ID de Contribution: **16** Type: **Non spécifié**

Robustesse des algorithmes

vendredi 25 septembre 2020 10:00 (45 minutes)

Des travaux récents ont montré que malgré l'utilisation de méthodes « classiques » de validation et de régularisation, les réseaux de neurones peuvent être vulnérables face à d'éventuelles attaques adverses. L'exemple de vulnérabilité est celui d'une modification légère d'une image sur quelques pixels qui peut suffire à tromper le réseau de neurones [Szegedy,2016]. Le cours introduira la formalisation de la vulnérabilité de l'apprentissage machine, des illustrations en reconnaissance de formes et quelques solutions envisagées pour rendre l' apprentissage plus robuste.

Orateur: Dr MARTINEZ, Jean-Marc (CEA - DES)