Dealerships may have a part to play in the war on terrorism

This item was submitted to Loughborough University’s Institutional Repository by the author.

Citation: SAKER, J.M., 2016. Dealerships may have a part to play in the war on terrorism. Automotive Management, September 2016, pp. 40-40.

Additional Information:

- This paper was accepted for publication in the magazine Automotive Management and appears here with the kind permission of the publisher.

Metadata Record: https://dspace.lboro.ac.uk/2134/23711

Version: Published

Publisher: Bauer Media

Rights: This work is made available according to the conditions of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) licence. Full details of this licence are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Please cite the published version.
Dealerships may have a part to play in the war on terrorism

By Professor Jim Saker

They say you should embrace change and that for many it is something which drives them forward. Since I wrote my last column for AM, we have a new Prime Minister, the protagonist who argued for Brexit have stabbed each other in the back. There has been a repeat of incidents of bloodshed on the streets of France and Germany, and somehow Boris Johnson is Foreign Secretary at time of writing. At least his capacity to make a diplomatic incident could make his tenure shorter-lived.

Of all the events of the past month, the terrorist attack on July 14 in Nice again raised the spectre of a motor vehicle being deliberately used to cause death to innocent people. Car bombs were widely used during the Troubles in Northern Ireland and car and truck bombs have been used with devastating loss of life in the Middle East more recently. However, apart from a small number of failed bombing attempts, including the Glasgow Airport attack, there has been limited use of cars and lorries as terrorist weapons in Britain over the past decade or so.

There is, however, an impending threat. The rise of the connected car and, in the longer term, autonomous vehicles may see vehicles become a more common terrorist tool.

As Nice showed, the risk does not come just from bombs. In fact, at a conference I attended recently in New York, a scenario was put forward in which it would take just three cars suddenly stopping at high speed in strategic locations to gridlock the city. To bring London to a standstill, it was suggested that it may take only four or five.

Securing the connected car
Manufacturers are spending large sums to protect their cars' computerised engine management systems.

There have, however, been reports that hackers have successfully compromised security systems on some Jeep models, the Nissan Leaf and the Mitsubishi Outlander. Some of these hacks were less serious, such as hijacking air conditioning and multimedia systems, but in the case of the Jeep breach, brakes, steering and transmission were all capable of being remotely controlled.

The dilemma is that the connected car has many benefits - not only to the driver, but also to the dealer and the manufacturer.

In servicing and maintenance, for example. As publicised in the aftermath of the disappearance of Malaysia Airlines flight MH370, Rolls-Royce uses a remote connection to monitor the performance of its aero engines and identify faults. This allows the company to predict when an engine needs a service intervention and allows it to have staff and parts ready, keeping downtime to a minimum.

On the other hand, any form of remote connection presents security challenges. If someone can intercept or alter the signal, then the whole system, as with the Jeep hack, can become compromised.

The whole concept of the connected car is to communicate not only information about the car, but also the individual owner. There is an ongoing debate as to who owns this information and who should have access to it, most of which will be decided by the Data Protection Act.

The manufacturers will continue to try to make their cars as secure as possible and will invest heavily to ensure that there is high customer confidence and acceptance of this type of connection and data sharing. With sufficient time and investment, it is possible to envisage that the integrity of the cars will be secure from outside attack.

Securing the dealership
However, even if manufacturers manage to perfect their security measures and individuals have all their data protected by law, another vulnerability remains.

In this scenario, the vehicle is at its most vulnerable when it is being serviced. Handing over your connected car is a bit like handing over your laptop to a complete stranger and telling them all of your passwords. Whoever is working on the car will have privileged access to the protocols, so they can upload new software and also make adjustments to the existing car management system.

When I mentioned this to some of our students at Loughborough, they immediately said that with the right type of information they would be able to alter the performance of the car remotely and in fact could put on the emergency braking system or potentially disable the engine.

The problem with this level of access is that, apart from basic criminal records checks, there is no formal vetting or licensing of technicians in the retail automotive sector.

Changes in technology mean our sector needs to change its approach to data and software security. Licensing of technicians is inevitable - the issue is how the industry goes about implementing it without it being imposed.

Someone joked that the motor industry was responsible for the start of the First World War when Archduke Ferdinand's car stalled, giving his assassin a point-blank target. I don't think we will be responsible for the start of World War III, but if greater dealership security can help make our world safer, then maybe it's a route we should take.

"The rise of the connected car and, in the longer term, autonomous vehicles may see vehicles become a more common terrorist tool"