

## The Eavesdropping Threat

Protecting one's information against the threat of technical interception, or eavesdropping, is complicated by the variety of techniques which the eavesdropper has at his disposal. If he is determined to intercept the information, he may employ any or all combinations of threat techniques. The level of his determination will be influenced by the value of the information (to him).

The problems presented by the area in which the eavesdropper must operate will also influence the choice of threat techniques. Those items that will limit the techniques at his disposal include: the physical standards and safeguards in the target area, his own capabilities and his access to specialist who can broaden his capabilities.

In evaluating the technical interception threat, several questions must be answered.

### 1. What is the value of the information to the potential eavesdropper?

This value, which may be completely different from its value to the owner of the information, tends to establish the threat level (the extent and expense to which the eavesdropper will go to gain the information). It also establishes, to some extent, the risk he will take to acquire the information. Obviously, if the information is of relatively low value, the eavesdropper will expend relatively little time and money and expose himself to very little risk.

### 2. Who constitutes the threat?

This question is best answered by determining who can benefit from the interception. Depending on who and what benefit can be determined, there is some basis for an analysis of technical capability and the probability that specialist will be employed.

### 3. What is the desired duration of the interception?

If the duration is short, (a two hour conference, for example) some interception techniques are more convenient and likely to be used than others. If the desired duration is an extended one (such as continuous monitoring of an office), techniques requiring batteries in the target area are much less likely to be used.

### 4. What other operational constraints are imposed on the eavesdropper?

In answering this question, one must realize that the eavesdropper requires three successful links to accomplish his purpose.

- He must have a concealable means of conveying the physical energy of the conversation to a medium which can be transmitted.

- He must have a concealable means of transmitting (wire, light beam, radio, etc.).
- He must have a location and the terminating equipment necessary to transform the transmitted data back to a form which can be used. Both the location and equipment must be concealed.

If any one of these three links are detected or prevented, the eavesdropper has failed.

Answering questions 1 through 3 may be relatively easy. The answer to question 4 normally requires expert evaluation of the specific problem area, if the evaluation is to be accomplished in depth. However, consideration of the data derived from the above questions will allow the non-specialist to make at least general threat evaluations.