Dean La-Vey ask whether it's possible for TSCM sweep teams to guarantee clients they have found every surveillance device, and examines some of the factors that affect their results

THE BUG-FREE GUARANTEE

Every technical surveillance countermeasure (TSCM) practitioner likes to think they are good at their job. The more experienced they are, the more confident they are that the job they do for their clients is the very best it can be. The client is, after all, only concerned with one of two possible conclusions: yes there is an eavesdropping problem or no there isn't. But in the case of a "negative", are TSCM operators able to give a 100 per cent guarantee to a client that this is indeed the case? There are a number of issues to consider before attempting to deal with the question, and the many new factors that greatly affect the conclusion.

The first issue concerns whether the TSCM team has a comprehensive knowledge base of what is actually technically possible to relay information covertly from one place to another? A direct understanding of the process and the size and operating requirements of eavesdropping devices is essential if search teams are to remain at the top of their game. Far too often there is a reliance on RF search equipment to do the job for you; and while this may have been cutting edge back in 1980, it has no relevance in 2014. Spread spectrum, packet data, GSM and ultra-wide band based devices do not shine out like a beacon on TSCM search equipment. You need to know what to look for and where on the frequency band a particular type of eavesdropping device will live.

Devices using unknown or new mediums of transmission can be difficult to find. To fully understand this we can equate the problem to that of computer virus detection software. Anti-virus software is only efficient at detecting viruses that the protection software knows about. If the virus protection knowledge base is not regularly updated, the chance of a new virus infiltrating the system is incredibly high. Serious hackers will write a dedicated viral program which will be initially unknown until it is eventually discovered and analysed. Increasing the knowledge base is not as difficult as it once was, as much is on the Internet; it does, however, require time and research. It also helps if you associate with other credible TSCM operators and share information on new technologies for eavesdropping. How many operators know where to look for specific new 4G GSM devices or a Belkin ultra-wide band unit? How about new design resonators? (How many readers are wondering what a new design resonator is)? No one knows everything, and therefore all TSCM personnel must assume their search capability in this regard is restricted to what they know about and what they are able to confidently detect.

In line with the knowledge base is the search equipment itself and the efficiency of the operator. It could be the best available, but totally useless if the operator has had only a day's training, or uses it once a month. RF equipment needs to be the most up-to-date possible in order to deal with new mediums of transmission. Non-Linear Junction Detector technology, for example, has greatly advanced during the last two years, with new 2.4GHz units able more efficiently to detect sim cards – something older 800-1,100MHz

©REI

©REI

While the latest equipment, such as REI's Oscor Green, is essential, teams must be adequately trained to know what it is telling them

units wouldn't do. In this regard, finds of covert cellular telephones in US prisons have skyrocketed since the introduction of searches with REI's 2.4 GHz Orion. In addition, search equipment such as QCC's "Searchlight" for detecting illicit GSM based devices efficiently and scientifically finds such devices (but how many TSCM teams have one)?

By far the most misunderstood areas of TSCM are those related to telephones. There are teams out there who have REI Talan equipment, but have no clue whatsoever as to what the equipment is stating. How many know the correct operating parameters of a VOIP system, or indeed what the packet data information really means on the VOIP analyser? It requires training and time. In addition to this, there is no shame here in asking someone who knows about something you don't know. As with the "knowledge base", no one knows everything. We can, however, confidently conclude that obsolete search equipment and/or the lack of training on up to date search equipment greatly affects the efficiency of the operator. Cost is the general controlling factor here. How much inexpensive obsolete TSCM equipment is on sale on the Internet with great claims of its technical prowess? One recent eBay advertisement hailed the values of the Mark1 Superscout 2nd Harmonic NLJD in modern TSCM searches, and highlighted how efficient this equipment was. The only thing efficient here was the sales pitch to the uneducated. It would, however, have made a superb NLJD museum piece.

A further factor is that of fatigue. It has been said that being tired at the wheel of a motor vehicle is as bad as being drunk at the wheel of a motor vehicle, with drivers not able to efficiently deal with the operation of the vehicle. In many cases, the errors made can have drastic consequences. So it is with TSCM. Long-haul travel and "through the night" searches eventually catch up with the best of us. The nature of the job often creates "back-to-back" searches in different countries and frequently different time zones, where getting through the first night becomes a difficult process. If fatigue creeps in, the efficiency of the search really does decrease significantly. Teams have to factor in rest days, especially where overseas travel is concerned. In truth, the very best equipped and most experienced TSCM

THE BUG-FREE GUARANTEE

©QCC Interscan

QCC's Searchlight product can efficiently find GSM-based devices, but how many teams have one?

operators will all make mistakes when fatigue is a factor. Let's face it – it happens to airline pilots!

Control devices present a further complication. A control device is a generic term for describing an eavesdropping device that has been placed in the search area by the client or client's representative for the TSCM team to find. It's their way of testing your capability, and when done fairly it can greatly boost a TSCM team's confidence. This author simply assumes that all search areas could have such a device, and they frequently do. Control devices are usually inexpensive RF transmitters and can be FM, VHF or UHF. Access by a client to these types of devices is fairly straightforward via the Internet. I have yet to hear of a client using a $6,000 packet data device just to test a search team. So what can go wrong here, even for the most efficient of teams?

In general it comes down to the knowledge of the client or their representatives, as to how and where a control device is installed. In this author's experience, some have included them inside a DVD box inside a locked cupboard, attached to the back of an automatic washing machine, at the back of a lady's underwear drawer (I kid you not)! There are of course clients who place passive devices or devices with no batteries attached. The bottom line here is that a fair control device test is one where the device is placed in a way whereby it has the ability to extract or relay the contents of a conversation from within the search area. An RF device hidden away inside a box where the microphone has no chance of relaying audio is not a fair control device test. There have also been cases of clients switching on a device mid-way through a search in areas where the RF searches in that area were incomplete. From the client's perspective, however,, one has to realise that their only expectation of you and your team is to locate their device, no matter where they have placed it.

Another factor to be taken into consideration is that of time constraints. Most new TSCM clients have no concept of what is involved in the process or how long it will take. If a client "chaperone" is on hand – and they frequently are – there will be the inevitable question of "how much longer?" It may also be that a client stipulates the exact amount of time allocated to a TSCM search. Many search teams have experienced the situation where they know a search area would take 12 hours to search effectively, but are only give four hours to do the job. Time constraints like this place undue pressure on the search procedure and technical analysis of search information. Specific key areas have to be looked at first, and other areas may not be searched at all. Access to service areas and adjacent offices may also not be possible.

Finally, team integrity plays a large part in regard to specific elements of TSCM searches, and could be mostly aimed at the physical search team. Even top government teams get it wrong. This author once ran a training course for a major EU country search team who aggressively searched a large hotel conference room. In four hours they had completely removed the air conditioning, the entire suspended ceiling and stripped a 50-inch plasma television down to its basic components. After declaring the area completely clear, I showed them the two active microphones they had missed. It happens, and it can happen to anyone. Search team leaders rely heavily on the information they receive back from their team regarding specific elements of the search. Everyone on the team has to do their job effectively for the team to be efficient.

Does the 100 per cent guarantee exist therefore? The truth is it doesn't, and it's a brave man indeed who says it does. TSCM search teams (even the most experienced) are not infallible. If you factor in the aforementioned scenarios, it is clear that what TSCM teams can guarantee is that they search the area to the best of their physical and technical ability. Training, building the knowledge base and adequate rest between searches greatly increase search efficiency; and time constraints are best dealt with by informing the client that the work will take a set period of time in order to be performed effectively. TSCM search teams have no real alternatives here but to strive to be more efficient at the job at hand. The more efficient they can become, the less likely they are to miss the well hidden and, sometimes, the obvious.

Dean La-Vey is a Security Consultant specialising in specialised products and techniques for both the government and private sectors world-wide. He is a founder member of the Technical Surveillance Countermeasures Institute (TSCMi), a body of excellence within the TSCM industry.