Remote Spectrum Surveillance and Monitoring (RSSM) ™

Paul D Turner, TSS TSI

Introduction

This whitepaper delineates the tactical advantages, key benefits, new detection methodology, RSSM system architecture, administrative maintenance, technical analysis, professional service levels (recommended), and the requirements for a deployable, working Remote Spectrum Surveillance and Monitoring (RSSM) ™ system.

Source | Presentation at ERII 2016 Conference | September 2016 | Old Alexandria | Washington

The Kestrel TSCM ® Professional Software is designed on an entirely new deployment standard that permits traditional operator assisted Technical Surveillance Countermeasures (TSCM) inspections to be conducted, and a new protocol threat model methodology specific to the operational deployment of the Kestrel TSCM ® Professional Software, referred to as Remote Spectrum Surveillance and Monitoring (RSSM) ™ under the Kestrel ® umbrella.

The following observations were gleaned from Glenn H. Whidden's book, entitled "The Russian Eavesdropping Threat – Late 1993".

Glenn reveals an important observation that proves timely, even in a modern threat environment, and is a concept we teach during our TSS Certification program and actively brief our client's routinely.

The first observation from Glenn's book that echo's across various chapters, is that it does not matter how low tech a device or method of compromise may be, it will not be found, if there are no defensive countermeasures being undertaken, as a routine practice.

This message is as timely today in 2016 as it was leading up to 1993 and is the core foundation of the Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™ concept.

> *"If the right person is not looking at the RF spectrum at the right time, with the right equipment, the mission will fail to mitigate the threat of a hostile RF compromise in the field".*
>
> *Paul D Turner, TSS TSI*

In-fact, not one of the Russian RF devices described by Glenn in his book, would not have been detected immediately, if 24 / 7 active defensive countermeasures, such as the Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™, concept was actively deployed at the time.

If you are not looking at the spectrum 24 / 7, the Probability of Detection (POD) will be dangerously eroded well beyond the ability of a chance opportunity to detect a potentially hostile emitter.

The other notable observation derived from Glenn's book is that an attacker might deploy any number of anti-detection strategies, taking defensive equipment limitations, and what we now refer to as human factors into account; placing a hostile device in a difficult to access or difficult to verify location will often defeat defensive countermeasures.

The less than motivated defensive operator, may rule out (in error), certain possibilities as not practical for the attacker, or the defensive operator may not be able to electronically sweep certain areas due to accessibility or other issues, for example an NLJD search is rendered useless in a room full of electronics or heavy furniture may not be able to be moved easily, and inspection tools may not reach some areas.

> *"The lesson we must all learn is that a motivated attacker will always succeed against a less than motivated defensive operator".*
>
> *Paul D Turner, TSS TSI*

RSSM ™ requires that the technical operator and ultimately the end-user understand that global economic-espionage has taken a dramatic turn during the past decade, as significant changes in how corporations and governments do business, both at home and internationally, have opened the flood gates of opportunity, driven by aggressive state sponsored espionage players.

Individual private offices have all but been replaced with trendy Ad Hoc shared work spaces, significantly increasing the potential for inadvertent disclosure of proprietary information, both from an insider threat and through traditional espionage activities, with virtually no controlled access to common work areas, in the modern workplace.

Executives are integrating themselves into these common work areas under a so-called open door policy placing the organization at an even greater risk of compromise of competitive-intelligence and economic-espionage.

These same corporate executives would never think of turning off the company network firewall or anti-virus system at the end of the work day, but very few organizations take the threat of competitive-intelligence or economic-espionage seriously, as is evident by the randomness and periodic nature in which professional level, Technical Surveillance Countermeasures (TSCM) services are requested and delivered.

The ability of the Kestrel TSCM ® Professional Software to bring a new methodology to the industry was not taken seriously by many technical operators, equipment manufacturers and any number of foreign origin want-a-be competitive products, however, moving just a few years ahead, all of the above are seen to be quietly claiming they have the capability of some sort of spectrum monitoring.

The reality is that it takes more than a follow-the-leader approach to bringing a new and very powerful tool such as the Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™ to replace obsolete periodic RF spectrum analysis techniques, which are unfortunately, still being utilized by many operators as per the expectations and inexperience of the end-user, as the only means of conducting the spectrum analysis phase of a technical inspection.

Fact: Professional Development TSCM Group Inc., is a Canadian innovator with a solid foundation and technical investment in Research and Development (R&D), and a substantial financial investment in the design, engineering and development of the Kestrel TSCM ® Professional Software, positioning Kestrel ® as an industry disruptive Canadian technology dating back too early 2009.

> *"To quote a respected Canadian scientist, "I am amazed at how far the software has progressed in just a few years. It is doubtful even the government, with a team of software engineers and several million dollars could have achieved this level of development in such a short time".*
>
> *Undisclosed Individual*

Our industry leading position as a 100% Canadian developed, and source code controlled product, brings with it, a level of integrity and credibility simply not found in any number of foreign controlled software products that may be procured internationally.

Professional Development TSCM Group Inc., recognized early on that marketing existing repackaged products, or acting as a distributor of foreign controlled software was not an acceptable solution for our corporate, government or military clients, worldwide, given the nature and purpose of the software application and the challenges of countering economic-espionage and enhancing national security.

> *"Kestrel ® is an original fresh approach to redefining electronic Technical Security (TSEC) at the core level, and developed along the vision of future scalability and more importantly, sustainability, with witness to an expediential acceleration in threat technology and Software Defined Radio (SDR) hardware".*
>
> *Paul D Turner, TSS TSI*

The nature and characteristics of modern Radio Frequency (RF) threats, changes on a daily basis requiring adaptive search technology to be deployed, similar to heuristic capability of modern anti-virus software to look for threats that technically have never been seen in the past by looking for certain known characteristics and unknown event classification.

Such characterization, might simply be to flag an unknown signal event, as not fitting a known pattern of classification for the operator or technical analyst to manually review.

Core Concepts | Probability of Detection (POD)

Fact: You cannot detect, identify, or locate a threat of which you are unaware of, or have no technical data to support a position on either side, as to whether a compromise exists, existed, or will exist in the time-frame of an unknown future event.

Fact: Approximately 95% of the TSCM operators surveyed are still conducting ineffective < snap-shot > style periodic electronic sweeps, believing the Probability of Detection (POD) is reasonably close to 100% (a concept often proposed by equipment manufacturers, referring to the sweep speed and other hardware factors), and in-turn have convinced the client or end-user this is the case, when in-fact it is not possible without 24 / 7 capture.

Fact: What operators often fail to understand, is that even a highly experienced and competent RF spectrum analysis conducted with the right equipment resources and the correct approach, for a period of 8 hours a month x 12 months = 1% POD over the course of a year, when not supplemented by the Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™ methodology.

Fact: The average "time-on-target" among surveyed operators is approximately 10 hours (or less) quarterly, or 40 hours (or less) annually, yet most surveyed operators insist that this meets an acceptable level of due-diligence requirements for most of their clients.

How do operators know, what they don't know?

Fact: Operators typically place the blame on the client requested Scope of Work (SOW) limitations and budget restrictions, rather than challenge the ineffectiveness of the approach or limitations of the TSCM equipment, program, method or techniques, in fear they will not get the assignment.

Fact: Operators need to understand the real Probability of Detection (POD) numbers, as opposed to the slick and uninformed marketing methods utilized to impress prospective client's that in some cases, continue to utilize sub-par TSCM services.

Fact: When any equipment resource is deployed for say, one (1) hour, and the equipment resource is in-fact capable of 100% Probability of Detection (POD), and the operator has the experience to identify a hostile event from the many thousands of friendly ambient RF signals, I guess one could argue that the POD is 100%, but this is only true for the actual deployment time of, in this example one (1) hour, and this is where most equipment manufacturers and operators miss the point completely regarding Probability of Detection (POD).

Fact: The belief is that such service levels or products achieve what ultimately, are unfounded levels of Probability of Detection (POD) and program effectiveness, when POD is utilized only as a sales or marketing tool, resulting in providing the client with a false sense of security and instilling unrealistic program effectiveness capabilities.

Key Requirements

Understanding the modern threat model is an essential first step in providing an adequate level of professional service for the end-user, and ultimately delivering a professional services program based on the perceived threat level, with the realistic objective of mitigating risk.

Our Technical Research and Standards Group (TRSG) continually engages in a wide range of R & D activities, academic consultation, and most importantly, interaction with experienced field deployed technical operators worldwide.

When it is all about the money for the operator, (either services or equipment sales, or both) they will simply do what the client is asking for, no matter how ineffective the service may be at the end of the day.

Educating the client is an absolutely essential first step, in understanding the Cost Vs Return expectations, which includes the fact that the ineffective application of the wrong professional services at the wrong time, actually increases the potential for an undetected compromise and a false sense of security, not to mention the financial cost of the services.

> *"If the client is serious about preventing economic-espionage and / or enforcing critical wireless policies at the facility level, and preventing the compromise of electronic eavesdropping incidents, they will look to a professional technical operator for his / her expertise, advise and guidance in implementing the best possible strategy, within an appropriate budget allocation, consistent with the perceived threat level".*
>
> *Paul D Turner, TSS TSI*

The "You don't now what you don't know" thought process, is the big unknown that many players in the industry are willing to ignore, when it comes to marketing and selling sweep work to unsuspecting end-user clients.

> *"Without consistent uninterrupted data collection, gaps of unknown certainty exist, reducing the Probability of Detection (POD) significantly, and this advances the potential and opportunity of economic-espionage to occur, costing the organization on average 1.4 million dollars per incident".*
>
> *Paul D Turner, TSS TSI*

In-fact, every 2 hours of daily (annually averaged) of missed data collection results in an 8% chance of failing to detect or identify a targeted incident of economic-espionage, based on the presence of an RF assisted eavesdropping event.

Some manufacturers and technical operators claim their equipment has a 100% Probability of Detection (POD) based on sweep speed alone, yet fail to understand that 100% POD for the typical deployment of 40 hours of actual time-on-target, out of 8,760 hours (based on 365 days @ 24 hours) annually is just 0.5% POD from a modern threat model perspective.

This is no longer effective from a due-diligence perspective!

Time-on-Target is a critical factor in determining the Probability of Detection (POD) from a field deployment perspective, and the operator needs to look at the big picture.

This clearly is, or should be, an incentive to change the way TSCM services are delivered, and perhaps more importantly, presented to management or the end-user client, from a risk mitigation perspective at the corporate and national security level.

The means of this transformation is found in the core foundation of the Kestrel TSCM ® Professional Software, which is based on an entirely new technically feasible, budget friendly, threat model that includes the application of Remote Spectrum Surveillance and Monitoring (RSSM) ™, now possible, due to recent acceleration in Software Defined Radio (SDR) technology advancements, during the past decade, and perhaps more so in the past several years.

Under the Kestrel TSCM ® brand, this methodology is referred to as RSSM ™, which is new terminology and methodology that significantly enhances the overall efficiency and timely identification of a wireless security policy breach, or identifying trends and patterns that may indicate potential breach conditions that need to be further investigated or analyzed.

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

RSSM ™ significantly improves the POD across the spectrum and perhaps can be compared to a video surveillance system, which records data indefinitely for analysis and review, perhaps months or years after a significant event has occurred.

Economic-espionage is rarely identified in real-time and requires a lot of data and other intelligence collected over a period of time to develop threat modeling and trends.

In-fact, the very core concept of Kestrel Analytics ® must include all relevant intelligence sources as part of the analysis cycle.

The capture of RF spectral data can be correlated against access control records, HUMINT, video surveillance systems, alarm system events, and other sensory based data to bring clarity and reason to any suspicious activity.

In the past, these systems were not available or integration was not possible, limiting the ability to apply analytics across multiple intelligence sources.

> *"Probability of Detection (POD) by the numbers is what Kestrel TSCM ® Professional Software, Remote Spectrum Surveillance and Monitoring (RSSM) ™, and Kestrel Analytics ® is all about, and we leave the "follow-the-leader" marketing hype, to those that are in the game only for the money".*
>
> *Paul D Turner, TSS TSI*

The following POD data provides insight that executive management, the technical operator, and the end-user must understand in order to establish an effective Technical Surveillance Countermeasures (TSCM) program within their respective organizations.

> *"The 100% Probability of Detection (POD) claimed by many manufacturers and 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*

Again, what you don't know, you don't know, and therefore you cannot build an effective strategy to detect, identify, and neutralize real-world compromises, without powerful analytical data, in-hand.

This thought process, in part, explains why economic-espionage is rarely identified, and organizations continue to remain increasingly vulnerable to compromise, costing millions of dollars annually in lost opportunity every year.

The charted data below is only part of the risk mitigation picture, with the next logical questions being, "what is the perceived threat level for the organization" and "what level of risk is the organization willing to accept"?

There is always a realistic trade off between < Risk Mitigation Vs Budget >, which management or the end-user rarely fully understands, due to the lack of factual information surrounding successful acts of economic-espionage, which are never known, and the few that are discovered, often involving high profile players that command some attention, but leave the more common competitive-intelligence and vast majority of economic-espionage cases, virtually under the radar.

Fortunately, the means is now available to achieve unpreceded levels of < Risk Mitigation Vs Budget > with the integration of Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™.

Probability of Detection (POD) Opportunity Chart | By the Numbers!

365 days @ 24 hours = 8,760 hours annually | 8,760 hours = 100% POD

365 days @ 23 hours = 8.395 hours annually | 8,760 hours = 96% POD

365 days @ 22 hours = 8,030 hours annually | 8,760 hours = 92% POD

365 days @ 21 hours = 7,665 hours annually | 8,760 hours = 88 % POD

365 days @ 20 hours = 7,300 hours annually | 8,760 hours = 83% POD

365 days @ 19 hours = 6,935 hours annually | 8,760 hours = 79% POD

365 days @ 18 hours = 6,570 hours annually | 8,760 hours = 75% POD

365 days @ 17 hours = 6,205 hours annually | 8,760 hours = 71% POD

365 days @ 16 hours = 5,840 hours annually | 8,760 hours = 67% POD

365 days @ 15 hours = 5,475 hours annually | 8,760 hours = 33% POD

365 days @ 14 hours = 5,110 hours annually | 8,760 hours = 58% POD

365 days @ 13 hours = 4,745 hours annually | 8,760 hours = 54% POD

365 days @ 12 hours = 4,380 hours annually | 8,760 hours = 50% POD

365 days @ 11 hours = 4,015 hours annually | 8,760 hours = 46% POD

365 days @ 10 hours = 3,650 hours annually | 8,760 hours = 42% POD

365 days @ 9 hours = 3,285 hours annually | 8,760 hours = 38% POD

365 days @ 8 hours = 2,920 hours annually | 8,760 hours = 33% POD

365 days @ 7 hours = 2,555 hours annually | 8,760 hours = 29% POD

365 days @ 6 hours = 2,190 hours annually | 8,760 hours = 25% POD

365 days @ 5 hours = 1,825 hours annually | 8,760 hours = 21% POD

365 days @ 4 hours = 1,460 hours annually | 8,760 hours = 17% POD

365 days @ 3 hours = 1,095 hours annually | 8,760 hours = 13% POD

365 days @ 2 hours = 730 hours annually | 8,760 hours = 8% POD

365 days @ 1 hours = 365 hours annually | 8,760 hours = 4% POD

If we make an assumption that the threat model should only cover the normal business work day, plus a risk buffer of say four (4) hours, for cleaning and maintenance operations, we might assume the following projection at just 50% POD, assuming the threat is an RF emitter and is active during the RSSM capture time-frame, as follows.

365 days @ 12 hours = 4,380 hours annually | 8,760 hours = 50% POD

However, this does not take into account the modern threat environment and the reality of on-demand transmitter remote up-load dumps, scheduled store and forward technology, and other remote control techniques and devices that are not likely actively transmitting during normal business hours, or actively disguise themselves by modulation type, or anti-detection characteristics, by device design.

Without 24 / 7 Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™, the identification of potentially hostile emitters, in-bound or out-bound, cannot with any reasonable certainty, be detected or identified, except by chance, when only periodic < snap-shot > style collection is utilized.

Tactical Advantages

The capability of RSSM ™ to capture real-time analytical data, allows the operator to identify potentially hostile signal events in real-time, on-demand, or to look at trends over a specific period of time, based on detailed historical data, captured from Kestrel Project Files (KPF) for playback, analysis and report generation.

A tactical advantage is gained when actionable intelligence is available.

This is not the case with periodic RF sweeps of the defined target area, as a sole means of service delivery, and therefore, definitive conclusions cannot be made as to whether or not a comprise exists, existed, or will exist at some future point in time.

Key Benefits

RSSM ™ is a cost effective, budget friendly solution that is fully scalable as deployment requirements change.

Kestrel ® captures powerful < date > and < time > stamped data source archival files.

Significantly enhanced Probability of Detection (POD) is realized over typical periodic < Snap-Shot > Style RF Sweeps alone.

RSSM ™ monitors the RF spectrum, even when the technical operator is not present.

RSSM ™ permits the technical operator to monitor any number of independent remote collection locations live, or as historical data sets.

Detection Methodology

Must provide for and include 24 / 7 data capture for critical infrastructure.

The capture of continuous spectra provides for real-time and post analytical review.

Event filtering or automatic flagging of significant spectra events facilitates, streamlined technical operator review and technical analyst hand-off on demand.

System Architecture

The deployment of a Remote Spectrum Surveillance and Monitoring (RSSM) ™ system at the base level involves a single area of critical infrastructure such as a primary boardroom, or executive office suite, consisting of approximately 2500 to 5000 square feet, depending the on area occupancy and structural configuration of the space.

At the entry level, or recommended test deployment level, a single < RSSM ™ Sensor > can be deployed and later relocated as requirements change, or becomes strategically necessary.

The RSSM ™ concept is fully scalable as tactical or business requirements and perceived threat level change, bringing yet another level of budgetary control, to the implementation roll-out.

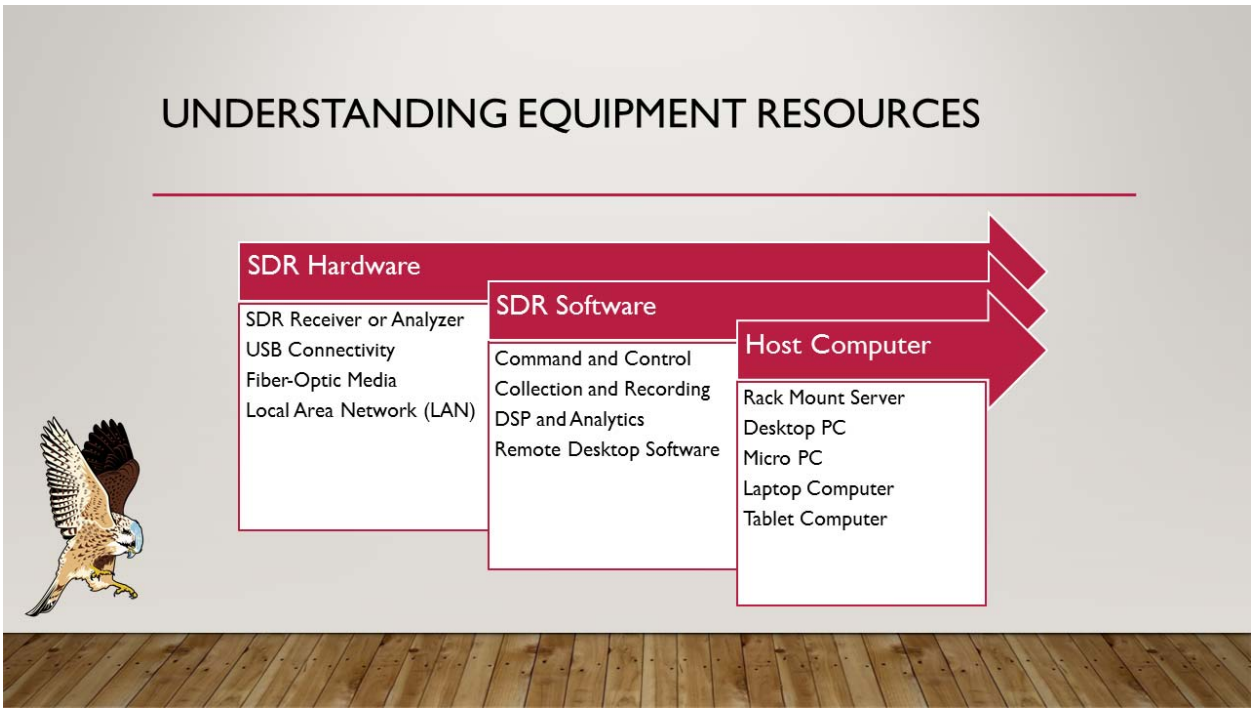
The term < RSSM ™ Sensor > in Kestrel ® terminology, describes and includes a suitable high-speed Software Defined Radio (SDR) receiver, such as the Signal Hound (BB60C) Spectrum Analyzer and RF Recorder, or other supported receiver or analyzer, a suitable collection antenna, such as the KestrelPod I infrastructure ceiling mount | Ultra Wideband Surveillance Antenna, micro-PC (Intel NUC | Core i7), or a suitable laptop or tablet computer to round out the system.

The RSSM ™ system can be configured into a Rapid Deployment Kit (RDK), should transportability be required by the end-user.

Collection antennas can be preinstalled in critical areas and monitoring hardware can be installed and connected quickly at any location on-demand, when the antennas, cabling, LAN or fiber-optic link infrastructure are already installed at the facilities level.

The KestrelPrey III | Advanced RF Locator ™ can be deployed as a low profile walk-about, full featured spectrum analyzer, minimizing the requirement for a separate broadband receiver.

The ability to detect, identify, track, and locate potentially hostile signal events that have been first detected and filtered for investigation by the RSSM ™ system, and easily transition to a familiar user-interface to localize the emitter is vastly more efficient.



Source | Presentation at ERII 2016 Conference | September 2016 | Old Alexandria | Washington

A reliable network connection, consisting of a dedicated DSL, Gigabit LAN, Wi-Fi, or 3G, 4G, LTE Modem is required for remote system communication.

Autonomous operation via an advanced software Activity Scheduler permit receiver level and band level automation programming, allowing the RSSM ™ system to run automatically in a patterned based collection mode, for operator review at a later time, when the site can be safely accessed.

LAN connectivity can be backed-up by a Wi-Fi network roll-over, to provide a measure of fail-safe redundancy.

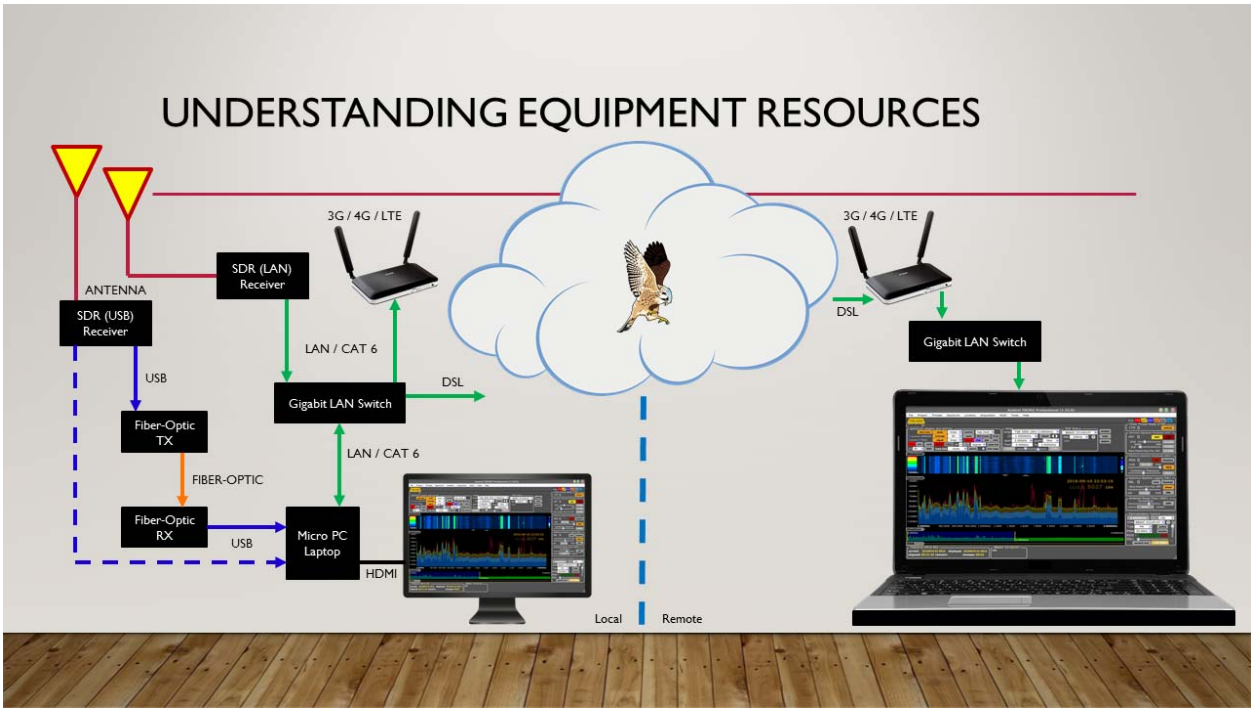
Remote Desktop Software (RDS) | A TeamViewer commercial or corporate licence can provide unlimited remote client connectivity access that allows remote system reboot, remote programming and operation, file transfer, demodulation audio streaming, and full spectral visualization over a secure encrypted connection.

Encryption | TeamViewer includes encryption based on 2048 RSA private / public key exchange and AES (256 bit) session encryption. This technology is based on the same standards as https / SSL and meets today's standards for security. The key exchange also guarantees full, client-to-client data protection. This means that even the TeamViewer routing servers are not able to read the data stream.

Code Signature | All program files are secured using VeriSign code signing technology. This allows you to verify the origin of the executables you have received.

Access Protection | In addition to the Partner ID, TeamViewer generates a session password that changes with every software start in order to provide additional security against unauthorized access to a remote system. Security relevant functions like file transfer require additional, manual confirmation from the remote partner. Also, it is not possible to invisibly control a computer. For data protection reasons, the person sitting at the remote computer has to be able to detect when someone is accessing the machine.

Two-Factor Authentication | Two-factor authentication adds an additional security layer to protect TeamViewer accounts from unauthorized access, with access control through white listing. With two-factor authentication, a code generated on a mobile device is needed, in addition to < username > and < password >, in order to sign in to a TeamViewer account. The code is generated via a time-based, one-time password algorithm. The code is protected by SRP and is thus safe from man in the middle attacks.



Source | Presentation at ERII 2016 Conference | September 2016 | Old Alexandria | Washington

Rapid Deployment Kit (RDK) can be installed virtually anywhere for temporary collection requirements at special events, tactical scenarios, strategic meetings and other application specific deployment, in potentially troublesome areas, and left totally unattended and unmonitored for a period of time, autonomously, to automatically collect and record RF spectrum data for later review by the operator, or accessed remotely for on-demand analysis.

Larger scale RSSM ™ systems may include multiple < RSSM ™ Sensors > across several areas of critical infrastructure, independently or on a shared network infrastructure.

In larger distributed RSSM ™ collection systems, monitoring may be deployed across multiple buildings, multiple sites or geographical regions, or span countries, as required.

Administrative Maintenance

RSSM ™ systems are remotely positioned and require careful planning and implementation, as well as an understanding of remotely maintaining the host computer for peak efficiency and trouble free operation, particularly at potentially inaccessible locations, is critical.

It is essential to ensure that all of the remote system components are powered by an Uninterruptable Power Supply (UPS), for a measure of fail-safe operation.

It is recommended that the technical operator consider a laptop computer and USB 3.0 powered receiver, which can provide a measure of backup power and surge protection, in the event that momentary utility outages occur.

Remember to ensure the Network connectivity is also part of the power backup strategy.

Utilizing a Remote Desktop Software (RDS) that permits remote system host computer reboot, OS maintenance and full system programmability of the system is essential.

Technical Analysis | Kestrel Analytics ™

The most important aspect of continuous RSSM ™ deployment is learning the application of targeted data filtering and event trigger capture, to bring clarity to complex data.

It takes some time to determine the normal ambient RF spectrum environment and some tweaking of the capture process, will likely be required.

> *"Kestrel Analytics ™ significantly enhances the ability of the technical operator to understand the complex spectra data captured, advancing the Probability of Detection (POD)".*
>
> *"Kestrel Analytics ™ brings a powerful new analytical approach to how captured Signals of Interest (SOI) are processed, during real-time analysis, and historical post event review".*
>
> *"The RF spectrum is increasingly complex, and it is often difficult, impossible, or not desirable to extract the actual intelligence, due to type of modulation, use of encryption, or privacy concerns.*
>
> *"Kestrel Analytics ™ looks at the signal analysis problem differently, by processing captured signal level activity against an Analytical Traffic Analysis (ATA) ™ profile, specific to the target area".*

There are a number of important tools that can be utilized to control file management and strategically filter captured data.

The following is a sampling of some of the tools within the Kestrel TSCM ® Professional Software, utilized to condition, characterize, capture, filter and display potentially hostile emissions for operator analysis.

Project Activity Scheduler

- Project Activity Scheduler
  - Receiver level | Start | Stop | capability
  - Spectrum (band) level | Start | Stop | capability
  - Operator defined | Maximum Duration | programmability
  - Unlimited number of operator defined events

Write Compression

- Significantly reduced Kestrel Project File (KPF) storage footprint is realized
- Improved PC memory utilization and system resources prioritization
- Enhanced allocation of host computer system resources
- Clarity and focus of distributed spectral energy profiles
    - Captures (1/n=?) traces as a single Kestrel Super Trace (KST) ™
    - Powerful compression algorithm enhanced Real-Time Event (RTE) and Waterfall Display (WFD)
- Significantly enhanced playback and analysis of normally complex historical data sets is realized when (1/n=?) compression is utilized by the technical operator.

Minimum Detection Amplitude (MDA)

- Triggered threshold | Exceedance | alerting
- Automatic Threat List (ATL) generation
- Manual ATL export to CSV format
- Automatic export of MDA ATL via optional Automatic Export Control (AEC) | OPT AEC |

Dynamic Alert Annunciator (DAA)

- Unlimited operator defined Dynamic Alert zones
- Triggered Exceedance detection
- Triggered Loss detection
- RED (Fail) | GREEN (Pass) Visual Annunciator
- Export DAA data to CSV format
- Real-Time Alert Condition Statistics data display

Automatic Export Control (AEC) | OPT AEC

- Operator defined Periodic Export of any supported trigger
- Provides a measure of Fail-Safe Data Backup
- Operator defined Write Storage location
- Export ALL or Export NEW programmability to CSV format
    - Minimum Detection Amplitude (MDA)
    - Spectrum Baseline Logging (SBL)
    - Dynamic Alert Annunciator (DAA)
- Triggered event CSV Export
    - Export Spectra
    - Export RSSI
    - Export IQ

Automatic Recording Mode (ARM)

- Sustainable Write Storage Management
  - REC Active | ARM Disabled | All data written to storage media
  - Automatic Spectrum Analyzer Mode (SAM) | Data not recorded to storage media
  - Automatic Recording Mode (ARM) | Only triggered event data is recorded
- ARM Mode | Only Dynamic Alert Annunciator (DAA) triggered events are recorded
  - Triggered event recording up to 60 Seconds prior to event appearance
  - Recording of active signal event duration
  - Recording up to 60 Seconds after event termination

Geographical Area Review (GAR) | Historical Data Comparative

The ability to access and import comparative Peak Envelope Capture (PEC) ™ data from other relevant geographically co-located RSSM ™ systems, brings significant value to the analytical process, allowing the technical operator to directly compare historical Kestrel Project File (KPF) ™ data.

This is accomplished utilizing the < Load Compare Bands > feature, to import any available Antenna Collection Location based < Peak Trace > spectral reference data for comparative purposes.

Imported historical data from other Kestrel Project Files (KPF) ™ is persistent within the current file and can be utilized for comparative purposes until removed.

Geographical RSSM Management (GRM)

Kestrel Central Visualizer ™ is yet another powerful tool on the horizon, under active development, in full tactical support of multiple geographically based < RSSM ™ Sensors > on a closed LAN network or across the Kestrel ® cloud (Internet) based infrastructure.

The larger the RSSM ™ system becomes, the more critical data filtering (signal level classification and characterization), and the use of Kestrel Analytics ™ will become.

The use of < Targeted Event Triggering > serves as a powerful data filtering tool when the target area is governed by a wireless policy prohibiting all, or certain types of wireless devices, within a well-defined security zone.

This permits the operator to quickly identify unusual patterns and characteristics within the ambient RF spectrum environment.

However, the issue is arguably more complex when wireless technology is an integral part of the day to day operation, as it is decidedly more difficult to resolve friendly from hostile emitters within defined target areas.

However, trends and patterns in spectral activity will surface over time permitting the operator to identify potentially hostile emitters, separate from those authorized.

Professional Service Level (Recommended)

The recommended service level is based on an entirely new threat model that includes the following approach and Scope of Work (SOW) elements, consistent with the perceived threat level anticipated, or ultimately determined for each organization.

Remote Spectrum Surveillance and Monitoring (RSSM) ™

- Critical Infrastructure (Continuous < 24 / 7 > Monitoring)
  - < Boardrooms > < Executive Office > < Security Zones >

Targeted Ad Hoc (Random Periodic Due-Diligence < 72 H / 120 H / 240 H > Monitoring)

- < Events > < Off-Site Meeting < > Hotel Rooms > < Executive Residence >
- < Off-Site Workers > < Disaster Recovery Sites > < Internal Investigations >
- < Non-Critical Areas >

Power Line Monitoring < Sensor Based >

- Critical Infrastructure (Continuous < 24 / 7 > Monitoring)
  - < Boardrooms > < Executive Office > < Security Zones >
- Targeted Ad Hoc (Periodic < 72 / 120 / 240 > Monitoring)
  - < Events > < Off-Site Meeting < > Hotel Rooms > < Executive Residence >
  - < Off-Site Workers > < Disaster Recovery Sites > < Internal Investigations >
  - < Non-Critical Areas >

Threat Considerations < Device Type >

The following threat probabilities describe the < type > < characteristics > that may be associated with the potential compromise.

- Analog (Audio) Transmitter | Probability | High-Threat
  - Presence of Remote Control | Medium-Threat

- Digital (Audio) Transmitter| Probability | High-Threat
  - Presence of Remote Control | High-Threat
  - Complex Modulation | High-Threat
  - Encryption | Medium-Threat
  - Anti-Detection Capability | Medium-Threat

- Digital Audio Recorder | Probability | High-Threat
  - High Compression Codec | Probability | High-Threat
  - Encryption | Probability | High-Threat
  - Presence of WI-FI or Bluetooth | Probability | High-Threat

- Broadband Over Powerline (BPL) | Probability | High-Threat
  - Presence of Multiple Nodes | Probability | High-Threat
  - Presence of < Data > < Video > < Audio > | Probability | High-Threat
  - Encrypted Data | Probability | Probability | High-Threat

- Analog | Power Line Carrier (PLC) | Probability | Medium-Threat
  - Presence of < Audio > < Signalling > | Probability | High-Threat

- Digital | Power Line Carrier (PLC) | Probability | Medium-Threat
  - Presence of < Audio > < Signalling > | Probability | High-Threat

- Optical | Visible Light Communication (VLC) | Probability | Medium-Threat
  - Presence of < Data > < Audio > | Probability | Medium-Threat
  - Use of Hybrid Technology | Probability | Low-Threat

- Optical | Infrared | Probability | Low-Threat
  - Presence of < Audio > | Probability | High-Threat

- Analog (Video) Transmitter | Probability | High-Threat
  - Presence of Embedded Audio Sub-Carrier | Probability | High-Threat

- Digital (Video) Transmitter | Probability | High-Threat
  - Presence of Embedded Audio Sub-Carrier | Probability | High-Threat

Traditional Inspection | Deployment (Mandatory)

- Periodic RF Spectrum Analysis "Snap-Shot" Localized Inspections (Critical Infrastructure)
  - Technical Security (TSEC) value is limited to < Live Event > monitoring
  - RSSM ™ direct data comparative (Strongly Recommended)
- Power Line Analysis "Snap-Shot" randomized inspections (Critical Infrastructure)
  - Technical Security (TSEC) value is limited to < Live Event > Monitoring
  - RSSM ™ direct data comparative (Strongly Recommended)

Additional Inspection Priorities (Not All Inclusive) | Beyond RF

The following information is offered as additional related inspection parameters that must be considered along with the Radio Frequency (RF) collection and analysis. It is by no means inclusive and other professional protocols are required to round out a detailed technical inspection.

Physical Inspection Protocol | There are some aspects of a Technical Security (TSEC) program that require the operator to periodically access the target area for the purpose of completing a detailed physical inspection.

It is strongly recommended that a formal physical inspection protocol be initiated on a periodic basis as a due-diligence practice, and immediately prior to, and after any sensitive meetings or event that are scheduled to take place within protected areas of the facility.

When the Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™ is the primary collection method, it will become necessary to provide the base training for an on-site individual to conduct periodic physical walk-through inspections of the target area.

Counter-Intelligence Review | Human factor elements are generally the most significant threats to the in-house protection of proprietary information.

The vast majority of vulnerability findings are not electronic in nature, but rather insider threats and human factor compromises.

The RSSM ™ concept is designed to effectively hunt Radio Frequency (RF) emitters, which must be supplemented by a carefully, periodic TSCM physical security inspection protocol.

The CI review looks at the facility from a people-flow perspective, looking at how sensitive information is processed, handled, stored, and utilized, both on-site and off-site.

A review of garbage and recycling practices, and base level penetration testing is required to determine the security posture of the facility.

Thermal Imaging | The application of a thermal imaging review of the target area, can quickly identify pinhole cameras and other similar powered devices, emitting thermal properties.

However, devices, such as those that may be buried inside walls or other cavities can often be identified, even when they are not powered, utilizing a thermal imager, as there will potentially be a significant differential in temperature of a device against the ambient background temperature, due to air-flowing across different types of materials inside a wall or other structure.

It will often be necessary to thermally condition the target area and thermally tune the radiograph image, to gain the most benefit.

Non-Linear Junction Detection | An NLJD is a very powerful TSCM equipment resource, yet it is just one more tool utilized to examine the target area.

There has unfortunately been considerable hype in the past few number of years, as to which technology is better, generally from a non-objective sales perspective, and certainly not from the perspective of an experienced field operator.

The industry standard was at or below 900 MHz and newer technology, extended into the 2400 MHz (and higher) transmit range.

The push to move to the 2400 MHz was recognized early by our Technical Research and Standards Group (TRSG) that 2400 MHz was not capable of detecting all technical threats, just like the 900 MHz NLJD was not capable of detecting all threats.

Every type of application and structure is different and it is absolutely essential that operators maintain competing technologies.

At least two NLJD manufacturers have now introduced additional 900 MHz products back into the market with updated technology.

It is for this reason that professional level technical operators maintain competing technologies and ignore the marketing hype.

The most important aspect of any equipment resource, is that the operator must deploy a range of competing technologies, and never rely on any one technology, expecting conclusive results.

Active (Wired) Microphone Identification | The threat of wired microphones is significant within a modern and perhaps one of the more challenging aspects of a technical inspection.

Wired microphones may be found on virtually any unused wire pair entering or leaving the target area and may or may not contain local side amplification.

Fiber-Optic (Microphone) Technology | The threat of fiber-optic technology has become a serious threat within a modern threat model has more and more fiber-optic technology has entered the consumer and commercial market.

The ability of the technical operator to first understand the level of adversary likely encountered is a function of understanding the perceived threat level faced by the client.

External (Infrared) Laser Interception | The technology remains a valid concern in a modern threat model, however, it is not a strong contender on the economic espionage stage, given significant limitations.

The presence of optical threats is relatively easy to detect and identify the source, whenever the technology is active.

The method is passive in nature and no intrusion into the target area is required.

Obviously, this method would require a clear optical path into the target area, such as a window or a reflective object within the target area.

High Speed Video (Audio) Interception | A relatively recent discovery is the ability to recover target area audio by use to high-speed video capture.

This capability only requires visual access into the target, a high speed camera and a computer based algorithm, so the system is totally passive in nature.

Telephone Network Analysis | The examination of the telephone network is complex and time consuming.

There is no one equipment resource to accomplish this task across all of the different technologies and network equipment currently in use.

There are a number of excellent resources available that are utilized extensively across the telecommunication industry that deliver excellent results.

Computer Network Analysis | Like the telephone network in many ways, the computer network is complex and requires very specialized examination, at both the physical and forensic level.

Physical inspection is generally the easy part of the inspection, and experience indicates that the vast majority of vulnerabilities and discovered compromises can be identified by a strong physical inspection protocol, and the application of solid RF Spectrum Analysis protocols.