Technical Surveillance Countermeasures is a counterintelligence activity and refers to the countermeasures that are employed to detect or to defeat attempts to gain any information, whether privileged, confidential or of a very personal nature through the use of a variety of eavesdropping and other listening and transmitting devices.

Technical Surveillance Countermeasures services require a combination of skills and specialised knowledge about electronics, technical know how, counterintelligence, countermeasures, security, investigations, the law and many other disciplines, all in an attempt to prevent the gathering of information from a subject without the person's knowledge.

Technical Surveillance Countermeasures is conducted with varying degrees within Governments, the commercial and corporate sectors and increasingly on a domestic level for high profile persons.

Technical Surveillance Countermeasures referred to as "debugging" and "sweeping" detects the presence and location of active/passive eavesdropping and surveillance devices. It also detects and identifies existing or potential information security and communication weaknesses.

Technical Surveillance Countermeasures has also been defined as the systematic physical and electronic examination of a designated area by trained and qualified persons utilising approved equipment and techniques in an effort to locate transmitting or surreptitious listening devices, security hazards or other means in which classified, sensitive or proprietary information could be intercepted or lost.

HOW REAL IS THE THREAT OF ELECTRONIC EAVESDROPPING?

Information gathering and business espionage is found at every level of our society and the innovations in surveillance devices heighten the threat to confidential business transactions and personal privacy. Everyone conducting business is vulnerable in some regard. Information that needs to be protected may range from business secrets to very personal information.

Information can make the difference between success and failure in business. It is difficult to assess how many companies or individuals are targets of electronic surveillance. Many companies and individuals are totally unaware that electronic spying has affected their businesses or private lives.

We have found that in South Africa and the rest of the World that many businesses and even large corporations do not realise the extent of the threat and do nothing to protect their premises, facilities or communications from illegal eavesdropping. Most do not

even have a counterintelligence policy or procedures.

Companies all have policies about such things as smoking, first aid, sexual harassment, drugs and alcohol abuse to name but a few, but do not have policies regarding counterintelligence and the protection of information against industrial and technical espionage.

No real statistics of reported incidents is available from any local Government Department, nor does the South African Government assist or advise the private sector regarding the threats of illegal eavesdropping and industrial espionage.

Incidents that come to light are regularly reported in the South African press. Listed below are some of the more prominent incidents that made news in South Africa over the past few years :

- The Sunday Times reported on 24 August 2003 that somebody illegally bugged a Durban-Westville's University Professor's home telephone line. A private investigator discovered the "tap wires" that has been connected to Professor Anand Singh's home telephone. On Monday 25 August 2003 News24.com reported that suspicions of widespread phone-tapping have surfaced at the University of Durban-Westville.
- On 27 May 2003 The Star news paper reported that a bugging device was found stuck underneath a table at the Transvaal Agricultural Show that took place in Rustenburg, a rural South African town.
- In March 2003, various South African newspapers and magazines reported on the alleged spying incidents in the Gauteng business circles. Peter Honey writing for the Financial Mail magazine (21 March 2003) wrote that "The Gulf War has broken out in Gauteng as some of the country's most visible businessmen go undercover to fight their corporate battles"
- On 14 April 2002 the Sunday Times in South Africa reported that a small South African tobacco company, Apollo Tobacco, obtained a court order to raid the offices of British American Tobacco in South Africa.(BATSA)It was claimed that BATSA hired private investigators and used bugging devices to conduct industrial spying activities against Apollo Tobacco.
- During July 2001 the Governor of the Reserve Bank of South Africa, Tito Mboweni admitted that bugs and listening devices were found in the Reserve Bank and that it appears that someone in London apparently benefited from the information (Financial Mail)
- During the same period the Mail & Guardian newspaper reported that the owner of the Spy Shop in Durban was arrested for illegally tapping a telephone of a shipping company

- During June 2001 it was reported that the CEO of the Umgeni Water in Pietermaritzburg paid with an Umgeni Water cheque for the illegal tapping of the telephones of workers and trade unionists
- During September 2000 the then Chief of the Golden Lion Rugby Board in Gauteng openly admitted that he had bugged the telephones of staff, coaches and certain players

- During March 2000 the Bedfordview & Edenvale News reported that a bug (RF Listening device) was found in the office of the Chief Executive Officer of the Edenvale/Modderfontein Metropolitan Local Council
- During December 1999 an advertising executive appeared in the Wynberg Magistrates Court in Cape Town on charges that he intercepted a rival's confidential information and also tapped a telephone
- During November 1999 "bugging" made headline news when the Democratic Party (DP) of South Africa alleged that evidence of a bugging device was found at their Cape Town Parliamentary office. During the same period a spy camera was found outside the German Embassy in Pretoria.
- Some other prominent incidents reported were the ABSA and Bob Aldworth saga, the alleged device found in Derek Hanekom's vehicle (former cabinet minister), the alleged bugging of the offices of the Northern Transvaal Rugby Union, the alleged bugging devices found at the Transnet Head Office and the alleged bugging of the telephone of Earl Spencer (brother of the late Princess Diana) in Cape Town.

Bugging and telephone "tapping" services are openly advertised in South Africa

Specialised shops selling "spy equipment" can be found in most of our major cities.

There are many "out of work spies". The political changes in South Africa and the fact that the "cold war" is over forced many former Government as well as agents and operatives from the liberation forces into the private sector, where they are fighting what many call the next war, which is an economic war.

Information theft is easy and eavesdropping difficult to detect

Whether you are an individual or part of a large corporation you should consider a **Technical Surveillance Countermeasures**
survey if you are dealing with sensitive information, trade secrets, product development, legal problems, negotiations, mergers or take-overs, financial, labour or other disputes.

You could also be considered a target if you are involved in a divorce case, contesting child custody or are involved in other disputes.

You also have to be careful of perverts when you share accommodation or live in a commune. A few incidents were recently reported in the local press where tiny "pinhole" cameras were discovered in bathroom ceilings.

Businesses should determine the risk factor by answering the following questions :

- Who would benefit from the information in your company?
- What is the value of the information in your company?
- Do you have local or foreign competitors?
- The level of security and countermeasures in place at your company?

If the information in your company is of potential value to your competitors, efforts should be taken to protect it

WARNING SIGNS THAT COULD INDICATE POSSIBLE EAVESDROPPING

- Your confidential business or trade secrets are known by competitors
- Your activities are known when they shouldn't be
- Technicians showing up to do work when no one has called them
- Secret meetings and bids seem to be less than secret
- Strange sounds or volume changes on your telephone
- Sounds coming from the telephone's handset when it is hung up
- The phone often rings and nobody responds or strange noise tones is heard
- Your radio or TV suddenly develops strange interference
- You have been the victim of a burglary but nothing was taken
- Electronic wall plates appear to have been moved slightly
- Wall, ceiling or partition dust is noticed on the floor
- Repair technicians show up to do work when no one has called them
- Service or repair vehicles and people are spending a lot of time near your office or home
- Your door locks do not "feel right"
- Receiving unexpected gifts from strangers operating on a power source

COMMON EAVESDROPPING METHODS

There are numerous methods how an eavesdropper can obtain information from the target or subject :

- Hardwired microphone with a recording device
- Radio Frequency (RF) transmitting device
- Miniature video cameras
- Telephone bugs and taps
- Recording Devices

- Interception of fax or computer generated information
- Infrared and Laser beam transmitters
- Tracking

SERVICE PROVIDERS

It is important that a systematic physical and electronic examination is performed of the designated areas. There are also different service levels. **Not all companies or individuals face the same threat.** Make sure that you get the right level of service for your company and the possible threat that you face.

It is also important to use trained and qualified people with proper equipment. See our equipment section for a reference to high level and appropriate equipment.

Many private investigators and security companies offer debugging or technical surveillance countermeasures services. Some provide services of limited value and many provide services offering no value, only installing a false sense of confidence.

Many companies and even corporations make use of low bidders, wannabe's, those who offer a service for every letter of the alphabet and sometimes even those who sell or install bugs, to conduct surveys and technical surveillance countermeasures of their sensitive areas. There are many service levels. **Enquire** about training, experience and equipment.

Excellent indicators of the level of professionalism of a private technical surveillance countermeasures specialist are a strong technical and counterintelligence background, past Government experience as a technical surveillance countermeasures specialist, proof of the regular attendance of technical surveillance countermeasures training, courses and workshops. Proof of related training about networks, telephone systems, electronics, etc is also important. (Ask for **proof** of background, training, etc)