O EMPREGO DE MEDIDAS DE DEFESA CIBERNÉTICA NOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO DO SISTEMA DE COMUNICAÇÕES DA BRIGADA

Samuel Bombassaro Neto[a]

RESUMO

Diversas mudanças ocorreram advindas da recente evolução tecnológica da sociedade moderna, tanto no campo civil quanto militar. O uso de meios de tecnologia da informação passou a ser um multiplicador do poder de combate, estando presente com frequência nos sistemas de comunicações dos diversos escalões. O presente trabalho apresenta o emprego de medidas de defesa cibernética que visem à redução da vulnerabilidade dos meios de tecnologia da informação utilizados em um sistema de comunicações de uma brigada. Para atingir o objetivo proposto, foi realizada uma pesquisa bibliográfica baseada na doutrina existente sobre o funcionamento das comunicações da brigada, bem como nos conceitos e princípios da guerra cibernética, enfatizando as principais formas de ataque virtual e medidas de defesa consagradas. O instrumento escolhido para a coleta dos dados que serviram de subsídio para apresentar o modo como os meios de tecnologia da informação são utilizados nas organizações militares foi o questionário misto, tendo obtido resultados que indicam a necessidade de utilização das medidas de defesa cibernética para que o sistema de comunicações esteja protegido de ataques virtuais. Foi elaborada uma tabela comparativa, a qual relaciona a deficiência em segurança encontrada com o apropriado procedimento de defesa cibernética. Por fim, recomendou-se a organização de uma equipe de resposta para incidentes de redes de computadores, a capacitação de pessoal e a adoção da política de segurança da informação.

PALAVRAS-CHAVE: Guerra cibernética. Defesa cibernética. Tecnologia da informação.

ABSTRACT

Various changes have occurred from the recent technological developments of modern society, both in civil and military areas. The use of means of information technology hás become a multiplier of combat power, frequently being present in various communications systems. This work sought to introduce the use of cyber defense measures aimed at reducing the vulnerability of information technology means used in a communication system of a brigade. To achieve the proposed objective, was conducted a literature search based on existing doctrine on the functioning of the communications of the Brigade, as well as on the concepts and principles of cyber war, emphasizing the main forms of virtual attack and defense measures. The chosen instrument for the collection of data that served to present how the means of information technology are used in military organizations was the joint questionnaire, and it obtained results that indicate the need of cyber defense measures so that the communications system keep protected from virtual attacks. It was drawn up a comparative table, which lists the safety deficiency found with the appropriate procedure for cyber defense. Finally, it was recommended to use a response team to incidents of computer networks, training staff and the adoption of the information security policy.

KEYWORDS: Cyber war. Cyber defense. Information technology.

---

[a] Capitão de Comunicações da turma de 2003. Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais em 2012. Realizou o curso Básico de Guerra Eletrônica para Oficiais no Centro de Instrução de Guerra Eletrônica no ano de 2006.

O EMPREGO DE MEDIDAS DE DEFESA CIBERNÉTICA NOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO DO SISTEMA DE COMUNICAÇÕES DA BRIGADA

1. INTRODUÇÃO

A evolução tecnológica recente e veloz que vive a sociedade moderna já modificou largamente a maneira de se agir em diversos campos. Educação, procedimentos médicos, comércio e pesquisas são apenas alguns exemplos (CANONGIA e JUNIOR, 2009, p. 22)[1]. O setor público, alinhado com esta evolução, já está há algum tempo aprofundando estudos na área da tecnologia. Procurando adequar os seus sistemas corporativos aos novos rumos ditados pela evolução tecnológica, as Forças Armadas, alinhadas com o compromisso governamental, seguem a mesma tendência, observando com muita atenção e cuidado a vertente cibernética, pois as estruturas críticas de sistemas do Brasil utilizam, em sua maioria, plataformas informatizadas para operar.

As instituições militares, dentre elas o Exército Brasileiro, vivenciam também transformações recentes no campo tecnológico. Bancos de dados corporativos informatizados, ligações em tempo real e videoconferências tratadas como reuniões oficiais são algumas novidades que não eram imaginadas em um passado não tão distante. Lógico que se trata de uma necessidade do país, pois a evolução fez com que não fosse mais possível executar determinados procedimentos sem o uso de tecnologia da informação (TI). De modo semelhante ocorre no campo militar, no qual a vertente da guerra cibernética já não é mais algo a ser tratado somente por países altamente desenvolvidos e em um futuro longínquo. É uma realidade, para a qual qualquer força armada deve estar preparada.

As diretrizes elaboradas pelo Comando do Exército Brasileiro, particularmente a partir do ano de 2007, revelam o grau de importância do assunto guerra cibernética para a Força Terrestre. O Departamento de Ciência e Tecnologia (DCT), Órgão de Direção Setorial (ODS) responsável pelo desenvolvimento e pesquisa no âmbito da tecnologia aplicada às operações militares, realiza os estudos e transforma a política de defesa cibernética do Comando da Força Terrestre em normas práticas para serem aplicadas no Exército em todo território nacional. Acompanhando a evolução e a crescente importância do assunto, a Estratégia

Nacional de Defesa, aprovada pelo Decreto n° 6.703, de 18 de dezembro de 2008[2], é o documento da Presidência da República que cita, por diversas vezes, o ramo cibernético como sendo um dos setores de maior importância estratégica para o país; prevê, inclusive, medidas genéricas para o desenvolvimento na área. A preocupação citada é facilmente compreensível: abdicando-se da tecnologia, perde-se em poder de combate.

Dessa maneira, faz-se necessário compreender que o uso de sistemas computacionais de informação, em qualquer nível ou escalão, é uma realidade da qual não se pode descuidar. Assim sendo, o presente trabalho visa realizar um estudo sobre a necessidade do emprego de medidas que possam ser adotadas para proteger, principalmente, as informações que trafegam nesses sistemas informatizados.

O emprego da tecnologia da informação é relevante no campo militar, haja vista o seu destaque na Estratégia Nacional de Defesa (END). Portanto, a utilização dos dispositivos de tecnologia da informação, classificados pelo Departamento de Ciência e Tecnologia do Exército como materiais capazes de armazenar e/ou veicular informações ou dados, é comum e tende a crescer no âmbito da Força. Nada mais lógico, pois o aproveitamento de tais materiais permite a obtenção de diversas vantagens em relação aos métodos anteriores, tanto nos níveis estratégico quanto tático, este foco do presente trabalho.

A brigada é o escalão escolhido no contexto apresentado por se tratar de uma peça de manobra, na qual se caracteriza o emprego combinado de Armas e Serviços. O Exército Brasileiro possui diversos tipos de brigadas, variando as suas características e formas de emprego; porém, de maneira geral, uma brigada possui diversos elementos de manobra, bem como de apoio, sendo que ela deve ser capaz de instalar os seus diversos sistemas e integrar-se ao escalão superior, de modo a suprir as suas necessidades e participar de manobras de maior vulto. Os sistemas de uma brigada são os de Apoio Logístico, de Defesa Antiaérea, de Pedidos Aéreos, de Alarme, de Inteligência, Operacional e de Apoio de Fogo. O sistema que permeia a todos e é o responsável pelas ligações necessárias às ações de comando das forças que lhe são subordinadas é o sistema de Comando e Controle. Este último está intimamente ligado aos diversos meios de comunicações, que permitem um eficaz exercício da autoridade do comandante sobre os seus subordinados (BRASIL, 1998, p. 2-2)[3].

No desdobramento do sistema de comando e controle, uma brigada faz uso de diversos meios ou dispositivos de tecnologia da informação. Não existe, atualmente, uma padronização de quais ou a quantidade desses meios que pode ou deve ser utilizada. Fato é que o largo uso desses meios ou dispositivos de TI aumenta o desempenho como um todo. E a instalação, exploração e manutenção desse conjunto de meios, constituindo o sistema de comunicações da brigada, é responsabilidade de um elemento orgânico da própria grande unidade: a Companhia de Comunicações de Brigada. É ela a unidade que possui a missão precípua de coordenar as comunicações.

O emprego dos meios de tecnologia da informação no sistema de comunicações de uma brigada começou de maneira experimental logo no início da evolução vivida globalmente com o advento de tecnologias mais modernas. Ainda que timidamente, passaram a ser utilizados computadores, redes sem fio, bancos de dados, entre outros, melhorando pontualmente setores importantes para o elemento de manobra. Mas os resultados foram tão satisfatórios que passou a ser, embora não oficialmente, obrigatório o uso da tecnologia da informação em algumas áreas, como, por exemplo, nas instalações de um Centro de Comunicações ou nos órgãos de um Posto de Comando. As vantagens obtidas, tais como velocidade de transmissão de ordens e facilidade de uso, determinaram o apoio que os sistemas informatizados iriam prestar.

A tendência do uso de meios de tecnologia da informação no sistema de comunicações das brigadas é a de aumentar cada vez mais. E aumentando-se os meios, aumenta-se o tráfego de dados ou informações, dados estes que apoiam e facilitam a tomada de decisões. Portanto, são informações que necessitam de proteção, tornando-se imperioso que este fluxo também seja protegido, de modo que não venha a ser invadido, interrompido ou sabotado.

Os antecedentes apresentados conduzem à formulação do problema da pesquisa que originou o presente Artigo: em que medida a aplicação de procedimentos de defesa cibernética reduz a vulnerabilidade dos meios de tecnologia da informação empregados no sistema de comunicações da Brigada?

A imposição em se utilizar recursos tecnológicos na área operacional não é uma mera questão de modismo. Trata-se de necessidade, pois em um conflito moderno é impossível agir ou combater com eficácia sem o uso desses recursos. Portanto, tudo que for capaz de multiplicar o poder de combate deve ser utilizado.

Não se admite mais a não utilização das inovações digitais, estando a Força que a relegar fadada ao insucesso.

O Exército Brasileiro vem dando passos importantes no sentido de utilização de tecnologia moderna, bem como da proteção da mesma. A principal medida é a adoção e implantação de políticas de segurança da informação, expedidas pelo comando da Força. A preocupação é atribuída a todos os escalões, pois um ataque cibernético pode acontecer em qualquer local e, sendo bem sucedido, abrem-se as portas para acesso a níveis superiores. Porém, a maioria das normas existentes atualmente aborda áreas administrativas e estratégicas. O objeto do presente estudo é primordialmente tático: a proteção da informação no escalão brigada.

O estudo proposto pretende, analisando uma grande quantidade de técnicas empregadas, apresentar aquelas que melhor se adequam e que possam trazer benefícios ou vantagens reais aos operadores e fiscalizadores do sistema de comunicações.

2. DESENVOLVIMENTO

A localização e obtenção de documentos que sirvam de subsídio para o presente estudo foi realizada de modo a selecionar aqueles que estejam relacionados com a temática inicial. A revisão buscou, primeiramente, bases teóricas acerca da importância do sistema de comunicações de uma brigada; posteriormente, passou-se para a pesquisa de fontes mais técnicas, relacionadas com a defesa de dados em dispositivos de tecnologia da informação. O objetivo foi mesclar o conhecimento existente na parte militar, sobre os sistemas de informação que empregam TI em uma brigada, com o conhecimento de guerra cibernética, no que tange aos seus fundamentos, conceitos e técnicas de uso, para que se possa ter um panorama do que pode ser nocivo para o sistema de informações considerado e as formas mais eficientes de protegê-lo, já que a defesa cibernética é o cerne do tema.

“A informática pode atuar perfeitamente integrada com a área de comunicações, fornecendo meios para que as mensagens possam rapidamente chegar ao seu destino, pela automatização de tarefas e pela utilização de recursos de transmissão de dados” (BRASIL, 1997, p. 5-9)[4]. Mas o fato é que nas operações e exercícios atuais, devido à modernização dos sistemas, a palavra “pode” poderia sem problema algum ser substituída por “deve”. Isso porque a quantidade de

informações, o tráfego intenso e as mais variadas formas de combate atuais exigem sistemas que operem dessa maneira. Porém, os manuais doutrinários ainda não padronizam quais meios fazem uso de dispositivos de tecnologia da informação.

Para realizar um aprofundamento no sistema de comunicações de uma brigada deve-se vislumbrar, antecipadamente, que o mesmo faz parte do Sistema Tático de Comunicações (SISTAC). O SISTAC de uma brigada é composto pelos sistemas de enlace microondas em visada direta (multicanal), rádio (nas faixa HF e VHF), físico e por mensageiro, podendo ser complementado por outros meios de comunicações.

O presente trabalho foca nos dois sistemas do SISTAC de uma brigada que possuem grande utilização no emprego em campanha, os quais também têm passado por inúmeras modificações em sua estrutura, haja vista a adoção dos meios de tecnologia da informação em suas redes: o sistema de enlace rádio e físico.

Atenção especial é dada ao aspecto segurança. Tanto o Manual C 11 – 30 (BRASIL, 1998) quanto o Manual C 11 – 1 (BRASIL, 1997) citam o meio rádio como uma fonte de informações de grande valor para o inimigo, no que diz respeito à localização de postos e unidades, análise de tráfego e conhecimento do conteúdo das mensagens, sejam em claro, sejam criptografadas. Portanto, doutrinariamente, as informações que circulam dentro das redes-rádio são alvo de atenção especial, devendo ser protegidas. O sistema físico também é muito utilizado devido ao seu alto grau de segurança, diminuindo as probabilidades de interceptação e interferência por parte do inimigo.

As definições do termo guerra cibernética e suas ramificações não são unânimes, mas a grande maioria transmite a mesma ideia. Max Gehringer e Jack London (GEHRINGER e LONDON, 2004)[5] explicam o termo cibernética como sendo "uma ciência com inúmeras ramificações, sendo uma delas a computação. Em computação, a cibernética trata da comunicação entre sistemas e de seus mecanismos reguladores". A palavra, inventada em 1948 pelo matemático Norbert Wiener, no livro Cybernetics (WIENER, 1948)[6], vem do grego *kubernetes*, título do marinheiro responsável por manobrar o timão do navio. O Glossário das Forças Armadas, MD 35-G-01, em sua 4ª Edição, no ano de 2007[7], define guerra cibernética como sendo "o conjunto de ações para uso ofensivo e defensivo de informações para negar, explorar, corromper ou destruir valores do adversário

baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil".

As mais novas ações de ataques virtuais, experimentadas em todo o mundo, já conferem um panorama das formas de ataque mais comuns, e mais eficazes, em uso atualmente. Uma das famosas formas de ataque virtual, e presente desde os primórdios da informática, é o código malicioso, ou na linguagem da informática, *malware*. Inicialmente os *malwares* eram quase em sua totalidade limitados a uma espécie somente, conhecida como vírus. Atualmente existem inúmeros tipos de códigos maliciosos: cavalos de tróia, *spywares*, *backdoors*, *keyloggers*, *worms*, *bots* e *rootkits* são os mais comuns. Em suma, todos eles são programas especificamente desenvolvidos para causar algum tipo de dano ao computador ou rede na qual está sendo inserido. Este dano pode ser físico ou lógico.

Outra forma de ataque muito presente na atualidade é a negação de serviço (geralmente conhecido como *DoS – Denial of Service*, na sigla em inglês). Não é difícil encontrar casos quase que diários desta modalidade de ataque em uma simples busca pela *internet*. O ataque consiste no uso de um computador para tirar de operação um serviço ou um computador que possui uma conexão com a *internet*. Existem várias maneiras de se realizar uma negação de serviço, tais como gerar uma sobrecarga no processamento dos dados de um computador, de modo que o usuário não consiga utilizá-lo; ou aumentar o tráfego de dados de uma rede, tornando-a indisponível. A negação de serviço tem a sua potência aumentada quando são utilizados vários computadores para se fazer um ataque, caracterizando o ataque de negação de serviço distribuído (*DDoS – Distributed Denial of Service*, na sigla em inglês).

O termo *phishing* descreve um dos mais famosos e comuns tipos de ataque virtual. A palavra faz alusão à pescaria (*fishing*, em inglês), simbolizando o que é a fraude: iscas são usadas para pescar dados sigilosos de máquinas através da ação do próprio usuário. Sumariamente, o *phishing* é caracterizado pelo envio de mensagens não autorizadas, normalmente por correio eletrônico, passando-se por comunicação de uma instituição conhecida (como um banco, empresa ou loja popular), e que busca induzir o acesso às páginas fraudulentas ou falsificadas na *internet*, projetadas para o furto de dados.

Outro ataque virtual extremamente danoso é a injeção de SQL (*SQL injection*, na sigla em inglês). Mais complexo de ser executado, permite ao atacante ler ou alterar dados que não poderiam sofrer esse tipo de ação. SQL é a linguagem utilizada por bancos de dados para realizar consultas e alterar parâmetros, portanto uma instrução de SQL manipulada pelo invasor e injetada em uma máquina pode dar acesso completo ao sistema.

Sniffer é um tipo de software que tem por objetivo fazer a análise de uma rede de computadores, monitorando e registrando o seu tráfego. O seu uso pode ser para a proteção e correção de problemas ou para a abertura de brechas e invasão da máquina. No caso de uma ação maliciosa, o invasor utiliza a técnica chamada de *sniffing*, através de um programa *sniffer*, para coletar pacotes no fluxo da rede, podendo filtrá-los posteriormente e extrair informações sensíveis dos mesmos. Obter senhas, confeccionar cópias de arquivos e monitorar conversações em tempo real são algumas das ações capazes de serem executadas em uma máquina que foi comprometida com um *sniffer*.

A ação de engenharia social consiste em fazer uso da persuasão, frequentemente abusando da confiança ou ingenuidade do usuário que é o alvo, de modo a se obter informações que possam ser utilizadas para conceder acesso não autorizado a computadores. Os típicos ataques são dotados de discursos que buscam induzir o usuário a realizar alguma tarefa, sendo que o ataque somente será bem sucedido se o alvo executar programas ou fornecer informações sensíveis; portanto, o ponto de inflexão da engenharia social está na decisão do usuário em realizar tais atos.

A gama de modalidades de ataque virtua é extremamente numerosa e volátil. Do mesmo modo, as técnicas de defesa crescem na mesma medida em que as suas ameaças também o fazem. Existem atualmente diversos métodos de proteção, que agem em diferentes fontes (humana ou eletrônica, por exemplo), para garantir a segurança desejada.

Uma das primeiras soluções criada para o combate aos ataques virtuais mais antigos, que eram em sua grande maioria os vírus de computador, pois a *internet* ainda não estava tão disseminada como hoje, foi um programa que permitiu a detecção e eliminação de programas indesejados. A esses *softwares* foi dado o nome de antivírus. Outro método de proteção bastante conhecido e eficiente é o *firewall*, que pode ser um programa ou uma combinação de programa com máquina,

utilizado para dividir e controlar o acesso a redes ou máquinas, funcionando basicamente como um filtro.

A criptografia é a ciência de escrever ocultamente; é uma das mais confiáveis técnicas para se proteger um dado e uma das mais seguras técnicas para se enviar informações através de um canal não seguro. São utilizados conjuntos de métodos que protegem o dado, consistindo na aplicação de chaves com algoritmos somente dominados pelos intervenientes previamente definidos. Como já vem sendo fortemente utilizada em aplicações que envolvem valores, notadamente nos sistemas desenvolvidos por instituições financeiras e bancárias, a certificação digital ou assinatura digital objetiva garantir a autenticidade da pessoa que acessa determinado sistema. Ela utiliza as técnicas de criptografia descritas acima para realizar todo o seu processo, sendo mais uma das medidas de defesa possíveis de serem aplicadas para a proteção de dados.

O *hardening* é uma técnica de blindagem do sistema contra ataques virtuais, preparando o mesmo para combater as tentativas de invasão. Esse fortalecimento consiste na realização de reforço nas medidas de segurança. As medidas de proteção implementadas são relativamente simples de serem aplicadas, sendo as mais comuns o gerenciamento criterioso de contas de usuários, controle de serviços do sistema, registros de entradas no sistema, controle de autenticação, rigorosa política de senhas, checagem da integridade de arquivos essenciais ao sistema e atualizações constantes de programas do sistema.

Rodrigo Faustini aborda, em seu artigo, uma das técnicas de defesa mais importantes do mundo virtual: a política de segurança de informação, um mecanismo de prevenção dos dados e dos sistemas de uma organização, que consiste em “procedimentos de como os meios de tecnologia da informação devem ser protegidos e utilizados, normatizando todas as condutas a serem seguidas pelo pessoal técnico, comando e usuários, sejam eles internos ou externos” (FAUSTINI, 2011)[8].

Diversos são os propósitos de uma política de segurança da informação. Primeiramente, identificar com precisão o que será protegido e o porquê. Em sequência, devem ser estabelecidas prioridades e deve-se analisar o custo necessário. Um grande benefício de uma política de segurança é amparar e justificar as limitações que cada funcionário ou integrante da empresa irá encontrar.

Foi realizado o levantamento e conceituação das variáveis a serem

empregadas no estudo, inserido no contexto do objeto formal da pesquisa. A variável dependente é caracterizada pela "**vulnerabilidade dos meios de tecnologia da informação do SISTAC da brigada**", tendo em vista que a sua análise é primordial e irá definir o que deve ser empregado para combatê-la, caracterizando, por sua vez, a variável independente, qual seja "**procedimentos de defesa cibernética**" aplicados. As variáveis de estudo apresentam características qualitativas, portanto são bem definidas e dimensionadas, para que possam ser medidas e observadas corretamente.

As dimensões das vulnerabilidades dos meios de tecnologia da informação do sistema de comunicações da brigada (portanto, a variável dependente) definidas para o presente estudo foram analisadas sob fatores preponderantes dentro do sistema. A realização de um mapeamento abordando esses fatores mede o grau de comprometimento que a vulnerabilidade pode trazer no emprego da brigada.

O dimensionamento das medidas de defesa cibernética (portanto, a variável independente) interage com o mapeamento acima, pois as mesmas foram selecionadas de acordo com a sua capacidade de combater determinada ameaça virtual. As suas dimensões apresentam os requisitos básicos considerados para se implementar determinada ação de defesa cibernética.

Para a realização da pesquisa apresentada, a amostra foi composta por todas as 9 (nove) companhias de comunicações (Cia Com) de brigada, por serem essas as organizações militares responsáveis pelo apoio de comunicações à Grande Unidade; excetuam-se as duas companhias de comunicações de selva e a companhia de comunicações leve, pelas mesmas operarem com características especiais não pertinentes para o estudo proposto. Foi enviado para cada Companhia de Comunicações um questionário misto, com as instruções detalhadas, para ser preenchido pelo Chefe da Seção de Operações. O mesmo questionário foi oferecido, simultaneamente, para preenchimento em página na *internet*.

A análise dos dados coletados permitiu propor as formas de ataque virtual que podem ser utilizadas contra determinado tipo de equipamento ou meio de tecnologia da informação, relacionando ainda o seu potencial de dano. A elaboração destas propostas seguiu critérios verificados durante a revisão da literatura, particularmente em duas áreas: as formas e tipos de ameaças cibernéticas e as medidas de defesa cibernética.

Após mensurar o potencial danoso a um meio de tecnologia da informação de

uma rede de dados, recomendou-se a adoção de medidas de defesa cibernética para minimizar ou neutralizar aquela ameaça, fruto também dos estudos de fontes constantes da revisão da literatura. A resultante da comparação acima foram exatamente as medidas de defesa cibernética necessárias para a proteção do sistema em tela; restou saber quais das medidas são passíveis de emprego prático. Para obter tais respostas o trabalho previu a análise de cada procedimento de proteção sugerido sobre um meio de TI conforme critérios fundamentais para a sua implantação efetiva em um sistema de comunicações de brigada.

As respostas ao questionário mostraram que o sistema rádio, o sistema físico e o sistema mensageiro correspondem aos enlaces mais utilizados pelas companhias de comunicações quando em apoio a uma operação da sua Brigada, o que corrobora com o abordado na revisão da literatura. Ainda, metade das OM utiliza meios dotados de tecnologia da informação no sistema físico e todas utilizam meios de TI no sistema rádio.

Foi verificado que a maioria das companhias de comunicações hospedam os seus meios de TI em infraestruturas mistas (nacionais combinadas com internacionais), o que aumenta a vulnerabilidade do sistema. A arquitetura tecnológica mista (parte de domínio de um proprietário e parte aberta) também figura como a maioria existente nas OM, com 63% das plataformas. Isso mostra a dependência que existe, ainda, de tecnologia de fornecedores externos, o que é temeroso do ponto de vista da segurança, já que o seu desenvolvimento não é do inteiro conhecimento de quem o utiliza.

O tempo de uso dos meios de TI em operações também é um fator explorado que contribui para a análise da dimensão segurança. 62% das OM utilizam esses meios há mais de 5 (cinco) e menos de 10 (anos) em seus sistemas de enlace, sendo que outros 38% as utilizam há mais de 2 (dois) e menos de 5 (cinco) anos, o que demonstra um aspecto positivo para o estudo, já que a experiência no trato com os equipamentos certamente gera lições aprendidas. As tentativas e acertos no uso dos meios tecnológicos produzem conhecimento para a OM.

Os resultados apresentados mostraram, dentre outras características, a necessidade de aprimoramento da política de segurança da informação. O suporte técnico também é utilizado, porém a terceirização é perigosa, já que exige maior cuidado com as pessoas que estão lidando com o problema. Utilizar o próprio pessoal é conveniente, mas também não se exime da responsabilidade de controlar

os acessos, em especial através da política de segurança da informação (FAUSTINI, 2011)[8].

Todas as OM atribuem a capacitação de pessoal como o principal problema na gerência dos meios de TI do sistema de comunicações. O resultado ratifica a ideia de se implementar a política de segurança da informação e dificulta a tomada de outras medidas que demandem maior conhecimento. Surge ainda a questão do impasse operacionalidade versus segurança. Nesse caso, a decisão cabe ao comandante da brigada, o qual deverá analisar a situação imposta, e decidir por uma linha de ação que priorize um ou outro aspecto.

Foi caracterizado pelo questionário a intenção de se trabalhar sem prever, na maioria dos casos, o ataque virtual planejado, o que pode ser perigoso quando o assunto é defesa cibernética. Mais uma ratificação de que a política de segurança da informação, aliada às medidas de defesa físicas, conforme descrito por Schneier (2007)[9], é de suma importância.

Metade do universo da amostra respondeu que o principal entrave para a implementação de um plano de contingência e recuperação dos meios de tecnologia da informação é orçamentário; a outra metade respondeu que o problema reside na capacitação e treinamento de pessoal. Desse resultado ratifica-se dois pontos analisados: a necessidade de utilização de medidas de defesa que dispensem altos custos e, ao mesmo tempo, não exijam grandes conhecimentos técnicos.

3. CONCLUSÃO

O cenário atual de evolução tecnológica crescente afetou a sociedade de maneira geral, inclusive o seu braço armado. As instituições militares aderiram aos sistemas informatizados para que não perdessem, precipuamente, o poder de combate.

Dentro do elemento básico de combate do Exército Brasileiro, qual seja o escalão brigada, a tecnologia também modificou o modo de trabalho. O uso dos meios de tecnologia da informação no sistema de comunicações de uma brigada é uma realidade em todas as companhias de comunicações. Dessa maneira, as informações que transitam por esses meios são uma fonte sensível e um alvo altamente compensador para um provável inimigo.

Um dos objetivos específicos alcançados pelo estudo foi a identificação de

conceitos, padrões e formas de ataques cibernéticos atuais. O entendimento dos termos acima permitiu o apontamento de formas de ameaça que podem ser prejudiciais para o sistema de comunicações.

A identificação das vulnerabilidades nos meios de TI do SISTAC da brigada foi alcançada através das respostas obtidas pelo questionário aplicado. Pode-se fazer uma ligação das respostas, ainda, com a apresentação das principais deficiências na defesa do sistema de comunicações da brigada, restringindo-se às áreas que empreguem meios de tecnologia da informação.

Evidenciou-se o grande uso de meios de TI no sistema de comunicações pelas companhias de comunicações, o que remete à aplicação de medidas de defesa cibernética para protegê-los. O questionário obteve os aspectos relacionados a seguir como principais vulnerabilidades:

a. uso de infraestruturas mistas (nacionais e internacionais);

b. utilização de tecnologia terceirizada;

c. grande falta de suprimentos e de equipamentos com tecnologia de ponta, devido à restrição orçamentária;

d. usuário interno é o responsável, sem intenção, pela maioria dos ataques virtuais (através de falhas de segurança em medidas adotadas pelo mesmo, abrindo portas de entrada para o sistema); e

e. falta de pessoal capacitado para lidar com os meios de TI.

Apresentou-se, portanto, medidas de defesa cibernética aplicáveis ao sistema, chegando-se a uma solução para o problema apresentado. Com os dados obtidos, foi possível relacionar as deficiências em segurança encontradas nos meios de TI com as medidas de defesa que atendam os parâmetros impostos pelas instaladoras e mantenedoras do sistema (as companhias de comunicações). Esse resultado encontra-se materializado na tabela a seguir.

Tabela 1 – Forma de ataque x medidas de defesa

Forma de ataque	**Medidas de defesa apropriadas**
Código malicioso (cavalo de tróia, *spyware, backdoor, keylogger, worm, bot* e *rootkit*)	- Antivírus - *Firewall* - Criptografia - *Hardening*
Negação de serviço ou negação de serviço distribuído (DoS ou DDoS)	- *Firewall* - *Hardening*
Phishing	- Política de segurança da informação - Assinatura digital - *Hardening*
Injeção de SQL	- *Firewall* - *Hardening*
Sniffing	- Antivírus - *Firewall* - Criptografia - *Hardening*
Engenharia social	- Política de segurança da informação - Assinatura digital - Segurança física

Fonte: o autor

As conclusões da pesquisa permitiram indicações específicas de ordem prática, de maneira a modificar ou implementar algo na conduta das OM, gerando as recomendações sobre o assunto.

A equipe de resposta para incidentes de redes de computadores está ausente em 37% das OM que responderam ao questionário. Apesar de compor uma vertente corretiva, ou seja, é uma medida para ser utilizada após um ataque bem sucedido, é também importante no isolamento de dados sensíveis e na própria recuperação do sistema. Por ter obtido um índice elevado de não existência, sugere-se a adoção de uma equipe de resposta para incidentes com, no mínimo, a exclusividade de atribuições voltada para a área de TI.

Considerado o maior entrave a ser superado na gestão dos meios de tecnologia da informação, a capacitação de pessoal é outro ramo que se recomenda investimento. Existem atualmente inúmeros estágios e cursos gratuitos fornecidos pelo Exército Brasileiro na área de informática, alguns permitindo até o seu desenvolvimento de maneira não presencial, o que pode capacitar pessoal para

atuar no campo tecnológico em questão.

A importância da capacitação avulta-se na medida em que se resolve o problema da falta de pessoal especializado para compor uma equipe de resposta para incidentes, ao mesmo tempo em que se investe em material humano. O conhecimento adquirido pode ser multiplicado através da difusão da informação em instruções para o efetivo permanente das companhias de comunicações.

A realidade da instituição Exército Brasileiro, apresentada nos resultados colhidos através do questionário, mostrou a dificuldade em se obter equipamentos modernos e seguros, principalmente pela falta de orçamento destinado aos meios de TI. A recomendação para esta situação é a de utilizar intensamente a política de segurança da informação, pois trata-se de uma medida de defesa de baixo custo que foca exatamente no recurso humano, um dos maiores responsáveis pela eficácia dos ataques virtuais. A normatização e fiscalização da conduta do pessoal que lida com os meios de TI, tanto interno quanto externo, regulada formalmente por um documento válido, além de não exigir grandes gastos, traz um ganho substancial em segurança para o sistema de comunicações.

REFERÊNCIAS

1. CANONGIA, CLAUDIA; JUNIOR, RAPHAEL MANDARINO. **Segurança Cibernética: o desafio da nova Sociedade da Informação.** Brasília: Centro de Gestão e Estudos Estratégicos: Ministério da Ciência e Tecnologia, 2009.

2. BRASIL. **Decreto n. 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa e dá outras providências.** Disponível em: <http://www.fab.eb.mil.br/portal/defesa/estrategia_defesa_nacional_portugues.pdf>. Acesso em 12 de julho de 2011.

3. BRASIL. Estado-Maior do Exército. **C 11-30**: As Comunicações na brigada. 2. ed. Rio de Janeiro: EGGCF, 1998.

4. BRASIL. Estado-Maior do Exército. **C 11-1**: Emprego das Comunicações. 2. ed. Rio de Janeiro: EGGCF, 1997.

5. GEHRINGER, MAX; LONDON, JACK. **Odisséia Digital 2.** Disponível em <http://www.lostdesign.net/glossario/informatica.htm>. Acesso em 2 de agosto de 2011.

6. WIENER, NORBERT. **Cybernetics: control and communication in the animal and the machine.** Cambrigde: MIT Press, 1948.

7. BRASIL. **Portaria normativa n. 196/EMD/MD, de 22 de fevereiro de 2007. Aprova o "Glossário das Forças Armadas".** 4. ed. Brasília: EMD/MD, 2007b.

8. FAUSTINI, RODRIGO. **Normas: Política de Segurança da Informação.** Disponível em <http://www.faustiniconsulting.com/artigo05.htm>. Acesso em 5 de setembro de 2011.

9. SCHNEIER, BRUCE. **Cyberwar.** Disponível em: <http://www.schneier.com/blog>. Acesso em 6 de julho de 2011.