Picture credit: Getty

VEHICLE INSPECTION

Amir and Ohad Hever *explain the technologies involved; what they are, how they help and what the future holds*

Vehicle inspections pose a distinct set of challenges for security professionals as they contend with greater demands for accuracy and efficiency in ensuring that security is maintained without causing major impacts to the operations of their missions.

In the hope of keeping pace with the scale and complexity of vehicle inspections across a variety of operational environments – ranging from airports to embassies, government offices, border crossings and many more – security professionals are increasingly turning to vehicle inspection technologies to give them the ability to do more with the resources that they have.

The threat posed by vehicles has existed for as long as there have been vehicles and something to hide in, on or under them. However, changes in the geopolitical landscape and threat actors who are actively using vehicles as a part of their asymmetrical tactics, have brought the need to improve how we do these inspections to the forefront.

In recent years, attackers inspired by the Islamic State and other terror elements have sought to utilise car bombs against targets throughout the world, at times with devastating effects. Trained on the battlefields of Syria and Iraq, these crews have professionalised the practice of designing and operating both armoured and covert vehicle-borne improvised explosive devices (VBIEDs), the common term for the more colloquial concept of car bombs.

Developing strategies to deal with vehicle-borne threats has become increasingly important

As the group's grip on territory has faded in those conflict zones, there are concerns that they are already exporting their accrued knowledge to their supporters in the West and elsewhere for use against softer targets.

According to researchers at the Action on Armed Violence (AOAV), there has been a marked rise in the number of casualties caused by VBIEDs over the past decade. During the years between 2011 and 2016, the centre recorded 21,000 deaths and injuries related to VBIEDs, of which they claim 73 percent were civilians. That number increased by 97 percent between 2016-2107, driven mostly by casualties in Iraq and Syria.

From a security perspective, we think about vehicles differently from other risks because they can be used to carry far greater quantities of illicit materials, such as explosives, than any individual, providing attackers with an easy to attain weapon of mass destruction.

The US Department of Homeland Security estimates that a compact car can carry up to 500lbs of explosive materials while a delivery truck can reach upwards of 10,000lbs, impacting an area of over 5,000ft. Along with any additional items like bolts and nails, the body of the vehicle itself can serve as shrapnel in the attack to increase its deadly effectiveness.

Beyond the direct threats posed by vehicle-borne improvised explosive devices (VBIEDs), there are other associated risks such as those stemming from weapons being smuggled or components of an IED, which could later be assembled inside a secure location.

MITIGATING THE RISKS

Developing strategies to mitigate the risks posed by weapons on wheels has become a must. However, guarding against these attacks is far from a straightforward task. Let us take an example of an airport security scenario – but it could just as easily be an embassy, border crossing or any other kind of sensitive facility that might be targeted by attackers – to try and better understand the difficulties involved.

For starters, VBIEDs are difficult to identify from afar so long as they do not resemble an ISIS-type armoured suicide vehicle (SVBIED). A closer inspection is often needed to identify explosives like gas canisters or other substances in the back seat or trunk of a car – an impossibility before it reaches the checkpoint itself.

Once the vehicle is at the checkpoint, performing a thorough inspection in terms of both speed and accuracy is still difficult. Dangerous items can be hidden within or under the vehicle, both of which are areas that are cumbersome to inspect with any real integrity. Beyond the effort of carrying out these searches by hand or attempting to look under the vehicle with a mirror, the extended time taken to do this inspection can raise the risk profile of the checkpoint as it creates a bottleneck that might itself become a target for attackers.

Then there is a less discussed issue regarding the fact that we do not always know what we are looking for when searching for threats. Unfortunately, not every IED soldered onto the bottom of a vehicle looks like a bomb with a cartoon-esq ticking alarm clock attached to it, making it easy to spot.

Spotting an auto part that is out of place is difficult, bordering on impossible, for the human eye, especially given the wide range of makes and models that a guard must contend with, a task not made any easier by the fact that the driver is now behind schedule having been held up for the additional screening.

When equipped with the right technology, security teams can gain a more comprehensive and accurate picture of threats posed by the contents of a vehicle as it moves through their checkpoint. The types of technologies that are commonly used include: undercarriage inspection; license plate readers for both identification and authorisation; facial recognition; x-ray; and weight. Surveying our technologies, we can group them into two basic categories, brought together with the common thread of automation.

License plate readers and facial recognition technologies are in a real sense our first line of the access point security process. They identify the vehicle and driver, working to authenticate whether they are who they say they are and if they are supposed to be there in the first place. This is, of course, ideal for situations like a sensitive facility where there is repeat traffic with authorised personnel. While this solution is useful for identification purposes, it can also raise a red flag if the vehicle has the right plates but is the wrong make or model, or does not have plates on it in at all as is the case for many attacks where they are removed.

> **UNFORTUNATELY NOT EVERY IED ATTACHED TO THE BOTTOM OF A VEHICLE LOOKS LIKE A BOMB**

The second group of undercarriage inspections – x-rays and even weight – fall into the anomaly detection section, providing teams not only with more efficient ways to view those hard to reach spots, but also to identify items that should not be there under normal circumstances.

One of the most significant advancements has been the introduction of deep learning anomaly detection in undercarriage inspections wherein we are teaching algorithms to understand what are the parts that make up a vehicle. To be clear, this is not to say that we are simply comparing the manufacturer's design of their vehicle to the image that pops up on screen.

Instead, we are feeding millions of scans of vehicles into our algorithms and helping them to learn what an exhaust pipe should look like. Not just on a Suburban, but on a Tahoe, Land Cruiser or a Mini as well. With this technology, we are taking the high-resolution images taken from under the vehicle and teaching the system how to tell what should not be there, thus flagging potential threats for closer inspection with a high level of accuracy in the hope of helping security operators meet the challenge of handling large-scale inspections with the necessary speed and accuracy to be effective in the field.

Building technologies that are capable of producing reliable results on-site and in real-time is difficult to get right. First and foremost is the need to collect

sufficient data to build a model with. Uveye has scanned over two-million vehicles in under three years in order to feed its algorithms and build up its accuracy. Next, it needs to design and train our algorithms to constantly improve the results. This process of regular testing and validation of data is intensive, but essential in developing deep learning capabilities.

Leaving the lab, there are also external, real-world challenges that need to be overcome. You can develop the best algorithm, but in the field you have environmental conditions that can impact the results, no matter how well you train your machine learning.

Environmental conditions such as light, water, dirt, lane size and other limitations can alter the quality of your detection results so they must be accounted for. In addition you have operational constraints to consider such as vehicle speed and traffic density that put stress on the human operators who are after all

BETWEEN 2011 AND 2016 THERE HAVE BEEN 21,000 DEATHS AND INJURIES RELATING TO VBIEDS

humans – which leads us rather neatly to our last point for consideration…

The future for vehicle inspections is integration with other systems, accuracy and efficiency. Even as vehicle inspection technologies rely more heavily on automated systems and deep learning, there will always be a human element in the process. The goal of these technologies is not to replace humans, but to help them to prioritise their efforts towards those potential threats that are most likely to need additional inspections.

The next generation of vehicle inspection technologies will be those that continue to improve their accuracy and speed, learning from the data that they collect to get better at identifying threats that might otherwise slip through and put the mission at risk. In part this is a numbers game for the companies that are developing these technologies, giving an advantage to those that are able to collect more relevant data than their competitors to train their algorithms on.

However, the sheer size of a data set is not everything. It's also about how you use it. We are still at the early days of the deep learning and Artificial Intelligence movement, and there remains massive space for growth and innovation as we learn how to ask better questions of this technology.

PLAYING WELL WITH OTHERS

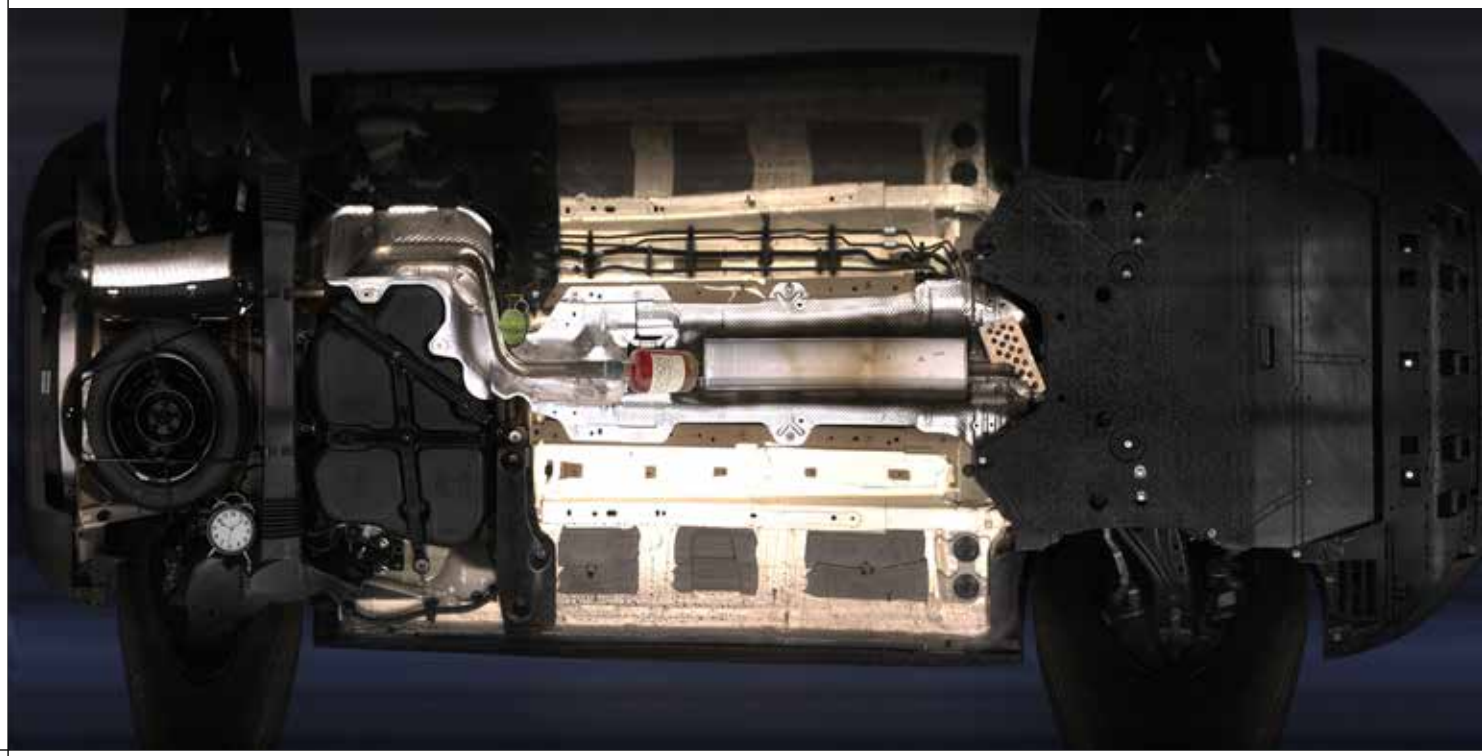
Beyond the maths that we are throwing at these challenges, it is also important to remember that security done right is layered, and that every system that we put in place needs to play well with others. These technologies need to be integratable with one another, sharing information with one another without too much manual interaction to correlate data and patch together actionable output for the users in real-time.

When a vehicle approaches a checkpoint, there should be systems in place to recognise the driver and license plate, checking with databases on the backend to be sure that the vehicle is supposed to have access to the site. At the checkpoint, the vehicle should be scanned for any anomalies that could be indicative of a threat on the undercarriage, and an inspection of the inside of the vehicle by human eyes or an x-ray should be performed.

Taken as a whole, these components of a comprehensive security posture should quickly give the security team a sense as to whether this vehicle needs a more intensive inspection or should be allowed to pass through. Cutting the time that this process takes to be carried out with a high level of confidence translates into better productivity for the entity that the security team is there to protect in the first place, allowing security to enable instead of hinder ●

Amir Hever is CEO & co-founder of Uveye. He has an extensive background of over 10 years working in the field of computer vision.

Ohad Hever is COO & co-founder of Uveye. A hardware engineer and entrepreneur, he specialises in the field of technical project and product management.



Spotting hidden threats is extremely difficult for the human eye

Picture credit: Uveye