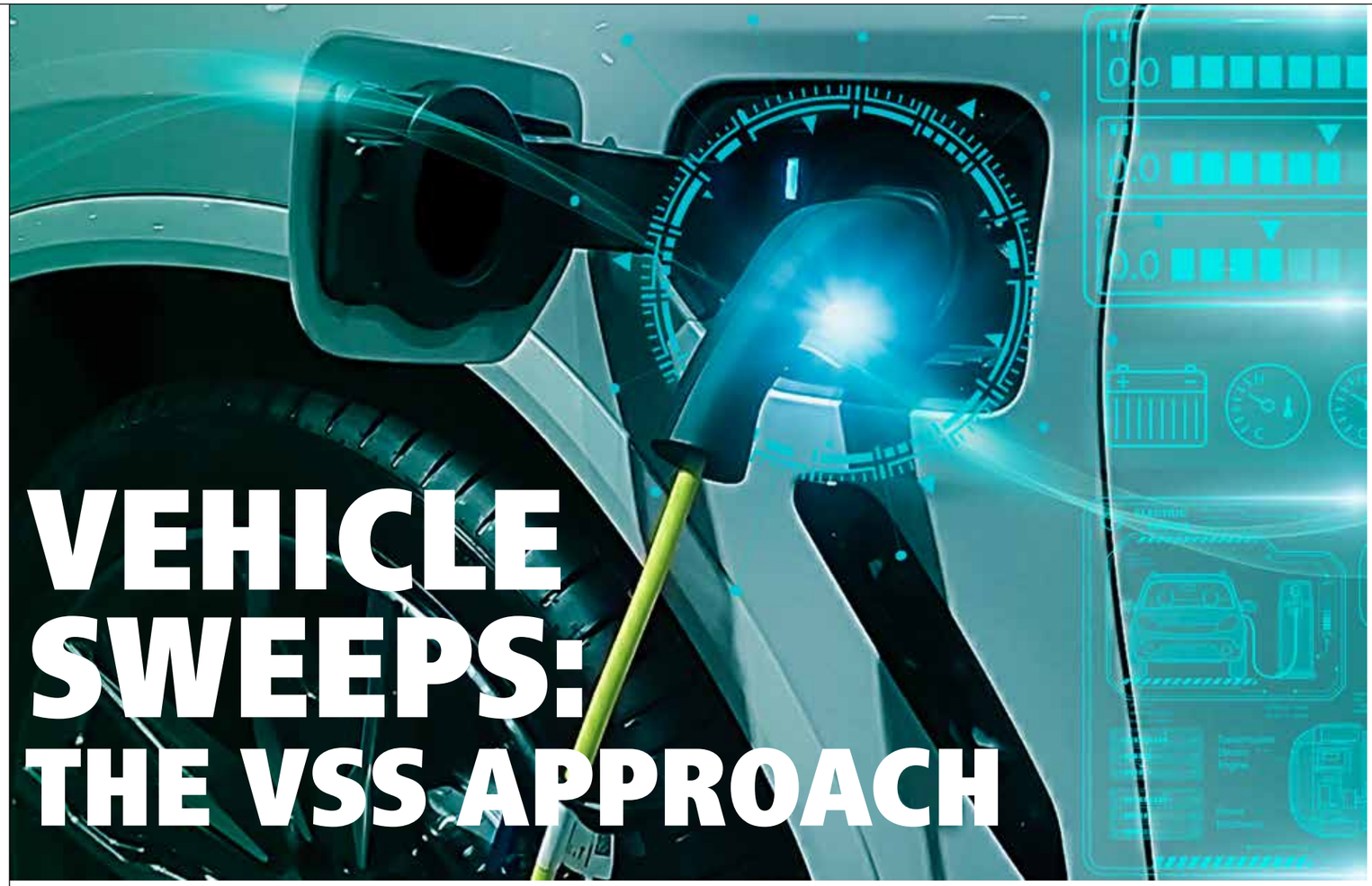

# VEHICLE SWEEPS: THE VSS APPROACH

Picture credit: AdobeStock

**PD Turner** *examines the changing dynamics of TSCM vehicle inspections*

**The role of the Vehicle Search Specialist (VSS) and the complexities of modern vehicle inspections have become a serious topic of discussion among professional technical operators and TSCM instructional technologists. Concern has been raised by organised government and private executive protection teams during the past few years, which in turn has promoted a rise in requests for a new search methodology and VSS training programmes. Personal reflection and years of field experience, must count in some importance; witnessing the historical development of technology driven vehicle evolution to where we are today and clearly are heading tomorrow.**

When it comes to TSCM-related technical inspections of vehicles and the potential relationship to state-sponsored espionage; potential assassination by vehicle; and the obvious direction of mass amounts of metadata being captured and collected by vehicle manufacturers and their so-called technology partners, is staggering. The danger lies in the rapid progression to innovate; opening the door to an unacceptably high-risk of under-tested technology and the introduction of undocumented technical vulnerabilities; by-design by the manufacturer; and threat-actor surveillance.

Operators that rely only on past training provided by equipment manufacturers that teach, in order to sell their equipment, leaves dangerous gaps in critical knowledge-base skillsets that continue to instil limitations which are then perpetuated across the industry by operators. The fundamental deployment experience comes from a vast pool of hands-on working knowledge; not only experience from a jack of all trades TSCM perspective.

The VSS must have direct working experience within the vehicle industry and fully understand the direct relationship to the complex wireless communication environment. A strong working knowledge of the anticipated threat-risk category, for which the vehicle inspection is required to be conducted, is essential. Our experience suggests that many technical operators have little or no recent training or equivalent current knowledge or understanding of the history and origin of modern vehicle systems. Most operators have even less recent training for hybrid and electrical vehicles, and virtually no experience with emerging autonomous vehicle technology.

History is an excellent teacher and is an essential starting-point to better understand and gain contextual knowledge that a spectrum warrior must deploy at the mission level. In 1917 electric-vehicle designers did not need to worry about hundreds of data-sensors, wireless devices, metadata capture or camera and optical technology. Experience, historical context, knowledge, professional training, motivation and pre-inspection planning and preparation are essential and not consistent as a do-it-yourself mission for untrained personnel using spy shop resources.

We have heard a lot recently about the concerns surrounding the Chinese EV market, while burying our heads in the sand about privacy, safety and protocol-based communication vulnerabilities; and a range of other concerns that must be applied across all EV manufacturers worldwide and not just the Chinese market. Privacy is eroding everyday, as society openly and willingly gives away the rights to highly sensitive personal information in the name of convenience. We are told the information is anonymous in nature, perhaps the biggest industry and government lie ever told. Frankly, if the government or military will not allow EV technology for use by its own personnel or permit EV technology on its respective military bases, what does this say about the millions of people being told to switch to EV technology? The amount of data being collected, stored, retrieved and analysed from not only EV technology, but from virtually all modern vehicles is staggering and concerning. As the next generation of automation and the reality of autonomous vehicles approach, the problem will only multiply significantly in depth.

Vehicles – including electric-vehicles – collect, process and store large data sets that include vehicle operational metrics, location-based coordinates, personal and biometric data. Privacy concerns include third-party in-vehicle apps, driver and occupant connected devices containing potentially sensitive personal data. Interconnected data-sharing EV charging stations at the elementary level monitor EV navigation; visual camera data; wireless network connectivity; and expose driver route and trip planning information which can be accessed by threat actors if strict privacy measures are not in place. Information from a wide range of sources can be combined to create profiles of EV operators, which may be sold or exploited by third-party data brokers. The integration of third-party applications within EV systems can significantly increase the risk of data breaches.

It was recently revealed that ethical hackers breached more than a dozen EV onboard applications from manufacturers such as Ferrari, BMW, Rolls Royce, Mercedes Benz and Porsche.

Third-party applications and embedded code may not adhere to the same security or privacy standards as the EV manufacturer, who would likely be held accountable for data breaches, and can result in unauthorised access and misuse of personal data. The number of wireless communication links at the vehicle and infrastructure level by comparison will seem insignificant next to the metadata streaming across, cellular, satellite, personal wireless devices, roadside infrastructure and traffic control platforms.

**The amount of data collected, stored, retrieved and analysed from modern vehicles is highly concerning**

The necessity to scan and detect common threat-actor placed GPS trackers may well become an obsolete technology, in light of the many positioning sensors, accelerometers, inertial navigation and roadside infrastructure links that might be compromised easier than you might want to believe. The VSS approach to vehicle sweeps has radically changed during the past decade, leading the way to a new training reality.

## THE THREAT ACTOR NEEDS TO PRECISELY PREDICT UNKNOWN INFORMATION FOR THE ATTACK TO WORK

We have seen tremendous advancements with crowd-enabled tracking technology during the past decade and witness many misconceptions about other similar tracking products. Standalone devices are quickly being replaced by fully integrated onboard vehicle technologies that can be hacked, accessed, intercepted, manipulated and exploited. There is a wide range of air-tag related products on the market that do not rely directly on wireless carriers at the primary level, by making use of unrelated nearby crowd connectivity before finding the cloud. It is therefore essential that the operator understands the extent of low cost, easily modified products that can impact vehicle inspections. The devices make use of Bluetooth Low Energy (BLE) and Ultra Wideband (UWB) for positioning, localisation and crowd connectivity. Bluetooth and Wi-Fi analysers are just another resource in our tool box, nothing more; many of the free BLE apps provide more significant analytical details than many of the so-called TSCM equipment resources.

The ability to spoof LiDAR sub-systems, causing them to hallucinate and identify targets that either don't exist – or ignore targets that do – open the door for threat actors to facilitate electronically assisted vehicle take-overs, car-jacking, kidnapping and even facilitate dangerous pranks. Unauthorised access to so-called autonomous vehicle data and personal information is a significant concern.

LiDAR spoofing attacks are designed to manipulate autonomous vehicle landscape perception by injecting phantom obstacles or masking real objects using external optical signals or well-timed laser reflections. Attack postures exploit the precise time-synchronisation with optical sensor pulses, achieving a high success rate in misleading the underlaying object detection software sub-systems. LiDAR spoofing attacks can be active or passive by relying on active signal injection using laser emitters or passive mirroring and reflection techniques.

Precise synchronisation is required and must be line-of-sight with the LIDAR sensor, providing a difficult but viable spoofing capability – successfully demonstrated in the 100m range. The threat-actor's ability to optically jam the LiDAR sensor signal requires the use of a high optical power pulsed laser to blind the sensor with optical noise. Defensive countermeasures at the sensor-level and

the underlaying sub-system exist, but the risk of compromise is still very real.

The loss of LiDAR can be detected and a safety-oriented response can be initiated at the vehicle level, however, rapidly slowing or stopping the vehicle for LiDAR safety reasons may not prove to be the best option during protection details, kidnapping attempts or armed car-jacking scenarios.

Many non-autonomous vehicles are equipped with LiDAR and/or radar-based Adaptive Cruse Control (ACC) systems as part of the ADAS platform and considered the training ground for the next generation of autonomous vehicle technology. These pose serious questions about the technology limitations.

## LIDAR SPOOFING ATTACKS INJECT PHANTOM OBSTACLES OR MASK REAL ONES FOR VEHICLES

In future generations of ADAS sub-systems, adaptive vehicle radar emissions will contain active vehicle-intelligence described as smart radar and communicate on a higher level with other vehicles, people and road side infrastructure. During an attack, the challenge is achieving the level of accuracy required to estimate the parameters to spoof the platform as you must predict when the radar is going to transmit the next pulse duration. Radio waves propagate at the speed of light and the timing is incredibly difficult to predict and synchronise.

During an attack the threat actor needs to know all of the radar parameters and precisely predict unknown information for the attack to work within an accuracy of approximately 40 nanoseconds. In an attack that does not rely on previous or predictive knowledge of the radar activity, the parameters are learned by intercepting and listening to the radar emissions, just like any other radio signal.

There are currently four primary bands for vehicle radar globally in the sub-millimeter and millimeter ranges. Earlier radar used the 24GHz band allocations. The more recent 76GHz to 81GHz is now accepted by most countries as the frequency band of choice for vehicle radars with a larger available bandwidth and better resolution.

The 77GHz frequency band for vehicle radar applications operates between 76 and 81GHz, providing a usable bandwidth of 4GHz compared with only 200MHz for the 24GHz band. The 4GHz wide bandwidth increases the range and velocity resolution of the radar, which measures the differences in phase-relationship between the transmitted and return signals to detect and measure the presence and velocity metrics. The resolution and accuracy of velocity improves as the wavelength decreases, proportionally, as sensors shift from the 24GHz band to the 77GHz band.

Enhanced resolution improves the detection and avoidance of large objects like vehicles and allows identification of smaller objects, providing drivers with better object resolution in low visibility. 77GHz radar components are smaller, as the relationship between the antenna size and the frequency is linear, the surface required for a 77GHz radar antenna is one-tenth the size of a 24GHz antenna. 77 GHz radar permits the use of a higher transmit power level with an Effective Isotropic Radiated Power (EIRP) of 55dBm, whereas for 24 GHz, the peak limit is 20dBm EIRP. In part two (next month) we will dive into vehicle sweep protocols ●

**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 45 years of experience in providing advanced operator 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.

**Fully integrated onboard vehicle technologies can be hacked, accessed, intercepted, manipulated and exploited**

Picture credit: AdobeStock