Véhicule comme arme à distance et sources d'informations avec les véhicules connectés

Dario Zugno
Adjoint au chef de l'Observatoire central des systèmes de transports intelligents
(pôle judiciaire de la Gendarmerie nationale)

Intervention faite le 7 octobre 2016 lors du colloque annuel de la Compagnie des experts de justice en criminalistique (CEJC) : "Criminalistique et technologies numeriques".

La conférence de l'Observatoire des systèmes de transport intelligents porte sur les risques de prise de contrôle à distance d'un véhicule autonome et d'en faire une arme par destination. Les surfaces d'attaque possibles sont passées en revue avec une estimation du risque « cyber » dans les véhicules. Un focus particulier sur la problématique des données contenues dans le véhicule est réalisé en mentionnant les opportunités quelles peuvent apporter à la gendarmerie.

Arme par destination / Cyber-attaque / Cybersécurité / Détournement / Données / Gendarmerie / Transport / Véhicule connecté / véhicule intelligent - ST, D, 02, 00

A recent conference presentation by the French think tank on intelligent transport systems covered the risk of the controls of a driverless car being taken over and the car being used as a weapon. Possible angles of attack were reviewed and an estimation provided of the extent of such 'cyber risk' to the vehicles. A specific focus of the presentation was on the problems related to the data contained in the vehicle and the resulting opportunities for the police to exploit it.

Une brève présentation en préliminaire de l'Observatoire central des systèmes de transport intelligents pose les fondements de sa création et les attentes de la Direction générale de la gendarmerie nationale le concernant.

Le sujet est le possible détournement de sa fonction initiale d'un véhicule autonome pour en faire une arme. Il est donc nécessaire de définir ce qu'est une arme par destination au sens du code pénal et d'en illustrer les propos à l'aide d'exemples concrets et récents, qui se sont produits en France et dans d'autres pays.

Il est également opportun de bien appréhender les différentes notions de véhicule connecté, intelligent et autonome pour se rendre compte que le véhicule de demain ne circulera plus seul dans sa bulle mais qu'il fera partie d'un ensemble de mobilité, vulnérable aux cyber-attaques par ses connectivités.

L'Observatoire a ainsi listé les surfaces d'attaque possibles sur un véhicule autonome avec une estimation du risque « cyber » lié à la sécurité et à la vie privée. Pour y remédier, une des solutions préconisées réside dans la « sécurité by design », c'est-à-dire la prise en compte des attaques possibles dès le début du processus de fabrication par une analyse des risques, l'application de standards et la conception des interfaces sur les risques de sécurité afin de construire un système robuste.


© iamsteckart

Se pose alors la question cruciale de la problématique des données et de leur appartenance. En France cette question n'est pas encore tranchée, alors qu'aux États-Unis les données appartiennent au propriétaire du véhicule. La gendarmerie a besoin d'avoir accès à ces données pour les raisons évoquées ci-dessous et milite pour l'installation d'un enregistreur de données dans le véhicule. Les constructeurs y sont également favorables ainsi que la Commission européenne des transports. Cet EDR (Event Data Record) permettra, en terme de sécurité routière, d'améliorer le comportement du conducteur par la simple connaissance de l'enregistrement. En terme de police judiciaire, l'EDR facilitera les enquêtes en apportant des données fiables de manière à répondre aux questions des enquêteurs et des magistrats.

Le projet de loi sur la justice du XXI° siècle, par l'adoption d'un amendement des députés et des sénateurs (art. L311-2 du CR), permettra aux forces de l'ordre d'accéder aux données et informations du véhicule par le système de diagnostic embarqué (prise OBD) pour vérifier la conformité du véhicule et des composants (VIN) afin de montrer si certaines pièces n'ont pas été frauduleusement remplacées.

L'application de principes clés serait un facteur de réussite afin de contrer les problèmes de cybersécurité sur le véhicule autonome ; parmi ces principes, la « sécurité by design », l'application d'un guide de bonnes pratiques et de standards pour obtenir une sécurité efficace et partager l'information recueillie sur des tentatives de piratage ou des piratages au sein d'un CERT, comme cela se fait pour les établissements bancaires. ■