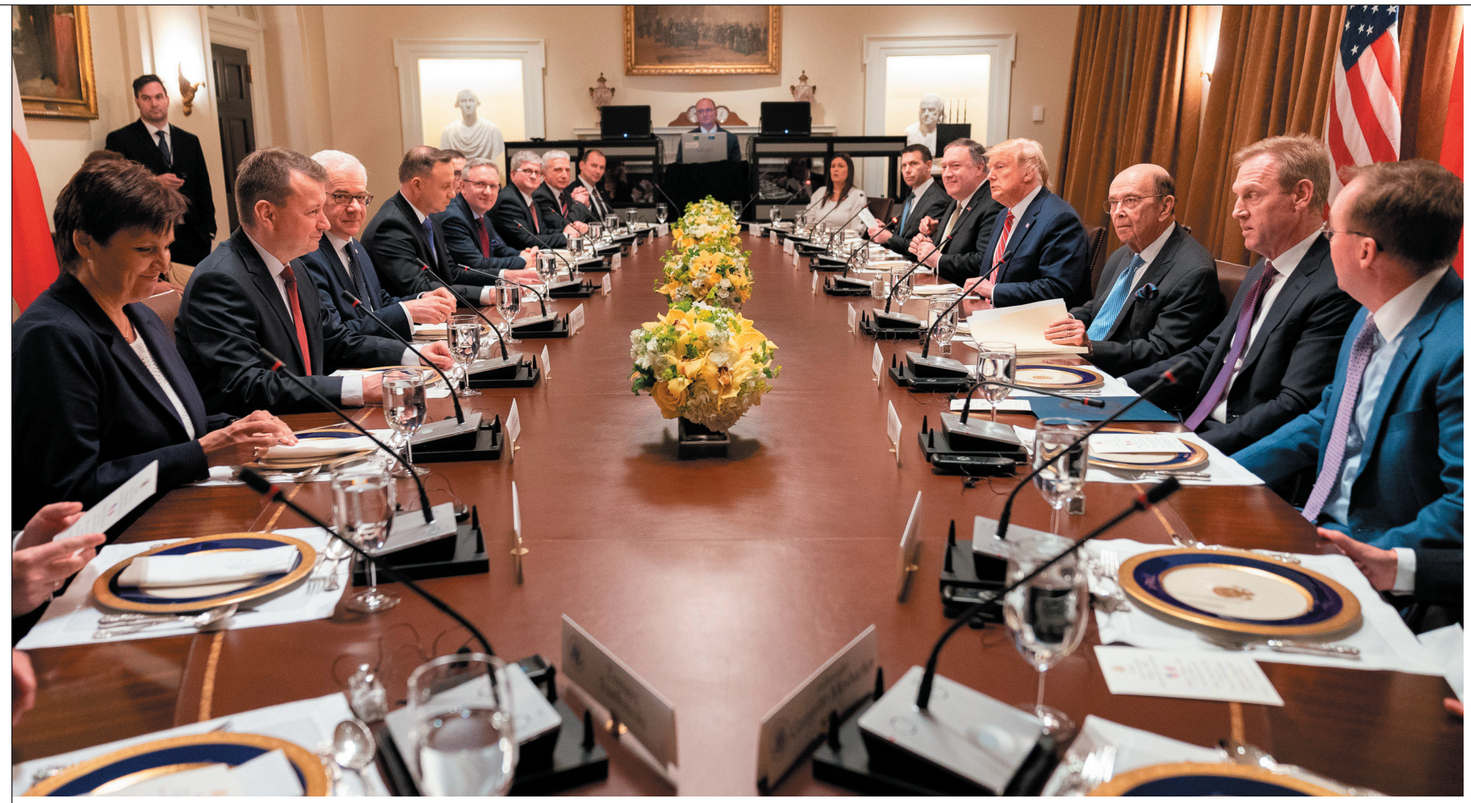


Picture credit: US Dept Defense

SEARCH AND DESTROY

Paul D Turner *explains the importance of Visible Light Communication when it comes TSCM*

It is vital that proper checks are carried out before any meeting likely to include sensitive information

Like all modern communication technologies, there are generally powerful security features and built-in safeguards that tend to provide a reasonable measure of technical security. However, threat actors have a nasty habit of finding and exploiting direct and indirect technology weaknesses, and finding inherent vulnerabilities that are often unrelated to the specific technology by exploiting other aspects of the overall system.

Optical threats are no exception and may include large window surfaces, gaps, openings and intercept technology. An array of human-factor issues relating to the improper deployment of the Visual Light Communication (VLC) technology; from an installation, setup and programming perspective, including physical security access vulnerabilities to critical infrastructure are problematic.

On another level, the compromise of input and/or output data streams and access to the underlaying driving technology is possible; bypassing an otherwise secure system. The vast majority of optical detection countermeasures devices are impactable to deploy effectively on more than one deployment perspective. Most optical detection devices fail to address the complexity and precision of the deployment detection methodology that is required to conduct a competent optical inspection within a TSCM role.

In a historical perspective and unfortunately, often by design, most optical countermeasure detectors fail to provide any measure of practical operator deployment-friendly features. As a result, any meaningful deployment strategy beyond the detection limitations suffers in practice. In this light, the remainder of this article will focus on introducing a competent operator-centric detection strategy.

OPTICAL INSPECTION PROCESS

Initially, the technical operator should consider setting up an appropriate SDR radio near the centre of the Operator Defined Target Area (ODTA) at table or desk height (facing upward) for an occupied work space and on the floor in an unoccupied space. The radio needs to sweep down to at least 9kHz. The software must allow runtime and demodulation, including real-time intermediate broadband (IFB) operation.

The optical probe technology can be deployed stationary on a laptop computer or deployed as a walk-about resource on a mobile tablet computer. The physical size of the ODTA will need to be considered in order to determine the required or recommended number of stationary collection points, similar to the radio-frequency collection process utilised in a differential signal analysis role. Small work spaces of up to approximately 350 feet^2 can generally be treated as a single collection point, utilising the optical sensor probes directional capability, across a methodical and highly organised search pattern. The time-on-target required is dictated by the perceived or determined threat level assessment and the nature of the critical infrastructure under inspection.

Multiple passive optical sensor probes can be cascaded to expand directional variation coverage across the ODTA. Connecting the optical sensors to suitable SDR radio, using a low-noise RF coaxial cable provides the necessary signal-level detection capability. A slightly reduced optical sensor probe sensitivity may be realised with cable lengths beyond 3m if required, for specific infrastructure installation and deployment objectives.

The advances and usability of software-defined radio hardware and specialised TSCM software provides the needed conversion of optical signals to a baseband radio-frequency spectrum for capture, display and analytics. The process is to setup the software utilising pre-configured optical inspection profiles or to define a custom set of parameters unique to the assignment. Once the setup is accomplished, it is possible for the operator to enter a runtime collection environment at the software level by selecting the spectrum band tab, directly representing the optical spectrum profile.

RUNTIME DEPLOYMENT OPTIONS

There are several methods available to the technical operator that can be employed to undertake both a fast search and a comprehensive (recommended) optical inspection manually. The technical operator can utilise a differential signal analysis process to directly compare historical trace information with the current runtime capture to maintain a managed optical reference database capability. The technical operator can capture a series of reference traces within a single-location runtime environment. This method of deployment builds a dedicated series of reference traces that can be stored and recalled as powerful comparative peak optical references spectra data, representing each phase of the optical detection process.

A comprehensive, methodical search technique is required to identify somewhat illusive optical emanations. In particular, those that are threat actor periodic, on-demand focused or highly directional in nature.

Multiple optical sources "sum" make separation of friendly and potentially hostile signals extremely difficult. A standards-based and methodical approach is required, given the optically high-dispersion factor and therefore, low apparent power of typical digital LIFI and other potentially "summed" optical emissions that may be present. The operator's decision to deploy one detection process over another is firmly based on the available time-on-target, the assessed importance based on the threat level determined, operator preference, knowledge and experience relative to the OTDA.

A METHODICAL SEARCH TECHNIQUE IS REQUIRED TO IDENTIFY ILLUSIVE OPTICAL EMANATIONS

It is the hardware that provides significant deployment advantages for the operator, who can select the best radios for radio-frequency work and simultaneously handle uniquely and separate functions like power line and optical analytics during the same runtime environment across multiple radios or a single radio environment. Equipment resources that fail to provide this essential level of deployment integration are simply obsolete by today's standards-based, modern-moving target threat model.

MANUAL SEARCH OPERATION

It is essential that the technical operator provide sufficient time-on-target. Optical searches are time intensive and the operator should consider dedicated time-on-target apart from the normally required inspection protocol. The operator can establish a runtime session by selecting a pre-defined spectrum profile and methodically paint the room with the optical sensor probe, watching for spectrum changes across the sweeping profile or real-time Intermediate Frequency Broadband (IFB) option. It is recommended that the technical operator import a previously captured reference trace file into the software as a direct comparative for the specific room-level ODTA. This level of inspection is essential in identifying possible hostile Technical Surveillance Devices (TSD) that might be deployed to intercept room level audio or data sources, without the presence of the more easily detected radio-frequency signatures.

A search from the centre of the room (upward), is best practice for LIFI emissions, however, direct LOS emissions are best identified by selecting logical positions to intercept emissions that might be directed out of the room via windows or gaps, *etc*. Detecting passive laser attacks is best accomplished with the sensor probe facing the windows and away from the windows, looking for modulated laser reflections from room-level objects.

DIFFERENTIAL SIGNAL ANALYSIS

A standard and perhaps familiar location-based deployment strategy can be utilised to capture any number of in-depth comparative optical focus traces. Each additional capture location can reference the sensor probe direction. It is recommended that the operator capture a baseline reference trace by completely shielding (covering) the optical sensor probe. The operator can then setup and capture a second software

location, perhaps with the ambient room-level lighting off and another location with the lights on. This process, creates a baseline of any ambient optical interference or noise emissions. There will always be natural and artificial ambient optical noise to consider. The largest source of artificial optical noise results from the room-level lighting. Different lighting sources respond uniquely and must be taken into consideration by the operator in determining the presence of "summed" emissions from hostile optical threat technology.

THE TECHNICAL OPERATOR SHOULD SET UP AN SDR RADIO NEAR THE CENTRE OF THE ODTA

Separate location-based traces can be captured for upward, downward, north wall, east wall, south wall and west wall; above any dropped ceiling and below any sub-floor structure. The differential deployment method provides an extensive, well-documented process for high threat assignments; for evidentiary purposes and to facilitate analytical operator review.

CASCADING (RF + OPTICAL) DETECTION

The advantage of software-defined radio is a unique and innovative ability to provide cascaded deployment for optimal real-time Optical Spectrum Surveillance and Monitoring (OSSM). A single optical sensor probe can be deployed for small spaces and multiple optical sensor probes can be deployed for larger spaces. Multiple, passive optical sensor probes can be electronically combined, utilising a suitable power-splitter technology, to increase room-level sensitivity and detection exponentially and better facilitate simultaneous, multi-directional coverage.

Advanced support extends to simultaneously combining and capturing both radio-frequency and optical signals across any number of multiple spectrum bands, utilising software-defined radio, multiple-band capability across a single radio. A power-splitter can be utilised to simultaneously capture radio-frequency via spectrum band separation using any passive RF antenna and simultaneously process the received and combined optical signals from the optical sensor probe, and both the radio-frequency and optical spectra can be displayed on separately defined spectrum bands at the software level.

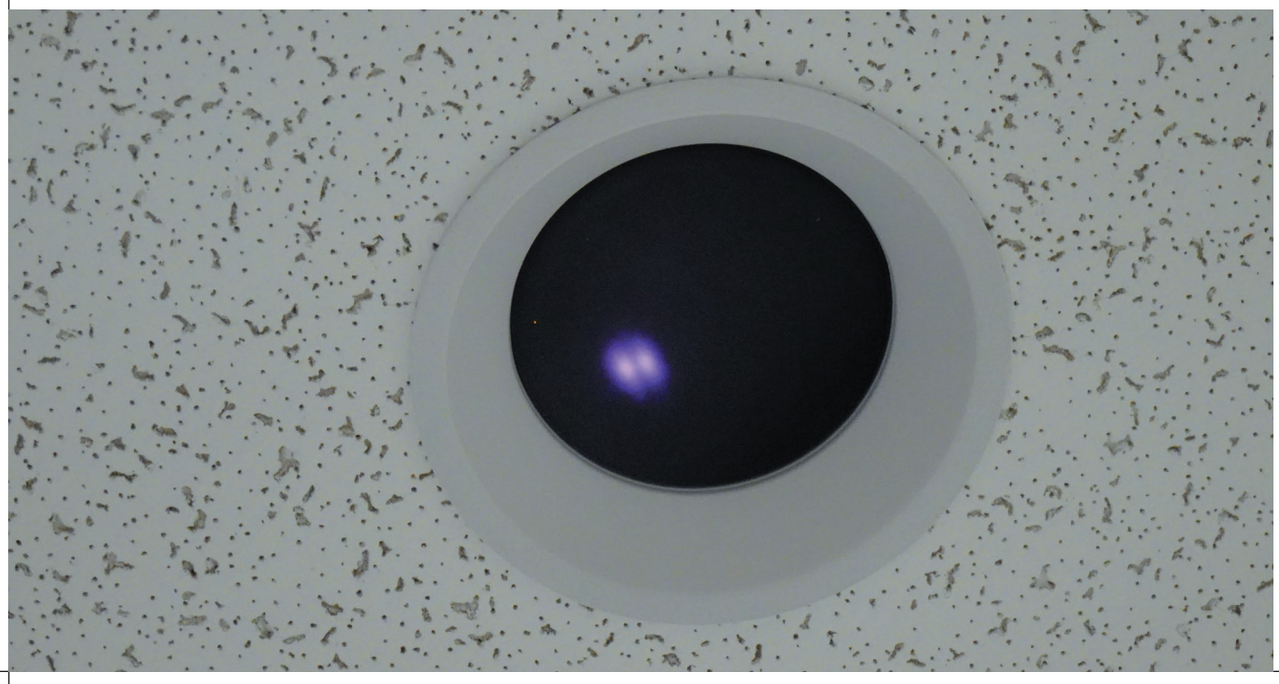
Multiple radio, multiple band operation is a powerful feature and supports combined simultaneous capture of RF, optical and facilitates power line analytics. The ability to cascade optical + optical, radio-frequency + radio-frequency, radio-frequency + optical and radio-frequency + power line is a powerful and innovative technology milestone. This level of diversity qualifies as a standards-based deployment process in support of live event monitoring and autonomous, extended Remote Spectrum Surveillance and Monitoring (RSSM) and Optical Spectrum Surveillance and Monitoring (OSSM) techniques; easily accomplished in a highly-scalable deployment process, providing an agile and highly focused collection platform.

IQ RECORD AND PLAYBACK

Software defined-radio provides an industry-unique TSCM ability to capture and playback IQ samples for post analytical analysis and review. IQ capture is an essential TSCM capability at all operational threat levels. IQ record can be used to capture a sample IQ file for detected optical emissions during the demodulation process and is used for signal-level analytics. The software must provide the ability to support a variety of IQ capture and playback formats. IQ based Time Reference Sub-Sampling (TRSS) provides a powerful editing resource to achieve analytical efficiency.

In conclusion, cascaded passive optical sensor probes deployed directionally across individual operator-defined target areas; utilising software-defined radio technology advances the probability of detection within a modern moving-target threat model. It is vital that operators seek professional training to better understand the importance of optical detection within a TSCM role ●

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 of 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.



Infrastructure LIFI device image taken with camera with its IR cut filter removed so that the illuminators that aren't visible to the human eye (the purple spots) can be seen

Picture credit: TSCM Group Inc