Cel Com GILMAR PEREIRA DA SILVA

GUERRA CIBERNÉTICA: PREPARO E EMPREGO DO EXÉRCITO

Rio de Janeiro

2006

Cel Com GILMAR PEREIRA DA SILVA

GUERRA CIBERNÉTICA: PREPARO E EMPREGO DO EXÉRCITO

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do certificado de Especialização em Política, Estratégia e Administração Militares.

Orientador: JOSÉ HELENO ZANGALI VARGAS – Cel R/1

Rio de Janeiro

2006

S 586 SILVA, Gilmar Pereira da Silva**.**
Guerra cibernética: preparo e emprego do Exército / Gilmar Pereira da Silva. – 2006.
46 f.: 30 cm

Trabalho de Conclusão de Curso (Curso de Política Estratégia e Alta Administração do Exército)-Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2006.

Bibliografia: f. 45 - 46

1. Guerra cibernética. 2. Guerra da informação. 3. Revolução em assuntos militares. I. Título

CDD 355

Cel Com GILMAR PEREIRA DA SILVA

GUERRA CIBERNÉTICA: PREPARO E EMPREGO DO EXÉRCITO

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do certificado de Especialização em Política, Estratégia e Administração Militares.

Aprovado em

COMISSÃO DE AVALIAÇÃO

_____

JOSÉ HELENO ZANGALI VARGAS – Cel R/1 – Dr. Presidente
Escola de Comando e Estado-Maior do Exército

_____

WILLIAM ROBERTO EHRLICH DE MIRANDA – Cel Inf – Dr. Membro
Escola de Comando e Estado-Maior do Exército

_____

RICARDO RIBEIRO CAVALCANTI BAPTISTA – Cel R/1- Dr. Membro
Escola de Comando e Estado-Maior do Exército

À minha esposa, aos meus filhos e aos meus amigos pelo apoio e paciência nesta jornada.

AGRADECIMENTOS

Agradeço a minha esposa e aos meus filhos, pela paciência e apoio.

Agradeço ao Exército Brasileiro pela oportunidade.

Agradeço a meu orientador Cel José Heleno Zangali Vargas, pela paciência e pelo apoio sempre presente.

Agradeço aos amigos, pelo apoio sempre presente.

RESUMO

A integração de telecomunicações e computadores, construindo redes eletrônicas, é a base para a organização da sociedade pós-moderna. O mundo virtual das redes de computadores, conhecido como ciberespaço, é o campo de batalha da guerra cibernética, uma forma silenciosa de conflito que pode colocar em risco a sobrevivência das organizações contemporâneas. A guerra cibernética é um ramo novo da guerra da informação que pode ser usado em ações assimétricas contra atores poderosos do cenário internacional. O Exército Brasileiro precisa estar pronto para proteger-se contra as ameaças existentes, bem como para aproveitar as oportunidades criadas pelas novas armas. Este trabalho analisa a dependência da sociedade pós-moderna com relação às tecnologias da informação, identifica as principais características da guerra da informação e da guerra cibernética, levanta aspectos relevantes para o emprego da guerra cibernética, avalia a situação atual do Exército e propõe ações estratégicas para aperfeiçoar o seu preparo.

Palavras-chave: Guerra Cibernética. Guerra da Informação. Pós-Modernismo Militar. Revolução em Assuntos MIlitares.

ABSTRACT

The integration of telecommunications and computers, building electronic networks, is the foundation of post-modern society organization. The virtual world of computer networks, known as cyberspace, is the battlespace for cyberwar, a silent way of conflict that can risk the survival of present organizations. Cyberwar is a type of information warfare that can be used in asymmetric actions against powerful actors of the international scenery. The Brazilian Army needs to be ready for protecting against existing threats, as well as for taking advantages of the opportunities created by the new weapons. This paper analyses post-modern society dependence on information technologies, identifies primary characteristics of cyberwar and information warfare, raises relevant aspects for cyberwar employment, evaluates present Army situation and proposes strategic actions for improving its readiness.

Keywords: Cyberwar. Information Warfare. Revolution in Military Affairs.

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica das últimas décadas provocou a complexa revolução informacional que está mudando rapidamente as relações sociais, os modos de produção, as hierarquias de poder e a doutrina militar.

A integração das telecomunicações e da informática, por meio de redes de computadores, criou um novo espaço (ciberespaço), de amplitude mundial, onde se processa, armazena e circula informações relevantes para a sobrevivência das organizações.

Esse mundo virtual é o campo de batalha da guerra cibernética, uma forma silenciosa de conflito, que é travado entre indivíduos, grupos não-estatais e governos (CÔRTES, 2000), por meio de ações que podem produzir resultados no mundo real.

Nessa nova dimensão do conflito moderno, o ritmo acelerado da evolução tecnológica está sempre a criar novas armas (ALLEN, 2004) e enfraquecer defesas, aumentando a vulnerabilidade das organizações, inclusive as militares, à medida que se tornam mais dependentes da tecnologia da informação (CÔRTES, 2000).

Segundo alguns especialistas (KOCH 2005), ataques cibernéticos bem sucedidos contra a infra-estrutura (sistemas financeiros, redes de energia, controles de tráfego aéreo, etc.) de países fortemente dependentes de TI, podem provocar danos imprevisíveis de elevado custo político, social e econômico. Desse modo, a guerra cibernética pode representar a oportunidade para que indivíduos e pequenos grupos conduzam ações assimétricas contra atores poderosos do cenário internacional (CORTÊS, 2005; FELSTEAD, 2005).

Nesse contexto, a segurança da informação ganha dimensão estratégica, porque as ações cibernéticas podem não só interromper a continuidade dos negócios, mas também comprometer a sobrevivência das organizações contemporâneas.

As iniciativas tomadas nos últimos anos para automação dos sistemas de informação militares inseriram o Exército Brasileiro nesse contexto, obrigando-o a posicionar-se estrategicamente e preparar-se face ao problema.

Diante dessa situação, coloca-se o seguinte problema: como preparar o EB para enfrentar os desafios da guerra cibernética?

O objetivo deste trabalho de pesquisa é, portanto, sugerir ações estratégicas, que se destinam à melhoria do preparo do Exército Brasileiro para atuar no mundo virtual de computadores e redes, visando obter o domínio da informação, por meio de ações ofensivas contra os sistemas de informação de possíveis adversários e de defesa dos nossos próprios sistemas. Para alcançar esse objetivo, conforme consta dos capítulos seguintes, procurou-se analisar a dependência da sociedade pós-moderna com relação às tecnologias da informação, identificar as principais características da guerra da informação e da guerra cibernética, levantar as condicionantes mais relevantes do emprego de ações cibernéticas, avaliar a situação atual do Exército e propor ações estratégicas para aperfeiçoar o seu preparo.

O resultado da pesquisa poderá contribuir para a construção do conhecimento do Exército sobre o assunto, subsidiando ou originando novos estudos que objetivem a atualização da doutrina e do planejamento estratégico (preparo e emprego). Também poderá apoiar trabalhos sobre a atuação coordenada das Forças Armadas, uma vez que o problema alcança igualmente os sistemas de informação das três Forças Armadas e da Estrutura Militar de Defesa. Finalmente, para a sociedade brasileira em geral, poderá provocar efeitos positivos indiretos, decorrentes da melhoria do desempenho da Instituição, durante o cumprimento de suas missões constitucionais.

2 GUERRA DA INFORMAÇÃO

2.1 A SOCIEDADE PÓS-INDUSTRIAL

Conhecimento é poder, pois a partir do conhecimento é possível obter terra, mão-de-obra e capital. Essa constatação tornou-se evidente depois que as inovações tecnológicas das ultimas décadas, relacionadas com o trato da informação, mudaram o poder relativo que havia entre os fatores de produção desde a Revolução Industrial. O conhecimento passou a preponderar sobre os demais, provocando o surgimento de um novo modelo de sociedade que, dentre outros rótulos, tem sido chamada de pós-moderna, pós-capitalista, pós-industrial, do conhecimento ou da informação. Essa mudança de paradigma tem provocado transformações importantes, de amplitude global, nas interações entre as coletividades, na geração de riqueza e nas relações de poder.

Dentre as inovações revolucionárias, como a microeletrônica, o laser e a fibra ótica, o desenvolvimento da tecnologia digital merece atenção especial. Por meio dela, a informação contida nos sons, imagens, vídeos e textos pôde ser convertida para uma linguagem codificada, composta de “ uns” e “ zeros” . Uma vez transformada nesses dois dígitos, a informação ficou em condições de ser processada nos computadores e distribuída, sem perder a qualidade original, por fios telefônicos, fibras óticas, microondas, satélites, etc.

A digitalização da informação possibilitou, desse modo, a combinação da rapidez do computador com o alcance das comunicações, diminuindo o tempo consumido pela informação para vencer o espaço físico existente entre indivíduos e organizações. A partir daí, as relações sociais tornaram-se mais estreitas, dinâmicas, interativas e, portanto, mais poderosas. Assim, as novas ferramentas tecnológicas penetraram em todos os domínios da atividade humana, criando novas possibilidades de comunicação e cooperação, aumentando a complexidade da trama social, acelerando o ritmo das mudanças sociais e estimulando a organização da sociedade em redes.

Segundo Castells (2001), “ rede é um conjunto de nós interconectados.” A natureza dos nós depende do tipo de rede a que estamos nos referindo. Numa rede logística, por exemplo, os nós são fabricantes, transportadores, depósitos, varejistas

e clientes, que se interligam por meio de fluxos de mercadorias e de informações, para satisfazer suas necessidades específicas. As redes representam um modelo antigo de organização social, com a vantagem de ter maior flexibilidade, sem prejuízo do desempenho. Elas podem crescer sem limites, incorporando novos nós, sem perder o seu equilíbrio. O desenvolvimento das tecnologias da informação permitiu superar a dificuldade de administrar a complexidade de grandes redes, possibilitando que as mesmas se tornassem a forma predominante de organização das atividades humanas. Em virtude do seu melhor desempenho, as redes estão substituindo as estruturas centralizadas e hierárquicas.

Uma nova economia surgiu da inserção das tecnologias da informação nos processos de produção, gerenciamento e distribuição, e do estabelecimento de uma rede global de interação, que passou a servir de espaço para a organização das atividades econômicas, para a movimentação dos fluxos de capital e para a concorrência entre agentes econômicos. O novo sistema contribuiu para a expansão do capitalismo e fortaleceu o poder econômico dos países mais ricos, mas também excluiu muitas coletividades. Tendo em vista essa interdependência crescente, os Estados têm hoje dificuldade para estabelecer políticas econômicas genuinamente nacionais que assegurem a competitividade das empresas locais e estimulem a captação de capital estrangeiro.

Para sobreviver e ter lucratividade no ambiente dinâmico da concorrência global, as organizações passaram a empregar o conhecimento como instrumento para obter vantagens competitivas. Como resultado, dentre outras ações, foram realizadas a racionalização e automação dos processos internos, a adoção de estruturas mais flexíveis, a descentralização do poder para equipes e pessoas, a terceirização de atividades secundárias e a organização da empresa em rede. O esforço para a melhoria do desempenho econômico, no entanto, é apenas a primeira responsabilidade da organização contemporânea, que também deve estar comprometida com a sobrevivência e o bem-estar da sociedade.

O homem é o agente de todas essas transformações, porque o principal fator de produção da sociedade pós-capitalista – o conhecimento – está na sua mente. A contribuição do homem para a melhoria da produtividade da empresa depende, inicialmente, da sua qualificação adequada, que deve ser resultado do esforço individual de aprender continuamente para acompanhar as mudanças ambientais. Em segundo lugar, é necessário que o indivíduo tenha autonomia suficiente para

fazer o aproveitamento máximo e oportuno das tecnologias que estão à sua disposição. Finalmente, tem de estar motivado para inovar, tomar a iniciativa, decidir, analisar e realizar outras ações que só o cérebro humano pode realizar.

Através de redes globais, problemas como terrorismo, crime organizado, protecionismo econômico, ajuda humanitária, migrações ilegais, degradação do meio ambiente, proliferação de armas de destruição em massa e tantos outros, atravessam as fronteiras nacionais, sob a ação ou influência de governos, organismos, empresas, grupos e cartéis internacionais, desafiando o princípio territorial do Estado Moderno. Na outra extremidade dessa estrutura política, encontramos cidadãos mobilizados por meio de redes locais, monitorando o Governo e cobrando resultados, o que pode representar uma ameaça para a sua legitimidade, se os interesses desses cidadãos não forem atendidos. O resultado dessa combinação de servidões externas e internas é o enfraquecimento do Estado, que tem de ser submetido a reformas centradas no conhecimento, para ganhar agilidade e tornar-se apto a enfrentar com sucesso as mudanças ambientais que ameaçam a sua sobrevivência. Uma alternativa pode ser o estabelecimento de redes com países regionais para contrapor-se a grandes potências. Para auxiliar a resolução de problemas internos, uma solução pode ser o estabelecimento de programas de inclusão social ou de governo eletrônico.

A principal inferência sobre o mundo atual é que todos dependem das redes para conduzir suas atividades. Simplesmente não se pode estar isolado num mundo cada vez mais interligado. Uma prova disso é a expansão crescente da Internet, para onde concorrem pessoas, atividades e organizações, com o propósito de aproveitar as vantagens de estarem “ conectados” . Deixar de participar é arriscar a competitividade e a sobrevivência.

2.2 A INTERNET

A Internet nasceu em 1962, quando J.C.R. Licklider, da Agência de Projetos de Pesquisa Avançada (Advanced Research Projects Agency – ARPA), do Departamento de Defesa dos EUA, imaginou uma rede de computadores que permitisse o trabalho cooperativo entre pessoas e o uso compartilhado dos supercomputadores existentes nas universidades. A primeira rede experimental, chamada de ARPANET, foi instalada em 1970, interligando quatro universidades

contratadas pela ARPA, e atendia tanto à comunidade acadêmica como à comunidade militar norte-americana.

Criada no auge da Guerra Fria, uma das preocupações dos idealizadores da ARPANET era construir uma rede com características militares, que lhe assegurassem a sobrevivência diante de um ataque nuclear. Desse modo, a fim de impedir a interrupção de seu funcionamento, em caso de ações inimigas ou avarias localizadas, a rede baseava-se na diversidade de conexões físicas entre os computadores e na inexistência de um ponto central de controle. A essa descentralização, que se manteve inalterada desde a sua concepção original, alguns autores atribuem a origem dos atuais problemas de segurança da rede.

Na década de 80, a ARPANET integrou-se à rede CSnet, que interligava todos os Departamentos de Ciência da Computação dos EUA, constituindo a primeira rede heterogênea, precursora da Internet. Outra rede que também merece atenção nessa época é a USENET, que se desenvolveu de forma descentralizada e anárquica, chegando, em 1986, a centenas de milhares de usuários, que para se ligarem à rede, precisavam apenas de um computador, um modem e uma linha discada.

Em 1987, a Fundação de Ciência Nacional (National Science Foundation – NSF) criou a rede NSFNET, interligando a comunidade acadêmica norte-americana, por meio da adoção do protocolo TCP/IP, que possibilitava a conexão entre redes independentes e heterogêneas. O TCP/IP resultou da combinação do Internet Protocol (IP), que era o endereço numérico usado para a localização dos computadores, com o Transmission Control Protocol (TCP), que era responsável pela entrega correta dos dados nas máquinas de destino. Em 1995, depois da considerável expansão da NSFNET provocada pelo TCP/IP, a NSF deixou de financiá-la, abrindo a rede para a exploração comercial, no que veio a ser chamado de ``privatização'' da Internet. Como evolução natural da NSFNET, surgiu a “rede das redes” que passou a se chamar de Internet.

A primeira conexão do Brasil à Internet dos EUA foi realizada pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) em 1991, empregando o protocolo TCP/IP e uma linha dedicada da Embratel, que podia ser acessada por várias instituições acadêmicas, através da Rede Acadêmica Paulista (Academic Network at São Paulo – ANSP).

A primeira versão da Internet no Brasil, entretanto, foi a Rede Nacional de Pesquisa (RNP), cujo “backbone” nacional começou a ser implantado a partir de

1991, sob patrocínio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Quando se tornou uma rede mista, carregando tanto o tráfego acadêmico quanto o tráfego comercial, a RNP passou a constituir a espinha dorsal da Internet brasileira. Até 1996, sua conexão com os EUA era feita através da FAPESP, quando então a RNP adquiriu uma linha própria, ligando-a ao exterior. Até hoje, a infra-estrutura da RNP é a única de abrangência nacional.

Com a posse do governo Fernando Henrique Cardoso, em 1995, estabeleceu-se o Comitê Gestor da rede Internet no Brasil, com a atribuição de coordenar e incentivar a implantação da rede no País.

A Internet não tem órgão regulador oficial, no entanto, desde 1992, está sujeita à atuação da Internet Society (ISOC), que é uma organização internacional com o objetivo de assegurar a disponibilidade, o desenvolvimento e a utilidade da Internet, em escala global. A sociedade atua como facilitadora e coordenadora de iniciativas sociais, comerciais, educacionais e técnicas, relacionadas com o futuro da Internet, por meio de um largo espectro de atividades, das quais a sua conferência anual (International Networking (INET) conference) é a mais conhecida. A ISOC compreende ainda os grupos responsáveis pelos padrões da infra-estrutura da rede, dentre os quais se incluem a Internet Engineering Task Force (IETF) e o Internet Architecture Board (IAB).

Atualmente, os EUA também podem exercer considerável controle sobre a Internet, por intermédio da Internet Corporation for Assigned Names and Numbers (ICANN), que é uma organização sem fins lucrativos, contratada pelo Departamento de Comércio norte-americano, para gerenciar o Sistema de Nomes de Domínios (Domain Name System – DNS).

Todo endereço IP recebe um nome, como “ www.exercito.gov.br” , por exemplo, para facilitar sua identificação. Os nomes são divididos e estruturados hierarquicamente em domínios, constituindo o DNS. Para se chegar a determinado computador, consulta-se inicialmente um servidor do topo da hierarquia (correspondente ao .br, por exemplo), chamado de servidor de raiz, e segue-se a cadeia, consultando-se os servidores intermediários (como .gov), até se chegar ao domínio desejado (.exercito). Hoje, existem treze servidores de raiz no topo da hierarquia controlados tecnicamente pela ICANN, dos quais dez estão sediados nos EUA. A FAPESP é a entidade que realiza a administração do domínio br e a distribuição dos números IP no Brasil, auxiliando o Comitê Gestor da Internet/BR.

Gerenciando o DNS, a ICANN pode alocar espaço da Internet, decidindo quem vai operar os domínios de nível mais alto (tais como .com e .org), dentre os quais estão os códigos dos países (.br, por exemplo). Esse controle proporciona poder econômico, decorrente da concessão de domínios, e poder político, resultante da possibilidade de interrupção do acesso à rede, por parte de países inimigos. O assunto é objeto de batalha entre os EUA, que não abrem mão do seu poder, e um grupo de países, entre os quais se inclui o Brasil, que deseja a transferência da gestão da rede para uma agência da ONU.

2.3 A GUERRA DA INFORMAÇÃO

A fim de vencer a competição contra seus possíveis adversários, assegurando respostas adequadas durante a ocorrência dos conflitos armados, os estados procuram alcançar a vanguarda da arte e dos instrumentos da guerra, por meio da observação, adaptação e adoção das melhores políticas e estratégias empregadas pelos países escolhidos como referência mundial.

Após a Guerra Fria, a estratégia militar predominante no mundo tem sido marcadamente influenciada pela superioridade militar dos EUA, cujo modelo fundamenta-se na crescente dependência da tecnologia para melhorar a eficiência, minimizar as baixas e acelerar a solução dos conflitos.

Melhorar a eficiência traduz-se em observar, decidir e atuar com velocidade e precisão, por meio do emprego de sistemas que integram o planejamento, a aquisição de alvos, a manobra, o ataque, as comunicações e a logística.

Aqui se entende velocidade não só relativa ao desdobramento e à movimentação de tropas nas áreas de operações, mas também quanto à rapidez na percepção das mudanças ambientais, na tomada de decisões, no aproveitamento das tecnologias emergentes e na readaptação organizacional diante daquelas mudanças. A eficiência também está ligada, portanto, à reorganização das estruturas militares, que tendem a ser menos rígidas e a compor combinações híbridas de hierarquias e redes, componentes públicos e privados, homens e máquinas.

A precisão, por sua vez, estende-se além do simples acerto de alvos a grandes distâncias, provocando os efeitos físicos planejados. Ser preciso também significa conduzir as operações militares, produzindo as percepções, crenças e atitudes desejadas no inimigo, na população não combatente do país adversário e do próprio

país, bem como no público internacional, que acompanha e tem interesse na evolução do conflito. Nesse contexto, as relações entre civis e militares tornam-se relevantes, especialmente quando se trata de questões relacionadas com efeitos colaterais do uso do armamento, direitos humanos, privacidade e direitos civis.

A nova estratégia é reflexo da sociedade pós-capitalista, de modo que o conjunto de mudanças por ela representado é normalmente chamado de Revolução em Assuntos Militares e o período atual, particularmente depois da Primeira Guerra do Golfo, é conhecido como Pós-Modernismo Militar.

As origens do Pós-Modernismo Militar remontam à década de 80, quando a evolução e proliferação da tecnologia da informação (sensores, comunicações, computadores, etc.) no campo de batalha, provocou o desenvolvimento da doutrina de comando e controle. Resumidamente, o processo de comando e controle é um ciclo que se inicia com sensores observando o terreno e o inimigo, passa pela decisão do comandante, prossegue com a mudança do ambiente por atuadores e reinicia-se com nova observação (SILVA, 1996).

Como subproduto do comando e controle, surgiu a idéia de superioridade do comando e controle, pois aquele que completa o ciclo mais rápido, modifica o ambiente antes do adversário atuar, tornando inócuas as ações deste último. Garantir a superioridade do comando e controle consiste, portanto, em agilizar o próprio comando e controle e retardar o processo correspondente do adversário (SILVA, 1996).

Nesse contexto, a guerra eletrônica atua ofensivamente para retardar o ciclo de comando e controle do inimigo ou defensivamente para proteger o das forças amigas. Essa visão, centrada na variável tempo, também estimulou o emprego, a proliferação e a dependência de meios de comunicações e de computadores de maior capacidade e cada vez mais velozes, com o propósito de agilizar o processamento e o trânsito de informações e ordens. Na ocasião, utilizou-se largamente, no ambiente internacional, a expressão “ guerra de comando e controle” , para definir a natureza desse confronto.

Após a Guerra do Golfo de 1991, desenvolveu-se a doutrina de guerra da informação, como resultado da evolução e da adaptação dos antigos princípios do comando e controle aos novos ambientes operacionais e às novas capacidades revolucionárias, proporcionadas pelo avanço tecnológico. A mudança tirou o foco do

"comando e controle" para a "informação", o que reflete uma postura mais descentralizada.

A guerra da informação abrange as ações realizadas para obter o domínio da informação, atuando contra as informações, processos baseados em informação, sistemas de informação e redes de computadores dos adversários, bem como defendendo os recursos similares das próprias forças (EUA, 1996; SOUZA, 2003).

Domínio da informação é o grau de superioridade da informação que permite ao seu detentor usar os sistemas de informação para obter uma vantagem operacional e controlar a situação, enquanto nega essas capacidades ao adversário (EUA, 1996; SOUZA, 2003). O conceito é análogo aos de "superioridade aérea" e de "controle de área marítima", normalmente usados nos combates aéreo e naval, respectivamente. Também é semelhante ao de superioridade do comando e controle, comentado anteriormente.

A superioridade informacional é a essência do pós-modernismo militar e a chave do sucesso no espaço de batalha, uma vez que o sucesso dependerá de quem achar primeiro o adversário. Daí a importância da inteligência e da segurança, a ser obtida, respectivamente, por meio de ações de reconhecimento e dissimulação. Desse modo, a superioridade da informação pode desequilibrar a correlação entre tropas oponentes, conduzindo à vitória forças quantitativamente inferiores.

A guerra da informação é um conceito "guarda-chuva", onde estão abrigadas atividades ofensivas e defensivas de natureza diversa, cujo traço comum é o trato da informação, tais como: guerra eletrônica, destruição física de instalações, telemática, imagens e informações geográficas, inteligência, operações psicológicas, comunicação social, etc. (EUA, 1996). Ataques contra computadores são uma forma de guerra da informação, da mesma maneira que a destruição física de uma instalação de comando e controle, uma vez que todos visam a prejudicar o fluxo de informações do adversário.

Em seguida à doutrina da "guerra da informação", desenvolveu-se a concepção de "guerra centrada em redes" (Network-centric warfare – NCW). A doutrina da guerra centrada em redes – ou das operações centradas em redes (Network-centric operations – NCO), como tem sido chamada mais recentemente – baseia-se na utilização da tecnologia da informação para construir redes resistentes, que assegurem a conectividade e o compartilhamento de informação entre decisores

e atuadores de todos os escalões da hierarquia militar. Além de melhorar a qualidade da informação produzida, esse compartilhamento possibilita a elaboração e a difusão de um quadro de situação, preciso e comum, do espaço de batalha, para todas as unidades. A consciência situacional (situational awareness) resultante facilita a tomada de decisão e a auto-sincronização entre as unidades. Da mesma forma que a guerra da informação, a guerra centrada em redes é extremamente dependente do largo uso da tecnologia digital.

O modelo norte-americano, entretanto, não se aplica a todos os países. Estados com poucos recursos intelectuais ou financeiros não podem se dar ao luxo de usar tecnologia para resolver seus problemas estratégicos. Além do que, os conflitos não estão restritos ao confronto entre Estados-nação, havendo um grande número de atores não-estatais envolvidos em ações militares, cujos recursos também são limitados. Para esses Estados e grupos, a guerra assimétrica pode ser uma boa alternativa.

Guerra assimétrica é a forma de conflito armado no qual há desequilíbrio entre os poderes militares oponentes e o lado mais fraco procura compensar a sua desvantagem, normalmente empregando meios, táticas e estratégias não convencionais, para evitar os pontos fortes e explorar as vulnerabilidades do adversário. A assimetria pode referir-se, dentre outros aspectos, à quantidade de meios, à tecnologia do material, à estratégia empregada e à disponibilidade de tempo para conduzir o conflito.

Os exemplos históricos são numerosos e estendem-se desde as primeiras lutas do homem pré-histórico contra a dominação de adversários mais fortes até os conflitos recentes do Vietnam (1965-1973), do Afeganistão (1979-1989) e do Iraque (a partir de 2003), apenas para citar alguns exemplos.

Conceitos relacionados com a guerra assimétrica podem ser encontrados nas obras de grandes estrategistas militares. Sun Tzu escreveu na Arte da Guerra que “ o vencedor sabe quando lutar e quando não lutar” . Liddel Hart, por sua vez, salientou que se deve “ evitar o ponto forte do inimigo e atuar contra a menor resistência” . Segundo Mao Tsé Tung, “ as vulnerabilidades do inimigo são seus pontos vitais, que devem ser atacados, dispersados e exauridos” .

Existem várias maneiras de diminuir ou neutralizar a superioridade do adversário. A principal estratégia consiste em minar a sua vontade de continuar a luta, evitando o confronto direto em condições desvantajosas, prolongando a

duração do conflito e conduzindo ações que provoquem o seu desgaste físico, moral e político. No nível tático, é possível inibir ou restringir a capacidade militar do adversário operando em áreas que limitam a eficácia do armamento empregado e facilitam a ocultação das forças irregulares, tais como cidades, florestas ou montanhas. Atores fracos podem ainda atuar por meio da dissuasão, adquirindo armas de destruição em massa (químicas, biológicas, radiológicas e nucleares) ou armas convencionais avançadas (minas marinhas, mísseis anti-navios, submarinos a diesel silenciosos e mísseis terra-ar).

Os contendores mais fracos normalmente conduzem ações ofensivas de efeito tático limitado, mas de grande significado político e estratégico. Aproveitam a impossibilidade do inimigo defender-se em todos os lugares e a toda hora. Empregando a surpresa, a mobilidade e a ação de choque, concentram-se para explorar uma vulnerabilidade do adversário e retiram-se em seguida. Podem atuar isoladamente ou de forma combinada com outras atividades de natureza militar ou política.

3 GUERRA CIBERNÉTICA

3.1 ANÁLISE DO RISCO

Computadores, programas e redes são comumente alvos de ameaças e ações conduzidas por vários atores, em diversas áreas de atividades, motivados pelos resultados favoráveis que o aproveitamento oportuno de vulnerabilidades e o emprego de tecnologias de invasão proporcionam para a consecução de seus objetivos pessoais, grupais ou organizacionais.

O conceito de risco é importante para a avaliação da possibilidade de ocorrência dessas ações. Há muitas definições sobre risco, dependendo da atividade onde elas se aplicam. De um modo geral, o risco está relacionado com as perdas causadas por um determinado evento e a probabilidade de ocorrência desse evento. Assim, quanto maior for o dano e a probabilidade de ocorrência do evento, maior o risco.

No caso de ataques contra computadores, o valor do alvo, a natureza da ameaça, as vulnerabilidades dos sistemas e as medidas de segurança adotadas são as variáveis mais importantes para se determinar o risco existente. O valor corresponde à importância da informação a ser protegida. Esse valor determina os recursos que serão alocados para proteção da informação, não sendo conveniente gastar em segurança mais do que o valor do bem protegido. Em função desse valor é que serão estabelecidas as prioridades de segurança, uma vez que nunca haverá recursos suficientes para atender a todas necessidades.

A ameaça refere-se às pessoas e organizações que estão tentando acessar os sistemas de informação sem autorização. O universo de ameaças é amplo, podendo incluir Estados estrangeiros, grupos não-estatais e indivíduos isolados, com diferentes motivações, como espionagem, ganhos financeiros, vingança ou publicidade.

As vulnerabilidades são deficiências dos sistemas de informação que, sendo passíveis de aproveitamento, representam uma oportunidade para a consecução dos objetivos do atacante. Se não existirem vulnerabilidades, as ameaças não podem explorar os sistemas de informação e portanto não há risco. A realidade, no

entanto, é que as vulnerabilidades não podem ser removidas por completo de uma organização, sendo necessário gerenciá-las por meio de medidas de segurança.

As medidas de proteção são os procedimentos e dispositivos empregados para tratar de vulnerabilidades específicas. Se a organização escolhe medidas de proteção que não estão direcionadas para vulnerabilidades específicas, ela está desperdiçando recursos. Em alguns casos, dependendo do valor a ser protegido e da vontade da ameaça, as medidas de proteção podem ter efeito dissuasório. Em outros, quanto maior for a defesa, maior é o desafio para o atacante e o seu interesse em derrubá-la.

Nesse contexto, as vulnerabilidades merecem atenção especial, porque conforme salientado anteriormente, só há risco se existirem vulnerabilidades. No caso particular das ameaças cibernéticas, a maioria das vulnerabilidades resulta de problemas no desenvolvimento dos programas ou da adoção de práticas operacionais e de gerenciamento inadequadas.

A fim de vencer a acirrada concorrência provocada pela rapidez da evolução tecnológica e na ausência de demanda dos usuários por mais proteção, os fabricantes procuram agilizar a colocação de seus produtos no mercado, priorizando requisitos referentes à facilidade de instalação e operação, em detrimento dos requisitos de segurança. Como resultado, são originadas deficiências durante o desenvolvimento dos produtos, que estão relacionadas com a concepção, a arquitetura ou a implementação dos programas. Em virtude de problemas na concepção dos produtos, por exemplo, podem resultar mecanismos de segurança complexos e difíceis de configurar, que geram vulnerabilidades, a partir de pequenos erros de ajuste dos usuários.

A maioria das vulnerabilidades associadas ao desenvolvimento dos produtos resulta de falhas de implementação (bugs) e pode ser corrigida por meio de atualizações (patches) distribuídas pelos fabricantes. O problema das atualizações é que nem sempre as organizações realizam as correções necessárias, ou demoram para fazê-las, porque, dentre outros motivos, a tarefa é complexa, recebe baixa prioridade do administrador do sistema, envolve grande quantidade de máquinas ou há problemas de compatibilidade entre os programas atualizados e os demais programas já residentes nos computadores. Algumas falhas de desenvolvimento, que decorrem de problemas no desenho (design) da arquitetura dos programas, no entanto, são difíceis de reparar e possuem vida longa, obrigando o usuário a

procurar outras formas de proteção, diferentes da simples correção do produto. Vírus, por exemplo, se propagam e infectam sistemas devido a escolhas de projeto, que permitem a importação e execução irrestrita de códigos.

Deliberadamente, o fabricante pode ainda colocar pontos de entrada (trapdoors) ocultos nos programas, com a finalidade de possibilitar o acesso futuro e não autorizado aos sistemas de informação dos usuários, desbordando os mecanismos de proteção existentes. Desse modo, produtos estrangeiros podem embutir vulnerabilidades, que são colocadas propositadamente por engenheiros e programadores simpatizantes da causa de possíveis adversários. A terceirização da produção de programas para outros países, como estratégia para enfrentar a competição econômica global, apenas contribui para ampliar essas vulnerabilidades.

Tendo em vista a continuada incorporação de novas redes e tecnologias, o espaço cibernético tem evoluído rapidamente e se tornado cada vez mais complexo, provocando a crescente falta de conhecimento e de conscientização das pessoas sobre assuntos de segurança. Devido ao desconhecimento de gerentes de negócios, administradores de sistemas e usuários, a prioridade atribuída à proteção de seus recursos de tecnologia da informação tende a diminuir, reduzindo a disponibilidade de recursos, treinamentos e indivíduos experientes, destinados para a segurança. Abre-se, portanto, espaço para a adoção de práticas operacionais e de gerenciamento inadequadas, que aumentam a probabilidade da ocorrência de novas vulnerabilidades.

3.2 DEFINIÇÃO E CARACTERÍSTICAS

Segundo PARKS (2001), a guerra cibernética é o subconjunto da guerra da informação que tem como objeto de interesse a informação processada e veiculada dentro da realidade virtual de computadores e redes (espaço cibernético).

" O espaço cibernético é o mundo artificial, criado por seres humanos, usando computadores (hardware) e programas (software)." Representa uma nova dimensão do conflito moderno, ao lado das dimensões tradicionais do espaço físico (terra, mar e ar) e do espaço eletromagnético (CÔRTES, 2000). Há vários espaços cibernéticos, dos quais a Internet é apenas o mais conhecido e de maior amplitude.

Conceitos como " ciberterrorismo" , " cibercrime" e " guerra cibernética" são de mesma natureza, uma vez que se desenvolvem utilizando as mesmas ferramentas, e dentro do mesmo mundo virtual de computadores, programas e redes, diferindo

apenas no que diz respeito ao propósito das ações realizadas. Em alguns casos, espelhando o mundo real, quando convergem os propósitos de organizações criminosas, facções terroristas e grupos militares, é muito difícil realizar a distinção entre os três conceitos.

Apesar de possuir pontos em comum com a " guerra eletrônica" , o " comando e controle" e o próprio conceito mais abrangente de " guerra da informação" , na qual insere-se atualmente, a guerra cibernética possui características, possibilidades, limitações e princípios de emprego peculiares (CÔRTES, 2003; PARKS, 2001) que precisam ser analisadas e avaliadas com atenção – separando o mito da realidade – a fim de que as ações conduzidas no espaço cibernético possam efetivamente contribuir para o planejamento operacional, aproveitando as oportunidades existentes.

As ações conduzidas no espaço cibernético podem provocar efeitos no mundo real, afetando coisas e/ou pessoas, o que garante a sua utilidade para emprego militar. Em função, obviamente, das vulnerabilidades existentes, é possível gerar efeitos físicos, tais como: abertura das comportas de represas, desligamento de estações de energia, acidentes ferroviários, etc. Pode-se, ainda, provocar efeitos típicos da guerra da informação, interferindo no processo decisório do adversário, aumentando a névoa do combate e influenciando a vontade de lutar do inimigo. Dados intencionalmente modificados, por exemplo, podem provocar a avaliação incorreta da situação, a escolha de linhas de ação inadequadas e/ou a falta de oportunidade no emprego de forças. A turbulência mundial causada pelo " bug do milênio" constitui uma forte evidência de que ocorrências no espaço cibernético podem causar sérios problemas no mundo real.

O comportamento do espaço cibernético é complexo, dinâmico, caótico, não-linear e imprevisível. A complexidade decorre da existência de redes compostas por um grande número de componentes distintos (nodos) e interconectados (relações), que se influenciam mutuamente. A dinâmica diz respeito ao modo como o espaço cibernético evolui ao longo do tempo, compreendendo mudanças tanto na organização (mutação) de suas partes constituintes, como nas relações (recombinação) entre as mesmas. O caos está presente porque, em função de realimentações entre as conexões, os eventos mudam a probabilidade de ocorrências de outros eventos, fazendo com que pequenas alterações possam produzir resultados desproporcionalmente significativos.

Por ser caótico, o espaço cibernético é não-linear e imprevisível, o que torna difícil o estabelecimento de relações diretas de proporcionalidade entre os meios empregados e os danos produzidos durante os ataques cibernéticos. Os equipamentos e programas – estes mais do que os primeiros – estão sujeitos a variações de desempenho e podem não operar como esperado. Vulnerabilidades identificadas durante reconhecimentos podem não ser as mesmas da hora do ataque. Não há como assegurar que os passos tomados durante o ataque produzirão os efeitos desejados. Por outro lado, ações ofensivas onde pouco se esperava de resultados positivos podem acabar sendo bem sucedidas.

A ações conduzidas no espaço cibernético desconhecem algumas restrições de tempo e espaço que são comuns no mundo físico. Desde que haja conectividade entre o atacante e a rede escolhida como alvo, seja por meio de linhas físicas, seja por meio de ondas radioelétricas, é possível atingir com rapidez qualquer ponto da rede, independente da distância e das fronteiras geográficas, administrativas ou políticas existentes. Assim sendo, ataques provenientes do computador do vizinho podem ter a mesma eficácia daqueles originados no outro lado do mundo. Dependendo das barreiras defensivas existentes, pode-se, em poucos segundos, alcançar e entrar no sistema alvo, instalar programas para facilitar o retorno do atacante, esconder as evidências da sua presença e começar ações contra outros sítios.

Os ataques são difíceis de rastrear, uma vez que para ocultar a sua localização e identificação, os atacantes utilizam vários provedores de serviço intermediários, antes de alcançar o alvo. Como as redes permitem o fluxo fácil de dados através de fronteiras geográficas, administrativas e políticas, o rastreamento do atacante através dos provedores depende da cooperação entre múltiplas organizações e jurisdições, cuja maioria tem pouca motivação para dedicar tempo e recursos nesse esforço, uma vez que não são prejudicadas diretamente pelo ataque. Se os provedores intermediários estão localizados em diferentes países, o rastreamento pode depender da cooperação internacional, o que nem sempre é possível, tendo em vista tanto a complexidade da lei internacional, como diferenças legais e ideológicas entre os países envolvidos. Atacar um país com armas cibernéticas torna-se, portanto, uma atividade atraente – especialmente se a iniciativa for realizada por intermédio de terceiros – porque, como os ataques são difíceis de punir ou retaliar, há baixo risco para o atacante, que se sente seguro, não percebendo

qualquer ação dissuasória. O espaço cibernético proporciona cobertura e facilita a fuga do invasor, do mesmo modo que o terreno difícil favorece a ocultação e a fuga de guerrilheiros.

O custo de um ataque é variável. Ações simples requerem recursos modestos: um pequeno grupo de especialistas em computação, alguns computadores pessoais e um acesso à Internet. Pode ainda empregar programas de intrusão livremente disponíveis na própria rede. Ataques complexos, por sua vez – como aqueles dirigidos contra a infra-estrutura de um país ou contra alvos múltiplos – podem requerer recursos significativos, além de anos de preparação, para que sejam criadas, desenvolvidas e testadas as ferramentas de invasão, bem como seja realizada a vigilância sobre o alvo.

3.3 AÇÕES DE GUERRA CIBERNÉTICA

Independente do valor e da natureza da força considerada, nunca há segurança completa, pois os meios sempre são insuficientes para eliminar todas as vulnerabilidades. Sob a ótica do atacante, dessa constatação decorre a possibilidade constante da existência de deficiência do adversário, a ser identificada e aproveitada, seja por meio de ação sistemática, seja por pura sorte. A lógica é típica da guerra assimétrica, onde o oponente mais fraco, para compensar a correlação desvantajosa de forças, evita os pontos fortes e aproveita as falhas do adversário. Do ponto de vista do defensor, a mesma situação implica a judiciosa distribuição de recursos, com base na análise e na priorização dos riscos.

Independente do propósito desejado com a intrusão, normalmente são realizadas as seguintes ações para ganhar acesso e assumir o controle de sistemas informatizados: reconhecimento, varredura, ganho do acesso, manutenção do acesso e dissimulação.

Na maioria dos casos, essas ações são conduzidas automaticamente, com o emprego de programas especiais, que possuem diferentes graus de sofisticação. As ferramentas sofisticadas são mais difíceis de detectar pelos meios de proteção, mas a sua distribuição é normalmente restrita ao grupo de especialistas que participou do seu desenvolvimento. As ferramentas mais simples, por sua vez, podem ser obtidas gratuitamente pela Internet.

Durante o reconhecimento, os atacantes vigiam a organização escolhida como alvo, na procura de informações que auxiliem as fases posteriores do ataque. Os

métodos mais comuns de vigilância incluem a engenharia social, o vasculhamento de material abandonado ou a utilização de programas espiões (spyware). O atacante pode ainda, por exemplo, usar programas que discam milhares de números de telefone, procurando por modens conectados a um computador, ou simplesmente tentar detectar sinais e entrar nas redes sem fio, circulando pela vizinhança.

O programa espião é um tipo de código malicioso, instalado sem conhecimento do usuário, para realizar a vigilância automática. Dependendo do grau de sofisticação, pode permanecer despercebido pelos meios usuais de detecção, como firewalls ou produtos anti-vírus, enquanto grava teclas digitadas, registra atividades da rede, captura imagens da tela e transmite a informação útil obtida, como senhas e nomes de usuários, para o atacante.

A varredura é uma forma de vigilância complementar ao reconhecimento, na qual o atacante investiga as configurações das redes e dos programas utilizados pela organização alvo, com o propósito de encontrar possíveis pontos de entrada. É um processo demorado, que pode se prolongar por vários meses.

Depois de ter realizado o mapeamento das configurações das redes e dos programas do alvo, o atacante pode explorar as vulnerabilidades encontradas para silenciosamente ganhar acesso ao sistema. Se o êxito obtido permitir que sejam alcançados os privilégios do administrador do sistema, o computador ou rede estará sob controle completo do atacante.

Para manter o acesso conquistado, o atacante pode secretamente instalar novos programas maliciosos, como root kits, back doors, ou cavalos de tróia, que rodam despercebidos, para permitir o acesso secreto à rede, quando desejado, ou permanecem inativos, até receberem comandos remotos, para atuar em favor do atacante. O atacante pode, ainda, eliminar as vulnerabilidades do sistema, modificando configurações ou instalando atualizações dos programas (software patches), para evitar o acesso de outros intrusos.

Finalmente, é preciso dissimular as ações conduzidas, a fim de que o sistema possa continuar sendo acessado de modo silencioso e sem impedimento, assegurando, desse modo, a continuidade na atividade de busca de dados, seja para alimentar o sistema de inteligência, seja para refinar as preparações e, conseqüentemente, maximizar os danos de um futuro ataque. Utilizando programas especiais (root kit, cavalos de tróia, etc.), é possível modificar os arquivos que registram todas as atividades do sistema (log files), ou criar arquivos ocultos para

esconder-se do administrador do sistema. Dependendo da sofisticação das ferramentas empregadas e das características do sistema invadido, a atuação do atacante pode permanecer despercebida por longo período de tempo.

Além das ações ofensivas e de inteligência descritas anteriormente, a guerra cibernética compreende também ações defensivas. As ações defensivas correspondem às medidas de proteção destinadas a assegurar a eficiência das operações apoiadas pelos recursos de tecnologia da informação (TI), a continuidade do funcionamento de redes – como a Internet – sobre as quais essas operações são estabelecidas e, em casos mais graves, a sobrevivência da própria infra-estrutura de informação. O conjunto de medidas de proteção adotadas normalmente é denominado de " segurança da informação" .

4 CONDICIONANTES DO EMPREGO DO EXÉRCITO

4.1 CONDICIONANTES LEGAIS

Como as armas cibernéticas são novas e revolucionárias, suas características ainda não foram bem determinadas ou compreendidas. A utilização precipitada dessas armas, sem a prévia avaliação dos resultados subseqüentes, tem sérias implicações legais. A falta de cautela no trato do assunto, além das sanções penais correspondentes, pode trazer custos morais e políticos para o transgressor, perante a opinião pública internacional ou de seu próprio país.

Mesmo não havendo aplicação direta de força física, é difícil classificar as armas cibernéticas como armas não letais, tendo em vista a natureza e a amplitude de seus possíveis efeitos. Considerando a permeabilidade das tecnologias da informação nos serviços essenciais à vida da população, as conseqüências podem ser extraordinárias, se não houver o devido controle sobre o emprego dessas armas. Esse potencial para causar danos indiscriminados amplia-se com a evolução da capacidade dos computadores e dos meios de comunicações, podendo mesmo ser multiplicado se houver o emprego combinado com outras armas.

Essa situação suscita questões sobre o que pode ou não ser feito e quando pode ser feito, segundo os princípios da “necessidade” e da “proporcionalidade”, constantes das leis do conflito armado. De acordo com esses princípios, um ataque pode ser realizado se ele for “necessário” para alcançar um propósito militar, devendo o dano que ele causa ser “proporcional” à vantagem operacional obtida.

O princípio da necessidade proíbe o ataque a civis, o que torna ilegal a ação indiscriminada contra a infra-estrutura básica de países adversários, limitando o alcance dos ataques cibernéticos, no máximo até os sistemas de informação que são usados conjuntamente por civis e militares. Nesse caso, os serviços de inteligência têm de ser utilizados para justificar legalmente o ataque, provendo evidências de que os meios civis, como estações de radiodifusão, centrais telefônicas e antenas de microondas, por exemplo, estão sendo utilizados com destinação militar.

No que diz respeito à proporcionalidade, o principal problema decorre da complexidade das interações existentes entre as redes. Como os sistemas

complexos normalmente não são lineares, os resultados dos ataques são difíceis de controlar ou limitar, podendo prolongar-se além dos alvos inicialmente planejados, espalhando-se por outras redes, provocando efeitos em cascata e alcançando sistemas não militares dos países conflitantes ou de países neutros, com danos desnecessários para a população, o que também constitui transgressão das leis de guerra internacionais.

Outro aspecto de natureza legal, que condiciona o emprego da guerra cibernética, está relacionado com a privacidade dos indivíduos. A guerra cibernética, enquanto atividade de inteligência, tem de lidar com o difícil equilíbrio que deve haver entre a busca da informação, para assegurar a segurança da sociedade e do Estado, e a preservação dos direitos relacionados com a privacidade das pessoas.

Nesse sentido, é de particular relevância o inciso X do Art 5º da Constituição Federal, que assegura serem " invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas" . Também trata do assunto, o artigo 10 da Lei nº 9.296, de 24 de julho de 1996, que constitui crime realizar, sem autorização judicial, a interceptação de comunicações telefônicas, de informática ou telemática. Por sua vez, o Código Penal, atualizado pela Lei nº 9.983, de 14 de julho de 2000, tipifica os crimes de divulgação de segredo (art. 153), inserção de dados falsos em sistema de informações (art. 313-A), modificação ou alteração não autorizada de sistema de informações (art. 313-B) e violação de sigilo funcional (art. 325).

Para atender às condicionantes legais, é necessário, inicialmente, assegurar que as autoridades responsáveis pelo emprego das novas tecnologias tenham consciência dos efeitos adversos decorrentes, antes de decidir utilizá-las contra os sistemas de informação dos adversários. Nesse sentido, é conveniente estabelecer uma metodologia que permita avaliar a conformidade do emprego das novas armas com a lei nacional e internacional. Em seguida, é preciso estabelecer diretrizes sobre a competência das autoridades decisoras e controladoras do emprego das armas, oportunidade e alvos dos ataques, ferramentas passíveis de utilização e regras de engajamento. Finalmente, devem ser estabelecidos instrumentos de controle que assegurem o fiel cumprimento da legislação vigente.

4.2 CONDICIONANTES TECNOLÓGICAS

Tecnologia de uso dual é o termo freqüentemente usado para referir-se à tecnologia que pode ser usada tanto para fins pacíficos como para fins militares.

Durante a Guerra Fria, por exemplo, os EUA e a URSS investiram no desenvolvimento da tecnologia de foguetes, para levar o homem ao espaço. O conhecimento adquirido desse uso pacífico da tecnologia, também serviu para o desenvolvimento de mísseis balísticos intercontinentais. Como resultado, muitos países industrializados exercem controle cerrado sobre a exportação de tecnologias de uso dual, para evitar a proliferação de armas de destruição em massa ou para limitar o poder militar de possíveis adversários. A efetividade desse controle é aumentada, se o mesmo é mantido por meio de acordos ou de organismos multilaterais.

A tecnologia empregada para conduzir a guerra cibernética é de uso dual. O mesmo sistema criptográfico empregado para proteger transações eletrônicas de alto valor entre instituições do mercado financeiro pode, por exemplo, ser usado para defender, contra investidas inimigas, as redes informatizadas de campanha empregadas na condução da manobra. Sendo de uso dual, computadores e programas, além dos regimes de proteção dos direitos de fabricantes, também estão sujeitos a mecanismos de controle de exportação internacionais, sendo necessário, em muitos casos, o desenvolvimento independente de tecnologia nacional para suprir as necessidades militares.

A indústria de software brasileira vem se ampliando e amadurecendo de forma significativa nos últimos anos. O mercado interno já alcançou valores bastante expressivos em termos mundiais, em função do aparecimento e desenvolvimento de empresas criativas e de elevado padrão de qualidade.

Impulsionados por iniciativas governamentais, como o Programa SOFTEX, do Conselho Nacional de Desenvolvimento Científico e Tecnológico do Ministério da Ciência e Tecnologia, e o Programa para o Desenvolvimento da Indústria Nacional de Sortware e Serviços Correlatos (Prosoft), do Banco Nacional de Desenvolvimento Econômico e Social (BNDES), existem hoje mais de vinte centros de desenvolvimento de software espalhados por todo o Brasil, numa intensa atividade, da qual fazem parte software houses nacionais, instituições de ensino e pesquisa, incubadoras de empresas e grandes companhias multinacionais. A produção é diversificada, incluindo software de bancos de dados textual, sistemas de automação industrial, software de gestão empresarial e jogos para aparelhos celulares.

Além do apoio governamental, tem sido fator crítico para esse sucesso a integração entre empresas, escolas e investidores privados, propiciando a

qualificação adequada de pessoas às necessidades empresariais, o aproveitamento imediato do pessoal formado, o desenvolvimento de metodologias para melhoria da produtividade e o fomento da atividade industrial.

O Brasil também reúne as condições para ocupar uma posição de destaque como provedor de soluções de segurança. Os sinais positivos da capacidade nacional em segurança de informação podem ser observados nos casos de sucesso que são referências mundiais, tais como o Imposto de Renda via Internet, E-banking, Eleições Eletrônicas e o Sistema de Pagamentos Brasileiro (SPB).

Nesse contexto, o grande talento dos profissionais brasileiros na área de informática é indiscutível. Um bom exemplo foi veiculado em revista de grande circulação nacional, no ano de 2003, referente a um analista de sistemas mineiro, que desenvolveu um dos sistemas antigrampos mais seguros do mundo na época. O programa, que se chamava Raesec Secure Phone, foi proibido de ser comercializado na Europa, nos Estados Unidos e em Israel, tendo em vista a dificuldade de ser quebrado. Funcionava com o suporte de um computador portátil e empregava criptografia de 256 bits.

Se por um lado encontramos grandes restrições internacionais à exportação de software, por outro vemos uma indústria nacional em franco desenvolvimento, com potencialidade para a produção de programas de interesse para a defesa nacional, e a conseqüente diminuição da dependência e do hiato tecnológico em relação ao mercado mundial, particularmente no que diz respeito à segurança da informação. Adicionalmente, torna-se mais fácil o recrutamento de recursos humanos com elevado grau de especialização profissional – conforme requerido para a elaboração de produtos relacionados com a guerra cibernética – em caso de mobilização.

4.3 CONDICIONANTES ECONÔMICAS

O setor das telecomunicações é estratégico para a vida nacional. Em virtude das dimensões geográficas do Brasil, as telecomunicações sempre foram consideradas como fator importante para a integração nacional, especialmente após o advento das comunicações por satélite, que permitiram a ligação com as localidades mais remotas da Nação. Com o surgimento da sociedade da informação, o sistema nacional de telecomunicações tornou-se o centro de gravidade da Nação, uma vez que são nas suas redes onde circulam os grandes fluxos de informações

que vivificam a política, a economia e a cultura do País. Parar o sistema nacional de telecomunicações é o mesmo que parar o País.

Sob influência do neoliberalismo, iniciou-se em 1995 a privatização do setor, com a sanção da nova Lei de Telecomunicações. O processo de desestatização estendeu-se até 1998, quando o Sistema Telebrás, composto por 27 empresas de telefonia, foi transferido para a iniciativa privada. Apesar dos sucessos alcançados com a consecução das metas de universalização e com a explosão da oferta de novos serviços, como a telefonia celular, a privatização trouxe o inconveniente de colocar, sob forte influência estrangeira, por meio do controle majoritário das empresas operadoras, o funcionamento do setor, que é estratégico para a vida nacional.

O caso da Embratel serve de exemplo. A empresa foi adquirida pelo grupo MCI, que esteve inicialmente sob controle da WordlCom norte-americana e depois foi vendida para a Telmex mexicana. O patrimônio da empresa, quando privatizada, incluía a única rede de satélites nacionais da época, a rede Brasilsat, que passou a ser gerenciada pela Star One, então subsidiária da Embratel. Atualmente, além dos satélites da Star One, existe o satélite Amazonas, que é operado pela Hispamar, sob controle majoritário da empresa espanhola Hispasat, e o satélite Estrela do Sul, sob controle da norte-americana Loral Space & Communications

As Forças Armadas ainda utilizam os serviços dos satélites da Star One para apoiar o comando e controle da Estrutura Militar de Guerra, por intermédio do Sistema de Comunicações Militares por Satélite (SISCOMIS). Além de operar na faixa de freqüências comercial, correspondente à “ Banda C” ,o SISCOMIS utiliza uma faixa especial de transmissão, conhecida como "Banda X", própria para comunicações táticas móveis, a partir de transponders localizados em dois satélites Brasilsat.

A fragilidade da situação ficou evidente em 2002, quando a WorldCom entrou com pedido de concordata nos Estados Unidos. Na oportunidade, o assunto preocupou as mais altas autoridades nacionais – dentre as quais estavam o Ministro da Defesa e o próprio Presidente da República – quanto à continuidade dos serviços prestados pela operadora nacional de longa distância.

Em todo o mundo, parcela significativa das comunicações militares é conduzida através de meios civis. Nos países desenvolvidos, essa utilização destina-se normalmente ao tráfego complementar, uma vez que suas forças militares possuem

redes próprias, de boa qualidade, capacidade e segurança, para o tráfego principal de informações, necessário à condução de operações militares. No Brasil, onde a realidade orçamentária das Forças Armadas é bem diferente, a dependência de redes comerciais é grande, em função da precariedade das redes exclusivamente militares, o que torna a utilização dos sistemas civis, uma vulnerabilidade estratégica.

4.4 CONDICIONANTES GOVERNAMENTAIS

A guerra cibernética envolve ações de inteligência e de segurança da informação, cuja execução está relacionada com as atribuições de diversos órgãos federais, a quem compete criar normas e coordenar atividades no âmbito governamental. As iniciativas do Exército nessas áreas deverão estar alinhadas com as políticas e diretrizes emanadas por esses órgãos.

No âmbito do Governo Federal, o Sistema Brasileiro de Inteligência (SISBIN), instituído de acordo com a Lei nº 9.883, de 7 de dezembro de 1999, e organizado conforme o Decreto nº 4.376, de 13 de setembro de 2002, é o organismo dedicado às atividades de produção, disseminação e salvaguarda da informação. O SISBIN tem como órgão de coordenação das atividades de inteligência federal, o Gabinete de Segurança Institucional da Presidência da República, e como órgão central, a Agência Brasileira de Inteligência (ABIN).

Os órgãos federais que compõem o SISBIN atuam observando os limites legais, o respeito aos direitos e garantias individuais e coletivos e a fidelidade às instituições democráticas. Relativamente aos atos decorrentes da execução da Política Nacional de Inteligência, estão sujeitos ao controle interno do Executivo, por intermédio da Câmara de Relações Exteriores e Defesa Nacional, e ao controle externo do Poder Legislativo, por intermédio da Comissão Mista de Controle das Atividades de Inteligência.

O Ministério da Defesa participa do SISBIN, por meio do Departamento de Inteligência Estratégica, da Subchefia de Inteligência do Estado-Maior de Defesa, do Centro de Inteligência da Marinha, do Centro de Inteligência do Exército e da Secretaria de Inteligência da Aeronáutica. No âmbito do Ministério da Defesa, é instituído, ainda, o Sistema de Inteligência de Defesa.

O Comitê Gestor da Segurança da Informação, instituído pelo Decreto nº 3.505, de 13 de junho de 2000, é o órgão de assessoramento da Secretaria-

Executiva do Conselho de Defesa Nacional na execução da Política de Segurança da Informação. O Comitê é coordenado pelo Gabinete de Segurança Institucional da Presidência da República e possui um representante do Ministério da Defesa.

Outra entidade importante, com atribuição relativa à segurança da informação, é o Instituto Nacional de Tecnologia da Informação (ITI). O ITI é a Autoridade Certificadora Raiz (AC Raiz) da Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil). Os documentos produzidos em meio eletrônico, são assinados e criptografados mediante o uso de certificados digitais emitidos pela ICP-Brasil. Além dos requisitos de segurança (autenticação, privacidade, integridade, e não-repúdio), a ICP-Brasil confere valor jurídico aos negócios eletrônicos, que passam a produzir efeitos iguais aos contratos assinados fora da rede. As leis e decretos elaborados pelo Governo Federal sobre a ICP-Brasil dão legalidade ao negócio digital, quebrando os paradigmas que se opunham à realização de transações financeiras entre pessoas físicas e/ou jurídicas através da Internet. O ITI é uma autarquia federal e está vinculada à Casa Civil da Presidência da República.

As decisões dos órgãos federais ligados à inteligência e à segurança da informação têm reflexos sobre toda a estrutura da Administração Pública Federal. A aproximação com esses órgãos traz benefícios para o Exército, particularmente no que diz respeito ao acompanhamento da evolução e a possível participação em assuntos de interesse da Instituição.

5 INDICAÇÕES PARA O PREPARO DO EXÉRCITO

5.1 CONSIDERAÇÕES SOBRE A SITUAÇÃO ATUAL DO EXÉRCITO

A Doutrina Militar Terrestre (DMT) é " o conjunto de valores, de princípios gerais, de conceitos básicos, de concepções, de normas, de métodos e de processos" , que têm por finalidades " orientar a organização, o preparo e o emprego do Exército", no nível estratégico, e " definir a estrutura organizacional, o equipamento e a forma de combater da Força Terrestre" , no nível operacional. Divide-se nos setores de combate, apoio ao combate, apoio logístico e comando e controle.

As fases de concepção, planejamento, formulação, difusão e aplicação da doutrina são realizadas por intermédio do Sistema de Doutrina Militar Terrestre (SIDOMT), que se encontra organizado de acordo com a Política de Doutrina Militar, a Diretriz Estratégica para o SIDOMT e as Instruções Gerais para a Organização e Funcionamento do SIDOMT (IG 20-13). As atividades do SIDOMT, conduzidas no nível estratégico, têm como produtos finais os livros do Sistema de Planejamento do Exército (SIPLEX). No nível operacional, têm como produtos finais: os manuais de campanha, manuais técnicos, quadros de organização, condicionantes doutrinárias e operacionais, e requisitos operacionais básicos. Dentre outros objetivos operacionais, o SIDOMT visa a obter " padrões de eficiência compatíveis com um exército moderno" , desenvolvendo a doutrina de acordo com as peculiaridades e as possibilidades do Exército e do País.

Doutrinariamente, o Exército realiza a gestão estratégica da informação de forma sistêmica. A Política de Informação do Exército, que integra as Políticas Específicas do Exército (SIPLEx-3), organiza o Sistema de Informação do Exército (SINFOEx) com as funções básicas de produzir, difundir e proteger informações, atribuindo-lhe os seguintes subsistemas: Sistema de Inteligência do Exército (SIEx), Sistema de Informações Organizacionais do Exército (SINFORGEx), Sistema de Informações Operacionais (SIOp), Sistema de Comunicação Social do Exército (SISCOMSEx), Sistema de Guerra de Eletrônica do Exército (SIGELEx), Sistema de Imagens e Informações Geográficas do Exército (SIMAGEx), Sistema de

Comunicações do Exército (SICOMEx), Sistema de Informática do Exército (SINFEx) e Sistema de Operações Psicológicas do Exército (SiOpEx).

Dentre outras missões, o SIEx produz conhecimentos de Inteligência, protege conhecimentos sensíveis e integra dados provenientes de fontes humanas, de sinais (SIGELEx) e de imagens (SIMAGEx). O Centro de Inteligência do Exército é o órgão central do Sistema de Inteligência do Exército (SIEx) e integra o Sistema de Inteligência de Defesa e o Sistema Brasileiro de Inteligência.

A organização do SINFOEx estabelece um referencial importante para o trato da informação no âmbito do Exército. Sua composição reflete uma visão atualizada do assunto, coerente com a doutrina militar dos países desenvolvidos. As atividades normalmente colocadas sob o "guarda-chuva" da "guerra da informação" estão todas representadas como subsistemas do SINFOEx. Como resultado, essa concepção estratégica serve de maneira adequada para abrigar os novos conceitos relacionados com a guerra cibernética.

Ainda não existe, contudo, uma percepção ampla, no âmbito do Exército, com relação à importância de assuntos relacionados com a guerra cibernética. As causas dessa visão pouco desenvolvida devem-se, possivelmente, à cultura organizacional do próprio Exército. Nesse sentido, o principal aspecto a considerar é a estrutura hierárquica e funcional da Instituição, que desestimula a formação de redes destinadas à troca de informações entre os Departamentos, deixando de aproveitar a potencialidade das tecnologias da informação para ganhar agilidade no enfrentamento das mudanças ambientais. Como a dependência da tecnologia não é grande, pouca ameaça é percebida e menor ainda é a consideração dada à possibilidade de usar essa tecnologia como arma para a inteligência ou para a realização de ações ofensivas. Contribui para essa situação a baixa divulgação sobre o assunto dentro da Instituição.

Constitui prova evidente dessa situação a proliferação de sistemas corporativos desenvolvidos isoladamente no âmbito dos vários Departamentos, com fluxos de informação nulos ou muito pouco significativos entre eles. Igualmente importante para reforçar esta argumentação é a dificuldade existente até hoje para se implantar efetivamente o Sistema de Informações Organizacionais do Exército. Outro sinal desse ponto de vista, foi a fusão recente de órgãos setoriais para a criação do Departamento de Ciência e Tecnologia, que tornou visível a diminuição da importância da tecnologia da informação para a Instituição.

Encontrando-se em um nível de dependência relativamente baixo, uma vez que a maioria das aplicações de tecnologia da informação ainda é localizada, o Exército, como um todo, está apenas despertando para a potencialidade dessas inovações e, conseqüentemente, para a importância das ações de guerra cibernética. Melhorando-se a percepção do Exército sobre o assunto, como resultado natural da sua evolução cultural e tecnológica, as nossas vulnerabilidades se tornarão evidentes, especialmente com relação ao Sistema Estratégico de Comunicações do Exército (SEC).

Tendo em vista condicionantes operacionais, técnicas e orçamentárias, não é viável isolar os computadores militares do ambiente externo, instalando-se uma infra-estrutura de redes com meios exclusivos da Força Terrestre, sem o concurso dos meios civis, o que torna o SEC perigosamente dependente desses meios. O sistema nacional de telecomunicações, que se encontra fora do controle ou influência do Exército, está sujeito às ações ofensivas de guerra cibernética. Ataques contra a infra-estrutura de telemática nacional poderão causar prejuízos ao EB diretamente, tendo as redes militares como alvo, ou indiretamente, tendo o próprio sistema nacional de telecomunicações como alvo. Como resultado desses ataques poderá haver a interrupção e/ou degradação de parcela considerável dos sistemas de comunicações estratégicos (EBNet, RITEx, etc.) e dos sistemas corporativos (pagamento de pessoal, controle de material, etc.), que são críticos para o Exército. Considerando a necessária integração que deve haver entre os sistemas de comunicações estratégicos e táticos, é razoável admitir que os danos poderão se estender até os menores escalões de combate, onde tenha sido instalada uma rede de computadores.

Essa vulnerabilidade serve para salientar a necessidade da segurança da informação – única componente da guerra cibernética que está estruturada no âmbito do Exército. A política de segurança da informação do Exército está consubstanciada nas Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19), que têm como principais objetivos: a definição de responsabilidades, o fomento de atitudes favoráveis, a redução da dependência externa, a promoção de intercâmbios, a capacitação de recursos humanos e a promoção da interoperabilidade. Aprovadas pelo Comandante do Exército – o que traduz o envolvimento do mais alto escalão da Força com o assunto – servem de referência básica para a elaboração de documentos normativos complementares.

Seu conteúdo é atual e abrange aspectos relevantes para a segurança da informação, como pressupostos, princípios, conceitos, regras gerais e responsabilidades. Apesar da grande quantidade de material doutrinário existente sobre segurança da informação, no entanto, ainda há pouca orientação sobre como avaliar os sistemas de informação existentes e sobre como proceder diante de um ataque cibernético.

Diferentemente das ações de segurança da informação, as ações de inteligência empregando armas cibernéticas não constam dos manuais doutrinários em uso no Exército atualmente. A inclusão dessas ações na doutrina, contudo, não constitui dificuldade, uma vez que é possível aproveitar as estruturas já constituídas do SINFOEx e do SIEx. Relativamente às questões éticas e legais normalmente associadas à realização da atividade de inteligência, a Instituição já tornou público o seu posicionamento de que " a busca do conhecimento de inteligência não se realiza, unicamente, por consulta a documentos ostensivos e de rotina" , sendo " indispensável recorrer a procedimentos reservados, sem que isso signifique o desrespeito a preceitos legais" . Para tanto, " as diretrizes que regem a atividade de Inteligência no Exército são rígidas, no sentido de que se desenvolvam com plena regularidade e legalidade, sem ofensas a direitos de qualquer natureza." Evidentemente que esse posicionamento requer o estabelecimento de mecanismos de controle que assegurem a conformidade legal do emprego das ferramentas de guerra cibernética, sem desgaste da Instituição, o que pode ser feito sob orientação do CIE, que é órgão central do SIEx.

No que diz respeito à tecnologia, as possibilidades são maiores que as limitações. Se por um lado, o desenvolvimento de software orientado para a aplicação em ações de guerra cibernética parece ser um desafio, por outro o Exército dispõe de especialistas muito bem qualificados, cuja possibilidade de produção depende apenas das prioridades e da capacidade de organização do próprio Exército. Tendo em vista a alta complexidade dos sistemas em geral e dos equipamentos envolvidos, bem como o alto grau de capacitação técnica e operacional exigido, é conveniente adotar medidas que assegurem a permanência do pessoal especializado na atividade. Desse modo, será assegurada a continuidade das pesquisas necessárias para o monitoramento da evolução tecnológica, o desenvolvimento de sistemas e a atualização doutrinária.

Um complicador para a preparação do Exército decorre da permeabilidade da informação. Como a informação é a matéria-prima para muitas atividades, existem vários sistemas (Ensino, Ciência e Tecnologia, Inteligência, Operações, etc.) envolvidos, o que abre a possibilidade da sobreposição de atribuições entre as organizações ligadas ao problema. O problema é relevante, tendo em vista a necessidade de cerrado controle, que deve haver sobre as ações de guerra cibernética, para evitar a geração de efeitos colaterais indesejáveis, como decorrência do seu emprego.

Outro limitador é disponibilidade de recursos. Os modestos orçamentos do Exército restringem o aporte de novos meios para a implantação e continuidade de iniciativas relacionadas com a guerra cibernética. Na ausência de provimento dos meios correspondentes, o simples acréscimo de novas atribuições, além de sobrecarregar os órgãos existentes, não produzirá resultados efetivos, particularmente nas fases de implantação dessas iniciativas, quando os riscos de insucesso serão elevados. A redefinição de prioridades estratégicas, procurando movimentar recursos de outras atividades, também não é solução viável, tendo em vista que os planos básicos dos órgãos de direção setoriais já estão sendo elaborados com grandes restrições às atividades mais importantes para a operacionalidade da Força. A alternativa resultante é, portanto, a busca de novas fontes de recursos, que pode ser realizada aproveitando-se a comprovada aptidão do Exército para o trabalho cooperativo com outras instituições públicas e privadas.

A prática mundial tem demonstrado que uma das melhores maneiras de se fazer frente a um ataque é atuar preventivamente e de forma cooperativa com outros órgãos que estão sujeitos às mesmas dificuldades. As coordenações e parcerias poderão ocorrer em instâncias diferentes, podendo ser realizadas, por exemplo, com as demais Forças Armadas, para realizar o desenvolvimento e emprego conjunto de software ou para eliminar a possibilidade de interferência mútua durante operações; com entidades reguladoras, para melhorar a qualidade dos softwares, diminuindo as vulnerabilidades; com outros órgãos governamentais, para trocar informações que facilitem a defesa; e com órgãos internacionais, para rastrear atacantes.

5.2 AÇÕES ESTRATÉGICAS PARA O PREPARO DO EXÉRCITO

A fim de permitir o aperfeiçoamento da capacidade do Exército para realizar ações defensivas e ofensivas, no contexto de guerra cibernética, as seguintes medidas poderão ser progressivamente executadas, em função da disponibilidade de meios:

Com relação ao planejamento estratégico do Exército:

- atualizar os planejamentos estratégicos e operacionais, considerando a ocorrência de cenários onde há interrupção do funcionamento dos sistemas nacionais de telecomunicações e de outras infra-estruturas críticas para o país, em virtude de ações cibernéticas adversárias;

- estabelecer diretrizes estratégicas sobre as ações de guerra cibernética, definindo as autoridades com poder de decisão e de controle sobre o seu emprego, as oportunidades e os alvos dos ataques, as armas passíveis de utilização e as regras de engajamento; e

- estabelecer objetivos de segurança, alinhados com os objetivos estratégicos do Exército, que possibilitem o dimensionamento dos meios, o estabelecimento de prioridades e a avaliação das ações de segurança da informação.

Com relação ao desenvolvimento da doutrina relativa à guerra cibernética:

- incluir questões relativas à guerra cibernética nos Elementos Essenciais de Informações Doutrinárias;

- orientar os adidos militares quanto ao interesse do Exército na coleta de dados externos sobre tendências doutrinárias e inovações tecnológicas relativas à guerra cibernética;

- definir temas sobre o assunto para teses de doutorado, dissertações de mestrado e trabalhos acadêmicos das escolas subordinadas ao DEP e ao DCT;

- realizar seminários sobre guerra cibernética, incluindo-se, nesse contexto, os intercâmbios doutrinários com outros países; e

- desenvolver programas e projetos de pesquisa e experimentação doutrinária, com a finalidade de obter informações básicas que possibilitem a atualização do Quadro da Situação da Doutrina, com as deficiências relevantes e os principais problemas relacionados com a guerra cibernética.

Com relação à organização da Força Terrestre:

- atualizar as atribuições dos órgãos que desempenham atividades relacionadas com a guerra cibernética;

- definir responsabilidades para os gestores da informação, em todos os níveis da Instituição;

- organizar um núcleo multidisciplinar de especialistas, dedicado exclusivamente à atividade de guerra cibernética;

- criar um grupo de resposta a incidentes, no Centro de Telemática do Exército;

- a fim de auxiliar na obtenção da superioridade da informação durante possíveis conflitos, compor uma equipe operacional com a tarefa de levantar dados e produzir informações, em tempo de paz, sobre as vulnerabilidades dos sistemas de informação de possíveis forças adversas, a exemplo das ações conduzidas no âmbito dos sistemas estratégicos de guerra eletrônica e de inteligência; e

- investir na melhoria do Sistema Estratégico de Comunicações, com o propósito de diminuir a sua dependência dos sistemas nacionais de telecomunicações, bem como aumentar a sua capacidade, qualidade, robustez e segurança.

Com relação à pesquisa, ao desenvolvimento e à aplicação da tecnologia:

- desenvolver a capacidade de executar ações de inteligência e ofensivas, empregando ferramentas da guerra cibernética;

- desenvolver metodologia para inventariar a informação produzida, armazenada e difundida no âmbito do Exército, com a finalidade de possibilitar a determinação de onde está a informação importante a proteger e o estabelecimento de prioridade para a aplicação dos meios de segurança da informação;

- acompanhar e avaliar o desempenho dos softwares em uso no Exército, quanto à existência de vulnerabilidades que facilitem as ações de guerra cibernética por parte de possíveis adversários;

- desenvolver ferramentas de hardware e/ou software destinadas ao emprego em ações ofensivas e defensivas de guerra cibernética;

- realizar atividade de pesquisa e desenvolvimento com vistas à produção de um sistema criptográfico próprio;

- acompanhar a evolução das técnicas de ataque e defesa dos sistemas de informação, bem como realizar estudos prospectivos e previsões tecnológicas sobre o assunto; e

- intensificar a utilização de software livre.

Com relação à capacitação de recursos humanos:

- intensificar as atividades de sensibilização dos recursos humanos para a importância da segurança da informação, por meio da atualização dos currículos e planos de matérias dos cursos e estágios do Sistema de Ensino do Exército, e dos programas-padrão do Sistema de Instrução Militar do Exército; e

- realizar cursos de especialização em segurança da informação.

Com relação ao emprego da Força Terrestre:

- assessorar as organizações militares com relação às práticas de segurança;

- compartilhar informações sobre ameaças cibernéticas e vulnerabilidades, no âmbito do Exército;

- levantar as vulnerabilidades dos sistemas de informação do Exército, passíveis de serem exploradas por forças adversas, por meio de auditoria ou da simulação de ações hostis contra esses sistemas; e

- elaborar diretrizes sobre como responder aos ataques cibernéticos, definindo claramente os papéis e responsabilidades dos órgãos e pessoas envolvidas.

Com relação ao estabelecimento de parcerias de cooperação mútua:

- estimular o desenvolvimento de uma doutrina de emprego combinado de ações cibernéticas com as demais Forças Armadas;

- estabelecer convênios com entidades de pesquisa e desenvolvimento, visando ao desenvolvimento conjunto de produtos destinados ao emprego em ações de guerra cibernética, com especial atenção para o desenvolvimento de sistemas criptográficos próprios;

- participar do esforço nacional de proteção contra ataques cibernéticos, compartilhando informações sobre ameaças e vulnerabilidades, e apoiando, quando necessário, a defesa de outros órgãos governamentais, especialmente no que diz respeito à proteção dos sistemas de controle da infra-estrutura crítica nacional;

- procurar, sempre que possível, participar do processo decisório de órgãos públicos com atribuições relativas à inteligência, segurança da informação, desenvolvimento de software e outras atividades de interesse para a guerra cibernética; e

- estimular o estabelecimento de acordos internacionais para facilitar o rastreamento da origem e da identificação dos autores de ataques cibernéticos provenientes do exterior.

6 CONCLUSÃO

A organização da sociedade em rede não é novidade. Na verdade, a sociedade em rede surgiu quando o primeiro grupo de homens resolver reunir-se para produzir o seu sustento e defender o seu território. A única diferença do dias atuais é que aumentou a quantidade de pessoas do grupo, diminuiu o tempo da produção e ampliou-se a extensão do território, em função da rapidez, do alcance e da conectividade proporcionada pelas tecnologias da informação. As redes eletrônicas são apenas ferramentas que potencializam as virtudes e mazelas da natureza humana. Curiosamente, junto com as redes eletrônicas desenvolveu-se uma lógica digital interessante, que passou a polarizar, displicentemente, diferentes aspectos da sociedade humana, potencializando opostos como a globalização e os nacionalismos, a rede e o indivíduo, os excluídos e os incluídos, os Estados e os atores não-estatais, dentre outras simplificações do mundo moderno. O paradoxo existente entre os benefícios e os perigos decorrentes do uso da tecnologia é apenas mais uma faceta dessa lógica binária.

Nesse contexto, as ameaças representadas pela guerra cibernética são de natureza estratégica, pois envolve a sobrevivência das organizações. A lógica é muito simples: como as informações permeiam todas as atividades da organização e as ameaças atuam contra as informações, toda a organização está em risco. Por isso mesmo, antes de ser um problema de informática ou de comunicações, a guerra cibernética é um desafio gerencial.

Como a continuidade do funcionamento das redes de computadores é vital para a sobrevivência de pessoas, empresas, governos e países, o problema adquire dimensão nacional, razão pela qual existe organismo nos mais altos escalões do Executivo Federal empenhado em tratar do assunto. Não se trata de ficção, de moda passageira ou de algo para o futuro, mas de uma mudança real, que já está presente no nosso dia a dia e assim deve permanecer por longo tempo. A tendência é aumentar a sua importância. A rapidez e o alcance das redes apenas nos aproxima do problema e, quem sabe, da sua solução.

Se o mundo está mudando, o Exército não pode ficar alheio. Não se pode esquecer que o custo para defender é muito menor que o prejuízo a sofrer. Do

mesmo modo que qualquer outra instituição contemporânea, o Exército está cada vez mais se tornando dependente dos recursos de tecnologia da informação. Como ainda encontra-se em um nível ainda baixo de maturidade tecnológica, essa dependência deve aumentar nos próximos anos, e demandará novos recursos para a segurança da informação.

Apesar das ameaças que representa, a guerra cibernética também abriu o caminho para novas oportunidades. Com recursos relativamente modestos, é possível aumentar a operacionalidade da Força e ampliar o leque de alternativas para se atuar assimetricamente contra forças superiores, o que estaria de acordo com a realidade nacional e a concepção de emprego da Força Terrestre nas estratégias da resistência e da dissuasão.

Tanto para o ataque, como para a defesa, a palavra-chave para as ações a realizar é "cooperação". Não adianta se contrapor às redes de atacantes com estruturas organizacionais pouco flexíveis. O segredo é utilizar as mesmas armas dos possíveis adversários, ou seja, se organizar em redes. Redes internas para aumentar a cooperação dentro do próprio Exército e redes externas visando a buscar apoio para as nossas realizações. Enfim, redes para divulgar o problema, redes para preparar os recursos humanos, redes para construir estratégias, redes para atrair recursos e redes para reagir contra os ataques cibernéticos.

O homem, no entanto, é o componente básico de toda estratégia. Mais do que em qualquer outra época, hoje essa assertiva é verdadeira, porque o homem é o detentor do conhecimento. Por isso, ele tem poder. Poder para tomar a iniciativa e reagir aos problemas. Poder para inovar e conseguir vantagens sobre os adversários. Poder para estabelecer relacionamentos e construir parcerias.

Considerando a elevada qualificação, a motivação, a coesão, a responsabilidade e a determinação do nosso soldado, é certo que sempre haverá alguém presente para se contrapor a qualquer ameaça contra os sistemas de informação do Exército Brasileiro.

GILMAR PEREIRA DA SILVA - Cel

REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, P. D.; DEMCHAK, C. A Guerra Cibernética entre a Palestina e Israel. **Military Review.** Kansas, n. 1, p. 51, 2004.

BRASIL. Estado-Maior do Exército. C-124-1: Estratégia. **3. ed. Brasília, DF, 2001.**

BRASIL. Exército. Comandante do Exército. **Portaria nº 102, de 18 de março de 2003: Plano de Modernização e Integração do Sistema de Comando e Controle da Força Terrestre.** Brasília, DF, 2003.

BRASIL. Exército. Comandante do Exército. **Portaria nº 483 de 20 de setembro de 2001: Instruções Gerais de Segurança da Informação para o Exército Brasileiro - IG 20-19.** Brasília, DF, 2001.

BRASIL. Exército. Escola de Comando e Estado-Maior do Exército. **Formatação de Trabalhos Acadêmicos, dissertações e teses.** Rio de janeiro, RJ, 2004.

BRASIL. Exército. Escola de Comando e Estado-Maior do Exército. **Trabalhos acadêmicos na ECEME**. Rio de Janeiro, RJ, 2004.

CASTELLS, M. **A sociedade em rede.** 5.ed. São Paulo: Paz e Terra, 2001, 617p.

CÔRTES, M. H. C. **A defesa nacional diante do pós-modernismo militar.** [Trabalho apresentado no I Seminário sobre Defesa Nacional, Rio de Janeiro, 20 nov. 2000]

CÔRTÊS, M. H. C. **A Guerra do Iraque no contexto do pós-modernismo militar.** PADECEME. Rio de Janeiro, n. 5, p. 13-18, 2003.

EUA. Department of the Army. **FM 100-6 INFORMATION OPERATIONS.** Washington, DC, 1996.

FELSTEAD, P.; HUGHES, R. Interview: Brigadier General Mark Kimmitt. **Jane' s Defence Weekly.** Surrey, n.9, p. 34, 2005.

PARKS, R. C.; DUGGAN, D. P. **Principles of cyber-warfare.** In: WORKSHOP ON INFORMATION ASSURANCE AND SECURITY, 5-6 June, 2001, West Point, NY. Anais ... IEEE, 2001, p. 122-125.

KOCH, Andrew. Tomorrow' s WMD.**Jane' s Defence Weekly.**Surrey, n.6, p. 27-29, 2005.

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO. **EBNET: Guia do Comandante.** Brasília, DF, 2004.

SILVA, Gilmar Pereira da. **A integração dos sistemas informatizados de campanha através de um sistema de comunicações moderno.** 1996. 62 f. Monografia (Doutorado em Ciências Militares)- Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 1996.

SOUZA, C. R. P. **Guerra da informação.** PADECEME. Rio de Janeiro, n. 4, p. 12-22, 2003.

TOFFLER, A.; TOFLER, H. **Guerra e antiguerra: sobrevivência na aurora do Terceiro MIlênio.** 1.ed. Rio de Janeiro: Record, 1994. 349 p.

WINKLER, IRA. **Corporate Espionage.** 1.ed. Rocklin: Prima Publshing, 1997, 365p.