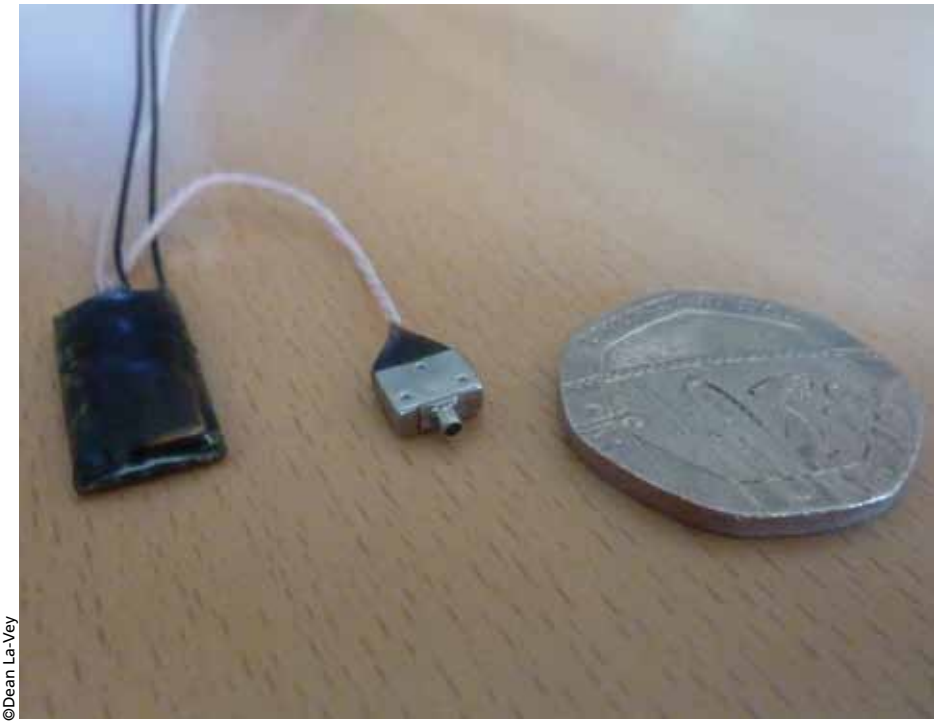
Dean La-Vey outlines the various types of counter-surveillance training available, and argues that every TSCM operator should engage in constant re-training to stay ahead of the threats

TSCM TRAINING –WHO NEEDS IT!?

Technical surveillance countermeasure (TSCM) training can broadly be divided into two distinct areas – training specifically on the operation of TSCM equipment, and training on the procedural elements of the search itself. Both are essential, but both are dramatically undersubscribed. There is the tendency among many operators to consider themselves totally prepared for the job at hand after undergoing just the basic equipment orientation (normally one day) and nothing else ever after. In truth, you can teach a ten-year-old child to physically operate TSCM equipment, but that doesn't qualify them to go out into the technical wilderness and competently carry out what is a difficult and demanding job. The carrying out of TSCM searches is a constant learning process. To keep sharp, disciplined and up to date, you need to train.

Most modern TSCM RF search equipment is multi-functional, with high speed receivers able to detect sophisticated surveillance transmitters over wide bandwidths and provide retrospective reference data. They have multiple display options and all the tools you need to investigate the entire radio spectrum. Digital Spread Spectrum Packet Data transmitters can be detected in almost real time – in theory. I say "in theory" because someone needs to have shown you such a device as detected on TSCM equipment. If you don't know what the signal looks like or where it lives on the frequency band, how do you know that what you are seeing on your equipment is a bugging device or not? You can't demodulate it and you can't listen to it; and there are plenty of legitimate spread spectrum and packet data transmissions out there.

Trawling through the frequency band with your headphones on may uncover the odd analogue bug once in a while, but no serious surveillance attack would involve that type of device. The serious end of audio surveillance requires a serious approach to TSCM searches. Knowledge is king here, and knowledge comes from training. TSCM RF search equipment will detect illicit signals, but if one cannot accurately interpret the received data, you are effectively blindfolded. Companies providing TSCM training services need to have an inventory of audio transmitters that represent the current and credible modern audio attack in order to demonstrate both their capability and method of detection. This requires a considerable investment with packet data burst transmitters costing upwards of £4,000 for one transmitter type alone. If you are carrying out TSCM searches and you've never been instructed on the detection of this type of device using the real thing, you'll never know what it is by trying to listen to it! A competent TSCM training body will have such devices and instruct on how to detect them. Please note, however, that a one-day training course on a modern TSCM receiver will not show you everything the equipment can do. It requires on-going training.



©Dean La-Vey

> "On-going training is absolutely essential to carry out TSCM efficiently"

Non-linear junction detector (NLJD) training requires firstly a modern NLJD and a basic understanding of its principle of operation. It also requires an understanding of the practical search limitations of NLJDs. This author has lost count of the number of enquiries as to why someone's NLJD is not detecting anything housed within a metal door frame, or why a 900MHz NLJD is reacting positively to "thin air"! Even basic instruction

©QCC Interscan

Hard target: successful TSCM operators must be trained in far more than just basic equipment operation

should cover these types of fundamental basic issues and queries. NLJDs won't detect anything when used on certain types of materials, even when a device is secreted within the material itself. Many just assume that no reaction on the NLJD means no detected electronic device. Not true! Credible training would explain clearly the areas of search where NLJDs can and cannot be used. You won't learn it from reading the manual.

If there is one area where TSCM training is lacking by the bucket load, it is in the field of telephone TSCM. As with RF training, the equipment available is advanced and competent, but operator knowledge and data interpretation is miniscule to say the least. No greater example of this can be found than that of voice over Internet protocol (VOIP) telephone system searches.

Let's first consider the equipment. Arguably the best dedicated telephone TSCM equipment in production is the REI TALAN. It contains within its multi-function facilities a VOIP analyser which captures VOIP packet data for analysis. How many TSCM operators know what the captured data actually means? VOIP has no relationship whatsoever to conventional telephony, so having such knowledge doesn't qualify you to interpret VOIP data for illicit interception equipment. You need training! What happens to the system voltages if you add four extra microphones to a Polycom conference telephone? Someone needs to show you. What happens if you disconnect a VOIP telephone and it won't re-boot and requires an administrator re-set? You won't guess the solution; you need to be trained. Even when searching for devices on conventional POTS or digital systems, there is great confusion as to what is normal and what is an anomaly. Someone well-versed on telephone systems has to show you and train you to confidently search telephone systems.

Knowing how to operate TSCM equipment is one thing, but knowing how to conduct the search itself is a completely different discipline. A search can be completely compromised if the search team steams on in with all guns blazing. All search areas are different, and the search itself may need to be procedurally modified to avoid such an occurrence. Competently trained TSCM personnel will check for covert CCTV transmissions before they even enter, will have an alternative reason for being there (checking IT, WiFi, or space planning etc), and have as much information on the search area itself in advance of the search. Training may cover areas which are not obvious to many, but which are extremely relevant to TSCM searches.

Health and safety requirements also have to be considered. Is the environment safe to work in, and has

TSCM TRAINING – WHO NEEDS IT!?

careful thought been given to areas of risk including asbestos? If you pop open a suspended ceiling or dry riser and the pipes are clad, can you recognise whether the material is safe? In many – and I really do mean many – buildings, it can be asbestos. TSCM teams need to be trained to be 'asbestos aware' and have a working contingency for it when discovered.

Procedural training will also include DNA preservation of evidence techniques should a device be found during the search. If the situation becomes a legal issue, how you examined and stored the device itself can greatly affect the outcome. If your physical search personnel don't receive this type of training, your entire forensic programme will go out of the window. Let's put things into perspective. This author has 28 years of experience in TSCM, but I still attend comprehensive training courses on the above subjects and others relating to TSCM procedures. It keeps you up to date and ultimately makes you more proficient at the job. No one should assume they know everything. TSCM is a constant learning process. Of course, the order in which particular parts of the search (RF, passive, etc.) are carried out is a matter of personal choice.

Specialised searches, such as those carried out on corporate aircraft, for example, require specific training courses before you can even step onto an aircraft. This isn't a choice – it's a mandatory requirement, and the legislation can change every year. In 2015, the European Aviation Safety Agency (EASA) brought in two additional training courses for those carrying out work on corporate aircraft. If you haven't done the training, you won't legally be able to carry out TSCM on aircraft in the EU. The Federal Aviation Agency (FAA) in the United States is also set to bring in the same legislation. It's all part of the aviation certification process. There are enormous consequences if untrained personnel clamber aboard a corporate jet and set about searching it without receiving training in regard to what they can and cannot do. Get it wrong and the aircraft itself will need re-certification. In simple terms, it may not fly for up to six weeks. Not ideal if the owner expects to fly out on his jet the following day.

TSCM training is something many operators do once when they purchase equipment. There are, of course, the inevitable know-it-alls who have a genuine unwillingness to learn or feel they don't need to be told how to do their job. It should be stated, however, that on-going training is absolutely essential to carry out TSCM efficiently. Knowing how to operate the basic elements of TSCM equipment is minor in terms of what else you need to learn to be proficient. Some training, such as the asbestos awareness training, is not TSCM specific but it is highly relevant to TSCM searches.

My concluding comment is this: serious electronic eavesdroppers aren't successful by accident. They train at their job. Some known to this author attend acting schools to learn how to appear credible in whatever guise they decide to use. They attend electrician courses, telephone courses, IT courses and locksmith courses to name a few. In this regard those engaged in TSCM have to up their game in regard to on-going training.

Dean La-Vey is a security consultant specialising in electronic countermeasures, specialised products and techniques for both the government and private sectors on a worldwide basis. He is a founder member of the Technical Surveillance Countermeasures Institute (TSCMi), a body of excellence within the TSCM industry.

Investment in training should be seen as equally important as investment in the latest TSCM equipment