Paul D Turner explains why a new moving target threat model requires a modernised approach to TSCM

REMOTE SPECTRUM AND MONITORING

Software Defined Radio (SDR) permits operator-assisted TSCM inspections to be conducted based on a new moving target threat model that is specific to the operational deployment of a budget-friendly, fully featured operator assisted, or Remote Spectrum Surveillance and Monitoring (RSSM).

The following observations were gleaned from Glenn H. Whidden's book, *The Russian Eavesdropping Threat – Late 1993*. Glenn reveals an important observation that proves timely, in a modern threat environment, and echoes across various chapters 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, and this is a concept we teach during training and discuss with our clients. This message is as timely today in 2017 as it was leading up to 1993 and is the core foundation of the principle behind RSSM deployment.

None of the Russian devices described in Glenn's book, would have avoided detection if 24/7 active defensive countermeasures were actively deployed.

SURVEILLANCE

> **RSSM systems can involve a single area of critical infrastructure such as a boardroom or executive office of up to approximately 5000 square feet"**

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 hostile emitter. Another notable observation derived from Glenn's book is that an attacker might deploy any number of anti-detection strategies, taking equipment limitations and human factors into account – placing a hostile device in a difficult to access or difficult to verify location can easily defeat defensive countermeasures.

Less motivated operators might rule out in error certain possibilities as not practical for the attacker, or might not be able to sweep certain areas due to accessibility, equipment limitations or heavy furniture that can't be easily moved.

RSSM requires that the operator understand that economic-espionage has taken a dramatic turn during the past decade, as changes in how corporations and governments do business, and has opened the flood gates of opportunity, driven by aggressive state-sponsored players. Individual offices have been replaced with trendy *ad hoc* shared work spaces, increasing the potential for inadvertent disclosure of information, from an insider threat and espionage activities. Executives are integrating themselves into these areas under an open-door policy, placing the organisation at a greater risk of compromise of competitive-intelligence and economic-espionage.

Corporate executives wouldn't ever consider turning off the company firewall or anti-virus system at the end of the day, but few organisations take the threat of economic-espionage seriously, as is evident by the randomness and periodic nature that TSCM services are requested and delivered.

The reality is that it takes strong industry leadership, a modern approach and powerful tools such as RSSM to replace obsolete periodic RF spectrum analysis techniques that are still being utilised by many technical operators.

The nature of modern Radio Frequency (RF) threats changes on a daily basis requiring intelligent, adaptive search technology that's similar to the heuristic capability of modern anti-virus software to look for threats which may not have been seen in the past. You cannot detect or identify a threat of which you are unaware, or have no 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.

Approximately 95 percent of operators surveyed are conducting "snap-shot" style sweeps, believing the POD is reasonably close to 100 percent (a concept often proposed by equipment manufacturers, referring to the sweep speed and other factors), and operators convince the end-user that this is the case, when in-fact, it is not possible without carrying out 24/7 monitoring.

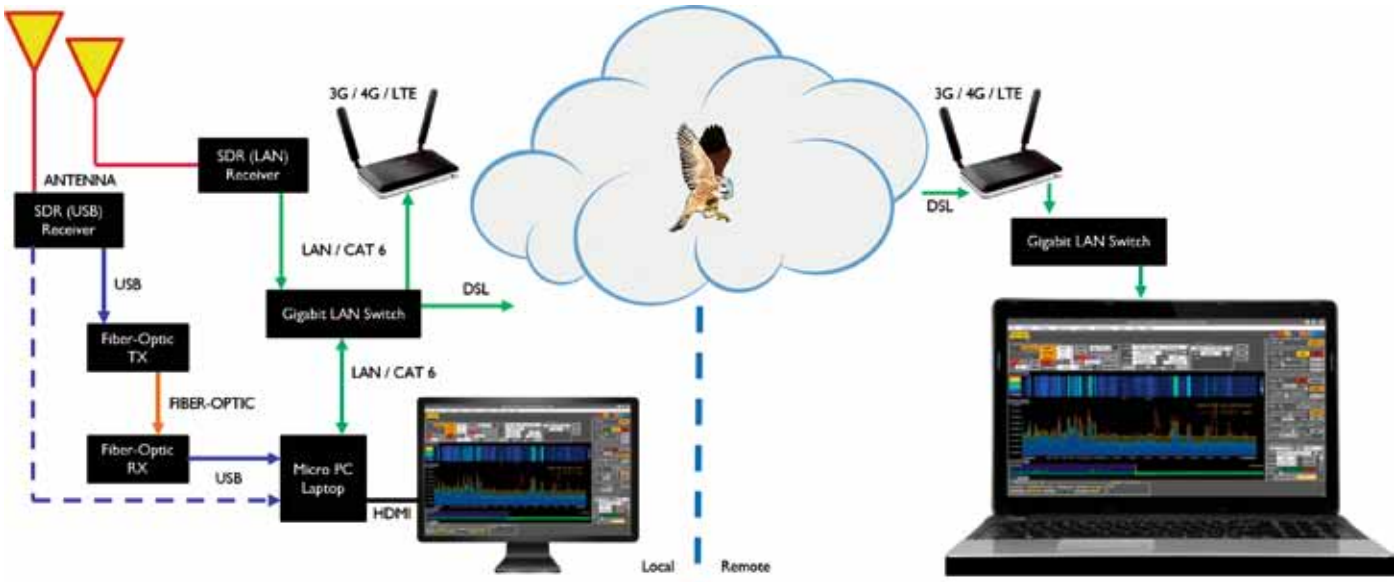
What operators often fail to understand is that even an experienced and competent RF spectrum analysis conducted with the right equipment and the correct approach for a period of eight hours a month every 12 months adds up to one percent over the course of a year when RSSM is not utilised. The average "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 for their clients.

How do operators know what they don't know? When any resource is deployed for example, for one hour, and the resource is in-fact capable of 100 percent POD, and the operator has the experience to identify a hostile event from the many ambient RF signals, I guess one could argue that the POD is 100 percent, but this is only true for the actual deployment time of – in this example – one hour, and this is where most operators miss the point completely regarding POD.

Understanding the modern moving target threat model is the first step in providing an adequate level of service for the end-user, and ultimately delivering an effective program based on the perceived threat level and meeting the objective of mitigating risk and liability. Educating the end-user is essential, to understanding the Cost versus Return expectations which includes the fact that the ineffective engagement of the wrong services at the wrong time increases the potential for a compromise to go undetected. The "You don't know 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 TSCM services to unsuspecting end-users.

Many operators claim their equipment has a 100 percent POD based on sweep speed alone, yet fail to understand that 100 percent POD for the typical

REMOTE SPECTRUM SURVEILLANCE AND MONITORING



deployment of 40 hours of actual "time-on-target", out of 8,760 hours (based on 365 days at 24 hours) annually is just 0.5 percent POD from a modern moving target threat model perspective, and clearly fails to meet an acceptable due-diligence standard!

"Time-on-Target" is a critical factor in determining the POD from a deployment perspective and the operator needs to look at the big picture and this is – or should be – an incentive to change the way TSCM services are delivered, and presented to the end-user.

The means of this transformation is found in the core foundation of Software Defined Radio (SDR) applications such as the Kestrel TSCM Professional Software, which are based on entirely new technically feasible, budget-friendly, threat models that include the application of RSSM, possible due to recent acceleration in SDR technology.

Economic-espionage is rarely identified in real-time and requires a lot of data and additional intelligence collection over a period of time to develop accurate threat modelling and trends. 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.

POD is only part of the risk mitigation picture, with the next logical questions being: "What is the perceived threat level for the organisation?" and "What level of risk is the organisation willing to accept?"

There is a realistic trade-off between, Risk Mitigation versus Budget that the end-user rarely understands due to the lack of factual information surrounding successful acts of economic-espionage, and the few that are discovered, and this leaves the more common competitive-intelligence and vast majority of economic-espionage cases under the radar.

The modern threat environment includes the reality of on-demand transmitter remote devices, store and forward technology or devices that actively disguise themselves by modulation type or anti-detection characteristics. Without 24/7 RSSM deployment, the identification of hostile emitters cannot with reasonable certainty be identified except by chance when only periodic "snap-shot" style collection is utilised.

The ability of RSSM to capture real-time analytical data allows the operator to identify hostile signal events in real-time, on-demand or to observe trends over a period of time. But that's not the only tactical advantage, RSSM is a cost effective, budget friendly solution that is fully scalable as requirements change; significantly enhanced POD is realised over periodic "Snap-Shot" style RF sweeps; RSSM captures the RF spectrum, even when the technical operator is not present and it permits the operator to monitor multiple collection sites in real-time or as historical data.

Detection Methodology, meanwhile, must include 24/7 capture for critical infrastructure, the capture of continuous spectra provides for real-time and post analytical review, event filtering and flagging of spectra events facilitates, streamlined operator review.

RSSM systems can involve a single area of critical infrastructure such as a boardroom or executive office of up to approximately 5000 square feet, depending on occupancy and structural configuration. Larger distributed RSSM collection systems may be deployed across multiple buildings, sites or geographical regions and can even span several countries. The ability to detect, identify, track, and locate hostile emitters, first detected and filtered for review by the RSSM system, can easily transition to a low-profile tablet computer with a familiar user-interface to localise the emitter, minimising the requirement for additional resources.

In conclusion, then, RSSM is ideal for temporary collection for special events, tactical scenarios, strategic meetings and application-specific deployment, left unattended for a period of time autonomously to collect and record the spectrum and accessed remotely for on-demand analysis by the operator.

Paul D Turner TSS TSI is CEO, Technical Security Specialist and Technical Security Instructor at Professional Development TSCM Group Inc. He has 37 years of experience, in delivering TSCM services to corporate, government, law-enforcement, and military clients worldwide, including certification training, and the development of the Kestrel TSCM Professional Software.