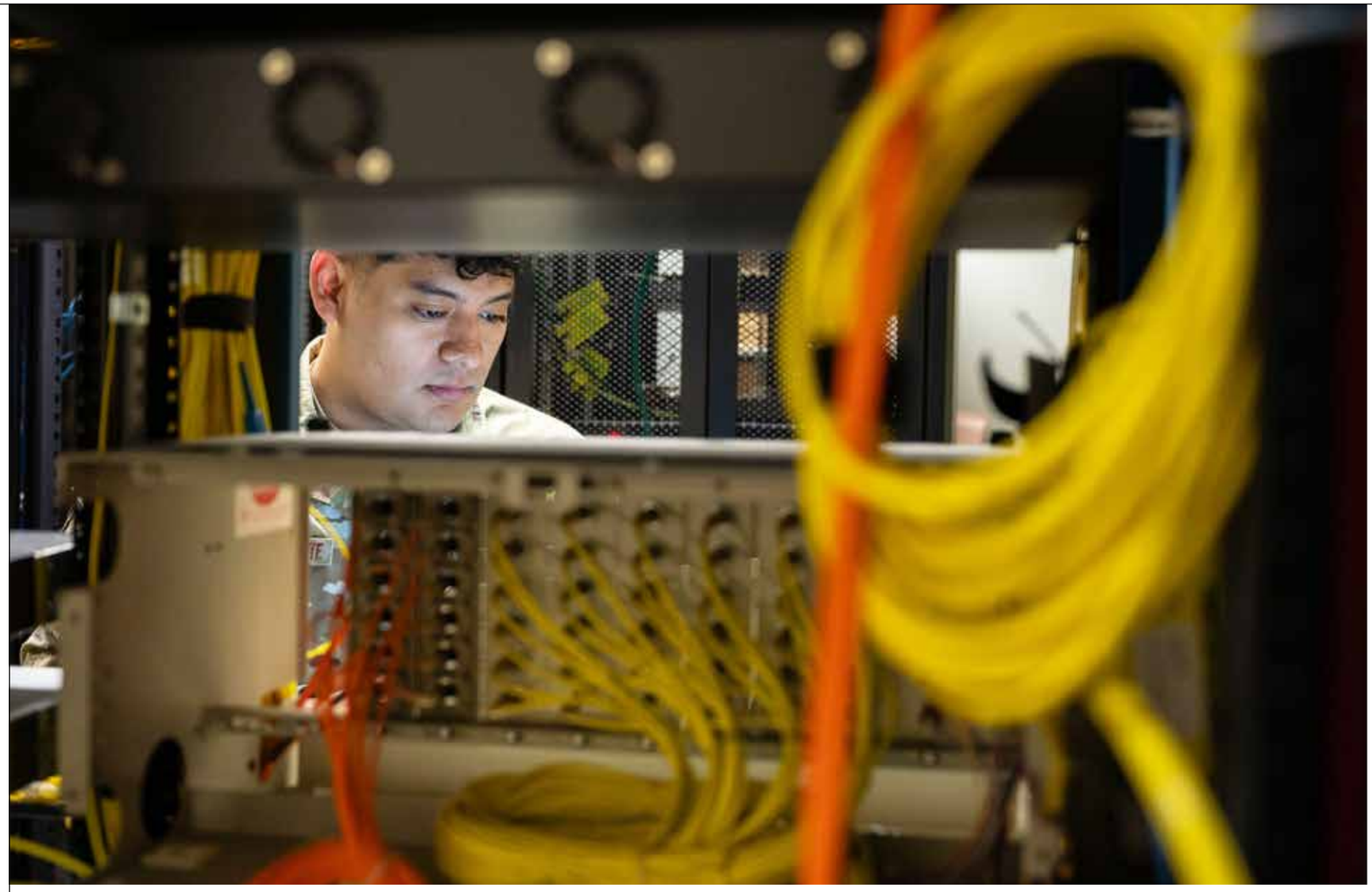

Picture credit: US Dept Defense

A NEW ERA

Paul D Turner *reveals the significance of 'Merging-Emerging' TSCM Technologies*

Understanding the importance of 'merging' currently available innovation, developing technology, recent scientific discovery, powerful new ideas and concepts, and fresh methodology are essential in their own right. However, unfortunately it is less considered the need to merge not only the well-established and accepted concepts, but rather merge current capability with all of the above emerging TSCM technologies and strategies.

As a somewhat unique professional services industry, we are all actively engaged in a powerful new era of a surveillance society and TSCM sub-culture far beyond the individual elements that are traditionally recognised as TSCM when it comes to radio-frequency spectrum requirements in particular, and the high-stakes analysis of complex radio-frequency signals across the spectrum. This includes powerline grid and optical (photonic) threat technology.

These are truly exciting and somewhat frightening times as all TSCM professionals at every operational level face a series of new technical challenges that cannot easily be quantified by any particular single point of success or ultimately failure. We are faced with a very complex and illusive matrix of potentially multiple layers and points of failure during every TSCM mission, requiring absolute focus and the application of critical thinking.

In a world of persistent and aggressive espionage trade-craft, by very definition, seasoned professional operators don't even know that they may have run head-on into a point of failure as there are few bench mark confirmations to the insidious and often invisible threat technology or adversary that we face globally.

Critical thinking and meticulous deployment pre-planning are absolutely essential to bringing focused resolution to the TSCM mission

Espionage, sabotage foreign interference, intelligence gathering and theft of information are all found proportionally to contribute to the challenges that technical operators face, over the past, when a single threat was more likely.

It is the combination of these threat metrics that perhaps is the most dangerous point of failure and at the same time allows some operators to fool everyone, but perhaps the threat actor as to the successful application of TSCM trade-craft.

It is this rational moment when every technical operator faces the reality and must make the decision to either continue without confidence, with the realisation that a standards-based approach is required to bring balance and positive success to the mission.

For the many TSCM operators, who may proudly achieve the 'luck of circumstantial success', there is also likely a high percentage of unknown failures in the mix. Simple mathematics bare-out this reality and a calculated point – or even points – of failure complete the threat matrix – referred to as "probability of detection by the numbers" within a standards-based approach.

Probability of Detection (POD) is the first realisation that there is a stronger 'miss' than 'hit' reality, mostly due to the operator's lack of ability to recognise a fast 'merging-emerging' global wireless threat environment – relying on obsolete concepts and detection resources. There is generally no single solution relative to guaranteeing absolute probability of detection (POD) at any operational threat level.

However, POD is recognised as the most important point in understanding and addressing significant operational deficiencies within the TSCM protocol that lead to failure to detect or identify sophisticated threat actor trade-craft.

POD is calculated as a factor of time-on-target along with operator assisted equipment resource capability, operator training and experience, and to an even greater degree the application of ruthless persistence and the application of critical thinking by an experienced and well-trained technical operator.

Critical thinking and meticulous deployment pre-planning are absolutely essential to bringing focused resolution to the TSCM mission – as is the operator's ability to apply a common set of application specific and tactically balanced approaches at each stage of the mission, shifting the high probability of failure to a higher and more confident chance of a successful outcome.

Our success is never absolute and there is always an element of uncertainty with every mission profile. Operators who understand is will take extraordinary measures to see the mission through by utilising the best TSCM resources that assist in liability mitigation, by powerful software feature design.

A standards-based approach demands the deployment of powerful customised Operator Deployment Logs (ODL) and Inspection Summary Checklist (ISC) technology to properly document all aspects of the inspection process.

Documentation of all aspects of the inspection process is a function of an Advanced Report Generator (ARG) to round out the reporting process. TSCM is not, or at least should not be a single event and requires a competency-based analytical comparative and trending analysis process over a period of time.

Equipment resources is our next concern within the point of failure chain as resignation to the fact that operators often state: "this is all we have", "there is no budget" or: "I heard this particular piece of equipment was the best", leads to denial over the more difficult decision to progressively improve the odds of a successful outcome.

Unfortunately, we have just identified and reviewed several important points of failure where the operator is sabotaged by the end-user TSCM program limitations, procurement process, lack of experience, competency-based training and ultimately a lack of any measure of control in the technical security programme's essential component parts.

MANY SCHOOLS ONLY TEACH USERS HOW TO OPERATE THEIR OWN EQUIPMENT RESOURCES

Training is high on the list with the vast majority of operators from those on their first on the job to those near the end of their career never having attended a progressive level of relevant training and certification, delivered by working TSCM professional Technical Security Instructors (TSI).

It is essential to understand that most technical security training is taught by independent manufacturers of TSCM equipment, who are invested only in selling their products – by teaching feel-good capabilities of their respective equipment over the many limiting factors and potential points of failure, not only on the equipment side, but also at the mission deployment level.

Rarely do these entities have or maintain current working field-experience or TSCM expertise as a mission specialist, let alone have the teaching skills necessary to instruct others – often just mimicking limited operator user manuals during the training.

Most manufacturers and instructors simply do not have any invested interest in the process beyond enhancing sales prospects, while pretending to be full service one-stop organisations. The lack of extensive experience is a serious point of failure within the TSCM mission cycle and deployment process.

Commercial and government alike, we often hear the same sad story of: "this is my mission or assignment", but: "I have no real experience" and: "there is no training budget this year!"

It is essential to purchase training as part of the overall procurement process when new technology and methodology is available, and ensure that annual professional development and recertification is included. Training, experience and on-going professional development are all needed before mission deployment, given the high-stakes professional TSCM services for which we are all engaged.

Relying solely on a learn-as-you-go strategy is a serious possible point of failure for consideration within the TSCM industry. There are far too many working in the TSCM sector that perpetuate the false premise that TSCM is easy and anyone can do it as an untrained, with no experience individual or

corporate security professional if you buy equipment resources and sit in on feel-good training.

This rationale is far from the truth and brings harm to the TSCM sector, as 'do-it-yourself TSCM' is a dangerous game that comes with significant liability. In-house programmes are only factionally effective bring a false sense of technical security.

Today's radio-frequency analysis requires more than just a spectrum analyser and an operator to press the ON button, no matter the perceived capability vs cost ratio. All training must be relevant and teach operational methodology far removed from cold-war era thinking.

POD IS THE FIRST REALISATION THAT THERE IS A STRONGER 'MISS' THAN 'HIT' REALITY

The ability of the technical operator to engage operationally relevant equipment resources and, perhaps more important than ever, the ability to apply a modern methodology and set of experience-based techniques is a direct function of today's competency training.

Most definitely, advanced technical training – and not just watered-down, initial concepts programmes – are often taught, or worse requested, by many technical security individuals and entities across the industry.

Feel-good training is simply not effective in meeting or maintaining an appropriate level of liability mitigation and many technical operators are simply not achieving the necessary level of initial training – and definitely not progressing with the required advanced training or on-going professional development requirements.

There is only a limited number of training and certification opportunities for professional technical operators, made of working industry Technical Security Specialists (TSS) who also have the specialised instructional expertise to deliver competency-based training and certification; particularly for government and military-intelligence end-users.

Many schools only teach how to operate their own equipment resources and lack any measure of practical, sanctioned research and development programmes, current career experience or competency-based training in-house.

The modern dangers of 'merging-emerging' technology must include a strong understanding of the radio-frequency environment and applied signal analytics far beyond the obsolete spectrum analyser or simply looking at the Bluetooth technology.

Software Defined Radio (SDR), including Real-Time Spectrum Analysers (RTSA) have decidedly replaced obsolete test and measurement gear masquerading has somehow TSCM qualified, with the use of limited capability hobby radios or ineffective spectrum analyser hardware. TSCM professionals worldwide now recognise the absolute importance and versatility of focused, multi-mission capability and transitional multi-tasking resources that are based on the concept of a modern moving target threat model.

This modern approach is now the widely accepted methodology across government and professional level commercial operators and this is only possible with the most powerful progressively updated SDR hardware and experience-based TSCM specific software ●

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 44 years' experience in providing advanced operator 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.

Training is high on the list for the vast majority of operators – from those on their first day, to those who are vastly more experienced

Picture credit: US Dept Defense