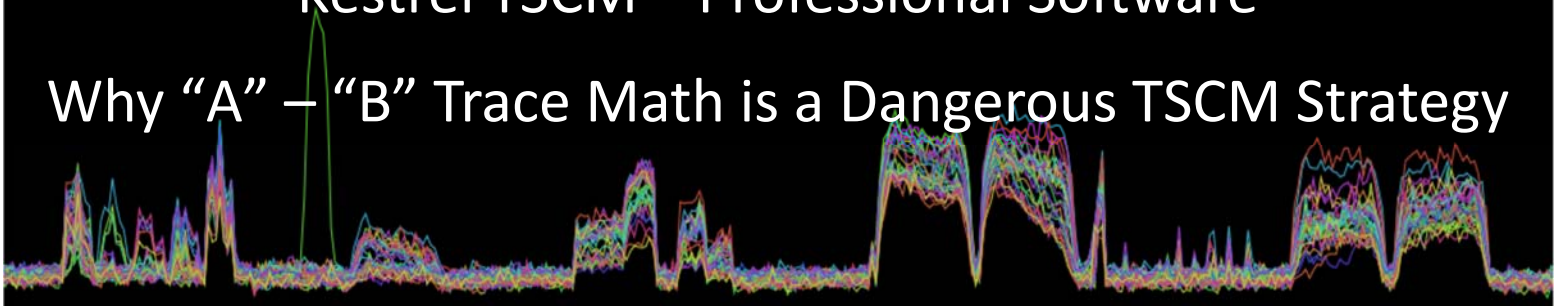
Kestrel TSCM ® Professional Software

Why "A" – "B" Trace Math is a Dangerous TSCM Strategy



March 2018 | Issue 33

Technical Research and Standards Group (TRSG)

Paul D Turner, TSS TSI

Why "A" – "B" Trace Math is a Dangerous TSCM Strategy at High-Threat Levels | Part II

The Kestrel TSCM ® Professional Software, threat methodology, based on a modern moving target threat model, breaks all the rules, or at least the obsolete rules, and sets a powerful new standard in deployment methodology, with the goal of advancing real-world Probability of Detection (POD).

As noted in the February 2017 newsletter.

"Some industry proponents continue to provide outdated TSCM training and concepts, by teaching obsolete and dangerous strategies for the detection and isolation, of potentially hostile signal events, and in doing so, are creating liability for themselves, and setting the end-user up for failure".

The practice of utilizing signal level analytics, to accomplish detection, identification, and isolation is used to surface potentially hostile RF threats, that have potentially made it past all other security protocols, and in plain view, continue to compromise the target facility.

"The sophistication and determination of key state-sponsored actors, can easily turn the simplistic "A" – "B" trace math game, into a dangerous signal level, game of deception, by design".

Paul D Turner, TSS TSI

The solution is realized by a combination of fixed and possibly mobile, Technical Surveillance Countermeasures (TSCM) based, geographically localized collection points, to provide unique analytical energy patterns, complete with supporting data, from multiple locations, to properly identify variations relative to these unique collection positions, both internal and external to the target area.

This concept is taught as part of the TSB 2000 (Technical) Standard ™, for high-threat level TSCM environments, within a modern moving target threat model, leaving behind obsolete "A" – "B" trace math as the only method of deciding which signal events to investigate.

"A" – "B" trace math, is a product of spectrum analyzers dating back some 50 years, and at low threat levels, with continuous analog signals, can be relatively effective, when the operator needs to isolate a discrete emitter within a known RF quiet zone, but fail as a filtering method to determine which signal events to investigate, when advanced offensive trade-craft is utilized against a real-world target.

Please note that for security reasons, some trade-craft elements, have been omitted from this briefing, to prevent further educating potential state-sponsored actors, from using the information.

We are more than willing to discuss and provide such information with a qualified end-user audience.

Our modern methodology, requires energy investigation at key geographical locations, both external to the facility, or target area, and also within, and external to critical infrastructure, at the internal level, to overcome the dangers of advanced hostile techniques being deployed by sophisticated state-sponsored actors, with nothing but patience, determination, and threat technology on their side.

Unfortunately, the offensive game is always ahead of the defensive game plan by nature and reality, allowing determined state-sponsored actors (who will find the obsolescence factor), in your complacency as a defensive, technical operator.

"If the TSCM program is not deployed as a heuristic countermeasure, much like the advanced application of an anti-virus software, the Probability of Detection (POD), will suffer significantly, placing the end-user entity at risk of an undetected compromise".

Paul D Turner, TSS TSI

We must also recognize that even outwardly friendly state actors, can have an interest in compromising other friendly allies, for both economic and / or political motivations.

Kestrel TSCM ® Professional Software

"Powerful Kestrel ® Heat Mapping Display (HMD)"

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

Anyone of these so-called "friendly" state actors, are likely to possess advanced threat technology, and have, at least some idea of the defensive capability, of the intended friendly target.

Defensive countermeasures must be applied in an obscure and random layered approach to have any hope of minimizing or defeating, technical vulnerabilities and compromises, within a defined high-threat environment.

The learn more about, "what you don't know, about you don't know, that you don't know", contact the Technical Research and Standards Group (TRSG), at Professional Development TSCM Group Inc.

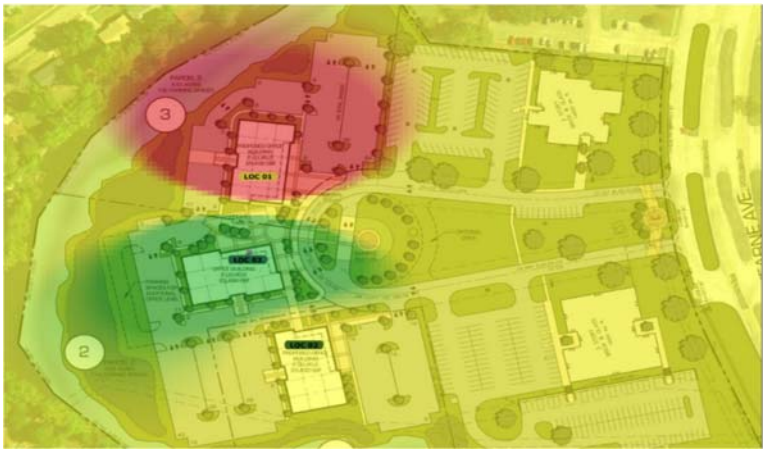
Heat Mapping Display (HMD) ™

The Kestrel TSCM ® Professional Software has a new and very powerful feature. Heat mapping is now fully integrated within the existing floor plan import structure, bringing a powerful new capability for Dual Receiver Operation (DRO) ™ and Multiple Receiver Operation (MRO) ™ deployment.

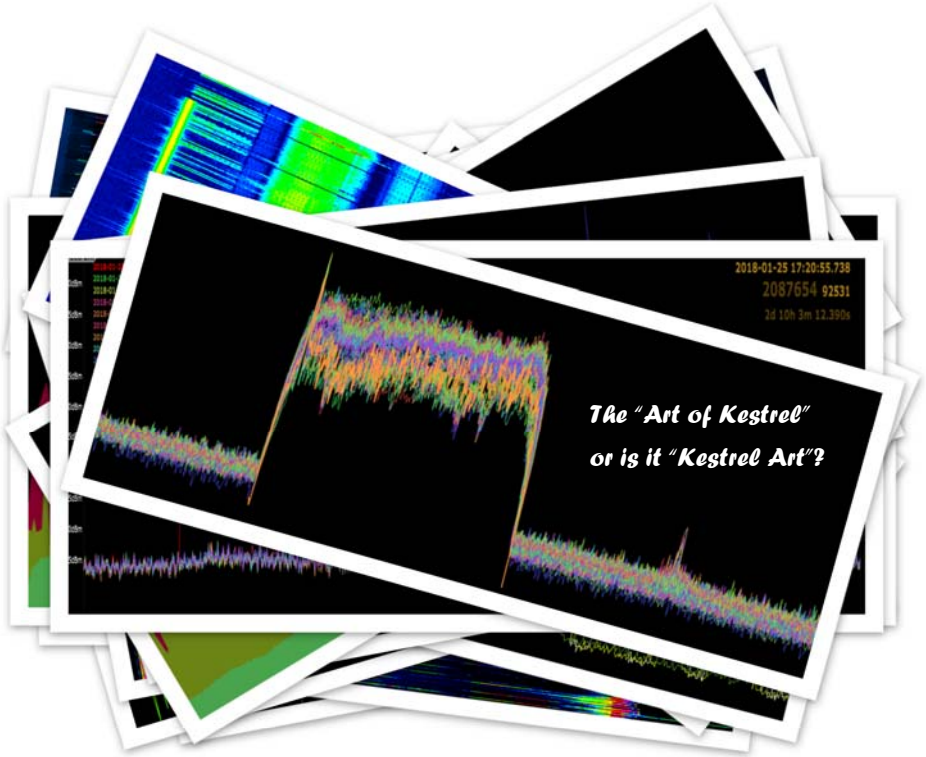
The HMD ™ permits any Range of Interest (ROI) center frequency and bandwidth, to be instantly mapped across all receivers within the target area, at the room level, facility level, or for wide geographical area.

There are two (2) operator defined algorithms provided with addition modes and functions under development.

The Kestrel Heat Mapping Display (HMD) ™ feature strengthens the Remote Spectrum Surveillance and Monitoring (RSSM) ™ strategy, by taking it to entirely new level of sophistication.



Join us at the Canadian Technical Security Conference (CTSC 2018) and learn how the Kestrel TSCM ® Professional Software can help you develop new and reoccurring revenue streams, through operator centric efficiencies, and powerful new tools and resources.



Kestrel TSCM ® Professional Software is innovative industry leading, disruptive technology, now sold in 30 countries worldwide.