REMOTE CONTROL

Paul D Turner *reveals the significance of Remote Spectrum Surveillance and Monitoring in part two of his TSCM series*

There is a relatively simple answer to dramatically improving both the Probability of Detection (POD) and the Probability of Intercept (POI) from a TSCM perspective.

What you don't know; you don't know and therefore, you cannot build an effective strategy to detect, identify and neutralise real-world technical compromises without meaningful analytical spectrum data in the hands of a qualified technical operator or analyst.

This thought process explains why economic-espionage is rarely identified and organisations continue to remain increasingly vulnerable to a technical compromise, costing millions of dollars annually in lost opportunity, across Canada, Australia, New Zealand, the United Kingdom and United States.

RSSM captures, monitors and reports the occurrence of significant spectral events within the ambient RF spectrum, even when the technical operator is not present; autonomously, without the need for operator intervention for days, weeks or months.

This industry-recognised strategy is accomplished through the application of managed Remote Spectrum Surveillance and Monitoring (RSSM) of the ambient Radio-Frequency (RF) spectrum and the facility electrical power grid, all on a 24/7, 365 days-a-year basis, or as a more informal, targeted supplemental extension for monthly, quarterly and/or annually administered Technical Surveillance Countermeasures (TSCM) site inspections.

In reality, this methodology has only existed in practical terms for the past decade, particularly within the private sector, mostly due to the prohibitive cost of the hardware resources and software required.

This is where Software Defined Radio (SDR) has played a tremendous role in the development of low-cost hardware and sophisticated standards-based software applications that fully benefit recent technological hardware innovation.

Technology in SDR hardware is accelerating in receiver sensitivity, dynamic range, real-time bandwidth and search speed

Highly focused SDR applications are now able to bring real-world technical operator experience and advanced software engineering together for the first time, to develop a new class of software architecture that addresses the day-to-day emergence of new threat technology.

Economic-espionage is rarely identified in real-time, based on a single defensive technology, method or technique. It takes a lot of validated technical data and other experience-based intelligence collected over a substantial period of time to develop accurate threat modelling.

During the past decade we have been witness to an industry-wide, disruptive development cycle of progressively advancing new SDR hardware that is well suited and more importantly, specifically designed for the detection, identification and analysis of modern wireless threat technology from a TSCM perspective.

SWEEPING CHANGES

This has opened the door for the development of advanced TSCM-specific, operator-centric software that advantages the required widening search bandwidths and even more importantly, the dramatic improvements in real-time IF bandwidths and search speed at the hardware level. The professional operator, now has the ability to see, observe, capture and analyse complex spectrum events that only a few years ago would have been missed entirely by the hardware and the vast majority of wideband TSCM-oriented spectrum analyser software.

We now see and expect working search speeds that meet or exceed the latest industry standards of 1THz as an acceptable threshold across at least 20GHz of active spectrum with up to 160MHz of real-time bandwidth, offering improved POI and a range of other advantages.

Consider for a moment the ITU Region 2 DECT 6.0 band (1,920MHz to 1,930MHz), consisting of 10MHz of bandwidth, swept at 30kHz RBW. We can achieve the awesome ability to sweep the DECT 6.0 band at approximately 3,280FPS, or 32.8GHz per second, providing a real-world POI of approximately 304.7uSec.

This POI calculation takes into account the sweep process, FFT data processing, CPU loading, memory allocation and write speed of the storage media.

Taking this to the next level, a sweep of the full hardware range of 20GHz of bandwidth @ 30kHz RBW for this particular radio, we realise a sweep rate of approximately 57.8FPS or 1,152GHz per second, providing a real-world POI of just 17mSec across the entire 20GHz of bandwidth.

There are a number of different factors that determine the technical operator's ability to detect, identify and confirm that any given signal event is either friendly or hostile in nature.

The first consideration is that a potentially hostile signal event must be present during the RF capture process. This is why when too few electronic sweep inspections are conducted, the opportunity for detection is minimised and the attacker's chances of a successfully undetected compromise is maximised.

This is where the subject of managed Remote Spectrum Surveillance and Monitoring takes on an entirely new focus in a modern moving target threat model. The ability to capture virtually all of the ambient RF spectrum, essentially turns an obsolete point-in-time snap-shot into panoramic high-definition analytical spectral experience.

The main aspect of continuous spectrum capture is that the operator has an opportunity to see complex, random, intermittent and periodic signal event patterns that would not be identified during a point-in-time snapshot.

The ability to use advanced software features, such as time and location filtering, bring order to a complex ambient RF spectrum. There may be a single short duration hostile burst event lurking alongside thousands of ambient friendly signals.

The combination of radio search speed, operational search bandwidth and actual deployment time all work together to make it possible for the technical operator to see the unseen.

Many operators are called to service, based on a panic scenario from an end-user, who offers little time-on-target, is in a rush to get the job done, provides little or no preparation time, fails to disclose all the facts leading to the inspection request and has expectations of a 100 percent POD at the end of the assignment.

ALL BUSINESSES NEED TO HAVE A FORMAL, SCALABLE TSCM PROGRAMME IN PLACE

Most professional attackers that engage in economic or state sponsored-espionage attacks are more than aware that the majority of organisations, pubic and private sector alike, do not provide adequate budgets, or time-on-target to be able to satisfy minimum due-diligence requirements, assuming that they engage in defensive countermeasures at all!

Managed RSSM is the only way to overcome the severe limitations imposed on the operator by way of limited budget, limited time-on-target and the potential sophistication of by design modern threat technology.

Modern SDR hardware and software are now available to harness and manage not only long-term RF collection, but also accommodate continuous power grid surveillance within a highly scalable platform.

The electrical power grid is the one network communication path in virtually every facility that does not have a firewall. The RSSM architecture addresses this by adding a dedicated radio to baseline and monitor hostile energy utilising the facility level and utility-side power grid as a hostile communication path.

The typical RSSM platform, targets critical infrastructures such as executive offices, boardrooms, conference rooms, engineering and R&D areas, *etc.* using easily reconfigurable and scalable resources to protect a single office, an entire building or multiple buildings on a large business campus.

The ability to deploy across large geographical areas is also possible, protecting military bases, airports, hospitals, colleges and universities, corporate interests, law-enforcement, Government facilities, correctional intuitions and the national security apparatus.

RSSM deployment can significantly enhance the Probability of Detection (POD), from below one percent up to 90+ percent utilising relatively low-cost components.

It is not possible to detect, identify or locate a threat of which you are unaware or have no technical data or intelligence 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.

The threat of economic state-sponsored espionage and illegal forms of competitive intelligence gathering is an invisible and insidious activity that includes insider attacks, employee dishonesty or carelessness.

More C-Level attention is required rather than a reluctant approach to justify, little more than a modest annual budget, compared with other financial obligations and requirements at the corporate level.

Economic-espionage effects all business types, and all businesses need to have a formal, scalable TSCM programme in place that is objective and free of the internal corporate culture trap. TSCM is not a do it yourself project!

MIND THE GAPS

Without consistent uninterrupted data collection, gaps of unknown certainty will exist, reducing the POD significantly and this in turn advances the potential and opportunity for undetected economic-espionage to occur.

Every two hours of daily, of missed data collection (annually averaged) results in an eight percent chance of failing to detect or identify a targeted incident of espionage, based on the presence of an RF eavesdropping device.

The typical RSSM system consists of a single radio, antenna and software running on a laptop computer, and is easily scalable to include additional radios for expanded RF and Power Line (PLC/BPL) monitoring, as requirements change. Radios can be easily remoted standalone or on a dedicated LAN converter or multimode fiber-optic remote. SDR hardware connectivity may be USB 3.0, Gigabit LAN or Gigabit fiber-optic termination. Low-cost hardware-based communication media converters allow sensors to be placed virtually anywhere, as required.

There are a number of hardware manufacturer's worldwide, each with advantages and disadvantages when determining the best hardware for the intended purpose, from connection type, search bandwidth, search speed, power requirements, supported software and ultimately the cost.

Distributed RF platforms deployed in an RSSM role open the door for new revenue streams and greater efficiencies in surfacing hostile or unknown signal events that must be resolved by the operator.

TSCM software is the controlling factor in bringing all of the system components together to form a powerful RSSM platform and place the operator back in control of the mission and the analytical process. It is the features and functionality that define the collection process, but it is the operator that ultimately defines the successful identification of any given RF threat. The operator is the spectrum analyser and renders judgement on every unknown signal event captured and identified at the hardware and software level as potentially hostile.

In conclusion, a properly administered Technical Surveillance Countermeasures programme combined with managed Remote Spectrum Surveillance and Monitoring is a critical factor in mitigating loss, compromise and the associated liability of not taking the appropriate due-diligence steps to adequately protect your organisation against the growing global threat environment ●

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 40 years' experience in providing advanced 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.

The complexity of the fiber-optic and CAT 6e infrastructure cabling typical of corporate and Government facilities explains why the vast majority of TSCM network analysers are rendered useless

Picture credit: Professional Development TSCM Group Inc.