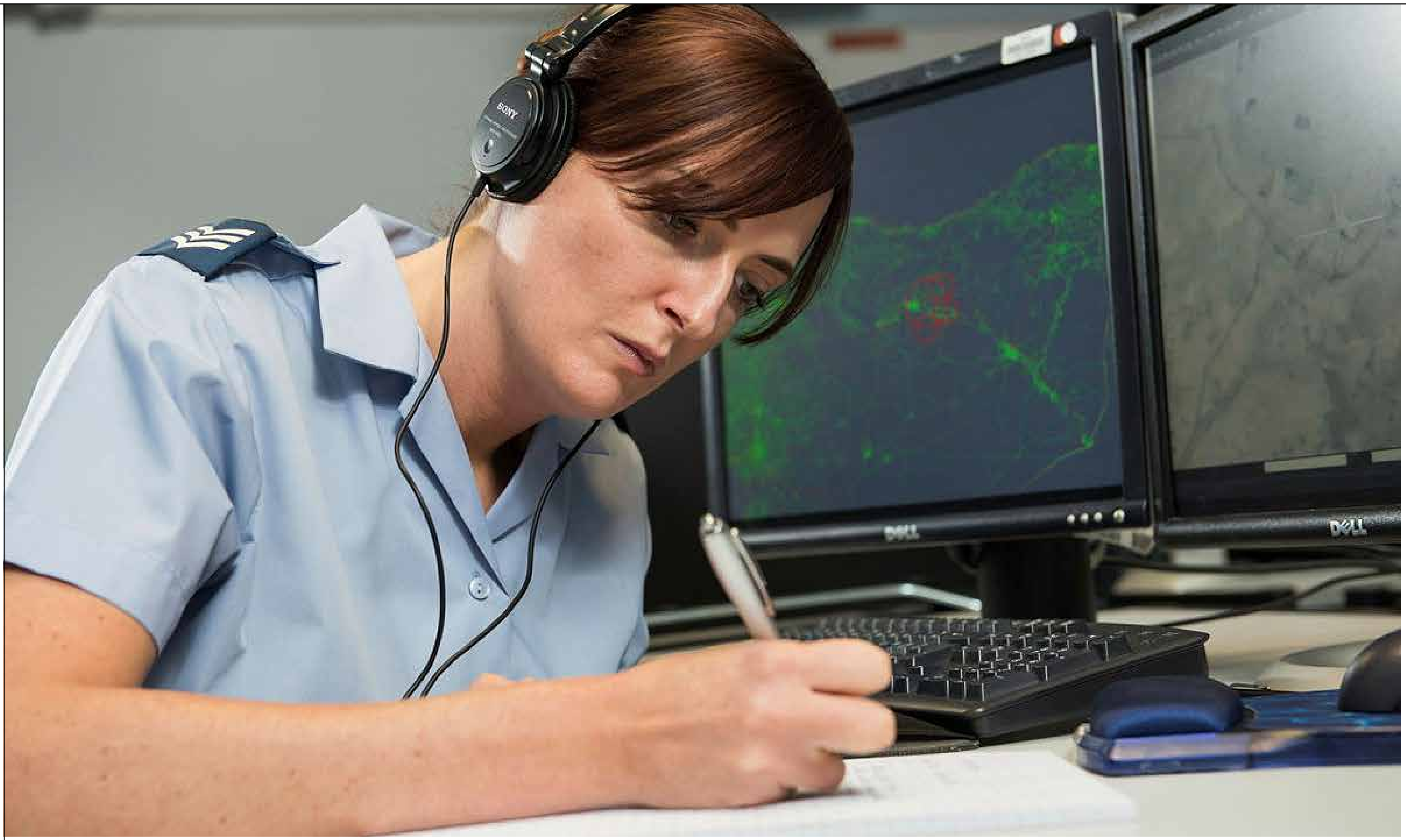

Picture credit: Crown Copyright

ARE YOU BEING COMPROMISED?

PD Turner *outlines the radio-frequency process and operator training considerations*

Before even deploying a radio-frequency resource the technical operator must give thoughtful consideration to Probability of Detection (POD). In a standards-based deployment methodology, we refer to this as 'POD by the numbers'. At this early stage of the game, the technical operator must take into account probability of detection, probability of intercept, time-on-target and a determination of the correct standards-based deployment approach.

POD by the numbers is always the first consideration and is a mathematical reality, that does not change from assignment to assignment. In fact, it is one of the few known factors relative to the counter-espionage and counter-intelligence role. If we take the number of hours in a year, we soon realise that there are 8,760 hours available to the threat actor to deploy their tradecraft. The table at the top of the next page shows a few examples of POD by the numbers to highlight the reality of the problem.

Unfortunately, POD by the numbers, is only the starting point in the conversation; as there are other equally important factors that need to be addressed by the technical operator in practice.

If the right person is not looking at the RF spectrum or other aspects of a technical security inspection at the right time, with competent TSCM equipment resources and sufficient time-on-target, the mission will fail to mitigate the threat of a hostile radio-frequency or other threat actor compromise. Even when sufficient time-on-target and separately, time-on-task, is available, detection is not guaranteed in real-time and therefore a full post capture and analytical review of all spectral data is essential!

> **If the right person is not looking at the RF spectrum at the right time with competent TSCM equipment resources, the mission will fail to mitigate the threat of a hostile radio-frequency**

PROBABILITY BY THE NUMBERS (STATISTICAL REALITY)		PROBABILITY OF DETECTION (POD)
Daily (RSSM)	24 per day x 365 = 8,760 hours	100 percent
Daily	12 per day x 365 = 4,380 hours	50 percent
Daily	8 per day x 365 = 2,920 hours	33 percent
Weekly	8 per day x 52 = 416 hours	21 percent
Monthly	8 per day x 12 = 96 hours	1.1 percent
Quarterly	8 per day x 4 = 32 hours	0.37 percent
Twice Annually	8 per day x 2 = 16 hours	0.18 percent
Annually	8 per day x 1 = 8 hours	0.09 percent

Operators are often sold a proverbial bill of goods when it comes to POD and POI in a modern threat environment. POI extends well beyond the TSCM equipment resource capability. Unfortunately, POI is often talked about by equipment manufacturers and many operators in the context of a lottery machine that only prints winning tickets.

It is essential that the technical operator fully understand POI from every possible angle and not just from specification sheet declarations. It is a given that 100 percent POI is only a reality when all the stars align and a threat signal is active, detectable and a competently trained technical operator recognises the signal as hostile.

It is equally possible that a believed to be 100 percent POI, can result in any actual realised value-based POI percentage, well below 100 percent all the way down to 0 percent without a competent approach and commonly taught techniques.

Modern threat technology is designed to take advantage of vulnerabilities in TSCM equipment resources; for example, the manufacturer's hardware claims, obsolete operator deployment protocols, obvious training deficiencies, and in general, a lack of understanding of how the POI question effects, whether or not a hostile signal is detected and identified as a threat technology.

Consider the following thought-provoking questions and determine the best possible POI when the equipment resource is presumed to have a 100 percent POI capability… What is the apparent POI when the operator sweeps to a range of 14GHz and the threat actor deploys a 39GHz TSD? What is the realised POI when the technical operator is not actively "time-on-target" engaged? What is the POI when the operator conducts a four-hour operator-assisted radio-frequency analysis and an active store and forward TSD is programmed to burst every 24 hours? What is the POI when a single SOI burst is captured in a 72-hour period, but the operator fails to identify the burst with applied post capture signal analytics? What is the apparent POI when the radio hardware sweep is 220 mSec, sweeps 4x per second and the threat signal is bursting at a rate of 25 mSec, every 14 minutes with a time-on-target of four hours? The answers to these questions tend to be rather complex and sometimes subjective, requiring the application of mission critical thinking by the technical operator.

There are three essentials of a TSCM focused training and certification process. These certainly include theory, application and tradecraft. The spectrum warrior must take an analytical approach to each phase of the inspection process. In a standards-based and balanced approach, training that is fully integrated with the correct intended operation of a software-defined radio solution must be experienced-based, balanced and include a strong mix of tradecraft, deployment techniques, modern methodology and analytical theory that includes critical thinking – not obsolete training practices that instill limitations.

In a modern training and certification methodology, it is real-world problems that must be considered, evaluated and resolved by every technical operator and their respective employers, and the end-user of counter-espionage professionals.

> A FULL POST CAPTURE AND ANALYTICAL REVIEW OF ALL SPECTRAL DATA IS ABSOLUTELY ESSENTIAL

Modern competency-based training is all about applied theory, practical experienced-based application and analytical critical thinking. It is not about building limitations by smoke and mirrors training in mock hotel rooms, bedrooms, meeting rooms or boardrooms. The approach is the same regardless of the physical environment. Many TSCM programs focus on these methods, but in practice no two inspections are ever the same and limitation-based training is not a practical method; in short, it is not the room it's the approach!

Modern standards-based TSCM training is not about product training – it never has been in reality – but rather it teaches the spectrum warrior to definitively think outside the box and look at all six sides of every inspection environment in a three-dimensional, 360° sphere of operation, and then apply a specific and unique focus for every Operator Defined Target Area (ODTA) and extended Functional Target Area (FTA).

For the most part, many technical operators consider training a necessary evil cost and often fail to consider or address the importance of not only the initial training requirement, but the need to seek annual currency training and other professional development opportunities.

The technical operator must look beyond the slick marketing hype and determine very specifically, what training is required. Okay, so you see the importance of total energy capture, POD, POI, certification training, currency oriented professional development, time-on-target, *etc.*, so let's move onto the radio-frequency process in a more practical way.

Nothing can happen until a signal-of-interest, referred to as SOI, is detected, captured, recognised, identified, selected, filtered and reviewed by the spectrum warrior. This is no easy task and the failure of the TSCM equipment resource or the technical operator to detect a potentially hostile signal at this stage can be the direct or indirect result of inspection timing, the equipment resource deployed, operator technique, motivation or experience and threat actor tradecraft.

IT IS ESSENTIAL THAT THE TECHNICAL OPERATOR UNDERSTAND POI FROM EVERY POSSIBLE ANGLE

Okay, so a SOI has been captured/observed within the ambient radio-frequency spectrum and is possibly hostile in nature. Perhaps this signal is just one out of hundreds or thousands of ambient signals observed, relevant to the operator's TSCM equipment capabilities or limitations and the operator's deployment process. In a modern standards-based deployment a maximum effort approach is necessary to achieve total energy capture. The capture of IQ for the SOI is the first step and tracking down the source of the emitter, is the second! The minimum IQ capture standard for TSCM is 160MHz (or wider). However, IQ capture on its own merits is not on its own a useful TSCM process, without real-time broadband interoperability that allows real-time IQ streaming. On to the next step.

Now, without over analysing, it is essential that the technical operator be able to determine with reasonable accuracy; identify that the signal event is in fact, a signal of interest and quickly determine the level of analysis that may be required; or even possible. Once the signal identification process is accomplished, isolating and conditioning the signal for optimum characterisation is essential. This is yet another failing point in the signal analytics process. Operators must learn to properly isolate, condition and characterise each signal-of-interest. It is not possible to accomplish characterisation based on a wideband spectrum review.

Once the signal event has been optimised for the analytical process, the next step involves the demodulation of the SOI, utilising available visualisations and demodulation resources. The demodulation process allows the technical operator to capture multiple analytical IQ files, screenshots and video captures and audio recordings. The demodulation of digital signals can be beneficial; however, the vast majority of threat signals are highly encrypted and yield no actionable intelligence as an off-set to the enormous amount of time-on-task required. The ability to demodulate common trucking, broadcast signals and many commercial wireless signals makes the operator feel powerful and competent. However, the reality is that complex signal analysis is a job for the SIGINT analysis and not the operator.

Every signal type is unique and has both an outward spectral signature or envelope, and a more complex internal modulation scheme as part of the signal level structure. It is essential that the field operator analyse both levels of characteristics to best determine how the signal will be categorised and handled within the operator's threat matrix. TSCM-specific software-defined radio features are required beyond the basic spectrum analyser and well beyond test and measurement resources.

The most obvious factor in identifying a signal of particular interest is the signal localisation process, whether or not the emitter is believed to be within the ODTA or not. If the emitter is within the ODTA, find it, validate it or terminate it. No complex demodulation or decoding is necessary. If it is not within the OTDA, further investigation is required to categorise the signal as unknown, not-relevant or potentially hostile. An expanded search into the Functional Target Area (FTA) may be required or possible, and is strongly recommended. No unknown signal can be ignored and a process must be implemented to resolve unknowns, by clearing them or flagging them for further analysis ●

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 over 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.

The spectrum warrior must take an analytical approach to each phase of the inspection process

Picture credit: Crown Copyright