Kestrel TSCM ® Professional Software

Are You a Snap-Shot Hunter — Or a Spectrum Warrior?

A Focus on Training and Certification

September 2019 | Issue 51

Technical Research and Standards Group

Paul D Turner, TSS TSI

The Kestrel TSCM ® Professional Software is by design, perhaps one of the more technically sophisticated and somewhat complex Software Defined Radio (SDR) applications available in the face of a modern moving target threat model, yet the Kestrel TSCM ® Professional Software is surprisingly simple and straight-forward to deploy in a modern real-world operational working environment at all levels of responsibility.

The Kestrel TSCM ® Professional Software definitively departs from many of the obsolete old-school concepts still be taught across the industry.

As noted in the August 2019 newsletter.

“The 3D Energy Probe provides complete galvanic isolation between the power line and the radio, spectrum analyzer or other test and measurement instrument, allowing for safe technical measurements of high-frequency signals, power line communication signals and electromagnetic interference or inductive coupling. From a TSCM perspective, the technical operator is primarily concerned with the presence of any signal whether magnetic, OTA radio-frequency, or unintentional radiator potentially containing signaling, remote-control, audio, video, or data streaming related intelligence. Such signals may be unintentional radiators, intentional unintentional radiators, client authorized devices or equipment resources and a wide range of sophisticated Technical Surveillance Devices (TSD) containing both encrypted and unencrypted intelligence”.

The Mighty Kestrel ® never sleeps, providing 24/7/365 radio frequency spectrum over-watch for private and public sector entities worldwide, from corporate to national security.

The Snap-Shot Hunter

Many technical operators, both private and pubic sector focus on hand me down generational training and Standard Operating Procedures (SOP), which are rarely questioned, let alone updated to tackle new threats, or best practice concepts offered by a modern deployment methodology.

The practice of snap-shot style inspections yield an unacceptable Probability of Detection (POD) in a modern moving target threat model.

If we look at Probability of Detection (POD) by the Numbers we can clearly see why most inspection reports simply state “nothing found” as a final conclusion.

Even at a professional service delivery level of 240 hours annually or (20 hours / Month), the Probability of detection (POD) is only 2.73% that the technical operator will detect and identify even a moderately sophisticated Technical Surveillance Device (TSD), which is actually operating within the current RF spectrum collection window of opportunity.

Now consider all the other variables, such as inexperienced technical operator’s, non-optimal equipment resources or deployment techniques, working blind in an unknown threat risk environment, etc., it is easy to understand why Probability of Detection (POD) by the numbers, is an essential due-diligence consideration in a modern training and certification model.

Economic-espionage is rarely identified in real-time, based on a single defensive technology, method or technique.

It takes validated spectrum data and experience-based intelligence collected over a significant period of time, to develop accurate threat modeling and trends for each unique target environment.

“The 100% Probability of Detection (POD) claimed by many manufacturers and many technical operators is likened to a fast food restaurant claiming they use 100% pure beef, when the reality is that 100% pure beef is only a single ingredient in the overall product and therefore by design is intentionally misleading, but rarely questioned”.

Paul D Turner, TSS TSI

The threat landscape has significantly changed in that RF vulnerabilities might be exploited by organized crime, cyber criminals and terrorists who have all proven themselves to be able to circumvent and exploit even the most complex countermeasures implemented to protect facility level systems and controlled information resources.

Kestrel TSCM ® Professional Software

The Metrics of Training and Certification — It is not a Life-Time Assurance of Technical Competence!

Professional Development TSCM Group Inc. **Technical Security Branch (TSB)**

We are no longer simply concerned with competitive intelligence at a fundamental level and it is essential that technical operators not only recognize this reality but take proactive steps to change the approach at every level to deal with the likelihood of technological terrorism and sophisticated organized crime related attacks.

The Spectrum Warrior

The true spectrum warrior first and foremost is totally up-front with the Probability of Detection (POD) by the numbers concept and is one with the reality of the effectiveness of the delivery of professional services, and manages end-user expectations with integrity.

It is essential that the best inspection program be presented to the end-user, taking into consideration cost effectiveness, based on a balance approach, with the potential for a strong POD, based on the perceived threat level.

This process requires that Remote Spectrum Surveillance and Monitoring (RSSM) ™ be calculated as part of the overall balanced approach either 24/7/365 or a more moderate approach targeting up to 30 days quarterly on a randomized deployment schedule.

Since most technical resources are simply not up the challenge, operators are encouraged to look toward the Kestrel TSCM ® Professional Software as the way to the future of Technical Surveillance Countermeasures (TSCM) and Signals Intelligence (SIGINT).

The Importance of Recurrent Training and Certification

On-going professional development training is an essential best practice for every technical operator; just as important as the modern equipment resources we all endeavour to deploy.

Unfortunately, many technical operators do not attend regular recurrent training, certification, or seek advise on new techniques and methodology, falling back on training knowledge received in the past.

We have trained and certified hundreds of technical operators and the one constant we see, is a lack of in-depth working knowledge on the current threat environment and the an understanding of many powerful new features that are often under utilized, therefore getting only about 60% of the software benefit.

Participants who have taken the time to attend our Certified Technical Operator (CTO) ™ training are quite surprized about the many features they were not using or were using without an informed understanding of the intended design and deployment methodology.

The CTO ™ program is not only about learning the software operation; it is firmly about learning how to deploy the software features and gain insight into the rationale behind the design of any given feature in reference to identifying new and emerging threat technology in the field.

Innovation is Simply the Beginning!

| www.pdtg.ca | www.kestreltscm.com | pdturner@pdtg.ca |