EDITORIAL

Lorenzo Quolantoni
Rédacteur en chef adjoint

Créateurs d'icône auto recherchés

Le «père de la Ford Mustang» s'en est allé. Lee Iacocca est, en effet, décédé début juillet à l'âge de 94 ans, à Los Angeles. Le fils d'émigré italien a été l'une des figures les plus emblématiques de l'automobile durant les 30 glorieuses: il deviendra en 1970 le patron de Ford, avant de prendre la barre de Chrysler – au bord de la faillite – au début de la décennie suivante. Toutefois, Lee Iacocca restera dans les anthologies des grands hommes de l'automobile, non seulement pour sa brillante carrière de manager, mais aussi pour avoir participé à l'enfantement de la Ford Mustang de 1964. En effet, avant d'être gestionnaire, Lee Iacocca était ingénieur automobile, avec de l'essence à la place du sang. Cette sensibilité particulière, cette passion, l'ont poussé à croire dans le projet «Mustang», alors qu'il pouvait sembler risqué à l'époque. Une intuition gagnante, car Lee Iacocca mettait ainsi au monde l'une des plus grandes icônes automobiles. Ce qui nous renvoie à notre époque actuelle: où sont aujourd'hui les créateurs d'icônes automobiles?

A quelques exceptions près, ces dirigeants d'entreprises sont des managers, issus des plus grandes écoles du genre au monde, avant d'être des passionnés d'automobile. Ils ne sont obsédés que par quelques idées: croissance et rentabilité, afin de distribuer le maximum de dividendes aux actionnaires, tout en s'assurant bonus et pérennité au passage.

Oui, quand vient l'heure de prendre une décision, ces managers se démontrent froidement cartésiens: c'est ainsi que Ford a gommé toute sa gamme de berlines aux USA, pour vendre plus de SUV; c'est ainsi que Peugeot a biffé la descendante de la 208 GTI (avec moteur thermique). Bien sûr, l'industrie automobile ne peut vivre d'amour et d'eau fraîche, de Mustang et de Camaro, il faut produire des modèles rentables pour faire tourner la machine. Toutefois, ces modèles iconiques ont une portée bien supérieure au gain (éventuel) immédiat: leur aura rayonne sur toute la gamme, ce qui contribuera à la faire vendre. Ces «halo cars» sont surtout vecteurs d'image pour la marque; ce sont elles qui résisteront à l'épreuve du temps, qui feront rêver par-delà les générations. Elles sont l'héritage, l'empreinte qui restera d'un patron. Les profits milliardaires réalisés s'oublient vite, les modèles emblématiques, non.

Rendez-vous le 25 juillet

Chers lecteurs,
Vous retrouverez la prochaine édition de la Revue Automobile (n°30-31) dans deux semaines, le jeudi 25 juillet. Nous vous souhaitons, d'ici là, de bien recharger vos batteries et vous donnons, bien sûr, rendez-vous pour une édition avec son lot habituel de tests et de passion. **RÉDACTION RA**

Les nouveaux pirates de la route

Lorsqu'il est proche de l'auto, le pirate peut pénétrer dans la voiture via les interfaces Wi-Fi ou Bluetooth. Il peut aussi tromper les différents capteurs (radars, lidars, caméras) par des brouilleurs ou usurpateurs, pour faire voir à la voiture des obstacles inexistants.

CYBERSÉCURITÉ L'arrivée de la voiture autonome ira de pair avec l'émergence d'une nouveau danger pour la sécurité routière, le hacking. De quoi menacer l'existence de l'auto sans conducteur?

Lorenzo Quolantoni

La voiture autonome représente, depuis des décennies, une sorte de fantasme automobile; elle est la promesse d'arriver frais à sa destination, après un trajet passé à se relaxer. Les constructeurs se sont engagés depuis plusieurs années dans son développement, appâtés par l'énorme potentiel économique qu'elle recèle: avantage concurrentiel sur les autres marques et développement de services de robot-taxis.

Le développement de nouvelles solutions de mobilité deviend de toutes façons nécessaire, puisque 68% de la population mondiale vivra dans des villes en 2050 (contre 55% aujourd'hui), d'après un rapport des Nations Unies de 2018. Ce qui signifie davantage de bouchons potentiels, alors que la situation actuelle n'est déjà pas enviable dans certaines métropoles: il suffit de penser qu'à Tokyo, la vitesse moyenne d'une voiture n'est que de 15 km/h, selon l'équipementier Bosch.

Sans sécurité, pas d'avenir

Toutefois, un grain de sable pourrait enrayer cette splendide machine à faire du cash, avant même qu'elle ne démarre: le manque de sécurité. Si les autos sans conducteur ne se montrent pas beaucoup plus sûres que les humains, leur acceptation par le public serait compromise. Comme l'expliquait, en novembre dernier, le président du directoire du Groupe Volkswagen: «Un rapport de un à dix est de loin insatisfaisant. Nous avons environ 3200 morts par an sur les routes en Allemagne. Ce serait un désastre si nous avions 320 tués dans une voiture autonome.»

Pour prévenir cette situation, les constructeurs sont engagés dans le développement des voitures autonomes afin de les rendre fiables et sûres dans toutes les situations. Cependant, tous ces efforts pourraient être réduits à néant par les pirates informatiques qui pourraient «s'inviter» dans ces autos. La démonstration organisée par le magazine américain Wired avait passablement défrayé la chronique en 2015, quand deux hackers – Chris Valasek et Charlie Miller – avaient pris le contrôle d'une Jeep Cherokee à distance. Les deux acolytes avaient, en effet, exploité une faille du système d'infodivertissement pour agir sur les freins et l'accélérateur de l'auto. En 2016, un groupe de chercheurs chinois réussissait à pénétrer dans une Tesla Model S, via son navigateur internet et son système wifi; ils ont eu ainsi accès à différentes fonctions bénignes (le réglage des sièges arrière) mais aussi critiques, comme les freins.

Des ordinateurs sur roues

On le comprend, comme tout objet connecté, une automobile devient vulnérable dès lors qu'elle est reliée à internet. «Les voitures sont devenues des ordinateurs sur roues, explique Thierry Hayoz, en charge de l'innovation et du développement de la 5G chez Swisscom. Pour assurer un service de sécurité de bout en bout, il faut agir sur les trois éléments que sont le véhicule, le réseau de transmission ainsi que les applications.»

Prenons d'abord le premier maillon de cette chaîne, l'automobile elle-même. Les pirates informatiques peuvent exploiter une faille de leur interface Bluetooth (utilisée pour téléphoner en mains-libres) ou Wi-fi pour s'immiscer à l'intérieur de

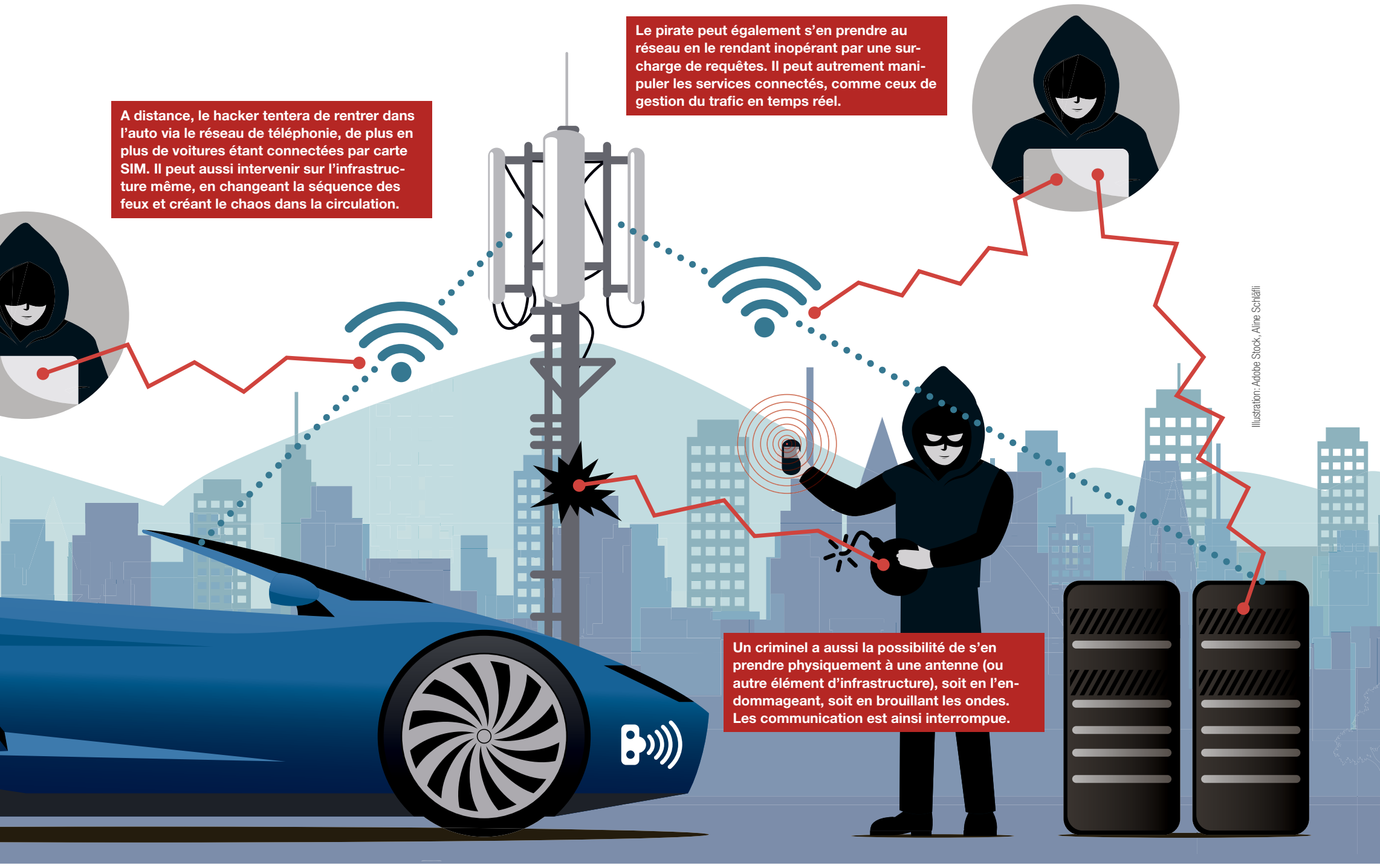

Illustration: Adobe Stock, Aline Schläfli

l'auto, s'ils se situent à proximité de la voiture. Les hackers peuvent autrement brouiller les différents capteurs utilisés par une voiture autonome, comme senseurs de proximités, caméras, lidars, radars et GPS. Le but: faire voir à l'auto une autre réalité, afin que l'auto prenne la mauvaise décision. En 2016, des chercheurs des Universités de Caroline du Sud et de Zhejiang (Chine) ont trompé les capteurs d'une Tesla Model S avec des brouilleurs et des usurpateurs acoustiques ou lumineux. Ils faisaient ainsi voir à la luxueuse berline électrique des obstacles qui n'existaient pas dans la réalité, causant des comportements erratiques de l'auto.

Des «fausses» antennes-relai

Pour mener ce genre d'attaques, les hackers doivent se situer près de l'auto. S'ils veulent rester assis chez eux, ils essayeront de s'immiscer par le réseau de téléphonie mobile auquel sont connectées les autos récentes, via une carte SIM. «Il existe aujourd'hui des ‹micro-cell›, qui se font passer pour des antennes des opérateurs, détaille Dimitri Konstantas, professeur à l'institut des sciences de l'information de l'Université de Genève. Les voitures autonomes peuvent s'y connecter, en pensant être reliée au réseau traditionnel. A partir de là, le hacker a le contrôle sur les flux de données qui entrent et qui sortent de l'auto.» Le pire des scénarios prévoit que les hackers prennent le contrôle des organes critiques pour la sécurité, tels les freins, l'accélérateur ou la direction, comme dans le cas de la Jeep Cherokee en 2015 (la marque a immédiatement apporté un correctif).

Le second niveau d'attaque concerne le réseau lui-même. Comme pour l'automobile, des offensives de proximité peuvent être menées via une attaque physique à une antenne (attentat) ou via des brouilleurs d'onde. Un danger que Thierry Hayoz relativise: «Il faut savoir qu'un véhicule est toujours connecté à plusieurs antennes en même temps pour assurer une continuité en déplacement. Ainsi, même si une panne affecte une antenne, le service sera assuré grâce aux autres antennes alentours.»

Réseau submergé

Le réseau peut aussi faire l'objet d'attaques «virtuelles», par exemple par une surcharge de requêtes qui bloqueront la connexion. Ces attaques, dites de «déni de service», rendraient inopérantes la transmission de données entre l'auto et les différents émetteurs/récepteurs nécessaires au fonctionnement de la voiture autonome. «Nous prenons cette thématique très au sérieux, d'autant que la 5G s'accompagne d'une augmentation de la bande passante, ce qui signifie des volumes de transmission plus grands, souligne Thierry Hayoz. Nous observerons si des anomalies se passent sur le réseau mobile, afin de les contrer et assurer la continuité du service en cas de cyberattaque. Nous sommes capables de segmenter et de rejeter les appareils qui sont à l'origine de l'attaque.»

Des services détournés

Enfin, le dernier niveau de l'attaque concerne les services offerts à ces autos connectées, comme la gestion du trafic en temps réel. Par exemple, un pirate pourrait envoyer des mauvaises informations aux véhicules autonomes sur l'état de la circulation, dans le but de faire converger toutes les autos vers un seul et même point.

Ces menaces pourraient ainsi sérieusement affecter l'adoption de la voiture autonome, en cas de désastre. C'est l'avis de Solange Ghernaouti, experte internationale en cybersécurité et directrice du Swiss Cybersecurity Advisory & Research Group: « Si c'est spectaculaire ou massif, cela peut effectivement avoir de fortes répercussions. Je pense qu'on peut faire le parallèle avec le clouage au sol des 737 MAX de Boeing à cause de la faille du dispositif de pilotage.» Conscientes du danger, les marques prennent des initiatives, à l'instar de Tesla, qui a organisé un concours de «hacking» autour de sa Model 3, en juin: la marque a récompensé par un prix en espèces les pirates qui ont mis au jour une faille de sécurité informatique de leur berline. De plus, on envisage d'isoler complètement les organes sensibles (accélérateur, frein, direction) du reste des systèmes de l'automobile.

Toutefois, ce ne sont là que les prémices d'une lutte sans fin. «Le hacking, c'est simple, c'est le jeu du chat et de la souris: à chaque fois que l'on barricade, le pirate tente de trouver une autre faille. Qu'on colmatera, ce qui poussera le hacker à trouver une autre vulnérabilité. C'est une bataille éternelle», lance Dimitri Konstantas. Sauf que nul ne sait ce qu'il se passera entre deux mises à jour du système embarqué. ●

LA 5G, UNE NÉCESSITÉ

L'avènement de la voiture autonome ne peut se faire qu'avec le déploiement du nouveau réseau 5G, mais l'avantage ne réside pas tant dans l'augmentation de la bande passante (jusqu'à 10 Gb/s). «La 5G, par rapport à la 4G, apporte surtout un temps de latence plus faible, (ndlr: le temps de réponse du réseau), explique Thierry Hayoz, de Swisscom. Sur l'ensemble de la chaîne – y compris la connection à nos serveurs – on parle d'une latence de 10 ms. C'est 4 à 10 fois plus performant que ce qu'on a sur le réseau 4G actuel. Une auto connectée a besoin de temps de transmission très bas afin de pouvoir prendre une décision la plus rapide possible.» L'autre avantage inhérent à cette technologie, c'est la possibilité de «découper» le réseau en fonction du niveau de criticité de l'application, continue Thierry Hayoz: «Certains objets connectés, comme un frigo, n'ont pas besoin d'une garantie de connexion permanente, contrairement aux véhicules autonomes, qui doivent être reliés en permanence et avoir une qualité de transmission. Ainsi, en cas de surcharge du réseau, nous serons en mesure de fractionner la capacité et de l'allouer en fonction des priorités.» Swisscom, pour rappel, avait déjà testé les besoins en connectivité d'une voiture autonome, via une expérience avec un prototype sans conducteur menée à Zurich en 2015.

«Des attaques inévitables»

CYBERSÉCURITÉ Pour Dimitri Konstantas, professeur à l'Université de Genève, le piratage d'une voiture autonome n'est qu'une question de temps; mais, selon lui, cette menace se sanctionnera pas la fin de cette technologie.

Interview: Lorenzo Quolantoni

On n'arrête pas le progrès: c'est ce qu'il ressort de l'entretien avec Dimitri Konstantas, professeur à l'institut des sciences de l'information à l'Université de Genève, à propos de l'avènement des véhicules autonomes. L'expert est concerné très directement par cette technologie, puisqu'il coordonne le volet genevois d'Avenue. Ce projet a vu le déploiement de petites navettes autonomes dans plusieurs villes du continent européen – Lyon, Luxembourg, Copenhague et Genève.

Revue Automobile: A quels niveaux se situent les vulnérabilités d'une voiture autonome?
Dimitri Konstantas: Il y aura de toute façon des attaques, c'est une certitude, on ne peut pas les éviter, surtout s'il y a de l'argent à se faire. Imaginez le cas suivant: vous circulez avec votre voiture autonome sur l'autoroute, quand un pirate se met à votre hauteur et vous demande de lui transmettre vos données de carte bancaire, car il a pris le contrôle de votre véhicule. Si vous n'obéissez pas, il menace de vous envoyer dans le décor. Le hacking, c'est simple, c'est le jeu du chat et de la souris: à chaque fois que l'on barricade, le pirate tente de trouver une autre faille. Qu'on colmatera, ce qui poussera le hacker à trouver une autre vulnérabilité. C'est une bataille éternelle, il est quasiment impossible de garantir un logiciel sans bugs. De plus, les mises à jour continuelles risquent de créer de nouvelles failles; il faudra des tests et des protocoles de contrôle beaucoup plus poussés dans le domaine automobile pour assurer la sécurité. Sans compter qu'il y aura tous les problèmes non prévisibles: certaines formes de hacking qui n'existent pas aujourd'hui verront le jour. Il faut aussi imaginer que certains voudront «bidouiller» leur automobile, en modifiant le système informatique embarqué: est-ce que ces ajouts seront compatibles avec le reste du réseau ou le paralyseront-ils? On le comprend, dans la chaîne de vulnérabilités, l'auto est le premier maillon, mais l'infrastructure, elle-même, représente aussi un danger: un pirate pourrait par exemple changer la séquence des feux de circulation ou, pire, bloquer le canal de communication via une attaque de déni de service.

Qu'est-ce qui pourrait motiver un hacker à pirater une voiture autonome?
Les principales raisons sont la fierté d'avoir piraté un système complexe et l'argent. Par exemple, si votre flotte de taxis autonomes a été piratée et immobilisée, peut-être serez-vous enclin à débourser de l'argent à un hacker, pour qu'il la libère; faute de quoi, vous perdrez de l'argent, car incapable d'exploiter vos véhicules. Le hacker peut aussi être terroriste ou criminel, pour éliminer un individu ou un groupe d'individus, en détournant son auto. Cela peut aussi être une guerre industrielle, entre concurrents.

Une série de graves accidents liés à un hacking peut-il «tuer» la voiture autonome?
Si cela arrive, on va certainement faire un pas en arrière, car les gens en auront peur. Le gouvernement mettra peut-être des lois plus strictes encore. Mais il faut mettre les choses en perspective: il y a eu des millions de tués ou blessés liés à l'automobile, mais personne ne veut pour autant interdire la voiture tout court. J'ai de la peine à imaginer un retour en arrière brutal, à cause d'une série de tués. Ce sera de toute façon un progrès, il y aura moins de morts. ●

Dimitri Konstantas pilote aussi le projet Avenue.

«Les consommateurs ne doivent pas servir de testeurs»

Solange Ghernaouti, experte internationale en cybercriminalité et directrice du Swiss Cybersecurity Advisory & Research group, craint que les logiques commerciales prennent le pas sur les questions de sécurité, en mettant des produits trop tôt sur le marché.

Revue Automobile: Quels sont les risques réels en rapport avec la voiture autonome?
Solange Ghernaouti: On retrouve ici les mêmes problèmes qu'avec la thématique de l'hyperconnectivité et de la dépendance au numérique. Il y a d'abord tout un volet lié à la protection de la sphère privée, puisque l'on est en permanence épié par tous ces capteurs reliés à leurs fabricants. Vient ensuite le problème des vulnérabilités qui peuvent engendrer des dysfonctionnements et être exploitées pour réaliser des cyberattaques. Après tout, la voiture connectée n'est rien d'autre qu'un smartphone dans lequel on peut s'asseoir. Certains constructeurs ont déjà dû rappeler des automobiles, car des failles de sécurité du système informatique ont été décelées. On se rend compte que la technique du «security by design» est encore assez mal maîtrisée par les constructeurs. C'est de là que vient la principale menace aujourd'hui. On peut imaginer des scénarios catastrophes, avec des prises de contrôle à distance, des détournements du fait d'actions criminelles ou terroristes, même si cela n'est pas encore répandu. Cela dépendra beaucoup des décisions prises en matière de cybersécurité. Ce qu'il manque à l'industrie du tout-connecté, c'est comme une agence internationale du médicament, qui certifierait le degré de sécurité, de fiabilité et d'innocuité d'un système avant sa commercialisation.

Solange Ghernaouti ne s'inquiète pas uniquement des risques de piratage, mais de l'utilisation des données des utilisateurs.

Les constructeurs automobiles sont-ils en retard dans le domaine de la sécurité informatique?
Non, je pense qu'ils ne sont pas plus mauvais que ceux qui gèrent des infrastructures critiques et qui n'ont pas assez pris en compte les cyber-risques; il y a peut-être un manque de maturité et de volonté. Le problème est complexe et la compétition économique dans ce secteur est énorme. Les constructeurs sont soumis à une logique de captation du marché et veulent être les premiers. Le temps pour passer de l'innovation technologique au produit du marché est limité, les investissements coûteux. La logique économique ne permet pas d'investir suffisamment dans la sécurité. Les logiques de marché prévalent sur les logiques de sécurité.

Toutefois, les risques liés à un hacking automobile sont bien plus élevés: on parle d'un danger de mort.
Bien sûr, mais tant qu'il n'y a pas de la part des consommateurs une pression pour refuser d'être les testeurs de systèmes non finalisés et non robustes au hacking, il est probable qu'il n'y aura pas d'amélioration de la cybersécurité. C'est le même problème rencontré avec le pace-maker connecté: des appareils ont été piratés. A leur conception, le choix a été fait de ne pas intégrer de mécanisme de sécurité, notamment pour économiser la batterie. Cela est la résultante de choix économiques et informatiques, qui correspond à une vision du monde de faire porter la nuisance du défaut de sécurité sur le consommateur.

Est-ce que des accidents répétés de voitures autonomes, liés à du hacking, pourraient «tuer» la voiture autonome?
On peut faire le parallèle avec les crashs des avions 737 MAX de Boeing, à cause d'une faille du dispositif informatique de pilotage et qui sont désormais cloués au sol. Voyager avec un tel système ne peut pas faire envie ! Si le hacking de voitures autonomes est spectaculaire ou massif, cela peut effectivement avoir de fortes répercussions.