Technical counter measures

The threat of surveillance in corporate and government environments is real. Co-workers, professionals hired to repair and maintain certain building components, and even professionals from other companies may want to plant surveillance equipment in your office, your home, your car and any other location that you use to converse with other individuals about private matters.



While heightened security protocols can prevent some devices form being planted, the only way to remove these devices is by thoroughly searching and disposing of them.

Technical surveillance countermeasures (TSCM) is a term created by the United States government that describes the action of sweeping for devices that may be spying on you.

**What Do Technical Surveillance Countermeasures Encompass?**  
Originally, TSCM were aimed at sweeping rooms just for listening devices. This was done by using various pieces of technology that could detect the emission of radio waves.

This process has evolved to the point where non-radio emissions can also be detected. This means sensitive equipment can be used to search for magnetic waves, thermal emissions and light-emissions, such as lasers that may be broadcasting a silent signal to a receiver.

The field of TSCM has evolved far past just searching for listening devices. It encompasses securing communications technology, thoroughly inspecting and fortifying information technology, and ensuring that there is a heightened protocol of physical security to prevent future espionage.

That makes TSCM a lengthy process best left to professionals, as it requires expertise and equipment that the common person likely does not have.

**What Techniques and Technology are Used in Technical Surveillance Countermeasures?**  
Multiple techniques and technologies are vital in the process of securing an individual or place from the threat of surveillance, but they can be broken down into three main categories:

* Physical Security
* Communications Security
* Information Technology Security

In all three categories of TSCM, the following are likely to be employed as “general use” tools:

* Flashlights to search in dark places where hidden eavesdropping devices are usually located.
* Ladders to search for hidden devices in vents, on rooftops and in other hard-to-reach places.
* Multimeters to test for heightened electrical usage, which can be a telltale sign of an eavesdropping device.
* Tools such as sledgehammers, screwdrivers, hammers and crowbars that may be used to disassemble and to search for hidden listening devices.

Physical security involves looking for physical signs that a person or place is being watched. This can include sweeping rooms for radio frequencies using a frequency scanner, using spectrum analyzers to search for malicious RF signals, employing nonlinear junction detectors to sweep for obscured eavesdropping devices, and using portable x-ray scanners to search for surveillance technology inside of walls.

Communications security focuses on securing devices such as telephones, cellphones and fax machines. Time-domain reflectometers are key in performing this, as they can test the integrity of copper lines to determine if a phone tap has been put in place. The implementation of secure phone lines may also be part of this process.

Other tools used in communications security tend to coincide with those used with physical security, which includes multimeters and x-ray machines.

Information technology security is the last major category of TSCM, but it also tends to be among the broadest. It encompasses components of computer, software and network security to ensure that espionage, which tends to be easier to perform with IT infrastructure, cannot happen.

Steps of IT security can include installing virus scanners, implementing hardware and software firewalls, sweeping for any eavesdropping applications or devices put in place already, establishing damage control measures, and teaching individuals whom might use a computer with sensitive information on it steps to better safeguard against eavesdropping.

**Why Would Someone Require TSCM?**  
There are numerous reasons that an individual such as yourself may require technical surveillance countermeasures, but the most common is that you may work in a position where you need a high degree of security to keep your information as private as possible.

The most common reason for TSCM in a corporate environment revolves around keeping company trade secrets secure from prying eyes. This makes searching for devices that record and transmit voice information, wireless network information and anything else that could potentially compromise your valuable information all the more important.

Another reason for TSCM could be that you have a suspicion that someone is trying to spy upon you. This could be a jealous partner, someone from your past or even someone whom simply holds a grudge against you, your business or something else that you represent.

**Are Computers Something that Should be Covered in a TSCM Sweep?**  
While computers are not normally covered as part of standard TSCM sweeps, they are definitely a vector that malicious individuals can utilize to eavesdrop upon your information.

The interesting thing is that computers do not necessarily have to be connected to a network to communicate information. “badBIOS” is an example of a virus that attacks the underlying hardware of a computer that spreads through the utilization of speakers and microphones.

This malware can be picked up from almost any affected hardware, given that the target computer can pick up the ultra-high-pitched frequency that speakers infected with badBIOS utilize.

badBIOS itself took years and several strokes of luck for researchers to find in a controlled environment. There is no telling how prevalent this malware is in the real world, nor is there an easy way to test for infected systems.

While your computers may not be infected with badBIOS, it could still be the potential target for a myriad of computer-based viruses, malware or line taps. This can put the information that you hold dearly on even your most secure servers are risk for being stolen by prying eyes.

This makes computers something that the standard TSCM sweep should inspect, clean and secure regardless of if your computers are in a government office, corporate headquarters or something that you simply take home with you at the end of the day.