

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



INTELIGÊNCIA

FCA 200-1

PREVENÇÃO DE ESCUTA CLANDESTINA

2008

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA**



INTELIGÊNCIA

FCA 200-1

PREVENÇÃO DE ESCUTA CLANDESTINA

2008



**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**

PORTARIA Nº 2/CIAER, DE 19 DE DEZEMBRO DE 2008.

Aprova o Folheto que dispõe sobre a
Prevenção de Escuta Clandestina.

O CHEFE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA,
tendo em vista o disposto no Inciso II, do art. 4º do Regulamento do Centro de Inteligência da
Aeronáutica, aprovado pela Portaria nº C-7/GC3, de 27 de setembro de 2005, resolve:

Art. 1º Aprovar a edição do FCA 200-1 “Prevenção de Escuta Clandestina”,
que com esta baixa.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Brig Ar PAULO AFONSO PINHEIRO LARI
Chefe do CIAER

(Publicado no BCA nº 013, de 21 de janeiro de 2009.)

SUMÁRIO

PREFÁCIO	7
1 DISPOSIÇÕES PRELIMINARES	9
1.1 <u>FINALIDADE</u>	9
1.2 <u>ÂMBITO</u>	9
2 A INTERCEPTAÇÃO	11
2.1 <u>TELEFONE</u>	11
2.2 <u>RADIODIFUSÃO</u>	12
2.3 <u>TELEFONIA CELULAR</u>	12
2.4 <u>MICROFONES PARA AMBIENTE INTERNO</u>	12
2.5 <u>MICROFONES PARA AMBIENTE EXTERNO</u>	13
2.6 <u>GRAVADORES</u>	13
2.7 <u>REDE DE COMPUTADORES</u>	13
2.8 <u>REDE SEM-FIO</u>	13
3 MEDIDAS PREVENTIVAS	14
3.1 <u>GENERALIDADES</u>	14
3.2 <u>MEDIDAS DE OBSTRUÇÃO</u>	14
3.3 <u>MEDIDAS DE CONSCIENTIZAÇÃO</u>	15
3.4 <u>MEDIDAS DE DETECÇÃO</u>	15
4 DISPOSIÇÕES FINAIS	16

PREFÁCIO

Há muitas razões para que pessoas ou organizações tenham o desejo de monitorar os canais de comunicação.

A prática da escuta clandestina existe desde que o homem desenvolveu a capacidade de se comunicar por meio elétrico e eletrônico. Atualmente, com o avanço da eletrônica e da informática, ela pode ser realizada, não só por um ouvido indiscreto, como também pela utilização de dispositivos até mais sofisticados e engenhosos do que os apresentados pelos criadores dos filmes de agentes secretos.

No âmbito interno das organizações, a preocupação com a segurança das comunicações, na maioria das atividades, é muito elevada. Segurança é aqui referida como a proteção dos assuntos sigilosos contra as ações violadoras e de sabotagem.

Por outro lado, arquivos, bancos de dados, processos e documentos encontram-se sujeitos a riscos não menos graves ou importantes.

As pessoas talvez se esquecem de que temas que tratam do interesse da administração e da aplicação do poder militar devem ser preservados da indiscrição de terceiros. É difícil calcular quantas Organizações Militares (OM), indústrias e indivíduos são vítimas de vigilância ilegal.

A evidência de vigilância ilegal é freqüentemente suprimida para evitar publicidade ou, em alguns casos, alertar o espião. Espionagem e vigilância podem afetar muitos aspectos da segurança e o sucesso das operações.

São alvos de escuta clandestina, entre outras, as atividades relativas ao campo da ciência e tecnologia, ao planejamento militar, à definição de estratégias de emprego, à avaliação da capacidade de emprego e pronta-resposta e àquelas ligadas à informação financeira.

Os serviços de inteligência dos países desenvolvidos normalmente dispõem de um setor destinado à pesquisa e ao desenvolvimento de “softwares” e equipamentos especiais, miniaturizados ou não, destinados à escuta clandestina.

Por outro lado, pensa-se que os dispositivos típicos de vigilância são produtos disponíveis somente para espiões cobertos pelas entidades governamentais. Porém, como a tecnologia do mundo continua avançando, “softwares” e equipamentos de alta qualidade estão sendo disponibilizados no mercado comercial, até mesmo como produtos domésticos comuns.

Um monitor de bebê, constituído por um microfone e um transmissor sem-fio no quarto, ligado a um receptor instalado no quarto dos pais, é um exemplo de um sistema de vigilância completo, que pode ser comprado por menos de US\$ 50.00 (cinquenta dólares americanos), podendo ser colocado sob o forro do teto, debaixo de mesas de salas de reunião, atrás de escrivaninhas ou mesmo em uma pasta.

O interessado pode adquirir equipamento sofisticado facilmente, bastando somente determinar o valor da informação a ser obtida.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O presente Folheto tem por finalidade recomendar aos Comandantes, Chefes e Diretores procedimentos referentes à prevenção de escuta clandestina no âmbito do Comando da Aeronáutica (COMAER) para os riscos dela inerentes.

1.2 ÂMBITO

O presente Folheto aplica-se a todas as OM do COMAER.

2 A INTERCEPTAÇÃO

A interceptação é a maneira mais prática da realização da escuta clandestina. Serão abordadas, a seguir, algumas formas de como ela poderá ocorrer em equipamentos específicos.

2.1 TELEFONE

O telefone é o meio de telecomunicações mais utilizado e, por este motivo, é o alvo preferido dos interceptadores. Em torno deste meio de comunicação, desenvolveu-se uma variada gama de modos de escuta clandestina, a partir do local onde se encontra o aparelho ou do percurso por onde se veicula a voz (fiação ou cabos de rede, caixas de controle, central telefônica, "links" de microondas, transmissão satélite, etc.). Existem muitos processos e técnicas para a escuta telefônica, sendo apresentados a seguir os usualmente empregados por agentes adversos.

2.1.1 A PARTIR DOS FIOS

É o mais comum. O interceptador pode ter acesso à central telefônica, às caixas de junção, à distribuição geral ou, mesmo, à fiação. Após identificar o par de fios que lhe interessa, simplesmente transfere o sinal veiculado para fones de ouvido, gravador ou radiotransmissor, para monitoramento em outro local. Por vezes, este tipo de escuta é facilitado pela existência de:

- a) extensão telefônica, conhecida ou não do alvo;
- b) equipamento destinado a transferir chamadas, o qual transfere a ligação recebida para o telefone residencial ou para outro telefone pré-programado;
e
- c) linhas telefônicas fora de uso.

2.1.2 UTILIZAÇÃO DO TRANSMISSOR INFINITO

2.1.2.1 Consiste de um dispositivo instalado no telefone-alvo ou na sua linha, o qual permite a escuta dos sons do ambiente-alvo. Recebe este nome por transmitir por tempo e distância indeterminados. Para operar, o interceptador liga para o telefone-alvo e, antes que a campainha toque, aciona um gerador de harmônico no bocal.

2.1.2.2 Enquanto a escuta estiver ativada, a linha permanece ocupada, e os sons do ambiente alvo estarão sendo captados.

2.1.2.3 Uma variante desse processo dispensa o uso do gerador de harmônico. O telefone-alvo toca e, após ser atendido e recolocado no gancho (constatado o "engano"), a linha permanece aberta, transmitindo os sons do ambiente.

2.1.3 OUTROS DISPOSITIVOS PARA TELEFONES

2.1.3.1 Existem ainda outros sistemas de escuta, os quais requerem pequenas modificações no circuito eletrônico do telefone-alvo. Um desses sistemas desvia o interruptor liga/desliga do telefone (descanso), de modo a não afetar sua operação normal, permitindo que o aparelho funcione como um microfone remoto quando não estiver em uso. No caso, basta "grampear" a linha, para captar os sons emitidos no recinto.

2.1.3.2 Certamente, o telefone não é um meio seguro para veicular mensagens sigilosas. Até mesmo a utilização de equipamentos especiais para detectar "grampos" não o torna mais confiável, pois os dispositivos de escuta clandestina, quando de boa qualidade, provocam pouca modificação nas características da linha e, por essa razão, não são facilmente detectáveis.

2.1.3.3 No âmbito do Comando da Aeronáutica, portanto, o telefone não deve ser utilizado como meio de comunicações para o trato de assuntos sigilosos, a não ser que esteja protegido por um equipamento cifrador com o nível de segurança adequado.

2.2 RADIODIFUSÃO

2.2.1 A comunicação por meio da radiodifusão é ainda mais vulnerável do que a por telefone. Basta que o interceptador disponha de um receptor apropriado para tornar-se ouvinte não-convidado.

2.2.2 Este meio de comunicação só é seguro quando utilizando equipamentos destinados a cifrar a voz na radiodifusão ou, mesmo, a ocultá-la (por compressão, salto ou espalhamento na faixa de transmissão).

2.3 TELEFONIA CELULAR

2.3.1 O telefone celular, dentre os meios de comunicação, é o mais vulnerável, pois herda as vulnerabilidades da telefonia fixa e da radiodifusão.

2.4 MICROFONES PARA AMBIENTE INTERNO

2.4.1 O microfone é o meio mais utilizado para a escuta em recintos fechados, principalmente nos locais onde não haja telefone.

2.4.2 Um sistema de escuta por microfones é composto, basicamente, por um ou mais microfones adequadamente "plantados", fios e interruptores de acionamento, podendo, também, operar com radiotransmissores, transmissores infinitos, gravadores e outros dispositivos que convertam sons em sinais elétricos ou digitais.

2.4.3 Existem diversos tipos e tamanhos, que são selecionados em função do ambiente-alvo, dos recursos de energia e da distância a transmitir. Alguns necessitam de bateria para operar, outros utilizam a energia da rede elétrica ou aquela advinda de uma fonte de radiofrequência (como, por exemplo, uma parede por onde passa a ligação com uma antena de "High Frequency" - HF).

2.4.4 Alguns já se encontram no ambiente-alvo (alto-falantes desativados), outros são "plantados" em locais escondidos (atrás de um móvel, no forro, dentro de uma divisória, etc.) ou mesmo ocultos ou disfarçados em quadros, enfeites de mesa, brindes, etc.

2.4.5 O ambiente escolhido para a implantação desses dispositivos é, normalmente, aquele onde são tratados assuntos sigilosos. Assim, deve-se estar atento: o local de trabalho pode estar "preparado".

2.4.6 Nas janelas, principalmente nas envidraçadas, o vidro trepida com os sons do recinto; existem dispositivos óticos apropriados para captar e tornar inteligíveis essas vibrações.

2.5 MICROFONES PARA AMBIENTE EXTERNO

2.5.1 O trato de assuntos sigilosos fora do ambiente de trabalho oferece maior segurança, por sair do local mais visado pelo interceptador. Por outro lado, existe, além dos riscos habituais dos ouvidos indiscretos dos "bem-informados" (ascensoristas, motoristas, garçons, etc.), a possibilidade de escuta à distância, com a utilização de microfones direcionais.

2.5.2 É importante salientar que ambientes barulhentos não impedem esse tipo de escuta. Existem filtros que separam a voz humana de outros tipos de sons.

2.6 GRAVADORES

2.6.1 Os gravadores de fita magnética ou digitais são exemplos de ferramentas de escuta clandestina. Geralmente são utilizados em pastas do tipo executivo ou bolsas ou, ainda, "plantados" no ambiente-alvo, sendo, neste caso, miniaturizados.

2.6.2 O sistema escolhido pode incluir interruptores ativados pela voz, microfones na fechadura da pasta, interruptores de pressão ocultos na alça da pasta, radiorreceptores e transmissores para ligação à distância.

2.7 REDES DE COMPUTADORES

2.7.1 Outro ponto a considerar é o relacionado às redes locais e remotas. Estas não são meios seguros para a transmissão de mensagens sigilosas sem a devida proteção de sigilo.

2.7.2 O acesso de assuntos sensíveis através de rede de computadores sem a criptografia pode não apenas causar prejuízos à administração, mas também pôr em risco a segurança da organização, do emprego operacional e da própria integridade pessoal do efetivo da OM e seus dependentes.

2.7.3 Hoje em dia, tornou-se muito fácil a interceptação das comunicações processadas por redes locais, comprovados pelos inúmeros casos divulgados pela imprensa.

2.8 REDE SEM-FIO ("Wireless", "wifi" ou "blue tooth")

2.8.1 Ferramentas para exploração de redes sem fio são encontradas gratuitamente na Internet e em revistas especializadas. Os riscos já existentes da rede com fio são agravados na rede sem fio, uma vez que a facilidade de instalação e o baixo custo dos equipamentos permitem que usuários com pouco conhecimento instalem e conectem uma rede sem fio à rede local da OM, sem o conhecimento e a autorização do administrador da rede local.

2.8.2 Os equipamentos baseados em redes sem fio emitem o tráfego de rede em um ambiente público sem controle, permitindo a interceptação dos dados, de forma a comprometer as informações que trafegam na rede. O risco criado não expõe somente a rede sem fio, mas também toda a rede que nela estiver conectada, vulnerabilizando o controle de acesso e a autenticação, reforçada pela utilização não recomendável de configurações de fábrica nos pontos de acessos, ou o gerenciamento remoto dos ativos de rede, bem como o uso de criptografia fraca ("Wired Equivalency Privacy – WEP").

2.8.3 É importante que, antes de instalar uma rede sem fio, os usuários e administradores da rede local da OM entendam os riscos da utilização destas novas tecnologias e possam estar aptos a implementar todas as medidas de segurança necessárias para poderem utilizá-la.

3 MEDIDAS PREVENTIVAS

3.1 GENERALIDADES

3.1.1 A imprensa é pródiga em divulgar casos de espionagem em que foram utilizados meios de escuta clandestina. Entretanto, muitos permanecem desconhecidos por não terem sido descobertos ou porque depõem contra a imagem da instituição.

3.1.2 A ameaça é real e não existem meios de transmitir conhecimentos de maneira absolutamente segura. Contudo, com a adoção das medidas preventivas e cuidados preconizados nesta publicação, pretende-se minimizar a possibilidade de escuta clandestina de modo a ficar bastante reduzida.

3.1.3 Conforme a doutrina de Contra-Inteligência, o acesso a assuntos sigilosos deve restringir-se às pessoas credenciadas, no grau de sigilo adequado, e que tenham a "necessidade de conhecer". Não basta tratar de assuntos com as pessoas certas, é necessário, ainda, precaver-se contra a escuta clandestina, adotando-se medidas de obstrução, conscientização e detecção.

3.2 MEDIDAS DE OBSTRUÇÃO

São procedimentos destinados a impedir, tornar ineficazes ou minimizar a implantação de dispositivos eletrônicos de escuta clandestina, dentre outros:

- a) prover o isolamento acústico das salas de conferências e outros locais utilizados para o trato de assuntos sigilosos, inclusive dos seus dutos de ar condicionado;
- b) inspecionar os espaços vazios que existem nas paredes e rodapés, principalmente quando utilizados materiais pré-moldados, que facilitam a instalação de dispositivos eletrônicos;
- c) remover telefones fixos e celulares, bem como sistemas de intercomunicação dos locais julgados sensíveis. Caso não seja possível, equipar esses aparelhos com “plugs” desconectores que sejam acionados quando assuntos sigilosos forem tratados nas proximidades;
- d) remover todos os fios desnecessários às instalações elétricas de dados e de telefonia, pois os mesmos podem ser utilizados para auxiliar e camuflar a colocação de escuta clandestina;
- e) construir salas isoladas, bloqueadas para a emissão de radiofrequência, inclusive de celulares e redes sem-fio, realizando as conferências no centro dessas salas; se possível, utilizar um gerador de sinais de frequência variável, com o som saindo em alto-falantes instalados nas paredes (ou música cantada por mais de uma voz). Com isso, poderão ser mascaradas as vozes das pessoas e cancelados os efeitos de possíveis microfones instalados nas paredes, pois eles serão mais sensíveis aos sons mais próximos. Além disso, a frequência, sendo variável, torna inócuo o uso de filtros destinados a "limpar" uma possível gravação;
- f) assegurar-se sempre do credenciamento de todos os participantes da reunião. Se possível, utilizar um detector de metais e circuitos eletrônicos instalados na entrada, visando a detecção de transmissores, gravadores e outros dispositivos eletrônicos ocultos;

- g) verificar quadros de distribuição telefônicos (DG) e conferir a fiação e os enlaces de fios de extensão, atentando para a eventual presença de objetos estranhos; conferir o trancamento a cadeado; e evitar identificação facilitada dos cabos e pares telefônicos, adotando alguma codificação; e
- h) acompanhar, com técnico da organização que conheça os métodos de escuta clandestina, qualquer trabalho executado na área sensível por elementos estranhos à organização (faxineiros, instaladores, etc.)

3.3 MEDIDAS DE CONSCIENTIZAÇÃO

3.3.1 Visam a alertar as pessoas quanto aos riscos da escuta clandestina e de como evitá-la. Devem, ainda, destacar a necessidade de permanecer alerta com as condições anormais, tais como a instalação ou reparo de telefones ou o aparecimento de objetos estranhos no ambiente.

3.3.2 As pessoas também devem ser orientadas a respeito da verificação das credenciais de todos os que ingressem na organização e alertadas no sentido de que assuntos de serviço, classificados ou sensíveis, devam ser discutidos apenas nas áreas destinadas a esse fim, enfatizando-se o perigo de falar sobre assuntos sigilosos em locais públicos, até mesmo em seu carro ou residência.

3.4 MEDIDAS DE DETECÇÃO

3.4.1 Envolve uma completa e detalhada inspeção física e eletrônica (varredura) da área a ser protegida, realizada por pessoal treinado e adequadamente equipado.

3.4.2 Além disso, é prudente monitorar as áreas sensíveis quando tratando de assuntos sigilosos, para detectar emissão de radiofrequência, pois sempre existe o perigo de um transmissor oculto no local.

4 DISPOSIÇÕES FINAIS

4.1 O Centro de Inteligência da Aeronáutica (CIAER), Órgão Central do Sistema de Inteligência da Aeronáutica (SINTAER) e/ou os Elos de Inteligência das Organizações Militares atuarão, quando solicitados, no processo de assessoria aos respectivos Comandantes, Chefes ou Diretores, objetivando implementar, por meio de procedimentos específicos, o sigilo das comunicações ou, ainda, a adoção de meios mais seguros, dotados de proteção criptotécnica.

4.2 Este Folheto substitui o FMA 205-3 “Escuta Clandestina”, aprovado pela Portaria nº 966/GC3, de 14 de setembro de 2004.