WikiLeaks revelations raise new questions about the death of journalist Michael Hastings

Bryan Dyne
9 March 2017

One of the 8,761 internal CIA documents leaked by WikiLeaks on Tuesday reveals that the agency's Center for Cyber Intelligence has been exploring methods to hack into vehicle systems since at least 2014. As WikiLeaks noted in its release accompanying the documents, "The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations."

While the anti-secrecy organization makes no specific charges in this regard, this information raises new troubling questions about the car crash that killed journalist Michael Hastings in June of 2013.

Hastings, who was 33 when he died, was the *Rolling Stone* reporter who wrote an article in 2010 that led to the removal of General Stanley McChrystal from his post as ranking US commanding officer in Afghanistan. Hastings perished at around 4:30 a.m. after losing control of his car and crashing into a tree while traveling at about 100 mph.

At the time of his death, Hastings was investigating another major figure within the Obama administration's military and intelligence apparatus, then-CIA Director John Brennan. At the time, police declared that there was no "foul play" involved in the accident. Before the accident, however, Hastings had informed his colleagues that he was under government surveillance. He also suspected that his own vehicle had been tampered with, having asked a neighbor to lend him a car.

What the WikiLeaks documents show is that Hastings' suspicions about his vehicle could very well have been justified. Meeting notes dated October 2014 show that the CIA has a division known as the Embedded Development Branch which lists "potential mission areas," such as software and networking devices, as targets for hacking. One of the targets listed is "vehicle systems (e.g., VSEP)," likely referring to the embedded computer systems that play a major role in the operation of modern cars (though the acronym is not spelled out).

Embedded systems are computers designed and built to solve only a few specific problems. They are not designed to take human input, but rather are a combination of hardware and software that is designed to do a specific task as a permanent part of a larger system, such as traffic lights, airplane controls or assembly lines in a factory. While in general the software of embedded systems is hard to change by design, the CIA memo indicates that gaining the ability to control many types of these computers is one of the goals of the agency.

One piece of software in embedded systems specifically mentioned by the CIA memo is the operating system QNX, which the memo states is a "*big player in VSEP.*" Indeed, according to QNX Software Systems Limited, the software has been deployed in more than 50 million vehicles across at least 14 different brands, more than 50 percent of the market share of modern cars.

While QNX is generally advertised as an infotainment system—regulating things such as Bluetooth connectivity, GPS, and music—it has been increasingly used to operate more critical systems of the car, such as the safety and navigation systems, which include things like power steering and acceleration. Thus, if a person or an agency were able to hack a car equipped with QNX, it is possible that they could force the car to crash by disabling brakes,

causing uncontrolled acceleration and depriving a driver of steering. And since recovering software commands after the hardware has caught on fire is difficult at best, such hacks would be very hard to detect.

Though there is not a clear indication that the CIA developed these tools beyond the “potential” for them to exist, one tool mentioned in the memo, “Weeping Angel,” has been developed and deployed. Weeping Angel is designed to infest smart TVs and transform them into microphones that covertly record nearby conversations and send what was said back to the CIA. No doubt other tools in the list of hacks wanted by the agency have also been developed.

Moreover, if the CIA has developed the ability to hack the QNX operating system, it would give it control over more than just automobiles. In January, the company announced a new version of its software that is available for tasks that involve “surgical robots, industrial controllers and high-speed trains,” raising the potential for sabotage on an international scale.

Going further, it would apparently also be possible for the CIA to attack a car (or a factory, or a train) and make it seem as if another country did it. Part of the WikiLeaks revelations include a program known as “Umbrage,” which is a library of cyberattack techniques developed in other countries, including Russia. If one of these is designed to attack embedded systems, or if the CIA can make it look as if their code was developed in another country, the next time that a journalist investigating the CIA dies in a car crash, it might be claimed that it was the “Chinese” or the “Russians” who did it.