

## **A ESPIONAGEM**

Vamos dar apenas alguns aspectos básicos sobre esse assunto, uma vez que dificilmente o Detetive terá envolvimento com casos dessa natureza.

As origens de espionagem são remotas, utilizada especialmente em época de guerra, constitui, em todos os tempos, forma de obter vantagem sobre o inimigo. Os hebreus, de há muito tempo, já a utilizavam.

Encontramos nas Sagradas Escrituras, no livro de Josué, no Capítulo 2, o próprio Josué, organizando um serviço secreto de espionagem contra a Cidade de Jericó, onde mandou dois agentes secretos para aquela cidade fazerem levantamento das defesas militares do local.

Encontramos também na Ilíada de Homero, a história de Tróia, quando os gregos, não conseguindo penetrar naquela cidade, ali deixaram um “presente” **O CAVALO DE TRÓIA**, que nada mais era do que um serviço secreto de espionagem, camuflado naquela obra fantástica de espionagem, na barriga do cavalo, que pela sua aparência artística, seduziu os troianos a recolhê-lo como troféu de guerra, levando-os a capturarem de maneira ridícula, pela inteligência dos serviços secretos dos gregos.

A realidade é que, a história dos serviços secretos que utilizam a espionagem, se perde na noite dos tempos. Pode ser inspirada por idealismo ou por interesses venais e mercenários.

## **ESPIONAGEM INTERNACIONAL**

Constitui crime contra a segurança de Estado, punida sempre com o maior rigor pelos países atingidos, em tempo de paz ou de guerra, não obstante ser considerada lícita durante as guerras, de acordo com o Direito Internacional – Regulamento de Haia, data de

18 de outubro de 1907, o que não livra os espiões ou agentes secretos, quando apanhados, de julgamento e punição perante os tribunais dos respectivos países e mesmo até à pena de morte.

Os serviços diplomáticos, se de um lado veio estreitar as relações internacionais, de outro serve, freqüentemente, para acobertar espionagem, feitas por agentes especializados, que recebem longo e cuidadoso preparo, a fim de estarem em condições de agirem com inteligência, arrojo, discrição e astúcia. Com o intuito de contrabalançar esses problemas, quase todos os países do mundo mantêm agentes secretos de contra-espionagem e só permitem acesso a certos locais ou serviços considerados de importância estratégica para a defesa nacional, mediante rígido controle.

## ESPIONAGEM E CONTRA-ESPIONAGEM TÉCNICA



Diferentemente da Espionagem Clássica, que utiliza seres humanos para conseguir informações, a **ESPIONAGEM TÉCNICA** emprega dispositivos especiais que; quando profissionalmente instalados e manipulados tornam-se poderosos aliados na obtenção de informações. Infelizmente para o espião e felizmente para o Agente de Contra-Espionagem, a grande maioria destes dispositivos, mesmos os importados de países tecnologicamente desenvolvidos, são produtos de **BAIXA QUALIDADE**, tanto no que diz respeito ao seu projeto puramente técnico, até sua montagem propriamente dita, apesar de estarem envoltos em complexas siglas, que para o operador iniciante subentende-se como "**ESCUTAS PROFISSIONAIS**".

Esta matéria foi desenvolvida para auxiliar você, futuro Detetive, decidido a desenvolver seu **CONHECIMENTO BÁSICO** neste setor. Existe algo que, praticamente quase todos nesse setor desconhecem: Tais dispositivos somente serão eficazes quando forem designados e projetados para seus fins específicos. Exemplo pela qual agências de inteligência do mundo inteiro desenvolvem suas próprias escutas clandestinas, pois sabem quando, onde e como utiliza-las. Torna-se óbvio que aparelhos vendidos indiscriminadamente e sob produções massivas jamais podem intitular-se "Profissionais", uma vez que utilizam esquemas idênticos, frequências conhecidas e técnicas comuns.

Na prática os equipamentos clandestinos não se restringem somente ao uso de Micro-Transmissores e Gravadores, como usualmente nos limitamos a observar. Compõem-se dentro de uma vasta gama de circuitos engenhosos: Equipamentos Infravermelhos, Ultra-Violeta, Laser, Ultra-Som, Corrente Portadora (Telefone ou Rede), Emissão Secundária, Salas Quentes, Amplificadores Parabólicos de Som, etc. Além de poderem estar codificados, comprimidos ou pulsados!

Os **DISPOSITIVOS CLANDESTINOS** são classificados primariamente na Contra-espionagem conforme seus aspectos físicos e de irradiação, sendo:

Os **DISPOSITIVOS CLANDESTINOS** são classificados primariamente na Contra-espionagem conforme seus aspectos físicos e de irradiação, sendo:

- 1- Bugs Acústicos**
- 2- Bugs Ultrasonicos**
- 3- RF Bugs (Rádio- Frequencia)**
- 4- Bugs Óticos**
- 5- Bugs Híbridos**

Também são classificados RF Bugs em **NÍVEIS DE SEGURANÇA**. Estes , sendo de muito maior importância na Contra-Espionagem, pois dependendo do nível em que se encontra o dispositivo clandestino, consegue-se identificar a especialização do indivíduo que o introduziu, podendo-se ter idéia dos riscos que a vítima estabeleceu!

### **NÍVEIS DE SEGURANÇA**

**NÍVEL 1** -- Transmissores de **BAIXA QUALIDADE**, com potências acima de 50 mW, métodos de modulação comum, como AM, FM e de construção rudimentar, FACILMENTE RASTREÁVEIS. Exemplos destes são geralmente encontrados em anúncios de revistas, Spy Shops e de construção amadora.

**NÍVEL 2** -- Bugs também de **BAIXA QUALIDADE**, mas de construção massiva por empresas. Podem utilizar modulação AM, FM, OC, SSB, com frequencias limite em torno de 1 GHz (1000 MHz). São facilmente encontrados em Spy Shops e Agencias de Investigações, bem como FACILMENTE RASTREÁVEIS nas varreduras de Contra-espionagem.

**NÍVEL 3** -- Bugs de **MÉDIA OU ALTA QUALIDADE**, sendo o que os diferencia são os aspectos técnicos, podendo serem manufaturados ou industrializados em pequena escala. Utiliza métodos de modulações diferenciados como NFM, WFM, FSK, PULSO, CPM, etc... ; além de emitir potências menores que 20 mW e incluir frequencias até 3 GHz, com intuito de DIFICULTAR SEU RASTREAMENTO por "Scanners" e "Sweepers" comuns.

**NÍVEL 4** -- Nível **AVANÇADO** em se tratando de Bugs, pois utiliza-se de frequências acima de 3 GHz (até 40 GHz) e potências menores que 5 mW, além de operarem com métodos de modulação "não comerciais", como BPSK, DS/SS e QAM multi-megabit, podendo ainda estarem codificados (Scramblers) ou comprimidos em espaço de tempo (Dwell time). Técnicos ou Detetives sem equipamentos de ALTA PERFORMANCE e profundos conhecimentos neste nível, JAMAIS encontrarão ou anularão tais dispositivos na Contra-Espionagem!

**NÍVEL 5** -- Nível "**State of the Art**", desenvolvido por Agências de Inteligência de países desenvolvidos para uso próprio. Costumam ser **DISPOSITIVOS COMPLEXOS** apesar de **INCRIVELMENTE PEQUENOS**. Trabalham com largura de Banda (BW) de 500 a 800 MHz, frequências de 40 a 325 GHz e métodos de modulação "não comerciais", podendo até mesmo serem desconhecidos no mundo técnico das Agências de Detetives Especializadas. Como as potências de irradiação não ultrapassam 1mW, nessas frequências, torna-se praticamente **IMPOSSÍVEL SUA DETECÇÃO sem Analisadores de Espectro** de altíssima velocidade e sensibilidade, cujos valores de mercado ultrapassam US\$ 50,000.00 e ainda necessitam de calibração anual.

Estes **5 NÍVEIS DE SEGURANÇA**, são considerados na Contra-espionagem como **BÁSICOS PARA CLASSIFICAÇÃO DE DISPOSITIVOS CLANDESTINOS** podendo contudo, haver situações em que caberá ao Detetive especialista em determinar o nível de certo dispositivo, pois poderá haver características paradoxas de diversos níveis implantados nele.

Ainda nesse contexto gostaríamos de afirmar que não devemos nos iludir com qualquer que seja o dispositivo quanto ao seu nível de segurança. Um simples dispositivo de Emissão Secundária, por exemplo, baseando-se em sua construção, se limita ao Nível 1, mas, na frequência, potência e localização certa, nas mãos de um especialista, se toma tão profundamente prejudicial quanto ao Nível 5.

Outra observação importante em relação aos respectivos níveis de segurança, que poderá causar espanto aos iniciantes, está em suas **POTÊNCIAS IRRADIANTEs**, sendo proporcionalmente menor a cada nível superior, quando muitos pensavam o contrário, justamente para se obter maior alcance. Isso se deve ao fato de que na Contra-Espionagem se torna muito fácil interceptar qualquer sinal acima de 20 mW com equipamentos convencionais de rastreamento!

Mas, afinal, o que devemos fazer quando suspeitarmos de **GRAMPOS, ESCUTAS OU INTERCEPTAÇÕES** na empresa ou residência do nosso cliente?

## PASSE AO SEU CLIENTE AS SEGUINTE INSTRUÇÕES:

1 – **FAZER DE CONTA QUE NÃO SABE DA ESCUTA** , pois uma mudança brusca de comportamento poderá expor seu cliente junto ao espião, tanto para o descobrimento da escuta, quanto a possíveis ataques anônimos (chantagens);

2 - Não discutir mais assuntos de importância no ambiente, ou ao telefone, e não fazer sinais visuais, pois ele também pode estar sendo filmado;

3 - Não comentar sobre esta suspeita a nenhum funcionário ou amigo próximo, pois embora aquelas pessoas possam parecer de total confiança, seu cliente não saberá de seu comportamento a partir daquele momento, nem se foram eles que implantaram o dispositivo;

4 – Se você não estiver tecnicamente habilitado, ajude seu cliente a consultar um **ESPECIALISTA** em Contra-Espionagem, mas tenha em mente que no Brasil inteiro existem muito poucos deles e o custo de seus trabalhos são bem elevados;

5 - Na consulta, **JAMAIS** utilizem telefone ou E-mail próximos a área suspeita, procure um Orelhão distante ou Cabines de Internet em Shoppings Centers, e não esqueça de deletá-los após serem enviados;

6 - Caso encontrem uma Agência de Investigações com essa especialidade, procurem conhecer o especialista, verifique se o mesmo possui **Equipamentos Profissionais** e conhecimento profundo na área. (Eletrônica e Telecomunicações) Procurem fornecer o mínimo de informações a ele antes de um possível acordo;

7- Sejam discretos em todos os contatos;

8 - Não contatem a Operadora Telefônica pois eles não saberão o que fazer e se limitarão apenas a retirar os grampos;

9 - Não contatem a Polícia imediatamente, pois os poucos especialistas estão na Polícia Federal. Detetives e Peritos das Polícias Cíveis jamais descobrirão sua origem;

10 – **NÃO CONTATE AGÊNCIAS DE CONTRA-ESPIONAGEM LOCAIS** pois eles mesmos podem ter grampeado seu cliente. Contate se possível, agências localizadas em outro estado;

11 – Tomar cuidado com o que se fala ao Celular e Telefones sem fio , pois podem ser facilmente interceptados;

12 - Acompanhe o serviço de perto, senão seu cliente, poderá perder dinheiro e não ter sua segurança restabelecida.

Em resumo, podemos esclarecer que o SUCESSO de uma escuta clandestina se deve principalmente as suas características, sua construção e perfeita instalação, facilitada com a maioria INEFICIENTE de técnicos da Contra-Espionagem.