Picture credit: US Dept Defense

SIGINT versus TSCM

Paul D Turner *advances the art and science of the SIGINT/TSCM role*

During the past decade, technology advancements have shaped the software-defined radio environment within a Signals Intelligence (SIGINT) and Technical Surveillance Countermeasures (TSCM) role. SIGINT/TSCM have seen industry disruptive advancements at the hardware and software level with algorithmic coding to address technical challenges. A combination of hardware and algorithm development has proven to be directly responsible for emerging mission-critical capability.

This capability includes the subsets that directly aid the operator and the analyst with the detection, capture, collection, correlation, analysis, interpretation, reporting, and dissemination of reliable and strategically relevant over-the-air RF intelligence.

SIGINT is not a static deployment option and involves, fixed, mobile, UAV, airborne, marine, foreign deployment, satellite operations, tactical over-watch and remote intercept, within a live operator, linguist and analyst set of mission requirements; or an autonomous intercept process with limited operator intervention, and is different from a Technical Surveillance Countermeasures (TSCM) role. The SIGINT/TSCM roles are surprisingly similar within a standards-based work-flow and share similarities in approach.

SIGINT, ELINT, COMINT and TSCM all share common core capabilities with differing objectives and outcome expectations, across commercial, government, law-enforcement and intelligence roles. SIGINT is a primary umbrella function, while ELINT and COMINT fall under the SIGINT umbrella as specific mission-critical requirements. TSCM mission objectives are fast merging with the SIGINT role, and the SIGINT role is fast merging with a traditional TSCM role, that includes radio-frequency, optical spectrum, power line and acoustical mission components. There are, however, differences between, SIGINT/TSCM role, from a software development and operational deployment context, that need to be understood by the spectrum warrior.

SIGINT/TSCM share the same Real-Time Spectrum Analysis (RTSA) technology requirements, but it is here

Modern threat-actors are highly aggressive, surprisingly overt and attack with multiple attack postures

where both meet a fork in the road. TSCM is strongly aligned with the deterrence, detection and prevention of economic-espionage within a commercial environment; but is quickly emerging at the national security level, tackling more sophisticated and highly motivated state-sponsored threat actors engaged in espionage trade-craft.

We are no longer dealing with an invisible Cold War-era threat actor! Modern threat-actors are highly-aggressive, surprisingly overt, and attack with multiple attack postures; openly compromising any identified vulnerabilities using a technical or social engineering attack posture that is persistent on many levels. It only takes a single successful compromise for the attack to be effective.

The SIGINT umbrella includes Electronic Intelligence (ELINT), the detection of sensor-based emissions from non-intelligence bearing signals, providing traffic analysis, TEMPEST evaluation, enemy position and strength, estimation of resources and state of readiness, *etc*.

Communications Intelligence (COMINT) is the function of tactical intercept and extraction of intelligence-bearing communication-related emissions, and will include a multi-layer approach across an operator, linguist, and analyst. SIGINT/TSCM are a defined as a function of the respective roles. If we start with a competent TSCM-SDR focused application; port all of the key features across to a SIGINT application, we have a starting point to examine unique SIGINT features in detail.

Key SIGINT features must include a powerful Advanced Project Management (APM) resource, that extends far beyond the realised project management requirements needed with a TSCM context.

Advanced Radio Recovery (AAR) technology adds a measurable layer of flexibility and scalability, allowing for significant reliability and redundancy; with self-healing, automatic radio recovery at the system level without the need to stop or restart the collection process.

Hot swap radio technology, cold start radio replacement, selective radio type conformity; with interoperability across multiple radio types, multiple collection sites, multiple country operations, multiple signal analysts and multiple intelligence sector stake-holders, requires a well-balanced and coordinated technology approach.

The most important element in today's modern SIGINT platform is a powerful FFT based demodulation capability that includes innovative analogue, frequency domain, time and audio windows. The system must provide a Digital Signal Protocol Visualiser (DSPV) technology.

A DSPV sub-system is often integrated with an artificial-intelligence engine and machine learning capability for a deep dig into the signal-level spectrum for the recovery and exploitation of actionable RF intelligence.

The demodulation of complex signals is focused on an outward look at the signal's spectral envelope and not extraction of intelligence-bearing information, aside from the ability to demodulate, study waveforms and record an IQ sample.

The ability to decode signals and look inside the signal's envelope allows the analyst to demodulate, visualise, remove encryption, decode, determine the modulation type and extract vital intelligence. This separates the SIGINT/TSCM roles; as it is generally not a requirement to decode and extract intelligence within a TSCM role, but rather identify, locate and neutralise hostile emitters as the primary focus.

Automatic and autonomous direction-finding techniques differ across the SIGINT/TSCM role. A sophisticated approach is required within a SIGINT environment for large area augmentation of direction-finding signals that may involve a 3D battleground with detection across airborne, marine and land-based resources. Direction finding resources advantage modern SDR sensory-based technology that includes, Angle of Arrival (AOA) and Time Difference of Arrival (TDOA).

TSCM operators deploy in a relatively small area using Relative Signal Strength Indication (RSSI) and dimensional geo-location heat mapping algorithms, such as gaussian, inverse-square and free space power loss calculations.

AOA platforms within a SIGINT environment are harder to implement than TDOA that require minimal calibration. AOA requires a complex antenna array to determine direction of arrival of a signal across collection sites and does not require clock synchronisation.

TDOA direction-finding determines the emitter location by using the time difference of the received signal across three or more collection stations. TDOA requires clock synchronisation across the radio network.

Detection of real-world signals is the gateway to understanding how a SIGINT deployed SDR detects

SPECTRUM SIGNAL ANALYTICS REQUIRE CONSIDERABLE COMPUTING POWER

traditional and emerging over-the-air signals; including narrowband, wideband, intermittent, short-duration, pulse and burst emissions, across analogue and digital, frequency and time domain modulation standards.

The detection of signals, sets a positive pathway for high-accuracy and reliability for SIGINT/TSCM platforms across a range of commercial, government and military-intelligence applications, within a challenging mission-critical signal environment.

SDR hardware sweeps at high-speeds to maximise the Probability of Intercept (POI), across 40GHz or more, as a working standard.

The ability to upgrade SIGINT/TSCM platforms in the field and manage firmware, as new threat technology is identified or anticipated, to address emerging threat technology without replacing the entire platform is essential. The ability to update system individual components prevents the platform becoming obsolete too quickly relative to a narrowing expected life-cycle, including the threat detection software.

Without a means to aggressively field maintain SIGINT/TSCM platforms with new features and methodology across a life-cycle of three to five years, we see single-box systems become less-effective and require replacement, on a 12-to-18-month life-cycle.

This architecture better facilitates the analysis of new signal types and modulation standards, and adds new classification datasets, significantly extending the useful deployment life-cycle of the collection platform.

Life-cycle relevance has changed during the past decade with real-time push technology updates at the system level, combined with low-cost hardware options. The hardware is keeping up with the wireless sector and an equally challenging threat environment.

Real-time spectrum analyser hardware is the central component on which SDR development is possible; now embraced by nearly all SIGINT/TSCM stake-holders.

SIGINT/TSCM platforms, include powerful SDR-RTSA mission critical hardware used to detect, capture, process, store and analyse the ambient radio-frequency environment, as an operator assisted or fully autonomous resource with the aid of powerful hardware-based Application Programming Interface (API) technology.

This integration is used to tame the radio-frequency spectrum to a human and machine interpretive platform,

SIGINT/TSCM SHARE THE SAME REAL-TIME SPECTRUM ANALYSIS REQUIREMENTS

by maximising the detection of faint, low-powered, short-duration; and infrequent signals across an increasingly more challenging and fast-moving mobile and fixed collection environment.

The inclusion and support of GNSS-GPS and passive accelerometer technology – within today's modern and highly mobile SIGINT/TSCM platforms – with support for single and multiple independent, internal (hardware) or external (independent receiver) global positioning hardware provides accurate timing, clock discipline, time synchronisation, precise horizontal and vertical positioning in support of AOA / TDOA, and within a dimensional geo-location heat mapping, Total Energy Capture (TEC) environment.

A core requirement of SIGINT/TSCM platforms is the ability to deploy remotely with intuitive signal event triggering, within a continuous spectrum monitoring cycle, as a standards-based Remote Spectrum Surveillance and Monitoring (RSSM) environment.

The importance of continuous monitoring autonomously, or semi-autonomous level, requires an understanding of Probability of Detection (POD) by the numbers, as a starting point in mission integrity and sustainability. This new standards-based approach to examining POI / POD is beyond the obvious RTSA hardware connotations that can cloud reality.

There are 8,760 hours in a year, and if we deploy a SIGINT/TSCM oriented collection platform 2,190 hours annually, our anticipated POD is just 25 percent; if we deploy 4,380 hours annually, our realised POD is just 50 percent, and there are other variables that must be considered, including deployment at the right time and right place, together with well-considered equipment resources, and a competent operator strategy. Ask yourself how many hours you actively field deploy and do the maths!

Integration and interoperability with third-party software modules within the SIGINT/TSCM focus is another standards-based capability. Interoperability, open file formats and a powerful API-SDK help to stimulate innovation, and allows extended software support with strong mission-oriented integration with third-party software. It also provides building blocks for mission-critical deployment applications in support of advanced capabilities beyond the total sum of the system components.

Enhanced computer processing is required and not available on the vast majority of SIGINT/TSCM oriented spectrum analysers; realising more limitations than actual capability. Spectrum signal analytics require considerable computing power only found on systems that separate the components into software, computer processing hardware, radio hardware and antennas. Powerful processing optimises the operator's ability to run multiple instances of modern high-speed collection hardware to extract and process intelligence-bearing information from deep within the intercepted signal, in real-time.

The ability to record the In-Phase/Quadrature (IQ) data; rather than looking at the limited peak signal envelope, up to the maximum hardware bandwidth of at least 40MHz, is essential. The controller and radio hardware collectively enhance the performance and flexibility required by SIGINT/TSCM operators who deploy against a highly advanced threat actor ●

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 44 years' experience in providing advanced operator certification training, delivery of TSCM services worldwide and development of the Kestrel TSCM Professional Software. He also manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.

It is generally not a requirement to decode and extract intelligence within a TSCM role, but rather identify, locate and neutralise hostile emitters as the primary focus

Picture credit: US Dept Defense