A segurança da informação e sua importância na proteção dos sistemas informatizados em uso nas organizações militares do Exército brasileiro[1]

*Carlos Sérgio Camara Saú**

RESUMO

O título expressa o conteúdo do artigo. Ele destaca a importância da segurança das informações informatizadas nas OM do nosso Exército, diagnostica sua situação atual, caracteriza os principais problemas com que se defronta e propõe medidas para solucioná-los.

PALAVRAS-CHAVE

Informações, segurança, informática.

A riqueza de uma nação era, no passado, medida pelo montante de ouro armazenado em seus cofres. Era a chamada época do lastro ouro. Esse conceito evoluiu para uma forma mais abrangente de se medir a riqueza, que tinha como parâmetro o lastro moeda, o qual, por sua vez, resultou na concepção atual de base monetária. Isto é, o somatório de papel-moeda, depósitos à vista, títulos do governo, entre outros, em circulação no mercado. Hoje principiamos uma nova realidade: nação rica é aquela que tem o poder de obter e armazenar a maior quantidade de informações possível. Com segurança.

BETING, Joelmir, *Internet ou Infernet?, O Globo*, 31 de março de 1996, p. 28

---

* Major de Artilharia.

[1] Selecionado pelo PADECEME.

Informações armazenadas em arquivos magnéticos são uma realidade cada vez mais integrada à vida das pessoas, empresas, instituições e governos. Essa verdadeira revolução iniciou-se poucas décadas atrás, mas foi mais recentemente, com o barateamento dos preços e a conseqüente popularização dos microcomputadores, que a informática passou a fazer parte do dia-a-dia.

No mundo moderno, a velocidade na tomada de decisões aumentou assustadoramente, pelo fato de as informações terem passado a ser compartilhadas e atualizadas em tempo real, devido ao emprego maciço da tecnologia de redes, locais ou remotas.

A difusão do uso da *Internet* veio facilitar a troca de informações entre pessoas e entidades, para os mais variados fins. Com isso, informações confidenciais passaram a ser transmitidas por meio de linhas telefônicas, sujeitas a interferências de terceiros.

A responsabilidade pela proteção de dados assumiu complexidade enorme, pois além de estarem espalhados por diferentes áreas dentro da organização, esses dados podem ser acessados não só por outros setores dessa mesma organização, como também por outros elementos externos, bastando para isso que se utilizem os canais de transmissão desses dados.

Atualmente, não basta colocar computadores para trabalhar em rede, ou mesmo ter um serviço que funcione ininterruptamente, sem que haja uma política de segurança e ferramentas que protejam as informações tanto de ameaças internas quanto externas ao meio em que são trabalhadas.

Menosprezar a segurança em processamento de dados deve ser encarado como *suicídio profissional*, devendo os comandantes e chefes enfrentar o desafio de encontrar o ponto de equilíbrio entre a possibilidade de segurança absoluta e o perigo da total falta de segurança.

A informatização das Organizações Militares (OM) do Exército tomou grande impulso há pouco mais de uma década, acompanhando a onda da revolução tecnológica, que lançou sobre nós os microcomputadores baratos e com grande capacidade de armazenamento de informações. Com exceção de determinados setores da Alta Administração do Exército, todos os nossos arquivos eram baseados em papel. Essa informatização das OM ocorreu, na prática, de uma forma desordenada, não obstante os esforços desenvolvidos pela Força no sentido de buscar uma padronização e uniformização dos sistemas de *hardware* e *software* utilizados.

Na verdade, os equipamentos que eram adquiridos pelas OM, malgrado os grandes esforços financeiros realizados pelos comandantes, rapidamente passavam à obsolescência, pois os avanços tecnológicos vinham a velocidades surpreendentes, tornando máquinas recém-adquiridas completamente ultrapassadas. Aliado a isso, o desconhecimento das gerações mais antigas no trato com os novos recursos e suas potencialidades colaboraram para que sua implementação fosse um pouco demorada, tendo o computador sido inicialmente utilizado como uma máquina de escrever luxuosa e cara.

Esse início tumultuado trouxe alguns reflexos que se estendem até hoje, acarretando conseqüências para a segurança da informação, pela falta de uma cultura de segurança daqueles que operam esses sistemas.

Quando o assunto é segurança, parece existir uma falta de preocupação com o tema, pois o mesmo está sempre sendo desconsiderado ou adiado, muito provavelmente devido aos custos envolvidos. O importante é lembrar que esta deve ser uma das maiores preocupações na hora de se implantar uma rede de computadores, pois as informações transmitidas serão, muitas das vezes, classificadas, e sua manipulação por pessoas não autorizadas poderá causar, no mínimo, sérios embaraços administrativos.

A solução para o problema certamente passa pela necessidade de se treinar nossos recursos humanos para a nova realidade que estamos vivendo, não ficando as OM à sorte de encontrar em seus quadros algum integrante que se tenha qualificado em cursos civis, por sua livre iniciativa. Quanto mais for investido na formação e treinamento de pessoal militar habilitado, menor será o desperdício de recursos financeiros e mais rapidamente serão atingidos os objetivos programados.

Mensagens trocadas entre clientes de uma mesma rede ou dados armazenados eletronicamente precisam ser protegidos de maneira que apenas pessoas e processos autorizados consigam utilizá-los, evitando, dessa forma, o furto ou a adulteração da informação, bem como a criação de informação falsa ou a destruição da informação correta.

A segurança da informação descreve toda forma de prevenir o uso não autorizado de dados eletrônicos, ou seja, divulgar, alterar, substituir ou destruir qualquer componente que diga respeito a esses dados.

A segurança da informação abrange as áreas lógica e física, bem como mecanismos de auditoria.

A área lógica abrange todas as defesas contra um ataque à memória dos computadores e ao trânsito dos dados arquivados magneticamente, em rede ou não.

A área física abrange as defesas contra o acesso não autorizado aos equipamentos de *hardware*.

A auditoria de segurança é uma atividade cuja função precípua é fazer a estrutura organizacional trabalhar bem. Suas metas podem ser sintetizadas em prevenir e/ou corrigir falhas, irregularidades e vícios.

A segurança em informática tem que ser considerada parte integrante da segurança das OM e ambas utilizam conceitos e abordagens técnicas, administrativas e operacionais comuns.

Sob esse enfoque, é importante destacar os seguintes aspectos:

- segurança é responsabilidade de todos os profissionais militares, inclusive os da área de informática;
- o patrimônio da OM (recursos humanos, materiais, tecnológicos, etc) precisa ser preservado;
- a análise de segurança em informática implica correlacionar as medidas de segurança com as ameaças e situações de insegurança de cada local físico que compõe o ambiente de informática;
- para o estabelecimento e verificação da segurança, é necessária a determinação de um ponto crítico no ambiente de informática, que mereça acompanhamento, para serem evitadas ameaças em relação a erros, omissões, falhas, fraudes, roubo;
- a falha de segurança ocorrida em uma área pode ocorrer em outras áreas da OM; e
- a segurança é exercida via rotinas e métodos de controle.

Sendo a informação elemento fundamental para a sobrevivência das organizações, é uma velha preocupação dos profissionais de informática a manutenção da sua integridade, segurança e confiabilidade. Isso se deve à fragilidade e às possibilidades de perda ou recuperação de arquivos, principalmente pelo massivo uso das mídias magnéticas.

Quando os dados eram guardados em discos e fitas magnéticas produzidas por centros de processamento de dados (CPD) centralizados, a guarda e a recuperação de informações eram, de certa forma, mantidas sob melhor controle. Hoje, com o advento das redes, dos equipamentos portáteis ligados remotamente por meio de *modem* e outras facilidades, o controle sobre a integridade, confiabilidade e recuperação de dados tornou-se extremamente difícil e complexo.

Outra grande fonte de preocupação na salvaguarda dos arquivos informatizados é a vulnerabilidade destes à nova modalidade na guerra, chamada guerra da informação (*information warfare*), introduzida pela revolução tecnológica, e que irá afetar todos aqueles que utilizam redes de comunicações e computadores.

Um dos problemas com a guerra da informação é que ainda não existe uma definição oficial sobre a mesma, uma vez que sua concepção é muito recente e com muitos significados, tanto no meio militar como no meio civil.

Uma definição utilizada pelo Departamento de Defesa dos Estados Unidos da América (DoD), é a seguinte: *são ações realizadas para obter superioridade de informações, em apoio à estratégia militar de defesa nacional, afetando as informações e os sistemas de informações do adversário, e, ao mesmo tempo, impulsionando e defendendo nossas informações e sistemas.* O objetivo não será tão somente conseguir superioridade de informações, mas manipular o inimigo (ou sua população), com informação falsa ou deturpada, a fim de confundi-lo ou desmoralizá-lo.

A Guerra do Golfo foi o primeiro degrau da guerra da informação, pela utilização de armas inteligentes e computadores. Existiam mais de 3000 computadores na zona de combate, centenas deles ligados a computadores nos EUA.

A Guerra do Golfo foi o primeiro degrau da guerra da informação, pela utilização de armas inteligentes e computadores. Existiam mais de 3000 computadores na zona de combate, centenas deles ligados a computadores nos EUA.

Esse novo tipo de guerra fornece a potenciais inimigos o poder de destruir a capacidade de comunicações de um país e prejudicar sua economia. Pode, ainda, ser usado por terroristas, os quais, ao invés de plantar uma bomba em um avião, podem introduzir um poderoso vírus de computador num centro de controle de vôo em um aeroporto, colocando em risco dezenas de aeronaves ao mesmo tempo.

Embora se procure meios de proteção cada vez melhores, a própria evolução da tecnologia torna praticamente impossível criar um sistema absolutamente seguro.

Desde os tempos da antiga Roma, o uso de mensagens cifradas era amplamente utilizado nas guerras para garantir melhor segurança na troca de informações.

Durante séculos, técnicas criptográficas têm sido utilizadas para proteger e dar autenticidade à correspondência político-diplomática e às comunicações militares. Nos últimos trinta anos, a criptografia conheceu um crescimento espetacular, acompanhando a revolução da comunicação e dos computadores.

Nos Estados Unidos, a criptografia é considerada material bélico, sendo a exportação de *hardware* ou *software* criptográfico feita somente sob licença. As chaves para *software* de exportação sofrem limitações em seu tamanho, o que permite, com os recursos computacionais atuais, que elas sejam quebradas em um tempo relativamente curto, o que ainda permitiria o uso da informação privilegiada com oportunidade.

Acredita-se que as vulnerabilidades da criptografia podem ser bastante atenuadas adotando-se políticas de segurança adequadas.

Uma política de segurança lógica e física de sistemas criptográficos deve estar inteiramente comprometida em garantir a capacidade do tripé criptográfico, ou seja, algoritmo, gerência de chaves e procedimentos operacionais.

A implantação de um programa de segurança da informação, quer para o Exército brasileiro, quer para qualquer outra instituição ou empresa, deve levar em consideração os riscos a que os sistemas estão submetidos, os investimentos possíveis de ser realizados para a diminuição desses riscos, a conscientização dos usuários e o comprometimento da alta administração com o sucesso do modelo adotado.

Qualquer política de segurança da informação deve ser dotada de instrumentos que assegurem a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e informações de interesse para a Força.

No caso específico do Exército, diferentemente de empresas privadas, deve também objetivar o desenvolvimento da capacidade científico – tecnológica da instituição, no sentido de torná-la auto-suficiente no que diz respeito ao desenvolvimento de *software* e *hardware* destinados à criptografia das mensagens em trânsito, bem como em tecnologias de defesa contra ataques e espionagens aos nossos arquivos informatizados.

Mas, na verdade, o que se quer proteger, quando se fala em segurança da informação?

Uma resposta a essa indagação pode ser dividida em três aspectos.

Inicialmente, deseja-se a proteção dos dados arquivados eletronicamente, e que se mantenham a privacidade, a integridade, a disponibilidade e a autenticidade desses dados. Deseja-se, também, que os recursos computacionais sejam mantidos, preservando-os de ataques externos e do acesso por pessoas não autorizadas. E proteger a reputação da Força, evitando que seja desmoralizada por ataques bem sucedidos.

Outra pergunta que o responsável pela implantação de um programa de segurança da informação deve fazer para direcionar seu esforço de proteção é: *quem são os agressores e qual o seu objetivo?*

Segundo recentes pesquisas da *Price, Waterhouse and Coopers*, as maiores fontes das falhas de segurança e espionagem corporativa estão sendo atribuídas aos usuários autorizados e aos próprios funcionários das empresas atacadas (cerca de

55%). Uma boa parte desses ataques também partiu de ex-funcionários e *hackers* (aproximadamente 30%).

Essas agressões são provocadas com múltiplos objetivos: sabotagem ou desmoralização da empresa, provocada pela concorrência; vingança (no caso de ex-funcionários); furto de informação valiosa; espionagem industrial e militar; obtenção de vantagens financeiras ou acadêmicas; e furto de programas (*software*), entre outros.

O problema da segurança passa também por uma questão cultural. A nossa cultura, bem como a dos países latinos, é a confiança mútua, onde tudo o que não é proibido é permitido. Dessa forma, nossa vulnerabilidade a ataques aumenta, porque os aspectos da segurança são relevados, uma vez que todos confiam em todos.

Portanto, qualquer investimento em segurança deve considerar a necessidade de modificar hábitos socioculturais, ou seja, de nada adiantará adquirir poderosas ferramentas tecnológicas para proteção aos sistemas, se a mentalidade das pessoas que lidam com a informação e operam os equipamentos não for também trabalhada, a fim de capacitá-las para o uso pleno das novas tecnologias e iniciar, também, a difusão de uma cultura voltada para a segurança de dados arquivados eletronicamente.

Disso resulta que os investimentos na área devem considerar a constante atualização técnica do pessoal, por meio de cursos e estágios, os quais podem ser realizados dentro da Força (por meio dos Centros de Telemática de Área, por exemplo), ou mesmo fora dela, em instituições de ensino civis, desde que isso seja do interesse do Exército.

Qualquer investimento em segurança deve considerar a necessidade de modificar hábitos socioculturais, ou seja, de nada adiantará adquirir poderosas ferramentas tecnológicas para proteção aos sistemas, se a mentalidade das pessoas que lidam com a informação e operam os equipamentos não for também trabalhada.

Contudo, os investimentos em segurança não param nas questões de pessoal, mas continuam na implantação de uma política adequada à Força no desenvolvimento e implantação de sistemas de criptografia, na implantação de sistemas de proteção às redes (*firewall, virtual private network* e outros), no estabelecimento de grupos de pronta resposta a ataques e na implantação de uma auditoria nos sistemas internos para avaliação permanente dos mecanismos de controle da segurança.

Fazendo um diagnóstico da situação atual, encontramos os problemas abaixo listados para a segurança da informação:

• *Disseminação dos microcomputadores pela Organização* – Como vimos, o crescimento do uso dos microcomputadores foi explosivo, a partir do início da década de 90, com a tendência de os mesmos substituírem no todo ou em parte o processamento de dados corporativos, antes realizado pelos computadores de grande porte e segregados aos CPD. (Centros de Processamento de Dados).

• *Armazenamento de assuntos sigilosos* – As OM do Exército brasileiro, pos-

suindo centenas desses equipamentos processando a informação por toda a Instituição, necessitam utilizar com maior eficácia os meios existentes para a sua proteção, pois os assuntos sigilosos estão consideravelmente mais expostos ao risco de acesso indevido.

• *Manuseio inadequado das mídias magnéticas* - Além do que foi exposto acima, os usuários nem sempre se dão conta de que a mídia magnética - a mais utilizada para armazenar as informações e programas - composta por disquetes, discos rígidos e fitas, a par de conter ativos intangíveis fundamentais para o funcionamento da Instituição, carece de cuidados especiais de manuseio e proteção.

• *O compartilhamento e a comunicação de dados* - Outro aspecto relevante a considerar é que a colocação dessas máquinas em redes, remotas ou locais, permite um acesso fácil a uma vasta gama de informações. A informação é trocada entre dois pontos, sendo possível sua interceptação no meio do caminho, ou sua manipulação nos próprios servidores ligados à rede.

• O uso de microcomputadores portáteis - Além dos problemas de segurança provocados pela possibilidade de comunicação entre os computadores, o desenvolvimento tecnológico possibilitou, também, a portabilidade desses aparelhos. Microcomputadores portáteis, do tipo *laptop*, *notebook* e *palmtop*, apesar de convenientes, constitui-se no maior desafio para a segurança em informática, pois permitem que as informações sejam levadas para fora das OM, onde ficam vulneráveis à destruição, alteração ou furto.

• *O vírus de computador* - Há que se considerar, ainda, que todas essas máquinas podem ser vitimadas por *vírus*, intencionalmente ou não. *Vírus*, na realidade, constituem uma forma de acesso não autorizado. Uma das maneiras mais eficazes de provocar a disseminação desses *vírus* é a utilização de programas não recomendados, normalmente de origem desconhecida, e, também, por jogos, por parte dos usuários que, afastada a possibilidade de dolo, não se dão conta do perigo a que expõem a sua organização.

UMA PROPOSTA DE SOLUÇÃO

A segurança eficaz somente pode ser conquistada pelo uso de produtos apropriados e por procedimentos realizados por todos os usuários. Produtos, isoladamente, nunca são suficientes. É vital que se assegure que as pessoas envolvidas entendam totalmente o seu papel na segurança e sigam os procedimentos adequados. O comportamento profissional de quem utiliza o computador como ferramenta de trabalho é determinante para o sucesso ou insucesso das medidas de proteção que forem adotadas.

Com essa preocupação, propõe-se uma solução para o problema, por meio de uma diretriz, a qual deverá orientar a elaboração de planos de contingência, por parte das Organizações Militares. Essa diretriz deverá estabelecer procedimentos adequados para contrapor-se aos óbices até aqui descritos, quais sejam:

• *Formação de uma sólida mentalidade de segurança das informações* - O estabelecimento de uma cultura de segurança será o resultado da participação ativa de todos os integrantes da OM, fruto da consciência das ameaças à segurança e do per-

feito conhecimento da responsabilidade individual na busca e neutralização dessas ameaças.

Essa mentalidade, peça mais importante e base para se atingir as metas propostas, só poderá ser alcançada com a colocação em prática de um bem elaborado programa de educação de segurança.

• *Controle do acesso* - O controle do acesso deve ser entendido tanto quanto à possibilidade de utilização de um equipamento (acesso físico), quanto à necessidade de conhecer determinada informação (acesso lógico).

O controle de acesso físico requer a adoção de medidas de segurança orgânica, nem sempre de fácil implementação, em face da grande dispersão dos equipamentos por toda a Unidade. Entretanto, algumas medidas eficazes podem ser tomadas, tais como: distribuição de credenciais de segurança, segregação dos aparelhos utilizados para o trato de assuntos sensíveis em locais cujo acesso possa ser controlado, utilização de cofres para a guarda de discos, fitas ou outros meios de armazenamento de dados sigilosos, entre outras.

O acesso lógico está relacionado com a possibilidade de o usuário interagir com determinadas bases de dados, o que é facilitado quando os microcomputadores estão conectados a outros computadores.

Nesse caso, é importante assegurar-se de que os procedimentos de controle de acesso não conflitem nem sejam encarados como uma inconveniência desnecessária pelos usuários. Deve-se levar em conta que os administradores da rede deverão analisar, entender e implementar as restrições de acesso de acordo com a necessidade que cada usuário tem de conhecer.

É vital que se assegure que as pessoas envolvidas entendam totalmente o seu papel na segurança e sigam os procedimentos adequados. O comportamento profissional de quem utiliza o computador como ferramenta de trabalho é determinante para o sucesso ou insucesso das medidas de proteção que forem adotadas.

• *Cifragem* - Em ambientes multiusuários, ou quando for necessária a transmissão de dados classificados entre computadores de uma rede ou por meio de *modem*, utilizando linhas discadas, é mandatória a utilização de algoritmos de criptografia que forneçam um grau de proteção adequado ao grau de sigilo requerido.

• *Back-up* - A segurança dos dados não deve ser encarada unicamente no sentido de negar ao inimigo o uso das nossas informações sensíveis; há que se considerar a possibilidade de essas informações serem perdidas ou danificadas acidentalmente. A única medida real que pode impedir o usuário e a organização de perder dados é fazer do *back-up* uma prática natural e constante.

• *Uso de programas antivírus* - A melhor proteção contra os vírus de computador é não utilizar programas de origem duvidosa (principalmente jogos), cabendo aos administradores, além da tarefa de supervisão, a de conscientização dos usuários quanto aos riscos que essa atitude pode acarretar.

• *Realização de auditorias de segurança* - As principais metas de uma auditoria

de segurança podem ser sintetizadas em prevenir e/ou corrigir falhas, irregularidades e vícios. É uma atividade que deve ser desenvolvida diuturnamente, pois, de outra forma, o prejuízo causado por alguma negligência ou má fé já terá se tornado irreversível, ou seja, a oportunidade da ação de controle já passou.

A auditoria compreende controles operacionais visando a assegurar que só sejam processados dados completos, precisos e devidamente autorizados; evitar erros acidentais ou manipulação fraudulenta de dados, detectando-os se vierem a acontecer; e a proporcionar segurança contra destruição acidental dos registros, assegurando a continuidade das operações.

Como foi até aqui demonstrado, as ações a serem desencadeadas com a implantação da solução proposta, carrearão inúmeros benefícios diretos e indiretos para a Força, entre os quais se destacam: o efetivo controle da base de dados, o aumento da qualidade e da produtividade, a redução dos custos no processamento de dados e o incremento da mentalidade de contra-inteligência.

CONCLUSÃO

É preciso que se diga que, como Instituição Militar, a segurança é o negócio do Exército brasileiro.

O que se propôs foi, em última análise, a adoção de procedimentos que vêm ao encontro da manutenção da segurança interna das suas OM sob a ótica da informática, com vistas a salvaguardar os conhecimentos sensíveis e indispensáveis ao cumprimento de sua missão constitucional.

A segurança da informação é semelhante a uma corrente, cujo nível de qualidade vai ser expresso pela robustez de seu elo mais fraco. Por isso, é fundamental que a segurança seja implantada em um processo contínuo, dinâmico e em permanente evolução.

Como um bem intangível fundamental à própria sobrevivência das organizações, deve merecer o mesmo cuidado e atenção dispensados ao se definirem os requisitos dos equipamentos e sistemas que serão adotados.

Muito se tem falado sobre a importância das organizações estarem ligadas na tecnologia da informação, que não se pode pretender buscar o desenvolvimento se não estiver atualizado na área de informática. Entretanto, tudo isso é muito moderno e maravilhoso até que não se perca o controle da informação.

Os profissionais militares têm, por obrigação de ofício, o dever de estar permanentemente preocupados em salvaguardar um dos mais emergentes, potentes e importantes trunfos na guerra: a informação.

É importante, também, que as soluções que venham a ser adotadas pelo Exército brasileiro, principalmente no campo da criptografia, sejam nacionais, pois a dependência externa no campo da Ciência e Tecnologia constitui sério óbice ao seu desenvolvimento e soberania.

A tecnologia cresce com espantosa velocidade e na proporção inversa à aquisição da cultura que teremos de disseminar aos profissionais militares sobre a segurança de nossas informações. Entretanto, devemos ser incansáveis nessa empreitada, pois ela será, daqui para a frente, o mais poderoso instrumento para a sobrevivência das nações.

Quem tem a informação tem tudo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Augusto César Athayde. *A Internet como base tecnológica e meio auxiliar para a criação e o desenvolvimento da rede de informações do Exército Brasileiro (EBNet) a curto prazo.* Rio de Janeiro: ECEME, 1997. Monografia.

ARIMA, Carlos Hideo. *Metodologia de auditoria de sistemas.* São Paulo: Érica, 1994.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *Controle de acesso para segurança física de instalações de processamento de dados* - NB 1333. Rio de Janeiro, 1990.

BARROS, Otávio Santana do Rêgo. *A informática e a organização sistêmica do Exército Brasileiro.* Rio de Janeiro: ECEME, 1998. Monografia.

BETING, Joelmir. *Internet ou Infernet?* O Globo, Rio de Janeiro, 31 Mar 1996, p. 28.

CAMPOS, José Eduardo (eduardo.campos@br.pwcglobal.com). Envio de resultados de pesquisas sobre política de segurança da informação da Price Waterhouse and Coopers Global. 28 Jul 1999. Enviado às 14h28min. Mensagem para: Carlos Saú (csau@uol.com.br).

COSTA, Edwim Pinheiro, BEKER, Cemilton. *A informática no Exército Brasileiro - sua estruturação, transmissão e segurança de dados.* Rio de Janeiro: ECEME, 1993. Monografia.

DAMASCENO, Eumar Barros. *O aproveitamento racional dos modernos recursos de informática nas organizações militares.* Rio de Janeiro: ECEME, 1997. Monografia.

GOLDBERG, Ivan. *Information Warfare.* Capturado em 01 Ago 1999. Online. Disponível na Internet: http://www.psycom.net/iwar.html.

HAENI, Reto. *An Introduction to Information Warfare.* Capturado em 27 Jul 1999. *Online.* Disponível na Internet http://tangle.seas.gwu.edu/~reto/infowar/info-war.html.

INSTITUTO MILITAR DE ENGENHARIA. *Política para Segurança de Sistemas de Informações do Exército Brasileiro* (Proposta). Rio de Janeiro, 1998.

INTERNET nasceu há 30 anos, no meio militar. O Globo, Rio de Janeiro, 24 Nov 1999, Caderno Informática, p.6.

MAGALHÃES, Eduardo. *Empresas brasileiras não estão preparadas para falhas de segurança.* Computerworld, São Paulo, 13 Set 1999. *News.* Capturado em 14 Set 1999. Online. Disponível na Internet: http://www.uol.com.br/computerworld/news/9909/13/990913falhas.htm

MINISTÉRIO DO EXÉRCITO. *Diretriz Estratégica de Informática.* Port Min Nr 022- Res, de 25 de março de 1993. Brasília, 1993.

PROTEJA SEU MICRO CONTRA ATAQUES. *Mundo Digital do Universo Online.* São Paulo, 01 Ago 1999. Internet. Capturado em 20 Dez 1999. Online. Disponível na Internet: http: www.uol.com.br/internet/virus.

QUADRADO, Adriano. Brasil.gov.br é hackeado. IDG Now! São Paulo, 13 Set 1999. Internet. Capturado em 14 Set 1999. Online. Disponível na Internet: http://www.uol.com.br/idgnow/inet/inet1999-09-13a.shl

SALLES, Disnei Vieira, RODRIGUES, Alvaro Salio Teixeira. *Segurança de sistemas criptográficos: reflexões.* Revista Militar de Ciência e Tecnologia, Rio de Janeiro, v.14, n.1, p.29-37, 1° trim. 1997.

SAWICKI, Ed. Segurança. Rio de Janeiro: Campus, 1993.

TOFFLER, Alvin, TOFFLER, Heidi. *Guerra e Anti-Guerra.* Rio de Janeiro: BIBLIEx, 1995.

YEARY, Lon M. *Hackerwar and its influence on the Marine Expeditionary Force Commander.* Capturado em 15 Jun 1999. Online. Disponível na Internet: http://www.fas.org/cp/eprint/96/yeary.htm.