POWER PLAY

Paul D Turner *reveals why securing the unprotected power line network remains a vital security challenge for the year ahead*

The start of a new year often means reflecting on the past and year, perhaps more than usual given the global pandemic. As 2021 begins, I have found myself pondering a question asked by one of my students. "What makes a competent technical security specialist?" It is always a challenge to define the special qualities and abilities of a competent technical security specialist.

My response to this question was along the lines of the best professional technical security specialists that I have worked with or trained, all had the ability to connect seemingly unconnected events and to visualise the big picture with a uniquely dedicated focus, perspective and ability to identify technology trends that might have relevance or otherwise prove hostile.

Most technical operators respond to only what they know and see in front of them and not what they should know or be able to see. Some might call it connecting the dots, or the ability interpolate events that have not necessarily taken place yet or perhaps have not been made public for security reasons.

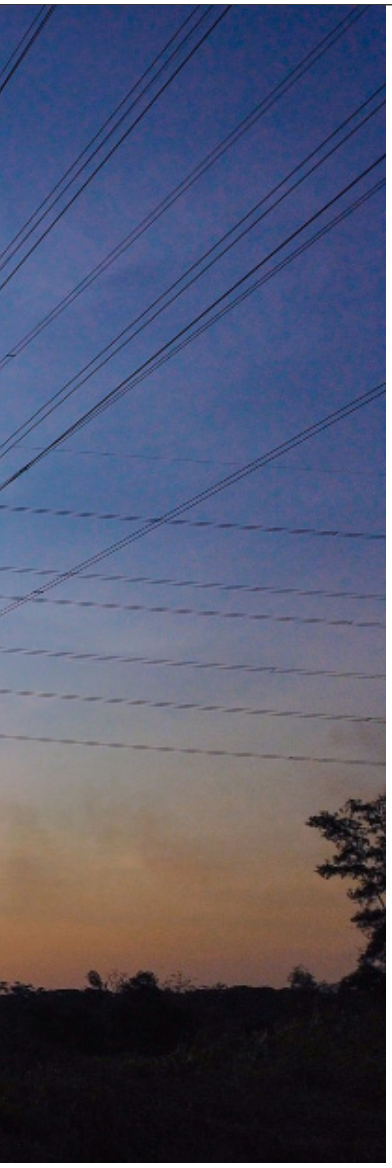
Technical operators cannot simply look at a snap-shot and make a sound set of conclusions. The ability to relate the present with the past and take into consideration with reasonable assurance of the future is an essential trait of any technical operator.

Power Line Carrier (PLC) and Broadband Powerline (BPL) threat technology are excellent examples of connecting the past, present and future of anticipated threat technology.

The local electrical power grid is the most vulnerable and reachable public networks. It provides an easily compromised communication path in virtually every residence, business, corporation, government, law-enforcement, military and national security facility for which technical security inspections are required.

The electrical utility is the one element that typically has no firewall or isolation, and extends freely beyond the confines of the generally secure exterior walls, doors and windows.

Even electrical transformers and UPS systems are vulnerable and provide only a limited inconvenience during a targeted intelligence gathering or state-sponsored espionage related attack of critical infrastructure.



Little research has been done on the effect of the electrical power grid being utilised as an in-bound conduit for personnel and equipment-level attacks

Power Line Carrier (PLC) threat technologies involve countless existing use cases by the commercial, private sector, public utilities, government, communication and transportation sector.

There are significant new emerging technological threats that utilise the generally unlicensed, unregulated and unmonitored emerging PLC spectrum well into the gigahertz range.

The risk of threat technology extends well into the bottom of the spectrum as technology previous limitations are overcome and traditional functional spectrum bandwidth becomes more limited.

Time-challenged technology limitations that once prevented the wide-spread use of PLC communication for offensive and commercial applications; in many cases are silently making a renewed appearance on the electrical power grid every day with staggering new modulation and data streaming capabilities compared with the bandwidth limited technology of less than a decade ago, most of which has changed very little during the past 100 years.

The ability of a threat actor in both theory and practice, to make use of directional PLC technology for active audio, video, and data streaming applications provides a somewhat invisible conduit or path to conductively, inductively, capacitively, or as a radiated Over-the-Air (OTA) signal, transfer vast amounts of intelligence beyond the confines of an otherwise secure facility.

Unintentional radiators consisting of existing authorised, and sometimes unauthorised equipment within the Operator Defined Target Area (ODTA) that are not intended to pass signals or intelligence onto the ambient power line may provide a communication path.

This is often by design, or intent of a threat actor, accident, poor design or installation, improper wiring techniques (accidental and deliberate), deteriorated physical condition, make the inclusion of a competent Power Line (PL) analysis an essential practice during every deployment.

As with most TSCM applications, doing half of the job, will generally equate to a tenth of the anticipated or expected inspection outcome, as a motivated threat actor will always defeat the unmotivated technical operator. The electrical power grid clearly fits into this unique category.

A key concern is the unintentional consequences of unauthorised devices being connected to the electrical power grid without an informed understanding of the potential technical vulnerabilities and security risks that are involved.

Such risks as supply chain compromise can involve sleeper technology that can be enabled as an in-bound or outbound attack in the future.

Many devices utilised within private sector and government facilities for security purposes, such as access control systems, video surveillance system components, all leak potentially recoverable intelligence onto the Power Line (PL) infrastructure.

Very few organisations give the electrical power grid a second glance when commissioning a new facility or when spending considerable time and financial resources on other aspects of the facility's overall security posture.

There is a significant surge of new Hybrid PL technologies starting to appear within commercial and consumer product applications that may utilise an obvious PL technology that is readily identifiable to the end-user or technical security specialist.

It is equally possible that such technology use might have a potentially hostile hybrid Power Line (PL) component within the underlying technology, which rarely is understood or assessed for potential technical security vulnerabilities during the procurement process.

The ambient electrical power grid is certainly a major concern, but not the only threat when it comes to the use of threat technology that are little more than unintentional radiators that communicate across any conductive surface from metallic-tape, telephone and network cables, a variety of common facility infrastructure (both existing and provided by the attacker), including copper or metallic plumbing lines and dropped ceiling structures, all of which can be altered, manipulated or modified for the express purpose of compromising critical informational intelligence at the facility level.

THE LOCAL ELECTRICAL POWER GRID IS AMONG THE MOST VULNERABLE PUBLIC NETWORKS

As recently reported about the possible use of high-energy weapon grade Radio Frequency (RF) attacks, little or no research has been conducted on the effect of the electrical power grid being utilised as an in-bound conduit for personnel and equipment-level attacks utilising high-energy radio frequency weapons.

The use of PLC technology is widely utilised in aircraft fly be wire systems and sub-systems, and has been for many years. More recently the use of PLC technology for remote computer and system-level Command and Control (C2), communication and signalling has been advancing exponentially and will continue to evolve with even more complex applications.

Aircraft, ships and vehicles of all descriptions, currently, utilise a wide range of multiplexed signals across common copper-wiring (and across fiber-optic networks) for bi-directional communications to and from sensors, status monitoring and to achieve C2 capability for systems, sub-systems, computers and modules.

The compromise of which can have consequences well beyond the confines of an informational technical intelligence attack.

Signal pattern recognition and RF visualisation skills have been the goal of many technical operators in better identifying and localising RF events of significance; and has become the only means of easily identifying *all* RF energy sources that are present within an Operator Defined Target Area (ODTA) to provide effective Power Line (PL) analytics.

The ability to utilise modern Software Defined Radio (SDR) hardware to baseline, capture and analyse energy-based or unintentional radiators is now an essential TSCM function.

Snap-shot style inspections are simply not an effective countermeasure for periodic in-bound and out-bound PL enabled informational intelligence compromises, nor does this approach detect targeted in-bound attacks involving potentially harmful or devastating high-energy.

Energy patterns must be captured continuously across all electrical phases in order to separate an array of swirling and churning noise artefacts from potentially hostile signals. All signals must be analysed by time characterisation to provide meaningful intelligence. Only continuous monitoring is an effective strategy at medium and high threat levels.

Hostile signal events may be intentional threat actor deployed technology or produced by the comprise of unintentional conductive or coupled emissions intercepted anywhere along the electrical utility path.

OPERATORS CAN'T SIMPLY LOOK AT A SNAP-SHOT AND MAKE A SOUND SET OF CONCLUSIONS

The captured energy patterns over-time tell a powerful story that cannot be ascertained with only periodic investigation.

The technical operator simply has insufficient reference information to properly assess whether any Signal of Interest (SOI) is in-fact a hostile surveillance device or is a random ambient noise artefact.

An extraordinary level of established reference data is necessary to identify potential threat technology associated with the electrical power grid in near real-time and can be achieved quickly with targeted Power Line geo-location heat mapping across the Operator Defined Target Area (ODTA) and the need to evaluate the presence of hostile technology into the extended Functional Target Area (FTA) to cope with utility appearance points external of the facility.

This is a powerful TSCM capability that involves hardware, software and a well-defined deployment methodology. It is about the methodology behind the hardware and software that has changed the way TSCM inspections are now conducted.

There are two distinct deployment techniques involved in securing the ambient power grid in both directions. Hostile and unintentional threats are bi-directional in nature and the threat actor can intercept intelligence-based signals out-bound and inject hostile signals in-bound to control or compromise vulnerable systems and equipment.

Hostile injection might be for the purpose of enabling dormant equipment determined to have backdoor vulnerabilities (unintentional and by design), including supply chain compromises of network and telecommunication equipment installed within the facility.

The vast majority of security validation for telecommunication and network systems involves the communication network side of the equation and not the potential of the powerline being used as a hostile network communication path.

The ability to walk the ODTA and capture localised power line energy patterns from each electrical appearance point for all, or targeted critical infrastructure, is an essential reality.

Continuous monitoring involves critical infrastructure areas of the ODTA, and all electrical phases associated with the critical infrastructure at higher threat levels.

Part two of this article will explore further deployment strategies for PLC and BPL baseline monitoring. The captured data-set becomes a powerful reference tool for future comparative analysis ●

Paul D Turner 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 technical operator has insufficient information to properly assess whether any Signal of Interest is a hostile surveillance device or a random ambient noise artefact

Picture credit: US Dept of Defense