibernética. Finalmente apontamos para a necessidade de um maior entendimento do assunto por parte de nosso país e suas instituições.**

***Palavras-chaves* — guerra cibernética, definição, princípios, repercussão nos planos civil e militar, vulnerabilidades, medidas de ataque, medidas de defesa, guerra cibernética no Brasil.**

I. INTRODUÇÃO

"Lutar e vencer todas as batalhas não é a glória suprema; a glória suprema consiste em quebrar a resistência do inimigo sem lutar."

Sun Tzu

A grande evolução tecnológica que vem sendo experimentada pela humanidade em sua história mais recente, tem modificado a maneira como as sociedades modernas se inter-relacionam.

A gradativa miniaturização de sistemas computacionais, bem como a grande redução de seus preços, permitiram que os computadores permeassem quase todos os aspectos do cotidiano moderno.

Com a conseqüente conexão de grandes sistemas informatizados, o capital passou a desconsiderar limites geográficos: grandes somas entram e saem dos mercados financeiros instantaneamente, através de transações eletrônicas; com a popularização da Internet, o acesso à informação e ao conhecimento tornou-se imediato e universal para qualquer um que disponha de uma conexão à mesma. Evidência disso, é o processo de globalização, pelo qual temos passado desde o final do século XX.

Como resultado desta situação, podemos citar o fato de que, atualmente, a grande maioria dos principais sistemas de informação, necessários para o funcionamento de qualquer sociedade moderna, encontram-se interligados através de redes de computadores. Schwartau[7] define esse fenômeno como sendo "Computadores em todos os lugares e a Rede Global" *(Computers Everywhere and the Global Network*, p.71 a 94).

André Melo Carvalhais Dutra, carvalhais@ita.br, Tel +55-12-39476897, Fax +55-12-39476893

Essas circunstâncias permitem que uma nação inteira possa ser conduzida à capitulação, sem que, no entanto, haja qualquer manobra política ou militar com esse intuito. Como exemplo do que hora foi dito, podemos citar a recente onda de ataques direcionada sítios de Internet de ministérios, partidos políticos, bancos e jornais, entre outras entidades estonianas, que segundo Traynor[8], quase conduziram aquela nação ao colapso.

Portanto, torna-se evidente que, num contexto de hostilidades e/ou beligerância entre dois Estados, a exploração das redes de computadores do país oponente constitui uma eficiente maneira de obter vantagens sobre o mesmo; no contexto militar, a exploração dos sistemas de informação computadorizados estabelecidos pelas forças inimigas durante o transcurso de suas operações, pode levar a uma superioridade no campo de batalha. É justamente destas duas situações de que trata a Guerra Cibernética (GC).

II. DEFINIÇÃO DE GUERRA CIBERNÉTICA

Ao que tudo indica, parece não haver consenso entre os autores sobre a definição do termo "Guerra Cibernética", o que pode ser explicado pelo relativo ineditismo do assunto.

Entretanto, um aspecto consensual, é que para ocorrer GC, é necessária a existência de patrocínio estatal, ou seja, ações oriundas de um indivíduo com motivações pessoais não podem ser consideradas como sendo GC, embora possam ser igualmente prejudiciais.

Com isso em mente, buscamos a definição proposta por Parks e Duggan[6], por considerar que a mesma se enquadra melhor no escopo do presente trabalho, e ser menos generalista, tornando mais clara e concisa a definição do termo:

> *Guerra Cibernética é o sub-conjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a Internet e as redes a ela relacionadas, as quais compartilham mídia com a Internet. A definição militar mais próxima para o nosso termo, guerra cibernética, é uma combinação de ataque a redes de computadores e defesa de redes de computadores, e possivelmente, operações especiais de informação.*
> *Nós definimos guerra cinética como sendo a guerra praticada no "mundo real". Todos os tanques e navios e aviões e soldados tradicionais são os protagonistas da guerra cinética.* (tradução do autor).

É importante observar que a definição acima abraça uma outra tendência aparentemente consensual entre os autores: a separação entre os mundos cibernético (ou virtual) e cinético (ou real).

Devemos considerar, porém, que embora exista essa separação, necessária, uma vez que definições e conceitos de nomes iguais diferenciam-se em sentido, em função do contexto que estejam inseridos (mundo cibernético ou mundo cinético), esse dois "mundos" encontram-se inter-relacionados, uma vez que ações adotadas no mundo cibernético afetam o mundo cinético e vice-versa.

Nesse instante, a frase de Sun Tzu apresentada no início do artigo ganha uma nova interpretação. No contexto da GC, quando dizemos "quebrar a resistência do inimigo sem lutar", estamos nos referindo a uma luta no mundo real. Pois, embora a GC permita que se quebre a resistência de um oponente sem qualquer litígio no mundo cinético, no mundo cibernético estão de fato ocorrendo conflitos.

III. PRINCÍPIOS DE GUERRA CIBERNÉTICA

A partir do trabalho realizado por Parks e Duggan, verificamos que alguns dos princípios de guerra clássicos (combate cinético) não possuem significado no combate virtual, sendo necessários, portanto, novos princípios. Seguem abaixo os princípios propostos por estes autores, com suas respectivas denominações, adotadas por Cahill, Rozinov e Mulé[3] num estudo posterior.

É importante ressaltar que a lista a seguir trata-se de uma discussão inicial sobre o assunto, não devendo, assim, ser considerada completa:

- **Princípio do Efeito Cinético (Guerra Cibernética deve produzir efeitos no mundo cinético):** não há sentido em desencadear quaisquer ações contra entidades cibernéticas, a menos que estas ações produzam algum efeito no mundo real, e que este efeito se traduza em vantagem.
- **Princípio da Dissimulação e Visibilidade (medidas ativas podem ser adotadas para se dissimular no mundo cibernético, mas qualquer coisa que alguém faça é visível):** como quaisquer ações adotadas no mundo cibernético envolvem a movimentação ou manipulação de dados, e estes residem em programas e equipamentos desenvolvidos por seres humanos, o próprio fato de alguém tentar desencadear ações de GC significa que algum bit em algum fluxo de dados é modificado de forma a refletir essas ações e a presença desta pessoa. Porém essa informação só será útil se puder ser detectada.
- **Princípio da Mutabilidade (não existem leis de comportamento imutáveis no mundo cibernético, excetuando-se aquelas que necessitam de uma ação no mundo real):** o mundo real é regido pelas leis da física; dessa forma é possível que se possa prever determinados comportamentos: por exemplo, pode-se prever a trajetória de um projétil disparado através da aplicação de conhecimentos de balística. No mundo cibernético, não existem quaisquer leis que permitam prever esse tipo de comportamento, devido à natureza caótica inerente à operação de equipamentos e programas (falhas físicas, flutuação na performance dos equipamentos, etc); excetuam-se aquelas que refletem uma ação tomada no mundo físico (espera-se que um equipamento apresente um melhor desempenho caso seu processador seja substituído por um mais avançado, por exemplo).
- **Princípio do Disfarce (alguma entidade no mundo cibernético possui a autoridade, acesso, ou habilidade necessários para por em prática qualquer ação que um atacante deseje realizar; o objetivo do atacante é assumir a identidade dessa entidade, de alguma forma):** não há parcela do mundo cibernético que não seja controla por seres humanos ou suas ferramentas (como programas, por exemplo); dessa forma, sempre existirá alguma entidade que é capaz de realizar o que o atacante deseja; assim, basta ao atacante assumir a identidade do ente que possa realizar a ação desejada, para que o ataque seja bem sucedido.
- **Princípio da Dualidade do Armamento (as ferramentas - ou armamentos - da Guerra Cibernética são de natureza dual):** no combate cinético, as ferramentas, equipamentos e armamentos possuem um uso único e bem definido: rifles são usados para alvejar, casamatas para se proteger e radares para detectar a aproximação do inimigo. No combate cibernético, as mesmas ferramentas são usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas alvo, e por administradores para descobrir as fraquezas de equipamentos e redes.
- **Princípio da Compartimentação (tanto o atacante, como o defensor de um sistema, controlam uma pequena parcela do ciberespaço que utilizam); e, Princípio da Usurpação (quem controlar a parte do ciberespaço que o oponente utiliza, pode controlar o oponente):** Parks e Duggan inicialmente propuseram a afirmação anterior como sendo um único princípio; Cahill, Rozinov e Mulé, entretanto, identificam na mesma o encerramento de dois princípios. Como todo o ciberespaço está contido em equipamentos, programas e fluxo de dados, todos subprodutos do trabalho humano, qualquer cibergrupo controla, no mínimo, a parcela de ciberespaço compreendida entre seus equipamentos e programas, e a interface com a infra-estrutura de comunicações (e raramente controla mais do que isso); caso um determinado grupo detenha o controle de um serviço utilizado pelo oponente, por exemplo, um servidor do tipo *Domain Name Server* (DNS), este pode, também, controlar o oponente.
- **Princípio da Incerteza (o ciberespaço não é consistente, nem confiável):** este princípio está relacionado com o princípio da mutabilidade; no ciberespaço nem os equipamentos, e muito menos os programas, irão trabalhar sempre da maneira esperada; dessa forma, nunca é possível saber, com total certeza, se o próximo passo numa ação cibernética irá funcionar.
- **Princípio da Proximidade (limitações físicas de distância e espaço não se aplicam ao mundo cibernético):** no mundo cibernético, ações desencadeadas do outro lado do mundo, ou da sala ao lado, são executadas com igual grau de eficácia; dessa forma, distâncias físicas não constituem um obstáculo na condução dos ataques.

IV. REPERCUSSÕES DA GUERRA CIBERNÉTICA

Como pudemos observar do que foi acima exposto, a GC impõe uma nova realidade para os teatros de operações militares.

Os alvos não são mais somente pessoal e instalações militares. Agora, bancos, usinas elétricas, empresas de telefonia e de telecomunicações, sistemas de transporte e logística, serviços de emergência e segurança pública, entre outros são alvos em potencial, uma vez que a indisponibilidade continuada de quaisquer destes serviços certamente levaria uma nação ao colapso.

Segundo Kumagai[5], quanto mais confiarmos em redes de computadores, maior será o medo de que adversários ataquem essas redes.

Schwartau (p. 95 a 111) também aborda esse fenômeno, referindo-se ao mesmo como sendo uma espécie de "esquizofrenia binária".

No contexto militar, Alford[1] aponta os sistemas de comando e controle, e sistemas de armas das forças em operações, como sendo os principais alvos de ataque.

Conscientes destes fatos, países como China e Taiwan vêm se concentrando em atividades de GC desde o início da década passada (Cahil, Rozinov e Mulé). Essa preocupação passa, inclusive, pela formação de novas unidades militares devotadas ao assunto. A literatura indica que outras nações também têm despertado um interesse semelhante pelo assunto.

V. VULNERABILIDADES E MEDIDAS DE GC

O estudo da identificação das vulnerabilidades e medidas de ataque e defesa é detalhado por Alford. Reproduziremos aqui algumas de suas idéias, adaptadas, contudo, ao escopo do presente trabalho.

Inicialmente, devemos ter em mente que a primeira regra na identificação de vulnerabilidades é que qualquer sistema computadorizado que possa aceitar entrada de dados, pode ser atacado.

A entrada desses dados pode ocorrer através de dois meios: meios físicos e meios de transmissão de dados. Meios físicos compreendem os dispositivos agregados à estrutura do equipamento: teclados e disquetes para computadores, ou manetes e botões para o computador de bordo de uma aeronave, por exemplo. Meios de transmissão de dados são aqueles que permitem a entrada de dados sempre que uma conexão direta, ou indireta for estabelecida ao sistema, por exemplo, através de redes sem fio, ou controle de um satélite através do qual passe as comunicações do sistema alvo.

Outra regra da identificação de vulnerabilidades de GC consiste em considerar que qualquer sistema de informações computadorizado possa ser alvo de um ataque, até mesmo aqueles que se encontram isolados; só assim teremos a garantia que não estamos negligenciando nenhuma possibilidade.

O autor ressalta, ainda, que a garantia da segurança física das entradas e saídas dos sistemas de informação computadorizados é a primeira linha de defesa. Além disso, o conceito de que o ser humano é o elo fraco na manutenção da segurança da informação, cresce em importância atualmente.

As medidas de defesa e ataque em GC são as mesmas utilizadas pelos especialistas de segurança da informação para garantir a integridade dos sistemas que administram, e pelos criminosos que buscam atacá-los. A única diferença é a intenção envolvida nessas ações (lembrar que a GC necessariamente abrange o patrocínio estatal).

Segundo Alford, o principal meio de proteção de sistemas cibernéticos é a sua segurança física. Essa afirmação ganha importância quando são consideradas as medidas passivas de defesa: isolar todos os sistemas críticos, colocar sobre controle manual as operações críticas (não podem ser realizadas por *software*, ou automatizadas), reduzir o nível de integração dos sistemas (o que reduz o número de entradas nos mesmos), e onde essa redução não for possível, manter o elemento humano no ciclo (embora ser humano seja o elo fraco da segurança, é o único elemento capaz de tomar decisões baseadas em sua capacidade de discernimento e de realizar inferências) e ater-se às potenciais brechas de segurança (as conexões de comunicação são sempre a porta de entrada esperada para os intrusos).

As medidas ativas de defesa envolvem o uso de senhas e autenticação, medidas antropomórficas (ou segurança baseada em biometria), uso de *tokens*, esquemas de autenticação multicamadas (autenticações distintas para níveis de acesso distintos), autenticação por múltiplas conexões (a autenticação em um sistema, por exemplo, ativa o funcionamento de uma linha telefônica, que será utilizada durante a comunicação de dados, e para a qual é exigida uma outra autenticação), autenticação por múltiplos endereços (a autenticação só é reconhecida se originar-se de mais de um endereço válido) e uso de *software* de monitoramento.

As medidas de ataque, por sua própria natureza, só podem ser ativas. Entre outras, podemos citar: programas de quebra de senha, programas de observação, obtenção de informação, disfarçadores de endereço e de identificação do alvo; programas de ataque (direcionados para um sistema específico); programas de marcação de alvos; programas de comportamento virulento, cavalos de tróia; programas de sobrecarga do sistema; manipulação direta de dados; e, por fim, bombas lógicas (seqüências de código específicas em arquivos de dados, que manipulam os programas que acessam estes arquivos ou o BIOS do sistema).

VI. A NECESSIDADE DE UM DESPERTAR BRASILEIRO PARA O ASSUNTO

É evidente que a Guerra Cibernética não se trata mais de uma ficção, na qual batalhas são irrompidas por comandantes por detrás de mesas, com simples acionamentos de botões. Grande parte do que foi dito até aqui comprova esta afirmação.

A preocupação demonstrada por países como a China e Taiwan, em criar unidades especialmente dedicadas ao assunto em suas forças armadas, e dos Estados Unidos da América, ao buscar desenvolver doutrina na área, indicam que não se pode mais desconsiderar essa vertente de emprego militar num teatro de operações moderno.

É importante observarmos aqui, que a GC não deve ser uma preocupação exclusiva das Forças Armadas brasileiras. Outras instituições também precisam estar comprometidas, pois como foi visto, os alvos de GC não necessariamente são pessoal, material e instalações militares.

Como a principal diferença entre a Guerra Cibernética e a Segurança da Informação reside na origem e intenção do autor, e não nas ferramentas, técnicas e conhecimentos utilizados, é seguro afirmar que grande parte das pesquisas de-

senvolvidas voltadas para a Segurança da Informação possuem aplicações em Guerra Cibernética. Dessa forma, devemos explorar o potencial brasileiro de pesquisas nesta área.

Contudo, alguns métodos computacionais encontram sua principal aplicação como ferramentas voltadas para a Guerra Cibernética, como é o caso do uso de algoritmos esteganográficos para permitir a ocultação de informações em canais aparentemente inócuos, conforme [9]. Não podemos, assim, negligenciar o conhecimento dos métodos, e realização de pesquisas nessa área.

Quando consideramos a vertente bélica da Guerra Cibernética, verificamos que os custos em equipamentos e treinamento de pessoal envolvidos com o uso da GC, são bastante reduzidos quando comparados aos envolvidos na aquisição de outros equipamentos militares e o respectivo treinamento. Porém, o emprego de GC é igualmente eficaz em reduzir a capacidade do oponente, quando o seu emprego é bem sucedido.

Um outro fator que deve ser levado em consideração no fomento de pesquisa na área, é que muito dos conhecimentos adquiridos, possuem uma aplicação quase que imediata em ambientes comerciais, industriais e corporativos, trazendo ao país um rápido retorno do investimento realizado.

Como diversas instituições públicas e privadas do país possuem pessoal de informática incumbidos de, entre outras atribuições, garantir a Segurança de Informação de seus sistemas, verifica-se que existe interesse brasileiro na área. Entretanto, esse interesse normalmente restringe-se às organizações e corporação que emprega esse pessoal.

Mas a Guerra Cibernética deve ser muito mais uma preocupação nacional e/ou institucional em proporcionar uma infra-estrutura que garanta essa segurança dos sistemas de informação (uma preocupação no nível macroscópico), do que uma preocupação puramente organizacional e/ou corporativa (preocupação no nível microscópico).

Existem iniciativas com o intuito de se estabelecer dispositivos nacionais voltadas para a segurança dos sistemas computadorizados, como, por exemplo, a instituição da Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil)[2], que garantiu a legalidade de documentos em forma eletrônica, além de tratar de outros assuntos. No entanto, a finalidade da ICP-Brasil é mais jurídica do que estratégica, e sua preocupação maior é a aplicação de técnicas criptográficas e de autenticação.

Assim, verificamos que ainda há espaço para o estabelecimento de uma infra-estrutura nacional com atuação no ramo de segurança da informação. É interessante que a mesma seja composta pelos diferentes setores do governo, bem como por diversas organizações da iniciativa privada, o que proporcionaria um maior grau de integração nacional no assunto, e atenderia a diferentes expectativas.

VII. CONCLUSÃO

Com a introdução do leitor à Guerra Cibernética, através da apresentação dos conceitos julgados mais importantes, tais como: princípios, identificação de vulnerabilidades, medidas de ataque e defesa, bem como de algumas de suas repercussões mais recentes, procuramos conscientizá-lo de que, indubitavelmente, a mesma é uma realidade.

Ciente desta situação, o leitor é, então, levado a uma reflexão a respeito da situação brasileira neste aspecto. Dessa forma, a necessidade de que o Brasil desperte para esse assunto acaba por evidenciar-se.

Criando esta consciência no leitor, o presente artigo busca atingir o objetivo a que se propõe: despertar a preocupação de uma massa crítica para o assunto, e fomentar o início de realização de pesquisas na área, o que, na opinião do autor, acabaria proporcionando o estabelecimento da anteriormente citada infra-estrutura nacional de segurança da informação.

REFERÊNCIAS

[1] ALFORD, Lionel D. Cyber Warfare: Protecting Military Systems. **Acquisition Review Journal**, Fort Belvoir, Fairfax County, VA, EUA, p. 100 – 120, 2000.

[2] BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Medida Provisória Número 2.2000-2 ce 24 de agosto de 2001**.

[3] CAHILL, T. P.; ROZINOV, K.; MULÉ, C. Cyber Warfare Peacekeeping. **Proceedings of the IEEE Workshop on Information Assurance**, West Point, NY, p 100 – 107, 2003. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2003, West Point, NY.

[4] ERBACHER, Robert F. Extending Command and Control Infrastructures to Cyber Warfare Assets. **Proceedings of the IEEE Workshop on Information Assurance**, West Point, NY, p 446 – 447, 2005. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2005, West Point, NY.

[5] KUMAGAI, Jean. The Web as Weapon. **IEEE Spectrum**, Nova Iorque, EUA, p. 118 – 121, janeiro 2001.

[6] PARKS, Raymon C.; DUGGAN, David P. Principles of Cyber-warfare. **Proceedings of the IEEE Workshop on Information Assurance**, West Point, NY, p 122 – 125, 2001. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2001, West Point, NY.

[7] SCHWARTAU, Winn. **Information Warfare**:: Cyberterrorism: Protecting Your Personal Security in the Electronic Age. 2. ed. Nova Iorque: Thunder´s Mouth Press, 1996. 768 p.

[8] TRAYNOR, Ian. Russia accused of unleashing cyberwar to disable Estonia. **Guardian Unlimited**. Bruxelas, 17 maio 2007. Disponível em: <http://www.guardian.co.uk/russia/article/0,,2081438,00.html> Acesso em: 5 agosto 2007.

[9] WANG, Huaiqing; WANG, Shuozhong. Cyber Warfare: Steganography vs. Steganalysis. **Communications of the Association for Computing Machinery**, Nova Iorque, EUA, v. 47, n. 10, p. 76 – 82, outubro 2004.