DEVER CLARK + ASSOCIATES

An Overview of TSCM

The acronym 'TSCM' (Technical Surveillance Counter Measures) is used to describe a range of *counterintelligence* activities conducted by an organisation to prevent or detect a technical surveillance attack against the organisation by external or internal threat actors.

Technical surveillance includes the use of listening devices, tracking devices, data interception devices, telephone interception, and optical surveillance devices, all of which can be used to covertly collect information about a target person or organisation.

Technical surveillance is a broad subject and encompasses numerous methods and techniques that can be used to illegally obtain information from a subject or a target area.

Some of the more common methods of *technical surveillance* are:

Eavesdropping on conversations in rooms or other places:

- Concealed microphone hard-wired to a recording system (e.g. tape, MD, 'solid state', MP3)
- Microphone connected to unused or spare telephone wiring, mains circuits or other building services wiring (LAN, alarm, EWIS, HVAC, etc)
- Radio frequency and light wave transmitting devices (also known as "bugs")
- Modified mobile (GSM/3G/4G) or cordless telephones
- Modified telephone instruments or systems
- Fibre optic microphones

Eavesdropping on telephone conversations and data transmissions:

- Wire-tapping of analogue copper telephone 'land-lines' (POTS)
- Installation of transmitting devices inside telephones
- Modification of telephone instruments
- Monitoring of facsimile, data and teleconferencing transmissions
- Monitoring of mobile and cordless telephone communications
- Modification of PABX software
- Monitoring of wireless data communications

Collection of images through the use of long range lenses or concealed video or photographic cameras

- Miniature CCTV cameras with microwave transmitters
- Concealed CCTV cameras fitted with 'pin-hole' type lenses
- Powerful binoculars and telescopes

Personnel and vehicle tailing and tracking systems

- Miniature tailing transmitters
- Miniature Global Positioning System (GPS) tracking systems

Data Interception Devices

- Keystroke loggers
- Wireless keyboard transmitters

Technical surveillance devices can be deployed against a target almost anywhere including offices, homes, vehicles, vessels and aircraft.

Contemporary technical surveillance threats are complex and diffuse. Traditional threat actors (such as foreign intelligence services) have been joined by terrorists, organised criminals, disgruntled or issue motivated individuals and groups. In today's high technology environment, the ready availability of technical surveillance equipment to these threat actors means that virtually anyone can conduct a technical surveillance attack.

For any TSCM to be effective, the threat and vulnerability of each target and target area should be systematically assessed before completion of a security risk assessment. The security risk assessment should be used to inform the decisions about which TSCM best suit the organisation's requirements. This approach will avoid unnecessary and costly sweep activities.

The most basic TSCM are good physical security, soundproofing, personnel screening, security awareness training, maintaining strict access control to sensitive areas and close supervision of external personnel when they are working in sensitive areas to prevent the placement of a technical surveillance device by those personnel.

A technical surveillance attack against an organisation will usually involve the installation of some sort of covert surveillance device (e.g. microphone, camera) in a target area and connection of the output of the device to a transmission system for conveying the collected information to an adversary's 'listening post'. Alternately, a small recording device can be installed and then recovered.

The technical surveillance device's transmission system may use wired or wireless technologies, or even a combination.

Wired transmission systems include the use by an adversary of the copper and/or fibre optic cabling infrastructure that belongs to the organisation (and possibly others)

as the transmission medium for a technical surveillance device installed in a target area by the attacker.

These days most organisations have internal and external wired communications networks within their facilities. These structured cabling systems are vulnerable to being used by an adversary for technical surveillance installations unless they are checked regularly.

An example of the vulnerability is that many wired networks (both analogue and digital) have 'spare' wiring (or circuits) that can be commandeered by an attacker as a transmission system for a collection device. The vulnerability of any wired networks to this type of technical surveillance attack is dependent on preventing unauthorised access to the network infrastructure.

The trend towards the use of VOIP telephony and integration of services has introduced additional technical surveillance vulnerabilities, which need to be assessed as part of a comprehensive TSCM survey.

In addition to computer and communications systems' wiring, other wiring such as power, alarm, public address, air conditioning, etc. can all be used as transmission systems for technical surveillance devices utilising a variety of techniques including 'carrier current' transmitters that convert information into signals that can be *carried* over mains and other building wiring.

Wireless (aka free space) transmission systems that are used for technical surveillance devices include radio transmitters, wireless microphones, baby monitors, wireless spy cameras, and ultrasonic wave, infra red or visible light transmitters. The eavesdropper can be just a few metres away from the target, hundreds of metres, or even kilometres away depending on the kind of system used.

Listening Devices

A listening device is designed to covertly collect audio from an area, and then either record or transmit the information out of that area to a listening post. Listening devices can be hard wired or utilise a transmitter of some sort. So-called 'quick plant' listening devices are self-contained with their battery and transmitter. A popular and probably the most common 'quick plant' listening device is the GSM mobile telephone.

Listening devices may be secreted in hollow walls, false ceilings, furniture, fixtures, power strips, radios and clocks and other common items, which have a legitimate place in the target area.

Telephones (analog, digital, VoIP), speakerphones, fax machines, print centers, video-teleconferencing equipment and their associated wiring / equipment racks, may be commandeered for eavesdropping.

It is also possible that an adversary could commandeer existing wiring associated with PA/EWIS[1], fire alarm, security alarm, air conditioning controls, CCTV as a transmission systems for a listening device.

TSCM Surveys

A '*TSCM Survey'* is defined as the systematic physical and electronic examination of a designated area by a competent *technical security specialist*, utilising specialised equipment and techniques for the purpose of precluding technical surveillance devices from areas where sensitive or classified discussions are held routinely. TSCM surveys are sometimes referred to as *'sweeps'*.

The primary purposes of a TSCM survey are:

- to detect and if possible locate and/or neutralise any covert listening or other technical surveillance devices installed in a sensitive location, and
- to observe any physical or technical security hazards by which classified, sensitive or proprietary information could be collected or lost.

Technical security specialists providing TSCM services require a combination of specialised skills and knowledge about electronics, protective security, investigations and technical surveillance.

To be effective against a range of threats, a comprehensive TSCM survey should start with a threat and vulnerability assessment leading to a documented technical security risk management strategy.

The technical security risk management strategy will effectively determine the nature and extent of the *'on-site'* TSCM activities to be conducted at any particular location.

Standard *'on-site'* TSCM inspection activities usually include the following activities as a minimum:

<u>Instrumented Electronic inspection:</u>

- Analysis of the radio frequency and electromagnetic spectrum
- Analysis of mains power and other wiring
- Telephone systems analysis

[1] PA/EWIS – Public Address/ Emergency Warning & Intercommunications System

- Audio soundproofing tests
- Search for CCTV/web cameras and other imaging technologies

Physical inspection:

- Detailed physical search
- Assessment of oversight (visual surveillance)
- Physical security assessment

TSCM surveys are specialised ***covert*** counterintelligence investigations and as such, are particularly vulnerable to compromise.

So as not to alert potential adversaries, TSCM survey activities require that a high level of *operational security* be applied to information about:

- Technical security personnel,
- TSCM survey equipment resources,
- TSCM survey tradecraft, and
- Timing of survey

The on site TSCM survey activities need to be carefully planned and executed in order to prevent the adversary becoming aware of the conduct of a TSCM sweep.

The on site TSCM activities, whenever possible, are divided into two phases, namely: the *'non-alerting'* phase, and the *'alerting'* phase

The Non-alerting Phase

During the 'non-alerting' phase every effort is made to keep any potential eavesdroppers unaware of the progress of a TSCM survey.

A preliminary ‘silent’ sweep will be conducted in order to late devices while they are in operation without alerting any potential eavesdropper

After all reasonable steps have been taken to determine if there are any unauthorised signals leaving the target area the alerting phase of the TSCM inspection begins.

The Alerting Phase

During the 'alerting phase' a physical search of the target area(s) is carried out. Music or other noise sources may be introduced into the area(s) to stimulate sound activated devices and to enable possible correlation of signals.

Electromagnetic Spectrum Analysis

Electromagnetic Spectrum Analysis (ESA) is the core component of a typical sweep and consists of a panoramic analysis of the radio, microwave and light wave transmissions in the target area to check for the presence of hidden technical surveillance transmitters.

The signals emitted by technical surveillance devices that transmit information via radio waves or other forms of electromagnetic energy (over the air or conducted by wiring) can be detected by a Technical Security Specialist (TSS) using specialised instrumentation including spectrum analysers, counter surveillance receivers and computer-controlled receivers.

By strategically locating measurement points in a building the ESA can allow inspection of whole office building floors and other large areas economically, inconspicuously, and in a short amount of time.

Since audio transmitters may be physically located some distance from their microphones (to avoid detection), the whole-building approach allows detection of surveillance transmitters not physically installed in the target area.

Different transmitter modulation techniques such as: voice activation, sub-carrier, frequency hopping and spread spectrum, scrambled, encrypted and burst transmitters are also addressed.

Vulnerable telephones may also be checked for evidence of any possible RF transmissions in the ‘on hook’ and ‘off hook’ modes.

Specialised instrumentation is used to detect the presence of ultrasonic, light wave and infrared emissions from listening devices utilising those parts of the electromagnetic spectrum.

Telephone Systems Analysis

Telephones and telephone wiring in the area of investigation are examined with a number of different instruments to check for modifications that allow room audio to be heard when the phone is not being used (on hook).

Telephones and lines in the target areas are checked from the instrument to the switching equipment for devices that would allow the conversation to be heard or recorded at another location.

Telephone instruments may also be disassembled and inspected for foreign devices and non-standard wiring or transmitters.

Telephone equipment (PABX) and distribution frame rooms may be physically inspected for devices that may have been attached to incoming telco lines.

Analysis of Mains Power and other Wiring

Mains power, alarm, LAN, TV and any other type of wiring present are checked for unauthorised transmissions.

Possible types of transmission include base band audio and radio frequency 'carrier current' and 'sub-carrier' signals.

All electrical devices in the office/room are inspected during this test to ensure that none are radiating or conducting these types of transmissions.

Physical Search

A thorough physical search is performed in the areas under inspection utilising specialised tools and protocols.

Electrical outlets, light switches, computer network and telephone outlets may be removed and visually inspected for the presence of technical surveillance devices.

Any electric and electronic office equipment and personal items (calculators, pencil sharpeners, radios, typewriters etc) picture frames, furniture, plants are also items of concern and are inspected.

Ceiling areas are checked and any suspect wiring is traced. The immediate outside or adjacent areas of the inspected place are also checked.

Audio Conduction Tests

The soundproofing of the target area(s) is tested by placing an appropriate sound source in the target area and listening for sound conduction through walls, partitions, ceilings, doors, air conditioning ducts or any other opening in the target area.

Assessment of Oversight (Visual Surveillance)

An assessment of oversight of the inspected place is carried out to determine vulnerabilities to visual surveillance.

Report

At the completion of the TSCM survey, an oral report is given followed by a detailed written report outlining the work performed, results, findings and any recommendations will be submitted to the client.

Technical security vulnerabilities and weaknesses in your present security arrangements will be detailed and recommendations for improving them will be made.

Summary

It should be remembered that a TSCM survey is only one part of an effective overall strategy to protect against information theft or technical surveillance. If insufficient attention is given to other factors, including effective physical security and access control, then the value of a TSCM survey is only short lived