DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

LES VÉHICULES AUTONOMES SONT-ILS COMPATIBLES AVEC LES HALLUCINATIONS DE L'IA ?

Publié le 27 septembre 2018

par Laetitia Theunis

En voiture, Simone! Dès le 3 octobre, une navette autonome emmènera les touristes du parking au pied de la butte de Waterloo. Un voyage d'un kilomètre à bord d'un véhicule piloté exclusivement par une intelligence artificielle (IA). Ce sera la deuxième expérience de ce type sur la voie publique en terre wallonne. Face au probable avènement futur d'une multitude d'engins roulants dénués de pilotes humains sur nos routes, on peut s'interroger : qu'en est-il de la perception visuelle de l'IA embarquée ? Est-elle infaillible ? Avant d'aborder cette thématique, petit tour d'horizon.

Le premier test belge de véhicule autonome sur la voie publique a cours depuis début septembre à Han-sur-Lesse (photo en tête d'article). Là-aussi, ce sont les touristes qui sont transportés sur une courte distance par un engin dépourvu de pilote humain. Le bus évolue à une vingtaine de km/h sur 500 mètres de route grâce à des données GPS et au lidar (télémètre déterminant la présence d'un objet dans un environnement proche) embarqué. Toutefois, la connaissance de la priorité de droite lui faisant défaut, il a fallu modifier localement les priorités pour éviter tout accident avec les conducteurs humains.

Six pays européens testent les véhicules autonomes

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

La Belgique fait partie des pionniers en termes de tests de véhicules autonomes sur la voie publique. Alors qu'il y a fort à parier que tous les pays européens emboîteront bientôt le pas, des essais ont aussi lieu aux Pays-Bas, en Allemagne, au Grand-Duché de Luxembourg, en Suède et en France. Ainsi, en février 2018, la société Berthelet, basée à Lille, a installé une navette autonome sur un site industriel à Dunkerque. Depuis lors, elle transporte 150 personnes par jour sur une distance de 800 mètres. Deux autres projets naîtront d'ici fin d'année. L'un consistera en une navette à l'aéroport de Lyon. L'autre est plus ambitieux : l'engin autonome sera plongé au coeur de la circulation automobile urbaine sur 1,5 km, et devra même emprunter deux ronds-points.

Nombreux sont ceux qui prophétisent que de curiosités évoluant sur de courts tracés, les véhicules autonomes pourraient rapidement envahir notre réseau routier. Mais quand exactement ? **François Bellot, Ministre fédéral (MR) de la Mobilité donne son pronostic :**

http://dailyscience.be/NEW/wp-content/uploads/2018/09/Ministre-Belot-SMART-MOBILITY.mp3

L'intelligence artificielle peut souffrir d'hallucinations

Le discours dominant clame que la technologie est au point. Mais ça et là, des chercheurs mettent en garde : l'IA souffre de faiblesses. Et non des moindres : il peut arriver à l'intelligence artificielle de souffrir… d'hallucinations.

Quand l'IA lit un panneau routier prioritaire en lieu et place d'un signal stop, vous conviendrez que c'est plutôt fâcheux dans le cas d'une voiture autonome. Trop gros pour être vrai ? Et pourtant, c'est bel et bien le résultat d'une expérimentation menée aux Etats-Unis. Des chercheurs ont recouvert un panneau stop d'un filtre algorithmique transparent ayant la caractéristique d'en modifier la valeur de quelques pixels. Alors que l'humain continuait d'y voir un panneau stop classique, le robot aidé de sa caméra l'identifiait désormais comme un panneau de priorité.

Concrètement, les risques de sécurité associés à un tel piratage visuel sont-ils importants? « Dans le cas spécifique des véhicules autonomes, je n'en suis pas sûr. Comme d'autres chercheurs l'ont souligné, il est beaucoup plus facile de renverser physiquement un panneau stop que de générer un autocollant qui peut, ou non, tromper l'algorithme de vision. Cela est néanmoins un sujet de débat parmi les chercheurs », explique le Dr Jonathan Peck, spécialiste des mathématiques des réseaux de neurones à l'Université de Gand.

Des dysfonctionnements visuels interpellants

La littérature scientifique comprend d'autres exemples d'hallucination de l'AI. L'un d'eux a été réalisé par des chercheurs de Google. Revêtant le costume de pirates informatiques, ils ont subtilement modifié la valeur de quelques pixels sur une photo de panda. Résultat ? Alors que l'œil humain continue d'y voir le même ursidé, l'algorithme, quant à lui, identifie un singe gibbon avec un degré de confiance de 99,3 %!

Si cela peut prêter à sourire, ça devient nettement moins drôle quand on se rappelle que ces algorithmes, qu'on peut aisément duper aux dires de spécialistes, sont voués à envahir notre quotidien. Qu'adviendra-t-il quand ils prendront un feu rouge pour un feu vert, une cellule cancéreuse pour un organe sain, un hôpital pour une cible militaire, le visage d'un terroriste pour celui d'un quidam sans histoire ? « De nombreuses méthodes ont été développées pour tenter d'éviter ces illusions d'optique, mais leur performance est loin d'être satisfaisante pour le moment », déplore le Dr Peck.

« Indépendamment du fait qu'ils présentent ou non un risque de sécurité réel, de tels exemples contradictoires soulignent que les modèles d'apprentissage automatique que l'on applique actuellement à l'intelligence artificielle ne se généralisent pas aussi bien que nous le souhaiterions.

Depuis 2017, l'intérêt pour la recherche sur ce phénomène a fortement augmenté. C'était d'ailleurs un des sujets principaux de la conférence internationale sur le Machine Learning de cette année. » Il faut dire que les chercheurs peinent encore à comprendre ce qui se trame réellement dans les réseaux de neurones profonds, briques de l'IA.

Cette faille visuelle de l'IA va-t-elle freiner voire sonner le glas de la révolution numérique en cours ? L'avenir le dira.