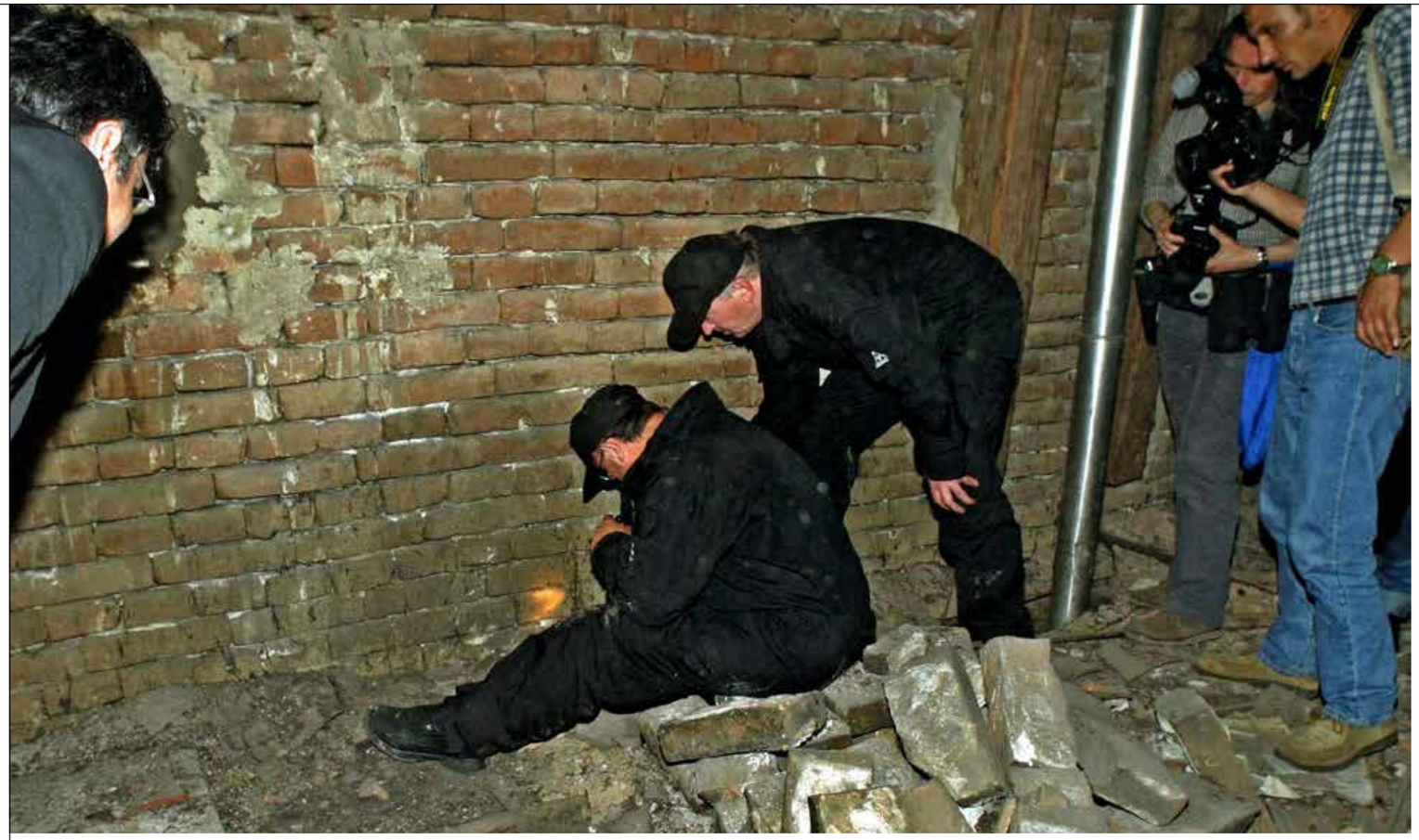


Picture credit: Getty

TECHNICAL SECURITY REALITY

Paul D Turner *explains why technical surveillance counter measures (TSCM) remain as vital as ever in the current climate*

Members of Serbia's secret service remove listening devices hidden in the walls above a minister's office

It is a well-established fact that cyber security generally sees the lion's share of the available budget and support resources often at the expense of a formal technical security programme. Confused? There is a difference between cyber security and technical security and it is essential that the often-subtle overlapping differences be understood and addressed by the organisation. A formal technical security programme is an often-overlooked professional discipline, mainly because those responsible mistakenly presume that somehow it is covered adequately under the cyber security or physical security banner.

A formal technical security programme must include a competent and wide-ranging Technical Surveillance Counter Measures (TSCM) component, which is just as important – and in some instances more so – to preventing the compromise of everything worth securing within the targeted organisation, including certain aspects and human factor vulnerabilities of the cyber-security programme.

Each of these professional disciplines has a different focus and related functions, however, they also share a number of important overlapping and common goal objectives and work together for the common good. It is considered an essential business practice that both disciplines receive equal consideration in the private and public sector, from business and corporate entities, to the national security apparatus.

When both professional disciplines are interactively implemented on a proactive basis, the financial impact of a technical compromise or discovery of an undocumented vulnerability can be managed, minimised or mitigated, reducing liability. When a formal technical security programme is not given equal consideration, the cyber-security programme is often weakened or compromised as a direct result.

Cyber security is considered to be a 24/7 function and those responsible for the cyber-security programme would never consider turning on the corporate firewall for perhaps only an eight-hour period a few times a year. Unfortunately, this is how the TSCM programme is often treated by the vast majority of organisations.

The Probability of Detection (POD) is shockingly low when the technical security programme is not implemented at the proper professional service level consistent with the perceived or ultimately determined threat level.

CONSIDERING ALL ASPECTS

A well-rounded technical security programme looks at the facility, uniquely from all sides and establishes a security posture baseline, across physical security vulnerabilities, human factors, counter-intelligence, counter-espionage, counter-terrorism, sabotage and many other areas of vulnerability, including the cyber-security programme. The importance of a formal externally implemented and managed technical security review on a monthly or quarterly inspection basis is considered an essential business practice and must be administered in conjunction with the application of a managed Remote Spectrum Surveillance and Monitoring (RSSM) component (a modern version of in-place monitoring), to provide a competent due diligence approach – this is what a formal TSCM inspection programme is all about.

During the past decade wireless threat technology has continued to advance in both sophistication and commercial availability. Much of this threat technology has ventured well beyond the capability of general-purpose detection equipment commonly marketed for TSCM applications, or administered by persons who are not trained in the technical aspects of modern threat technology.

Consider that virtually everyone in modern society now has a substantial grounding in using quite advanced technology in general at the consumer level, and a troublesome picture begins to emerge. Add to the mix a limitless number of consumer devices that are easily considered dual-purpose technology, many of which can be utilised for the intended purpose as designed or for purposes that they were not intended to be used for, either as is, or with simple modifications.

The Cold-War era is dead from a threat technology perspective and we are now faced with complex technology at the consumer and commercial level that rivals the sophisticated offensive tools of law enforcement, government and military of only a decade ago.

Modern threat technology has created a demand for advanced detection resources that are firmly based on versatile Software Defined Radio (SDR) technology and more importantly, a modern TSCM approach methodology.

Professional technical operators are faced with advanced surveillance technology that are frequency, power and modulation agile, making the identification of such assets all but impossible with obsolete equipment resources, ineffective techniques or an inadequate approach methodology.

Extremely sophisticated low-energy emitters are not only difficult to detect on their own merits, but when SDR anti-detection, anti-identification methods are used, you have a smart device that makes localisation extremely challenging and exponentially complex when compared with Cold War-era technology, on which the vast majority of general purpose TSCM spectrum analysers are based.

Within a defined modern moving target threat model, the professional technical operator, 'is the spectrum analyser' and becomes an extension of the hardware placing the technical operator back in control of the analytical process.

There is very little difference in today's modern threat environment as to the type of threat technology, the rationale for its use or the end result of a successful compromise within the private or public sector as there was in the past. State-sponsored espionage, competitive intelligence gathering and facility-level penetration for the purpose of social engineering attacks, access to computer resources, confidential and classified information theft, sabotage of critical data, disabling and/or circumventing network or physical security protocols, occur every day in virtually every protected environment.

WE ARE NOW FACED WITH COMPLEX TECHNOLOGY AT THE CONSUMER AND COMMERCIAL LEVEL

Perhaps the most troublesome aspect of TSCM accountability in a modern moving target threat model is the lack of understanding relating to Probability of Detection (POD) when reactive rather than proactive technical security programmes are implemented. The end-user expectation is that POD is 100 percent for any given inspection request, or at a minimum the expectation is that POD is extremely high.

Unfortunately, very few technical operators are willing to openly challenge the end-user's unrealistic expectations or talk about the POD reality with a perspective or established end-user client. This is always an excellent teaching moment and a brilliant opportunity to demonstrate the importance and need for more than a single annual inspection with the end user. Let's consider POD by the numbers and compare this with the end-user's expectations and explain that there are approximately 8,760 hours in a year, and if the organisation contracts an annual TSCM inspection of perhaps the executive office space, say 5 percent of the total office space compared with the total facility square footage. The inspection is likely to be conducted overnight or on the weekend, when the facility is not operating in a normal capacity; computers, office equipment, processes, *etc*. are off-line and the electronic sweep team is given, approximately eight hours to complete the entire inspection from beginning to end.

How we look at POD can be subjective, but let's take an honest look at the variables by the numbers and then add in other limiting factors. First and foremost, the POD is calculated as 8,760 x 8-hours (percent) (annually) = 0.08 percent POD. If, for example, the inspection programme provided 100 hours of time

on target, we would see a 1 percent POD annually. We establish this as 100-hours annually at 8.3 hours monthly, or 25 hours quarterly from a time-on-target perspective. We need to compensate for the actual frequency of inspections as the greater the frequency of inspections – just like increasing the hours – improves the time-on-target, yielding (at least in theory) an improved Probability of Detection by the numbers. If an eight-hour annual inspection yields a POD of only 0.08 percent and is considered the good news part of the story, POD on its own only means that the threat was detectable during the time-on-target window.

WIRELESS THREAT TECHNOLOGY HAS RAPIDLY ADVANCED IN SOPHISTICATION

It does not mean that the equipment resources utilised were actually capable of detecting the Signal of Interest (SOI), or that the operator has the experience or knowledge to observe any potential threat or is able to perceive the signal event as potentially hostile; assuming the signal is not dismissed as an ambient spectrum event.

The hostile emitter may well be a burst transmitter or include a store and forward component that is not scheduled to burst during the limited time-on-target. So, the POD by the numbers must be negatively enhanced to represent a number of practical considerations and is now worse than the good news story at 0.08 percent. All of this is simply a reality check in determining the best approach to maximise time-on-target for any given threat level. When technical operators, manufacturers of test and measurement or TSCM equipment claim 100 percent POD for their respective hardware and software-based products, remember that POD by the numbers must be an integral part of a formalised reality check to look at the Probability of Detection from a mission critical perspective and used to implement a technical security programme that meets the intended objectives.

When the client initiates reactive rather than proactive TSCM inspections of the ambient RF environment, there is little confidence that any given threat technology present and operating will be detected in a single inspection without a historical baseline being previously established, and if such a signal is detected, there is no guarantee that the threat will be properly identified by the operator within a snap-shot (point in time) inspection.

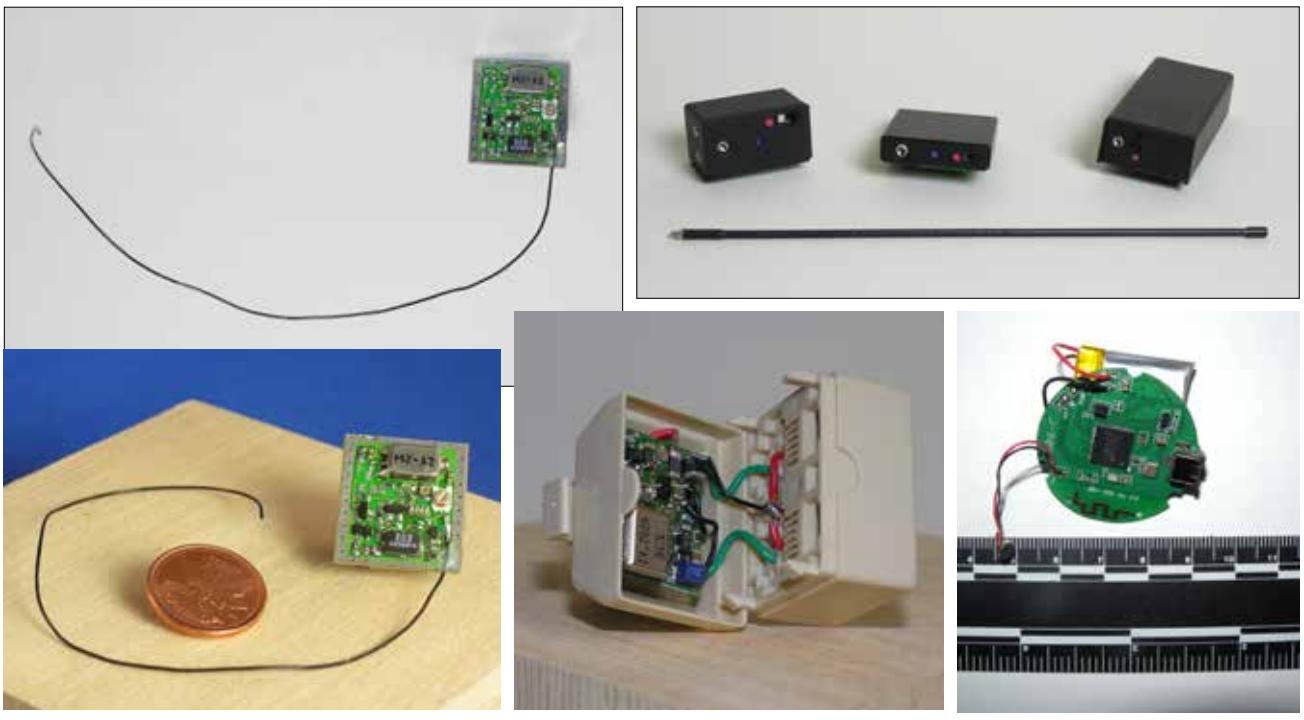
AN ABSOLUTE MUST

Remote Spectrum Surveillance and Monitoring (RSSM), when combined with the advanced aspects of TSCM focused geo-location heat mapping, RF propagation modelling, RF visualisation and multiple receiver (operation and hand-off), has become an absolute must in a modern moving target threat model and part of a modern threat detection methodology that significantly enhances the Probability of Intercept (POI) and Probability of Detection.

These modern TSCM methodologies are well entrenched in government and military circles, and are available to commercial operators to provide the operator with enough information to have a fighting chance of identifying any given detected signal or unknown energy as a potentially hostile threat signature ●

So how do we advance the Probability of Detection and improve Probability of Intercept exponentially through the application of the RSSM methodology? See part two of this feature next month when we will explore this in more detail.

Paul D Turner TSS TSI is the President/CEO of Professional Development TSCM Group Inc. and is a certified Technical Security Specialist (TSS) and Technical Security Instructor (TSI) with 40 years' experience in providing advanced certification training, delivery of TSCM services worldwide, developer of the Kestrel TSCM Professional Software and manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.



A selection of UHF crystal-controlled audio intercept transmitters (top row), a UHF audio transmitter with M2 mic, crystal control telephone audio intercept and a miniature bluetooth audio transmitter (bottom row, from left)

Picture credit: Professional Development TSCM Group Inc.