LOS ANGELES
Daily Journal
www.dailyjournal.com

WEDNESDAY, JANUARY 4, 2017

PERSPECTIVE

Hacked automobiles are a threat we must deal with today

By Jonathan Michaels

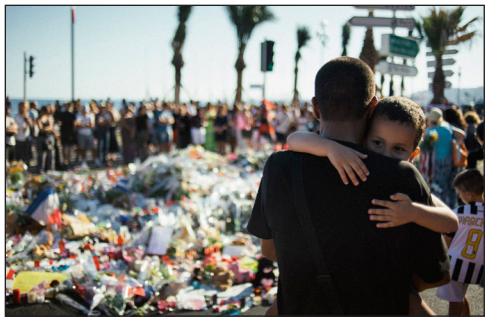
War used to be such a simple concept; tragic to be sure, but nevertheless fundamentally simple. A set of opposing troops would march toward one another, firing bullets into the faces of the other, with the last one standing claiming sovereign victory. War was always a matter of international politics — a dictator's attempt at a massive land grab, or an effort to impose the will of a society on the souls of another.

Today, conflict is defined by an entirely new set of rules that greatly complicate the discussion. The Islamic State group thrives on the element of surprise, with loyal followers engaging in suicide missions that kill and maim scores of the innocent. Historically, this meant using suicide bombers to inflict their terror, yet that is changing — and it should concern us all.

Twice last year, we saw attacks on the public were meaningfully different than any others that had come before. In July, a 19-ton cargo truck drove into a crowd of French citizens celebrating Bastille Day in Nice, killing 86 people and injuring 434 more. In December, another cargo truck was driven into a crowded Christmas market in Berlin, killing 12 and injuring 56. The Islamic State claimed responsibility for both attacks, saying that they were targeting "citizens of coalition nations that fight the Islamic State."

On the surface, the pair of events is concerning because it suggests a new, easier way of implementing terror. Driving a truck into a crowd is easier than assembling a menacing bomb that could be detected or deploy improperly. On a deeper level, it is greatly concerning that the terrorists regimes have stumbled on automobiles as a method of spreading their message.

What has begun as a crude act of driving a vehicle into a crowd can, and likely will, morph into a cyberattack on vehicles on a mass scale. Today's vehicles are more complicated and more advanced than ever before, each carrying an average of 100 million lines of code. As manufacturers make efforts to churn out autonomous or semi- autonomous vehicles, expect that number to jump to 200 to 300 million lines in the near future. As Mary Barra, the CEO of General Motors recently stated, "I fully expect the auto industry to change more in the next five years than it has in the last 50." And this is where the concern lies.



New York Times

People at a makeshift memorial at the Promenade des Anglais where a man drove a 19-ton truck through a crowd celebrating Bastille Day in Nice, France, July 17, 2016.

"White hat hackers" — those who work to identify security weaknesses in order to enhance overall security — have already proven that breaking into a car's computer is no difficult task. Those close to the industry will recall the publicized event last year where a group of friendly hackers placed a journalist in a Jeep Grand Cherokee to demonstrate how they could take over controlling the vehicle from a laptop thousands of miles away.

The Islamic State may be at the infancy stages of cyberattacks, but make no mistake about it, they have arrived. In April 2016, the Islamic State targeted 3,000 ordinary New Yorkers in a cyberattack, posting their personal information online and announcing, "We want them dead." The month before, an Islamic State group hacked into the New Jersey Transit Police website and obtained the names, home addresses, phone numbers and working locations of the officers, calling on its supports to carry out lone wolf attacks on the officers.

It is only a matter of time before the Islamic State — or another terrorist regime — begins attacking the interconnectivity of cars, reigning havoc on all. Reckoning back to the Jeep Grand Cherokee incident, imagine the destruction that could be caused if hackers simultaneously caused each Grand Cherokee to fully accelerate, while disabling the steering and brakes. Or consider the resulting damage if terrorists caused the vehicles to start in people's garages in the middle of the night, causing their house to fill with toxic exhaust. These scenarios are not that farfetched.

Mary Barra has recognized the concern: "The threat landscape is continually evolving, and sophisticated attacks are specifically designed to circumvent even the most robust defense systems. Whether it is phishing or spyware, malware or ransomware, the attacks are getting more and more sophisticated every day."

Counter-cyberattack company Security Mentor suggests that the auto manufacturers place "bug bounties" on their cars, offering rewards to anyone who can hack into their systems. The company believes that employing emerging hacking techniques is the only way automakers can guard against malicious intent. So far, manufacturers have been resistant to the idea.

Federal legislation will eventually join the conversation, but don't expect the cavalry to arrive soon. Sens. Edward Markey (D-Mass.) and Richard Blumenthal (D-Conn.), members of the Commerce, Science and Transportation Committee, introduced a bill called the Security and Privacy in Your Car (SPY Car) Act that would direct the National Highway Traffic Safety Administration and the Federal Trade Commission to establish federal standards to secure automobiles and protect drivers' privacy. The bill has languished in committee and died when the 114th Congress ended on Jan. 2.

Heraclitus of Ephesus, the pre-Socratic Greek philosopher, famously said, "If you do not expect the unexpected, you will not find it; for it is hard to be sought." As unfortunate as it is, we are all but a stone's throw away from the catastrophic implementation of a cyberattack on our vehicles of today and tomorrow. We cannot wait to create a defense after the carnage has occurred. We must act now, and expect the unexpected.

Jonathan Michaels *is the founding member of MLG Automotive Law, APLC, which specializes in representing clients in the automotive industry. You can reach him at (949) 581-6900 or jmichaels@mlgautomotivelaw.com*