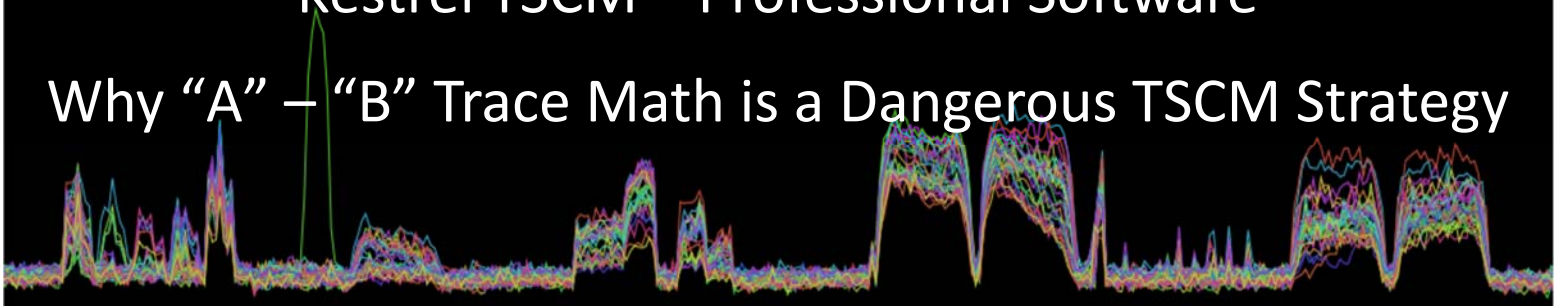
Kestrel TSCM ® Professional Software

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



February 2018 | Issue 32 **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 I

Some industry proponents continue to provide outdated TSCM training and concepts, by teaching obsolete and dangerous strategies for the detection and isolation, of potentially hostile signal events, and in doing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.

As noted in the January 2017 newsletter.

"As we blast into 2018, the future of tomorrows software—today concept, continues to generate a strong following worldwide.

2017 was a banner year in development history, with new powerful features that have tipped the scales in Kestrel ® being the go to resource for professional TSCM applications, with the introduction of new SIGINT tools.

The latest Receiver Differential Analysis (RDSA) ™ is now available, taking the software to an entirely new deployment level".

New powerful features are released regularly advancing the capabilities necessary to meet developing threat technology.

State Sponsored Espionage

The potential for trade-craft savvy state-sponsored actors to advantage gaps in defensive counter-measures is a major concern.

"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

When an attacker deploys a low-level transmitter, utilizing any number of difficult to detect modulation schemes, within the target facility, and then utilizes a higher power externally located repeater to receive and rebroadcast the low energy emission from within the facility, sending the outbound signal on the repeater system at a higher signal level, perhaps even rebroadcasting the signal from multiple geographical locations around the target facility, the "A" – "B" trace math concept, simply will not work on its own to identify the Signal of Interest (SOI), as a potential threat.

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 an authorized end-user audience.

Unfortunately, the result of advantaging the targets own defensive trade-craft vulnerabilities, can be the failure to detect in plain site, real-world hostile signal events.

The exterior signal level, by design and deception, will appear to be stronger, and perhaps appear to be arriving from several geographical directions, external to the target facility, when all that is available (or utilized) are internal and external RSSI values, or the resulting trade-craft, involves total reliance on the "A" – "B" trace math process, as the only means of signal level analytics.

Assuming the Signal of Interest (SOI) is actually evaluated, beyond the trace math, or is even investigated at all, once the trace math falsely indicates the signal event or level is stronger outside Vs inside the facility, the wrong conclusions may be realized.

To make matters worse, the attacker can utilize a number of "deception by design", transmitter and antenna locations that render, RF broadband evaluation ineffective and further lead the technical operator to the conclusion that the Signal of Interest (SOI) is originating from outside the facility, inaccurately resulting in dismissal as a threat.

Unfortunately, many equipment resources are designed around this outdated notion, and operators, continue to rely on this technique, based on the inverse square law,

Kestrel TSCM ® Professional Software

"Bringing Change the TSCM Industry Since 2009"

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

which is nullified when "A" – "B" is the only quantifiable data utilized, within the parameters of this type of attack sophistication by applying adaptive trade-craft measure, human factors, such as an unmotivated technical operator, or perhaps by the constraints of deployment. The total energy external to the facility, will always be higher than the energy from any point within the target facility, when repeater technology and trade-craft deception is utilized, as ambient, wide-area emitters, in combination with respect to superior trade-craft, leads the operator to the conclusion, that the signal is not emanating from within the facility, but rather is being detected within the facility, from a known outside source, resulting in a hostile signal event going unchallenged. The need for continuous external energy monitoring and real-time energy comparative, from a number of remote geographically localized collection points, external to the target facility, and multiple collection points internal to the facility or target area, is an absolutely essential technique, used to track and identify differing energy patterns, to properly identify signal relationships, and characterization.

"A" – "B" on its own, is a dangerous, and obsolete technique, and is clearly the wrong approach, particularly for critical high-threat levels, involving national security interests, that demand the technical operator to be defensively superior, rather than become offensively, a failure".

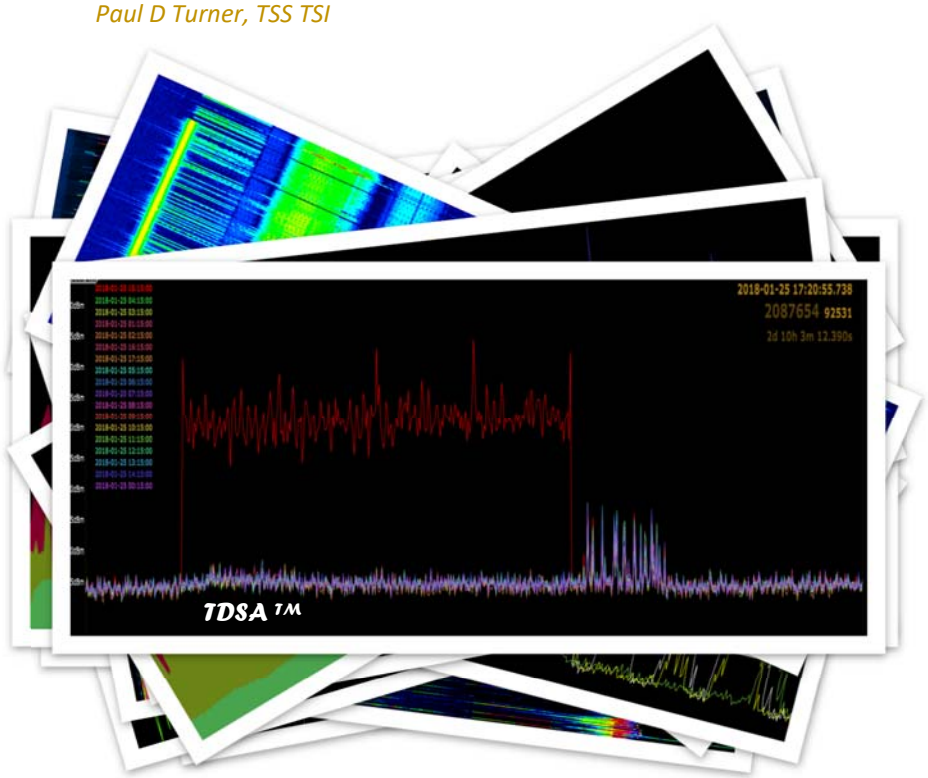
Paul D Turner, TSS TSI

Simple internal, external monitoring, and "A" – "B" trace math, cannot identify attacks of this nature and sophistication, because it fails to identify signal level variations that will occur when multiple repeater technology is utilized, unless Receiver Differential Signal Analysis (RDSA) ™ and Time Differential Signal Analysis (TDSA) ™ is utilized across multiple sensors, within, and external to the target facility.

The requirement of detecting in real-time, the small but identifiable power variations, and frequency off-sets, are only possible when collection is accomplished across multiple receivers. The competition says, this is too difficult for end-users to understand, or dismiss the concept, because they claim that it is simply not required. This is one of the keys reasons that the Kestrel TSCM ® Professional Software was developed, in the first place, was to provide the ability of professional technical operators to utilize advanced detection concepts, by actively applying a superior, defensive trade-craft methodology, and a powerful collection and analytical resource. The importance of turning defensive countermeasures in to offensive countermeasures, will aid in a higher Probability of Detection (POD), and provide an opportunity for exploitation of signals that may not otherwise be considered an active threat.

"Total Energy Analytics (TEA) ™ is essential in identifying threats within a modern moving target threat model, particularly at high-threat levels, such as homeland security, and national security related matters internationally".

Paul D Turner, TSS TSI



Kestrel TSCM ® Professional Software is innovative industry leading, disruptive technology, now sold in 29 countries worldwide.