MARINHA DO BRASIL

ESCOLA DE GUERRA NAVAL

C-EMOS 2005

C-III-6 (En) - ENSAIO

TEMA: (040) O CONFLITO, AS FRONTEIRAS VIRTUAIS E OS GUERREIROS CIBERNÉTICOS.

CONFLITO VIRTUAL E CIBERGUERREIROS:
AS NOVAS DIMENSÕES DA GUERRA PARA AS FORÇAS ARMADAS.

CC LEVS LEANDRO DE SÁ

C-EMOS 013

2005

MARINHA DO BRASIL

ESCOLA DE GUERRA NAVAL

CONFLITO VIRTUAL E CIBERGUERREIROS:
AS NOVAS DIMENSÕES DA GUERRA PARA AS FORÇAS ARMADAS.

C-III-6

2005

INTRODUÇÃO

A partir da Segunda Guerra Mundial, o desenvolvimento da ciência e da tecnologia, resultou na aceleração das transformações tecnológicas e científicas, causando uma verdadeira revolução, identificada por ALVES e BECKER, em seus trabalhos, "A Guerra de Informação" e "A Geopolítica na virada do milênio: logística e desenvolvimento sustentável", respectivamente, como a "Revolução Científica ou Tecnológica". Estas transformações foram principalmente devido às grandes modificações e evoluções da micro-eletrônica e da comunicação. O novo mundo industrial, fortemente tecnológico, reestruturou as técnicas de produção, reformando os processos de informação e de conhecimento, causando reflexos nas organizações sociais, políticas, militares e econômicas. (1:144-145) (4:287-288)

Esta "Revolução Científica ou Tecnológica" está fortemente apoiada na capacidade intelectual humana, através da produção de conhecimento dos cientistas, dos engenheiros, dos técnicos e dos especialistas, em especial nos setores de comunicação e microinformática, resultando na "Revolução da Informação", na qual, o extraordinário aumento no fluxo de informação, trocadas em todo o globo, vem modificando fortemente o perfil das sociedades mundialmente. (20:167-170)

O termo informação neste trabalho é aquele formado por CLAWSEWITZ, na obra "Da Guerra", que "[...] designa o conjunto de conhecimentos relativos ao inimigo e ao seu país e, por conseqüência, a base sobre a qual se fundamentam as nossas próprias idéias e os nossos atos". (8:127)

A essência da tecnologia moderna é a aceleração das transformações e inovações, tornando o domínio da informática, essencial para quem produz estas modificações no desenvolvimento do país, influenciando não só os setores tecnológicos e produtivos, mas também os das relações sociais e de poder, inclusive nos assuntos políticos e militares relativos à guerra. (1:144-146) (4:288-289)

A popularização da informática e seus meios (Internet), que no Brasil ocorreu em meados na década de 1990, trouxeram uma nova forma de sabotagem, a "Pirataria Eletrônica", a ser "plantada" em tempos de paz, ou em períodos de crise ou guerra, transformando a informática num elemento de valor estratégico, cujas ações poderão causar danos com grandes conseqüências ao País. Esta sabotagem só tornou-se possível devido ao aparecimento da "grande rede" de comunicação e interligação, a Internet.

Dentro deste aspecto de desenvolvimento, a informática, bem como a Internet, aumentou o fluxo de informações trocadas entre seus usuários, da mesma maneira que ocorreu uma falta de controle em relação à idoneidade das informações, que permitiu que ações malévolas viessem a ser praticadas, com os mais variados propósitos. O fato característico deste desenvolvimento técnico é a interdependência dos sistemas de telecomunicações e informática. A comunicação de dados e a Internet são duas constituições tecnológicas que demonstram bem a tendência para um melhor tratamento e domínio da informação.

Ações de contrapartida, preventivas e de proteção, a programas, sistemas lógicos e redes de computadores, necessários para a sobrevivência neste mundo virtual de abrangência global, são instrumentos que poderão ser usados por ambos os lados de um conflito. Estas ações de defesa no campo da informática destacarão a importância de um novo protagonista nos confrontos armados, militares ou não, que de acordo com a denominação cunhada por ALVES e PAGLIUSI, serão conhecidos como "Guerreiros Cibernéticos" ou "Ciberguerreiros". (1:150) (14)

O propósito deste trabalho é analisar os conceitos e possíveis efeitos de um novo tipo de guerra onde não existirão os confrontos físicos diretos, aonde ocorrerão a milhares de quilômetros de distância, de um ponto que poderá ser controlado e monitorado em um centro de operações ou informações, bastando um terminal de computador e um grupo de profissionais especializados em informática, compreendendo suas características e dominando suas vulnerabilidades. Essas novas tecnologias da informática modificarão a concepção da guerra, pois poderão influenciar os resultados dos combates no teatro de operações, sendo conhecida como "Guerra Cibernética" ou "Ciberguerra". (1:147)

As Forças Armadas necessitam de medidas necessárias e permanentes para pró-ação e reação contra uma tecnologia que evolui constantemente exigindo constantes atualizações de equipamentos, de *softwares* e de recursos humanos. Com base na NBR[1] 17799, para Gestão de Segurança da Informação, serão apresentadas algumas propostas (diretrizes) como subsídio ao início de debates sobre o tema e para a construção de uma estratégia de defesa virtual, a serem avaliadas por especialistas militares atuantes nesta área.

[1] NBR: Norma Brasileira de Regulamentação. Associação Brasileira de Normas Técnicas (ABNT).

PIRATARIA ELETRÔNICA

Na Internet, convencionou-se chamar de vírus os programas ou as rotinas malévolas, que são "plantados" ou distribuídos através de acesso a fontes de informação, ou por correio eletrônico, que podem causar prejuízos, perceptíveis ou não, a curto, a médio ou longo prazo. Da mesma maneira, foi popularizado o termo *hacker* para designar o indivíduo que causa danos (pirataria eletrônica) a ferramentas, *hardwares* e *softwares*, reduzindo ou anulando a capacidade de funcionamento de sistemas, redes e computadores. No meio militar este é um assunto que ainda demanda um número de diversos estudos mais aprofundados a este respeito. (19:1)

As leis, os meios policiais e a justiça não estão atendendo suficientemente as necessidades quanto ao crescente número de delitos eletrônicos. Roubo de informação, desvios de recursos ou chantagens pelo computador, ainda são difíceis de terem seus atores identificados, localizados e capturados devido à versatilidade dos meios e equipamentos utilizados. Além dos códigos penais desatualizados e pouco específicos para este tipo criminal, as ações realizadas pela Polícia Federal restringem-se a atos de pedofilia, prejuízos a patrimônios financeiros ou econômicos e tráfico de armas, drogas e entorpecentes. (19:1-2)

Alguns dos principais tópicos da pirataria eletrônica para melhor compreensão deste trabalho, estão definidos no Anexo A, de acordo com as definições mais utilizadas e usuais.

O QUE É CIBERGUERRA?

Cibernética é uma palavra de origem grega, *"kybernetiké"*, cujo significado é timoneiro. De um modo mais amplo é a arte do controle exercido pelo timoneiro sobre o navio e sua rota. O conceito de informação neste trabalho é o de WIENER, em seu trabalho, Cibernética ou Controle e Comunicação no animal e na máquina, que considera como informação os dados de entrada, saída e realimentação (*feedback*) de um sistema.

A informação de controle é quando se deseja que um movimento obedeça a um dado padrão, a comparação entre este padrão e o movimento realmente efetuado, é usada como nova entrada para levar a parte regulada a mover-se de maneira a aproximar o seu movimento daquele fornecido pelo padrão. A cibernética não se ocupa primordialmente, nem com

organismos, nem com produtos técnicos, mas com aquilo que é comum a ambos, ou seja, está centrada na informação e nos meios como será transmitida. (27:33)

A informação recebida não precisa ser utilizada de forma imediata, mas pode ser armazenada de modo que venha a estar disponível em algum tempo futuro. (27:71)

"Ciberguerra" ou "Guerra Cibernética" tem suas origens nos conceitos das técnicas cibernéticas, agindo nas informações. Sua atuação visa paralisar um adversário que pode ser um país, ou um bloco econômico, ou ainda uma aliança militar, pela invasão as suas redes de computadores que dirigem e controlam a maioria das atividades vitais da sociedade.

Os novos valores econômicos e estratégicos decorrerão da velocidade em acessar e passar informações, sendo condição essencial de sobrevivência no mundo globalizado, obrigando os Estados a lutarem para manter o controle sobre todos os processos nesta nova escala geográfica global. (4:288)

A "Ciberguerra" poderá ser utilizada por Forças Armadas, por elementos terceirizados para emprego militar, por forças não convencionais, por componentes de grupos de guerrilha, ou, por forças terroristas, que agirão de forma a estabelecer uma guerra psicológica, desencadeando ações seletivas ou generalizadas, instalando o caos e difundindo o medo através da redução da capacidade operacional ou destruição dos elementos estratégicos de uma Nação.

SERIA O COMPUTADOR UMA ARMA?

De modo geral considera-se arma, tudo que pode ser empregado com a finalidade de matar, ferir ou incapacitar o oponente, ou aquilo que irá danificar ou destruir objetos ou propriedades do adversário.

Um computador provavelmente não terá os mesmos resultados físicos, mas os estragos que poderá causar em sistemas de comunicação, comando e controle, ações que estarão incapacitando, danificando ou destruindo, podendo classificá-lo do mesmo modo que as armas ou os armamentos de destruição em massa[2]. (16:7)

As guerras e os conflitos do século XXI serão bem diferentes dos que foram travados até o momento. Serão introduzidas novas formas de poder de destruição, novas estratégias,

[2] Especialistas alertam para as conseqüências de um possível ataque "cibernético" a elementos da estrutura estratégica de um país (exemplo a destruição do sistema de controle e distribuição de energia elétrica) ou a disseminação de boatos através da Internet (notícias falsas para provocar o pânico na população).

novos meios técnicos, formas modernas de gestão científica, tecnológica e da informação. A Revolução Científica da Informática utilizará o espaço virtual[3] para empreender ações contra os inimigos. (18:3-4)

De acordo com o Professor Fernando G. Sampaio, em seu texto sobre "Ciberguerra", ao citar o trabalho do Major USAF David J. Di Censo, "Ciberdireito da *Infowar*. A questão legal da guerra de informação": (16:8)

> Se uma nação hostil definir o ato de guerra baseada no dano causado ou no dano potencial, em vez de na natureza do instrumento usado para praticar o ato... Se da operação da *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 [...] E que dizer dos *hackers*?
> Se uma dessas pessoas se envolvesse em um ato de hostilidade, esse indivíduo seria considerado um combatente ilegal e poderia ser punido pelas leis do captor. Os espiões não recebem qualquer tratamento especial pelas leis da guerra e são punidos de acordo com as leis da nação que os captura.

O computador não é arma sem os programas malévolos, estes, não são armas também, se não existir quem os opere e direcione suas ações com a informação capturada. A informação necessita de criteriosa avaliação para sua real aplicação.

A questão apontada levaria que fosse reconhecido o *hacker* como possível ou provável combatente regular, utilizando-se de um computador para alcançar seus propósitos. Suas atividades e as medidas de ação e reação precisarão ser autorizadas e avaliadas, preferencialmente centralizadas, evitando a dispersão e a demora para reunir informações e tomar as decisões necessárias para responder aos ataques e implementar as medidas de defesa. (16:8-9)

No final da década de 1990 surgiu o *Network-Centric Warfare*, na Marinha norte-americana, para que permitisse estabelecer uma rede de informações para que as estações possam estabelecer comunicações entre as estações e seus sensores. Este centro de comando e controle foi adotado pelo Departamento de Defesa norte-americano, principalmente durante as guerras no Iraque, para que auxiliassem os comandantes nos diversos escalões de combate, na transmissão de conhecimentos e compreensão da situação durante o transcorrer das operações, permitindo que fossem compartilhadas informações e orientações para as ações no campo de batalha contra o inimigo. (5:155)

[3] Espaço Virtual: dimensão ou domínio de uma realidade não física, constituída por elementos (equipamentos) e ações da informática, realizadas por um computador e seus programas.

Diversos profissionais apontam que o computador será a arma do futuro a ser utilizada numa Guerra Irrestrita, propondo também uma forma de Guerra Assimétrica, que poderia provocar uma paralisia estratégica.

De acordo com o Professor Francisco Carlos Teixeira da Silva: (18:4-7)

> **Guerra Irrestrita**: no seu potencial, extensão e intensidade, destrutiva e generalizada, sem limites de poder econômico ou tecnológico.
> **Guerra Assimétrica**: conjunto de formas de enfrentamento não-convencionais visando confrontar com um poder militar, técnico e econômico superior [...] meios de combate capazes de infringir um grande dano a um poder superior, sendo por isso mesmo considerada a forma por excelência da luta do fraco e pobre contra o forte.
> **Guerra Preventiva**: forma de agir de um estado que considera a evolução possível de uma ameaça exterior como inevitável e capaz, com o tempo, de potencializar sua capacidade específica que estaria sendo adotada por um adversário, e que numa guerra futura inevitável seja desfavoravelmente utilizada. Para sua realização é necessário que um extremo preparo prévio, com as medidas de uma inteligência militar competente, visando estabelecer o ponto de gravidade do adversário a ser atingido, evitando um contra-ataque fulminante.
> **Guerra Preemptiva**: trata-se de reconhecer a possibilidade de um ataque iminente, visando reduzir o potencial bélico do inimigo, de quem é retirado o elemento surpresa, baseando-se largamente em sistemas sofisticados de informação e alerta prévio, subordinando-se, portanto, a um amplo sistema de inteligência.

Com esse enfoque começa a ser observado um novo centro de gravidade[4] nos conflitos, onde a informação poderá ser usada para causar paralisia estratégica, seja na escalada de uma crise ou na guerra propriamente dita. O conflito produzirá uma nova e profunda mudança no mundo: o choque tecnológico do confronto virtual[5].

Ao destacar as possibilidades dos computadores, Alvim Toffler ao dissertar a respeito do "Infoterror" destacou: (21:179-180)

> Muito se tem escrito sobre vírus de computadores que podem destruir dados ou roubar segredos e dinheiro [...] Se tiverem acesso às redes adequadas, poderão, pelo menos em teoria, armar, desarmar ou alterar o alvo de armas [...] Os vigilantes dos computadores de hoje preocupam-se com o chamado "vírus teleguiado", uma arma esperta que foi preparada para atingir um alvo específico [...] É o equivalente, em programas de computador, ao míssil de

[4] Centro de Gravidade: É o ponto (ou pontos) onde a aplicação de força pode produzir os melhores resultados e, no limite, induzir ao sucesso na guerra, isto é, à obtenção do propósito político. (8)
[5] Confronto Virtual: Forma de conflito em que são utilizadas as redes de computadores para organização e desenvolvimento de suas doutrinas, estratégias e tecnologia. (3)

> cruzeiro inteligente [...] O vírus, então, salta para o computador e segue seu caminho. Uma vez lá dentro, lança a sua carga destruidora.

Países mais fracos, tecnologicamente inferiores, poderão desencadear ataques de dissuasão contra países mais fortes, tecnologicamente superiores, através de uma conjugação de esforços para causar danos irreparáveis ou redução de sua capacidade de reação através de suas redes de computadores, interferindo no "ciclo de decisão"[6] daqueles responsáveis pelos mais diversos escalões.

Novos parâmetros deverão ser incluídos nas comparações e avaliações dos pontos de força e dos pontos de fraqueza[7]. A Ciberguerra deverá ser enfocada como emprego das Forças Armadas em Operações Militares de Não-Combate[8] para um confronto a ser desencadeado por agentes civis ou militares, em território inimigo ou à longa distância, utilizando-se da Internet para concretizar as suas ações. (26:15, 23-24)

As Forças Armadas terão que realizar funções de aquisição, processamento, distribuição e proteção de informações, negando o acesso a esta e selecionando como irão distribuí-las. (21:170)

O CONFLITO NA ERA VIRTUAL

Para estudar e prevenir as possíveis ameaças do "ciberterrorismo"[9], alguns países organizaram uma conferência sobre o "ciberterrorismo" em Budapeste em 2001. O propósito era criar uma cooperação internacional, bem como uma legislação global que pudesse regulamentar os crimes cibernéticos. Entre as ações acordadas estão: prevenção contra acessos de interferências ilegais (ataques de *hackers*), pornografia infantil (pedofilia), fraudes e farsas relacionadas à informática (*crackers e script kids*), quebra de patentes e direitos autorais (espionagem eletrônica), interferências em sistemas e em dados e a má utilização de programas. A dificuldade em ratificar os documentos gerados está nas atitudes que poderão

---

[6] Ciclo de Decisão: Também chamado de Ciclo de Boyd ou ciclo OODA – "Observe, Orient, Decide, Act" (Observação, Orientação, Decisão, Ação).
[7] Pontos de Força e Fraqueza: Processo de Planejamento Militar (PPM).
[8] Operações Militares de Não-Combate: Operações militares outras que a Guerra ("Military Operations Other Than War" – MOOTW). Classificação outras de tipos de ações de guerras. (25)
[9] Ciberterrorismo: Terrorismo cibernético ou terrorismo virtual. O uso da informática para fins terroristas.

ameaçar a liberdade de civis comuns, que nada tem a ver com a ilegalidade dos atos dos *hackers* ou dos "ciberterroristas"[10]. (23)

O termo "ciberterrorismo" surgiu na década de 1980, bem antes da difusão em massa da Internet. "Ciberterrorismo" é um ataque premeditado e de motivação política contra informações, sistemas e redes de computadores, programas de computadores e seus bancos de dados. Tais ataques podem causar danos à sociedade, provocar prejuízos aos sistemas econômicos, perda de energia ou água, entre outros sistemas de infra-estrutura vitais, que servem à população, podendo causar pânico através da desorientação e/ou interrupção de serviços, muito mais que os causados pela destruição física em si. (23)

As Operações Cibernéticas dependerão muito menos das posições geográficas, não sofrendo os mesmos efeitos que as comunicações rádio-eletrônicas, constantemente expostas aos efeitos de atrição, influências ambientais que interfiram na qualidade de transmissão de informação. Dependerão de equipamentos adequados para a operação, softwares de última geração e operadores altamente qualificados. (3:44)

Os principais oponentes apontados por Arquilla e Ronfeldt no seu trabalho *"Cyberwar is coming"* serão: atores não-estatais; terroristas; fundamentalistas políticos e religiosos; criminosos comuns; e organizações estrangeiras. (3:49)

Estes oponentes poderão desencadear manipulações idealistas ou extremistas que serão exploradas nos conflitos na era virtual. Dentro desta realidade as perspectivas seriam identificar: os efeitos potenciais e os princípios teóricos e operacionais das atividades, formular doutrinas estratégicas e táticas para as Forças Armadas e Instituições de Inteligência, especificar os níveis de intensidade do conflito, distinguir os elementos tecnológicos dos não-tecnológicos e as diferentes modalidades de ataques cibernéticos. (3:49)

De acordo com Alvin e Heidi Toffler, no livro "Guerra e Anti-Guerra: sobrevivência na aurora do terceiro milênio", eles destacaram a necessidade de ampliar o alcance e a letalidade das armas influenciadas pelas novas forças econômicas e tecnológicas: (21:87)

> Destrua as instalações do comando do inimigo. Acabe com as comunicações deles, para evitar que as informações fluam nos dois sentidos pela cadeia de comando. Tome a iniciativa. Ataque em profundidade. Evite que os escalões de apoio do inimigo entrem em ação. Integre as operações no ar, em terra e no mar. Sincronize as operações combinadas. Evite o ataque frontal contra os

[10] Ciberterrorista: Terrorista cibernético ou terrorista virtual. Usuários da informática para o terrorismo.

> pontos fortes do adversário. Acima de tudo, saiba o que o inimigo está fazendo e evite que ele saiba o que você está fazendo.

Com o propósito de invadir os programas de controle e comando operacionais, aguardando o momento propício para ativar o ataque, destacam-se as principais vulnerabilidades de uma Nação que seriam os pontos críticos para a Segurança Nacional: (16:4-5) (14)

1) Redes de geração e distribuição de energia elétrica;
2) Redes de produção e distribuição de água potável;
3) Redes de controle e direção de transporte e tráfego (aéreo, rodoviário, ferroviário e naval);
4) Redes de informações de emergências (prontos-socorros, polícia, bombeiros, defesa civil);
5) Redes bancárias (movimento bancário);
6) Redes de comunicação em massa (rádio e televisão);
7) Sistemas interligados por satélites artificiais (telefonia, sinais de televisão, meteorologia, sistemas de posicionamento geográfico);
8) Redes do Ministério da Defesa;
9) Ministérios e Secretarias dos Governos (Federal, Estadual e Municipal) e suas estruturas de poder (Poderes Executivo e Legislativo);
10) Sistema Judiciário (Poder Judiciário); e
11) Sistemas de Justiça Eleitoral.

A guerra cibernética servirá para que grupos de combate recebam informações em tempo real, garantindo o sucesso da incursão. Forças regulares, com um número menor de elementos que anteriormente necessários, enfrentarão forças superiores em proporção, mas terão como maior vantagem, as informações a respeito do inimigo, dissuadindo o potencial agressor, obrigando-o a recuar ou desistir do conflito. (3:51)

Os efeitos produzidos pelos ataques da Guerra Cibernética são: (1:152)

- Inutilização permanente de componentes da estrutura, negando o seu efetivo serviço;
- Atacar a lógica operacional de um sistema, introduzindo atraso ou comportamento indesejável no seu funcionamento;
- Obter o controle dos processos de decisão e a sua capacidade de percepção e compreensão de acontecimentos ou fatos;

- Destruir a confiança que os utilizadores possuem no sistema de informação e na sua rede que os suporta; e
- Manipular, modificar e destruir o comportamento decisório dos utilizadores, influenciando as suas decisões e incapacitando-os a continuar operando seus sistemas.

As transmissões de informações aos elementos de combate permitirão tomadas de decisão apuradas em ações de ataque, bem como introduzir o elemento surpresa nas contramedidas, contra um inimigo que venha atacar uma força posicionada no terreno. Durante um ataque convencional, uma força atacante se vê obrigada a dispersar suas forças numa região em que suspeita encontrar o inimigo Possuindo as informações necessárias, um comandante poderá decidir onde será o melhor ponto para um ataque, ou no caso de uma reação, quais são as vulnerabilidades da força atacante. (3:52)

CIBERGUERREIROS

Na guerra do Golfo Pérsico, em 1991, a CIA (Agência Central de Inteligência - EUA), observou que durante o conflito, o governo da China, elaborou estudos para tentar derrotar os EUA através da área de computação desenvolvendo vírus ofensivos, além de um sistema de contra-medidas. De acordo com o FBI - *Federal Bureau of Investigation* (Bureau Federal de Investigação - EUA) um vírus, provavelmente gerado na universidade chinesa da província de Guandong, em nove horas de atividade, teria infectado mais de 250 mil sistemas, causando prejuízos econômicos em torno de 2 bilhões e meio de dólares. Após estes relatos, o Pentágono mantém uma equipe permanente de profissionais para proteção do seu sistema composto por 2,5 milhões de computadores. Apesar de todos os cuidados e um orçamento específico para defesa cibernética, eles têm sofrido invasões constantemente, como foi realizado pelo *RED CODE*, cavalo de tróia perigoso, que se instalou nos computadores localizados nos EUA, automaticamente transmitindo-se para outras máquinas ao redor do mundo. Ele teria sido criado para atacar especificamente a Casa Branca, desativando todos os computadores que participam de sua rede. Os administradores da rede conseguiram driblar o ataque através de trocas sucessivas de endereço fixo em cada domínio na Internet. Apesar de o *RED CODE* não ter conseguido atingir o seu objetivo principal, paralisou vários servidores localizados nos EUA. (1:148) (7)

Os computadores pessoais (PC) e os portáteis (*notebooks*), além de celulares com acesso a Internet, e *notepads* ou *palmtops*, estão cada vez mais popularizados, aumentando as

possibilidades de ameaça de invasão de redes de computadores e demais meios de comunicação. Esta ameaça produz efeitos no sistema comunicação atingindo as práticas de uma guerra, que poderia classificada como guerrilha eletrônica. Este fenômeno aumenta a cada dia, quanto mais cresce a Internet e maiores sejam os usuários, que motivados pelo desafio ou curiosidade, seja com objetivos pessoais ou corporativos, realizam invasões nos sistemas de todo o mundo.

Uma quantidade enorme de programadores, técnicos de informática e curiosos autodidatas, com tempo disponível e intenções maliciosas, por diversão ou profissão, navegam pela Internet à procura de falhas na segurança dos sistemas de informação de empresas, de corporações militares ou de particulares. Estes poderão se tornar armas militares, "ciberguerreiros", operando a partir de centros especializados, em tempo de paz ou de guerra, com a missão de obter informações confiáveis, ou penetrando nos sistemas do inimigo, com o propósito de desativá-los, ou obter elementos que possam contribuir para a derrota do inimigo durante o conflito. Estes "ciberguerreiros" também poderiam ser utilizados para o terrorismo internacional. (1:151)

Diariamente os jornais vêm alertando os usuários a respeito dos danos causados pela pirataria eletrônica em bancos, empresas de aviação, escolas, universidades, e uma diversidade de proprietários de redes. Diariamente novos casos são relatados, não poupando sequer o usuário comum, que tem seus dados retirados de sua máquina e utilizados contra sua vontade. Para cada sistema de defesa desenvolvido, são criadas novas medidas de ataque. Assim as Forças Armadas devem incentivar a qualidade em termos de recursos humanos, capacitando alguns elementos de seu contingente, para novas doutrinas, métodos de organização mais eficientes, treinamentos especializados (principalmente nos tempos de paz) e com melhores equipamentos e sistemas mais atualizados, adequados para enfrentar "ciberguerreiros".

Nesta nova perspectiva, os combatentes devem ser continuadamente capacitados no uso avançado da informática, visando assimilar um rápido fluxo de informações e, desempenhar missões num ambiente virtual multinacional. Seus oponentes poderão estar em qualquer lugar do planeta, prontos para causar danos irreparáveis, não somente em organizações militares, mas em todo o País e em possíveis aliados.

Cada "Centro de Comando e Controle de Combate", de instalações militares, ou em organizações de Estado-Maior, irão dispor de microcomputadores conectados na internet, onde militares atuarão numa realidade virtual, onde os danos causados poderão ser equivalentes, ou até, maiores que aqueles já vistos nas guerras até o momento. Estes militares

serão conhecidos como “ciberguerreiros”, enfrentarão inimigos que não respeitam regras ou condutas tradicionais de guerra, ou seguem uma doutrina específica, vencerá a guerra quem causar maiores danos ao adversário.

Esta nova realidade não poderá isentar as Forças Armadas de manterem-se atualizadas, bem como, manter permanente pesquisa de sistemas ofensivos e defensivos, visando a sua própria proteção e de todo o País.

PERSPECTIVAS PARA AS FORÇAS ARMADAS

As Forças Armadas deverão implementar ações para fazer frente à ameaça cibernética, além do tradicional uso de *softwares* de proteção, criptografia e garantia de segurança de redes locais. Os “ciberguerreiros” deverão absorver uma tecnologia que evolui rapidamente, requerendo constante atualização.

Em conformidade com a NBR 17799[11], são os seguintes, os aspectos que devem ser observados por organizações militares e órgãos estatais na implementação de medidas de qualidade na gestão de segurança da informação[12]:

1. Política de Segurança da Informação, provendo orientação e apoio da direção à empresa para a segurança da informação;
2. Organização da Segurança dentro da empresa, provendo infra-estrutura de segurança da informação na organização;
3. Classificação de informações e controle dos ativos, mantendo a proteção adequada dos ativos de informação;
4. Segurança aplicada a recursos humanos, reduzindo os riscos de erro humano, roubo, fraude ou uso indevido de instalações;
5. Segurança física e do ambiente da informática, prevenindo o acesso não autorizado, dano e interferência às informações e instalações físicas da organização;
6. Gerenciamento das operações e das comunicações, para garantir a operação segura e correta dos recursos de processamento da informação;
7. Controle de acesso, controlando o acesso à informação;

---

[11] NBR 17799, Comentários sobre a Gestão de Segurança da Informação. Disponível em: http://www.sphinxbrasil.com/arquivos/aplicacao/gap/iso_17799.PDF. Acesso em: 02 jul. 2005.

[12] BS 7799, ISO - International Organization for Standartization, ISO 17799-1 Comentários para Centros de Especialização em Segurança. Disponível em: http://www1.serpro.gov.br/publicacoes/tema/157/T151_02_a.htm. Acesso em 02 jul. 2005.

8. Manutenção e desenvolvimento de sistemas, para garantir que a segurança seja parte integrante dos sistemas de informação;
9. Gerenciamento da continuidade, não permitindo a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos; e
10. Conformidade com leis e regulamentos, garantindo a adequação dos sistemas com as leis, estatutos, regras, obrigações contratuais, políticas e normas institucionais de segurança e de quaisquer requisitos de segurança.

Por ser um assunto que atualmente vem chamando a atenção dos mais diversos tipos de especialistas, com base na literatura existente sobre o assunto e os aspectos apontados neste trabalho, as seguintes propostas são apresentadas para a adequação das Forças Armadas a esta realidade, desempenhando o papel de emprego tecnológico do Poder Militar:

- Adoção de um programa de Inspeção Administrativa e Auditoria voltada especificamente para a análise da Segurança Digital, identificando e avaliando as vulnerabilidades;
- Subsidiar a elaboração de Programas de Segurança Institucional em organizações federais, estaduais e municipais;
- Programas de conscientização, envolvimento, adestramento, qualificação e operação de Segurança Digital, levando ao desenvolvimento de uma cultura de segurança;
- Elaboração de Políticas, Normas, Planos, Doutrinas e Procedimentos de Segurança Digital e da Informação;
- Regulamentação e instituição de um Sistema de Segurança da Informação, detalhando as competências que deverão ser atribuídas aos órgãos de uma estrutura de defesa cibernética com a finalidade de assessorar o processo decisório em seus níveis correspondentes;
- Elaboração de Objetivos de Defesa Cibernética, destacando-se os campos de atuação nas áreas estratégicas, políticas, militares, econômicas, psico-sociais, científicas e tecnológicas a serem protegidas;
- Parcerias com os setores empresariais privados e acadêmicos para o desenvolvimento e o compartilhamento de experiências, buscando soluções eficazes para aperfeiçoar as ações específicas frente à ameaça cibernética;
- Desenvolver e implementar um programa de formação de pessoal nos níveis especialização e aperfeiçoamento, qualificando oficiais e praças com conhecimentos

de informática de alto nível, bem como prepará-los para operar num ambiente repleto de incertezas e que exige presteza e agilidade de resposta. Estes militares deverão ser hábeis na tecnologia da informação e da informática, capazes de aplicá-las e reconhecer quando irão auxiliar ou impedir que se alcance os ganhos pelo seu uso aplicado;

- As organizações militares deverão elaborar um Plano de Segurança Digital, que atenda a todos os escalões e setores, superiores, institucionais e individuais;
- Sistemas de monitoramento de redes e barreiras de proteção que impeçam o acesso remoto sem permissão, além de tramitação de mensagens e documentos criptografados, com chaves apropriadas para respectiva classificação;
- Medidas preventivas internas deverão ser tomadas para evitar a quebra de segurança. Uma das propostas seria a criação de duas redes independentes, à semelhança com das existentes (Intranet e a Internet), estanques, sem qualquer integração física. Todo o serviço administrativo e militar seria feito pela Intranet ficando para a Internet os serviços sem relação direta com as características das Organizações; e
- Desenvolver softwares de uso exclusivo para Intranet, incapacitando o compartilhamento de trabalhos realizados nos computadores da Internet. Informações poderão ser levadas por meio magnético dos computadores da Internet para aqueles do ambiente Intranet durante elaboração de trabalhos, mas inversamente não, onde dispositivos de proteção não permitiriam que informações da Intranet fossem compartilhadas com a Internet.

CONCLUSÃO

Diante da recente ameaça de “Ciberguerra” surge à necessidade da rápida adequação das Forças Armadas a esta situação. A capacitação de militares, a renovação de equipamentos e *softwares* é condição para proteção do espaço virtual brasileiro, das instituições nacionais e da população.

A “Revolução Científica” trouxe grandes evoluções na área da Informação, que permitiram que fosse conhecida como “Revolução da Informação”.

Essas evoluções tecnológicas permitiram que uma nova ferramenta fosse desenvolvida, a Informática. As Forças Armadas têm agora uma nova ameaça correlacionada com a Internet, a “pirataria eletrônica”. A vulnerabilidade dos sistemas obrigará que métodos

de defesa sejam criados para preservar a sua integridade e proteger as redes de informação e os seus meios de comunicação. Esta tecnologia permitiu que fosse observada uma nova frente de batalha, o ambiente da Internet, uma interpretação militar para a "pirataria eletrônica". Os combates irão ocorrer também num ambiente muito parecido com um videogame. Neste novo cenário exige-se que o pessoal das Forças Armadas tenha nível cultural e acadêmico, capacidade de processar informações, adaptabilidade e excelente domínio da tecnologia, com grande perspicácia, sagacidade, versatilidade e criatividade.

O governo brasileiro, através do Ministério da Defesa e dos Comandos Militares, incluindo as agências estatais de informação, deverá avaliar a criação de um quadro especial de *"hackers"*, capacitando e formando oficiais e praças para o desempenho desta função. Para essas atividades de inteligência (incluindo sabotagem, ataque e defesa), eles seriam considerados como militares de Forças Especais para Operações Digitais, os Ciberguerreiros. Estarão sob o comando de um órgão especial, subordinados aos Comandantes de Teatros Operativos para ações de auxílio à tomada de decisão, ou mesmo, ao Comandante Supremo, quando ações estratégicas e políticas estiverem em questão.

Estar preparado para a Guerra Cibernética seria uma ferramenta eficaz em escaladas de crise, uma resposta aos possíveis adversários, ações contra alvos estratégicos, prontos para ataques preventivos, ataques em resposta a ações de ataques cibernéticos já em andamento, buscando demonstrar força para atuar num novo tipo de confrontação entre países.

BIBLIOGRAFIA

1. ALVES, José Ricardo Rodrigues Teixeira. A Guerra de Informação. **Revista Marítima Brasileira**, v.122, n.10/12, p.143 - 153, out. / dez., 2002.
2. ANNUNCIAÇÃO, João Wander Nascimento de. **Ciberwar: Uma proposta genérica de ações defensivas para a MB**. Ensaio (CEMOS) – Curso de Estado Maior para Oficiais Superiores, Escola de Guerra Naval, Rio de Janeiro, 2003.
3. ARQUILLA, Jonh; RONFELDT, David. **Cyberwar is coming**. Comparative Strategy, vol. 12, nº 12, 1993. Taylor & Francis Inc. Disponível em: www.rand.org/publications/MR/MR880/MR880.ch2.pdf. Acesso em: 18 mai. 2005.
4. BECKER, Bertha K.. **A Geopolítica na virada do milênio: logística e desenvolvimento sustentável**. Em Geografia: conceitos e temas. Iná Elias de Castro, Paulo César da Costa Gomes, Roberto Lobato Corrêa. 2001, 3ª ed., Rio de Janeiro - RJ, Ed. Bertrand, Brasil. (p. 287 - 289)
5. BRAGA, Carlos Chagas Vianna. Poder Naval na Guerra do Iraque: fazendo a diferença. **Revista Marítima Brasileira**, v.125, n.01/03, p.155, jan. / mar., 2005.
6. BRANDT, D. Scott. **Information Technology Literacy: task knowledge and mental models**. 2001, Library Trends. Vol. 50, nº 1. The H. W. Wilson Company. Disponível em: www.informatik.uni-trier.de/~ley/db/journals/libt/libt50.html. Acesso em: 17 mai. 2005.
7. CARVALHO, Nino. **Internet: arena da próxima guerra**. Disponível em: http://jbonline.terra.com.br/papel/cadernos/internet/2001/09/05/jorinf20010905001.html. Acesso em: 12 jun. 2005.
8. CLAUSEWITZ, Carl Von. **Da Guerra**. 1976, Lisboa – Portugal, Ed. Perspectivas & Realidades, Artes Gráficas, Ltda.
9. COSTA, Darc Antonio da Luz. **Estratégia. A cooperação Sul-Americana como caminho para a inserção internacional do Brasil**, Rio de Janeiro, COOPE - UFRJ, 2003, p. 56 - 57. Na apostila de História, COOPEAD - UFRJ, Professor Francisco Carlos Teixeira da Silva, 2005.
10. DIGERATI BOOKS. **Segurança e Espionagem Digital**. 2005. Edição Especial.
11. DUARTE, Sérgio Luiz Goulart. **Tecnologias Aplicadas a Guerra da Informação**. ABIN - Agência Brasileira de Inteligência. Rio de Janeiro – RJ, 2005.

Palestra proferida na Escola de Guerra Naval (EGN) para o Curso de Estado Maior para Oficiais Superiores (CEMOS). Em 20 jul. 2005.

12. FILHO, Luciano Fabrício Riquet. **Guerra Estratégica de Informações: um novo meio de fazer a guerra?** Monografia (CPEM) – Curso de Política e Estratégia Marítimas, Escola de Guerra Naval, Rio de Janeiro, 2003.

13. ON LINE EDITORA. **Segurança. Conceito, proteção, vacina anti-hackers e cia**. 2005, Coleção Guia Fácil de Informática, ano 1, vol. 4.

14. PAGLIUSI, Paulo. **Guerra da Informação**. Centro de Análise de Sistemas Navais (CASNAV). Rio de Janeiro – RJ, 2005. Palestra proferida na Escola de Guerra Naval (EGN) para o Curso de Estado Maior para Oficiais Superiores (CEMOS). Em 20 mai. 2005.

15. PIROPO, Benito. Criando Botnets. **JORNAL O GLOBO**. Rio de Janeiro, 30 mai. 2005. p. 4, Caderno INFORMÁTICA.

16. SAMPAIO, Fernando G.. **Ciberguerra. Guerra Eletrônica e Informacional. Um novo desafio estratégico**. Texto para debate em 26/04/2001. Escola Superior de Geopolítica e Estratégia, Porto Alegre - RS, 2001. Disponível em: www.defesanet.com.br. Acesso em 19 mai. 2005.

17. SANTOS, José Athos Irigaray dos. **Agência Brasileira de Inteligência**. ABIN - Agência Brasileira de Inteligência. Rio de Janeiro – RJ, 2005. Palestra proferida na Escola de Guerra Naval (EGN) para o Curso de Estado Maior para Oficiais Superiores (CEMOS). Em 20 jul. 2005.

18. SILVA, Francisco Carlos Teixeira da. **As guerras e as revoluções do século XX. As grandes transformações do mundo contemporâneo**. Ed. Campus, 2004. (p. 2 a 12)

19. SILVA, Iberê Mariano da. **SOFTWAR**. Disponível em: www.uff.br/nest/softwar.htm. Acesso em 12 jun. 2005.

20. TOFFLER, Alvin. **A Terceira Onda**. 3ª ed., 1980, Rio de Janeiro, Ed. Record. (p. 23 - 32, p. 174 - 183, p. 147 - 160)

21. TOFFLER, Alvin; TOFFLER, Heidi. **Guerra e Anti-Guerra: sobrevivência na aurora do terceiro milênio**. Rio de Janeiro, Biblioteca do Exército, 1995.

22. UNITED NATIONS ORGANIZATION. **Developments in the field of information and telecommunications in the context of international security**. jul. 2001. Disponível em: www.un.org/documents/ga/docs/56/a56164.pdf. Acesso em: 24 jul. 2005.

23. VELOSO, Adriana. **De que forma a humanidade utilizará a tecnologia em seus conflitos?** Disponível em: http://www.novae.inf.br/pensadores/ciberguerra.htm. Acesso em: 18 mai. 2005.

24. VESENTINI, José William. **Novas Geopolíticas**. 2003, 2ª edição, São Paulo, Editora Contexto. (p. 94 - 95).

25. VIDIGAL, Armando Amorim Ferreira. **O Brasil diante dos desafios internacionais em segurança e defesa**. 2003. Disponível em : www.defesa.gov.br/enternet/sitios/internet/ciclodedebates/textos.htm. Acesso em: 25 jul. 2005.

26. _____. A missão das Forças Armadas para o século XXI. **Revista Marítima Brasileira**. Separata 2004, p. 13 a 27, dez., 2004.

27. WIENER, Norbert. **Cibernética ou Controle e Comunicação no animal e na máquina**. 2ª ed., São Paulo, Ed. Polígono, 1970 (p. 25 a 72)

28. WILSON, Clay. **Information Warfare and Cyberwar: capabilities and related policy issues**. jul. 2004. Congressional Research Service. The Library of Congress**.** Disponível em: www.fas.org/irp/crs/RL31787.pdf . Acesso em: 18 mai. 2005.

ANEXO A

VÍRUS, *WORM* (VERME), *SPAM* E CAVALO DE TRÓIA (*TROJAN*)

São programas ou rotinas, pragas virtuais, recebidos através de e-mails, com logotipos de grandes prestadores de serviços (ou empresas) ou de provedores conhecidos, com um *link* para acesso, que depois de efetuado, inicia um *download* de um anexo indesejado, ou ainda, alojando um arquivo (ou programa) para captura de dados da máquina, através do uso da correspondência eletrônica e seus anexos. Podem ser de ação imediata ou com data e hora especificados, copiando e enviando informações para um endereço remoto. (1) (2)

- **Vírus**: como nas análises médicas, tem a capacidade de causar sérios danos ao infectado, levando a sua incapacidade parcial ou total, precisando de um computador, onde se alojam para se multiplicar, causando danos ao sistema onde estão sendo executados, não infectando arquivos, mas explorando as vulnerabilidades operacionais e seus aplicativos;

- ***Worm* (verme)**: relacionando o nome ao uso, o parasita habita o hospedeiro sem que este saiba que está sendo danificado, apropriando-se de suas informações. Tem a capacidade de propagaram-se de um computador para outro através da rede (mobilidade virtual), não se multiplicando. Além de sistemas destroem arquivos;

- ***Spam***: lixo eletrônico recebido através de mensagens não solicitadas, não desejadas e não autorizadas que congestionam os sistemas de correio eletrônico. O *Scam* é o termo usado para designar os tipos de mensagem, que além de serem incomodas, elas trazem alojadas nas mensagens eletrônicas elementos para tentar obter informações confidenciais do usuário;

- **Cavalo de Tróia**: nome bem apropriado para a inserção (“presente de grego”) de um programa dentro do computador, sendo acionado através de um gatilho, de forma automática ou comandado remotamente. Não se autopropagam e nem se multiplicam. Ficam escondidos no sistema até realizarem as tarefas nocivas programadas.

PESCARIA DE SENHAS

Conhecido na internet como *phishing scan*, são roubos de senhas eletrônicas para serviços na internet, ou de números de cartões de auto-atendimento, bancários ou não, e suas senhas, por meio de e-mails ou contato direto por telefone, induzindo o usuário a prestar informações. (1)

HACKERS

Programadores ou especialistas profissionais em computadores, dedicados a descobrir brechas ou vulnerabilidades no funcionamento da Internet e das máquinas ligadas a ela. Principal objetivo é causar danos irreparáveis ou inutilizar sistemas, redes ou computadores, não perdendo tempo com computadores pessoais (PC). (1) (2)

- ***Hackers White Hats***: especialistas que dedicam seu profissionalismo para descobrir falhas de programas para auxiliar os fabricantes na busca por soluções das falhas de seus programas;

- ***Hackers Gray Hats***: defendem a idéia do *software livre*, assim, divulgam pela Internet as falhas e as maneiras de explorá-las. Praticam o desenvolvimento de ferramentas alternativas e baratas que concorram com o comércio da informática;

- ***Hackers Black Hats***: criminosos que têm grande capacidade de atuação na área da Tecnologia da Informação (redes e computadores), desenvolvendo ferramentas para espionagem empresarial, chantagem, furto de senhas, dados bancários, números de cartões de crédito, com a finalidade de obter retornos próprios, fornecendo pela Internet os meios para que curiosos possam executar suas atividades malévolas (são os fornecedores dos produtos que permitem a "pirataria eletrônica". Por isso que genericamente chamamos os "piratas" de ***"hackers"***).

SCRIPT KIDS

Ou *Lamers*, ou *Lummers* ou *Wannabes*, são piratas amadores, curiosos do mundo da segurança digital, utilizando ferramentas ou dispositivos comuns, desenvolvidos por *hackers*. Não dominam completamente as técnicas de invasão, dependem de outros para fornecerem os meios necessários. Após demonstrarem proficiência nas técnicas, poderão ser recrutados por alguma quadrilha profissional. (1) (2)

CRACKER

Adoram retirar informações digitadas nas caixas de e-mail (correio eletrônico) ou capturar o catálogo de endereços do usuário. São invasores profissionais ou espiões especialistas somente em sistemas operacionais de computadores, que também atacam focados no vandalismo, considerados pelos especialistas os verdadeiros vilões virtuais da atualidade. Normalmente estão associados à criação de rotinas malévolas para: vírus, *trojans*, roubos de arquivos, senhas, dados, programas, modificações de códigos, invasão, inutilização e destruição de redes, sistemas e computadores. (1) (2)

DEFACERS

Pichadores virtuais que se dedicam exclusivamente a desfigurar páginas na Internet para acarretar prejuízos à imagem da empresa afetada. Não apagam ou destroem informações de suas vítimas. (2)

ESPIÃO DIGITAL

Profissional que utiliza o meio eletrônico ligado à informática para ter acesso a informações normalmente inacessíveis através de programas espiões (*Spywares*). Existem dois tipos de espionagem: (1)

- **Espionagem Oficial**: Praticada pelo Poder Público, nos casos de guerra ou nos Serviços de Segurança Nacional, respaldados pelo poder Executivo. Estes serviços são executados por órgãos de inteligência institucionais e também, pode ser praticada pelo Poder Judiciário, que são os serviços de investigação das Polícias Civis ou da Polícia Federal, apoiadas em mandato judicial.

- **Espionagem Particular**: Praticada por indivíduos ou instituições privadas, recaindo em crime de espionagem, por não terem mandato ou ordem expressa do poder competente.

CARNIVORE

Sistema de "escuta" eletrônica, monitorando todo tipo de mensagem, comunicação telefônica, correio eletrônico e mensagens de *pagers*. Monitoram toda informação de entrada e saída, funcionando como um grande "farejador" (*sniffer*). Existem ainda no mercado programas semelhantes como o *ETHERAL*, *ECHELON* e *SEMANTIC FORESTS*, cujo

propósito é procurar por determinados assuntos ou parâmetros, interceptando a informação para sua captura. (1) (4)

BOTNETS

Criação de uma rede controlada remotamente para ataques do tipo "negação de serviço" ao usuário, recebendo uma mensagem indesejada com conteúdo não apropriado e com programas que permitem que qualquer computador seja controlado. Cria-se uma rede de operação remota ao ser contaminado o computador com a inserção de um programa "cavalo de tróia", de modo que o usuário não tenha a menor idéia que esteja participando ou sendo controlado, onde normalmente é difícil identificar a origem devido aos "saltos"[13] que são realizados dentro da rede. O controlador utilizar-se-á da identificação de qualquer computador contaminado participante da rede. (3)

BIBLIOGRAFIA

1. DIGERATI BOOKS. **Segurança e Espionagem Digital**. 2005. Edição Especial.

2. ON LINE EDITORA. **Segurança. Conceito, proteção, vacina anti-hackers e cia**. 2005, Coleção Guia Fácil de Informática, ano 1, vol. 4.

3. PIROPO, Benito. Criando Botnets. **JORNAL O GLOBO**. Rio de Janeiro, 30 mai. 2005. Caderno INFORMÁTICA.

4. VELOSO, Adriana. **De que forma a humanidade utilizará a tecnologia em seus conflitos?** Disponível em: http://www.novae.inf.br/pensadores/ciberguerra.htm. Acesso em: 18 mai. 2005.

[13] Saltos: Mudanças constantes de posição do controlador da operação remota na rede de computadores, dificultando a possibilidade de localização de sua origem.