Amateur Counter-Intelligence

How to detect spying

Counter-intelligence at the personal level is not as complicated as one might think. As you will see, the majority of the effort will be in record keeping. Rather than going to a private investigator who claims to do “de-bugging”, “a spy shop”, or some web site that sells “de-bugging” toys, invest in a small notebook you can keep in your pocket.

How does one begin a counter-intelligence (CI) mission?

The first thing to do is develop a plan. The following steps will help you:

1. Determine if there is an actual loss of information.
2. Determine who is spying on you.
3. Determine how the spy is getting the information.

Implement the plan

The first step in determining if there is an actual information leak, as opposed to your adversary knowing something you thought was private because of coincidence, is having some plausible but false information you can selectively distribute. This is where the small notebook comes in.

Make up several very different pieces of false information that sound true. The false information should be something your potential adversary would find valuable. If the person you suspect of spying is an estranged spouse, for example, the false information might be about a bank account you just opened. Keep this information completely secret. Do not tell anyone (children, mother, spouse) what you are doing.

Now the information must be selectively and carefully distributed. The information should be distributed orally, in writing, and on the telephone. When distributing the false information it is essential that accurate records be kept. The records should include the date, time, precise location (i.e., northwest corner of the master bedroom), person(s) present, and any other information that might be useful in tracking down the spy.

If your adversary ends up with the false information you distributed, it is time to implement Step 2 of your CI mission plan. Conversely, if your adversary does not get the information, then perhaps whatever information they had earlier was a coincidence and not obtained by eavesdropping.

Once again, you need to document the same who, what, where, and when information as when the false information was distributed. After analyzing your documentation you should have a good idea about the identity of the spy. The spy is often someone you thought you could trust,

so be prepared for the possibility of personal disappointment.

The third step in your CI mission plan is to determine how the spy is getting your information. The records about the false information getting to your adversary will show you how it is being done. Here are some examples of how to determine how the information is getting out:

1. Information written on a piece of notebook paper and thrown in the trash means the spy is looking through your trash. Get a good cross-cut shredder.
2. Information you discussed in person with a friend outside of the home or office where you believe an eavesdropping device is planted means your "friend" cannot be trusted. Do not tell that particular "friend" anything you don't want your adversary to know.
3. Information distributed during a phone call could indicate a phone tap, but it could also indicate that the person you were talking to cannot be trusted. Additionally, it could mean your cordless phone can be monitored with a radio scanner, or that there is a "bug" or recording device in the room where the call was made. To narrow down the possibilities, make sure to use all your telephone instruments, and make sure to set up your calls with different people.

4. Pretend to make a few phone calls without actually using the phone to call anyone. This will help determine if there is a "bug" or audio recording device in the room. A "bug" could also be a small video camera such as those built into pens and key fobs. Examples of these can be found by searching the Internet. A covert video camera of your own will identify the spy.
5. The information was left (as part of your CI plan) out in plain view on your desk. This could mean the spy either has legal access to your home or office, or they are breaking in. As in the previous example, a covert video camera will identify the spy.

The next steps

At this point you should have a good idea whether or not you are under surveillance by an electronic eavesdropping device. If you are not, you should now be able to relax. If you are fairly certain you are a surveillance target, implement your CI plan once

again. This time you will have a better idea of who your adversary is, and what type of device they are using. Be sure to document your actions and findings.

If your second CI mission verifies your initial findings, it is likely you are a surveillance target. Professional involvement is now in order.

There are several private sector avenues you can pursue. Law enforcement agencies will not provide technical surveillance countermeasures (TSCM), also known as “de-bugging” service. An attorney or private investigator is the best source for a TSCM provider. Look for attorneys and private investigators with experience in criminal matters. Electronic eavesdropping and surveillance are crimes covered by both federal and state criminal codes. The documentation of your CI mission will prove invaluable toward making your case with the attorney or private investigator.

Summary

The most important thing a private individual can do in cases involving electronic surveillance is documentation. The completion of the CI Mission plan described in this paper will make discovering any eavesdropping devices, and perhaps prosecuting the spy, much more likely.

It is possible to find an eavesdropping device yourself, but without professional involvement, law enforcement help is unlikely. Even with documentation from your CI Mission a law enforcement officer may believe you planted the device yourself. If you are not interested in prosecution, finding and removing the device yourself is certainly the least costly way to go. It is important to understand that securing the area against future eavesdropping installations is the most critical step toward a permanent solution to your problem. Good locks, an alarm system, and video surveillance are all excellent investments.

If you follow the advice in this paper your suspicions will be confirmed or refuted. The advice will also help you discover and possibly prosecute the spy.

I wish you success in your mission.