RADIO FREQUENCY INTERCEPT

Paul D Turner *explores the symmetrical 360-degree logic, beginning with the threat actor, the professional spectrum warrior and the role of the technical analyst*

The almost over-whelming increase and persistence; not to mention the aggressive nature of state-sponsored threat actors involved in espionage tradecraft and insidious intelligence-gathering efforts across the free world, is a growing concern. All industry sectors; government, law-enforcement, military and national security entities are being infiltrated and attacked from within, under a barrage of continuous attack posturing using multiple methods.

Law-enforcement in particular is being discredited by the same threat actors who spread false, misinformation and activist views across social media channels, all under the banner of so-called free speech, as a megaphone to the masses. The definition of espionage has not kept pace with the reality of new threat actor attack methods; with a shift, and significant variations in tradecraft, for which industry stake-holders have failed to adequately respond to with an updated methodology. Modern threat actors have everything in common with historical forms of espionage, sabotage, infiltration, and the capacity to undermine and bring havoc to the sanctity of democracy, however, thankfully new tactics, methods, tradecraft and the players themselves have evolved.

Social media has become a powerful influence of legitimate information and unfortunately disinformation! A new and very destructive insider class of threat actors has evolved, which no longer needs to infiltrate the society or way of life they wish to destroy. The need to refocus and sharpen the skills of the professional spectrum warrior, therefore, must take on a new approach to every aspect of the role they play in effectively conducting Technical Surveillance Counter Measures (TSCM) inspections.

New and emerging threat technology has mandated the introduction of a standards-based, focused and balanced approach to Technical Surveillance Counter Measures from the ground up.

It is essential that a structured approach and an entirely different perspective be taken, as part of a modern moving target threat model and risk assessment strategy. There are many aspects of the TSCM inspection process; starting from a position of risk assessment and management, to the rigors of a competent physical inspection, and a demanding radio-frequency, total energy capture requirement.

Total Energy Capture (TCP) is the only modern method of accurately identifying all active emitters within the Operator Defined Target Area (ODTA), and into the extended Functional Target Area (FTA) to capture threat relevant radio-frequency spectra.

Private sector operators are often slow to respond; however, public sector technical security teams are at even greater risk; the higher the classification food chain, the more likely the road to change is virtually non-existent. The ability to hide behind plausible-deniability; a disclose nothing mandate under the banner of classification, and a practice of drinking the cool-aid when it comes to procurement of resources and certification training, results in a progressive erosion of the capability of the entire team or entity.

Corporate boardroom, government offices, military battleground, or within a counter-intelligence, counter-espionage national security role; radio-frequency intercept and signal analysis is a growing national security concern worldwide. Yes, it is all about perspective! The process is only as good as its component elements that include a coordinated effort across a 'winner takes-all' high-stakes game of espionage.

Equipment resources and the technical operator must work in parallel to beat a cunning threat actor, by not only understanding the threat, but utilising defensive and offensive tradecraft as a weapon against the threat actors' brazen and often outwardly obvious objectives.

The modern threat actor fits into one of three general profiles, all of which are just as dangerous when insidious activities are not uncovered by a competent TSCM program. Threat actors can be characterised as amateurs with little or no tradecraft experience; with access to the many surveillance devices sold openly on the internet and plenty of do-it-yourself advice, along with the fact that almost everyone these days qualifies as tech savvy.

The professional threat actor is often a technically skilled individual who utilises dual-use technology and has a remarkable success in blending into society (maybe an insider) and can facilitate the diversion of technology and protected information for personal and/or professional gain while remaining totally under the radar.

The highly skilled state-sponsored threat actor has received specialised training in many aspects of tradecraft from facility penetration, social engineering, cyber-vulnerabilities and often knows more about TSCM offensively and defensively than many technical operators. This category of threat actor has the financial support of the state-sponsor. Careful approach and persistence often yield remarkable success in the compromise, theft or diversion of seemingly unimportant, unconnected, unprotected information to highly protected sensitive or classified information. Unfortunately, in a modern-day threat management reality, the definition of a state-sponsored threat actor must include individuals or entities that elevate or recruit, if you will, themselves to the position of a state-sponsored threat actor. This new type of threat actor is already embedded, trusted and is often more difficult to detect. We are seeing more reports of detected espionage incidents worldwide and often pat ourselves on the back for a job well done. But not so fast, technical operators falsely believe that their defensive countermeasures are working.

My extensive experience, leads me to believe that the successful detections are a drop in the ocean; and that there are so many active threat actors across a larger more diverse and highly structured attack posture that it simply makes sense that a few threat actors are bound to be detected, leading to a false sense of national security.

The analyst can extract significant evidence of threat patterns over time that can lead to the surfacing of technical compromises

ALL INDUSTRY SECTORS ARE FACING THE VERY REAL PROSPECT OF BEING INFILTRATED FROM WITHIN

We are seeing state-sponsored threat actor detection across the private sector and we as an industry are driving both a change in approach and are no longer willing to accept obsolete methodology as an approach to TSCM in today's complex threat environment.

There is considerable misinformation resulting in limiting factors and unknowns that continue to be perpetuated by key industry players. When the technical operator buys a product that claims to decode signals for example, the excitement builds until the realisation hits that the intelligence provided has little or no value whatsoever from a TSCM perspective.

When the operator fails to understand their role in the mitigation of technical vulnerabilities and real-world functional compromises, the entire process will fail leaving a false sense of accomplishment for the operator and unfortunately a false sense of security for the end-user. Understanding capabilities, limitations, and more importantly, the differences between the technical operator and technical analyst role is also crucial!

The role of the analyst is not seen as a common TSCM function, but rather a SIGINT or counter-intelligence role – separate to, and on an entirely different level, apart from the field operator role. The analyst can extract significant evidence of threat patterns over time that can lead to the surfacing of technical compromises. Operator activities on their own merits simply cannot identify such threats in the immediate here and now, during limited, time-on-target inspections. It's the technical operator that feeds the analyst by providing maximum effort, raw and first cut filtered data for analytical consideration.

This all-important data is derived from many functional tasks, including, understanding the threat, the anticipated risk, the context in which data is captured, while understanding gaps in the raw data source files provided by automated collection

Picture credit: US Dept Defense

strategies and operator-assisted capture is essential. However, without active intelligence beyond the spectrum reference data, the mission will likely fail to identify deeply buried threat activity.

THE DEFINITION OF ESPIONAGE HAS NOT KEPT PACE WITH THE REALITY OF NEW ATTACK METHODS

Knowing what to look for and where to look for it, is the analyst's role; not that of the technical operator, who is primarily tasked with providing the analyst with the widest possible range of radio-frequency and operationally relevant counter-intelligence data. Detecting something in the here and now, versus the long-term strategy of remote spectrum surveillance and monitoring, are distinctly different functions shared across the operator and analyst.

The analyst's job is to put it all together and extract actionable radio-frequency intelligence that will provide clarity and focus for the technical operator in deploying and redeploying resources relative to the risk identified. This process leads to a more relevant intelligence focus by the analyst, often resulting in a positive-finding of compromise; with the identification of the threat actor as a definitive objective.

This is all a rather circular process in which the technical operator and analyst work in parallel to achieve a positive outcome. Unfortunately, many analysts are not field deployed and lack a practical appreciation of the actual circumstances of the data for interpretation or the target environment in which the data was derived.

It is recommended that in a standards-based approach the analyst must be trained in the operational deployment process of a competent technical inspection before being tasked with the analytical evaluation of captured reference data.

Field decoding and competent signal level analysis of potentially thousands of ambient signals is simply not realistic, let alone the fact that many threat-specific signals are highly encrypted; and is therefore a waste of valuable time-on-target. Capturing field IQ and feeding the analyst from a maximum effort approach allows the technical operator and the analyst to share the responsibility of threat identification by the application of individual skill-sets that differ across the roles. The currently accepted minimum standard for IQ capture is 160MHz of real-time radio hardware bandwidth to address a modern threat reality ●

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 over 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.

TSCM EQUIPMENT RESOURCE LIFE-CYCLE

The effective life-cycle has decreased during the past four decades, but operators continue to deploy resources well beyond the effective life-cycle.

1980 to 1990 | Effective Life-Cycle ..... 7 to 10 Years
1990 to 2000 | Effective Life-Cycle ..... 5 to 7 Years
2000 to 2010 | Effective Life-Cycle ..... 3 to 5 Years
2010 to 2020 | Effective Life-Cycle ..... 1 to 3 Years
2020 and beyond | We are seeing the effective life-cycle drop to 12 to 18 months for this coming decade.

Radio-frequency intercept and signal analysis is a growing national threat, from the corporate boardroom to the military battleground

Picture credit: NATO/IMS