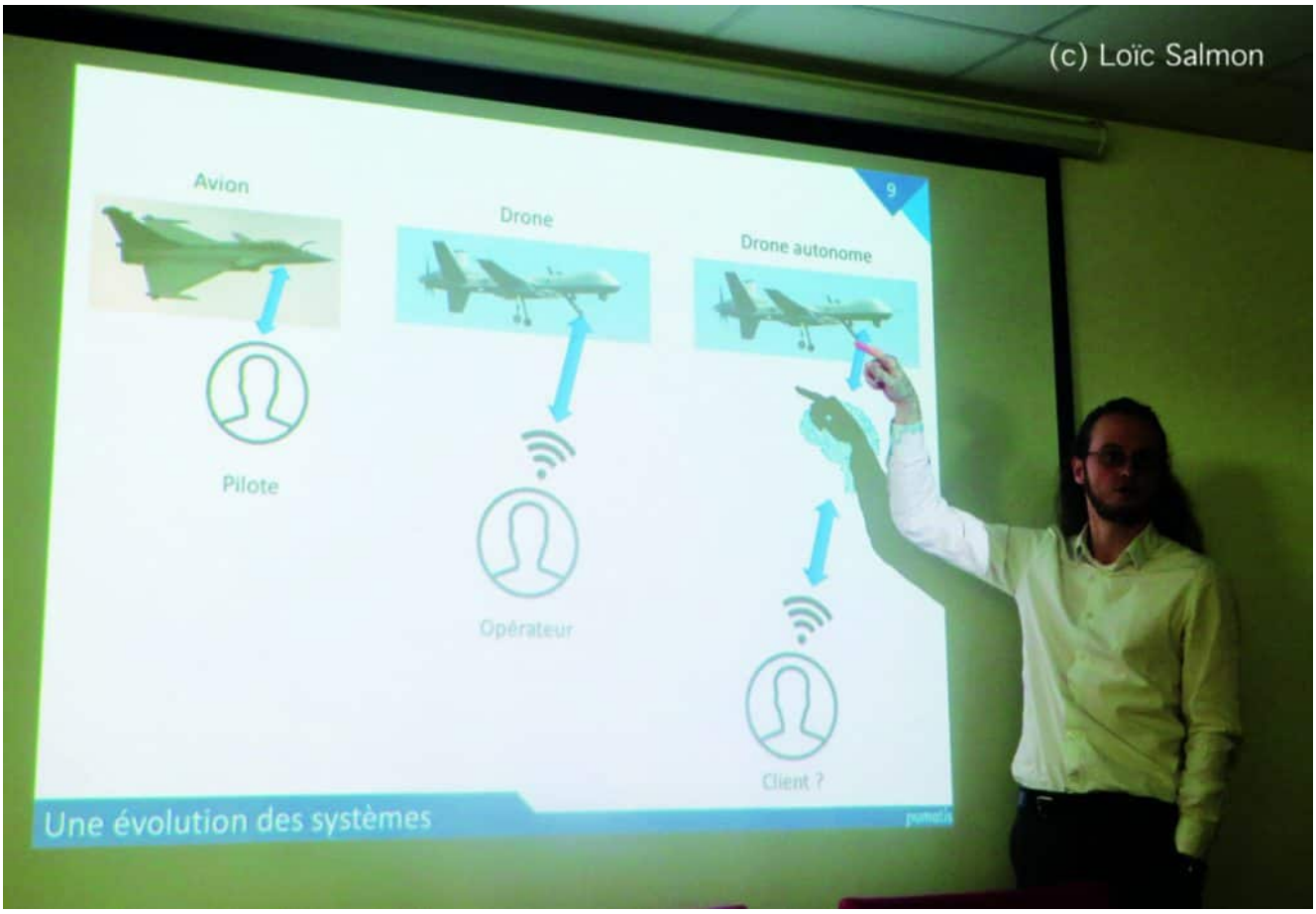
# Défense : intelligence artificielle, vers une norme internationale de fiabilité




La maîtrise des risques liés à l'intelligence artificielle (IA) dans l'industrie de défense implique la détermination de normes ISO pour assurer la fiabilité des systèmes futurs.

Arnault Ioualalen, directeur général de la société Numalis, en a expliqué les enjeux au cours d'une conférence de presse organisée, le 24 septembre 2018 à Paris, par le Groupement des industries de défense et de sécurité terrestres et aéroterrestres (GICAT). Numalis fournit des outils logiciels de validation et d'aide à la conception de « systèmes critiques » appliqués à l'aéronautique, l'espace et la défense.

**Evolution des systèmes.** L'IA trouve des applications directes dans la maintenance, la sécurité, la détection de cible, les drones, les missiles, la robotique et les systèmes optroniques. En matière de frappe, il s'agit d'apporter

une aide à la décision qui reste du ressort de l'homme. Ainsi dans le guidage terminal d'un drone autonome, il faut éviter l'automatisme du « fire and forget » (tu tires et oublies). Le « client » (utilisateur) fixe les exigences de la mission et en définit les paramètres pour atteindre l'objectif. Le pilote d'un avion ou l'opérateur d'un drone armé qui doit procéder au tir d'un missile, véritable robot qui suit la cible par sa signature thermique, peut décider de l'annuler au dernier moment pour une raison politique ou éthique (victimes collatérales). Quant aux tirs automatiques de systèmes d'armes américains, israéliens ou coréens (installés à la frontière entre les Corées du Nord et du Sud), la décision, prise en amont, ne peut empêcher les erreurs (ratés ou « bavures »). L'IA va permettre d'augmenter la capacité à comprendre et mieux évaluer la cible. Elle va améliorer les systèmes existants pour les rendre plus performants et moins coûteux pour l'utilisateur et l'industriel. Dans le flux des données, elle trie les informations nécessaires qui remontent la chaîne de décision pour la manœuvre ou le bombardement. Elle aide ainsi à la décision en amont, alors qu'une décision automatique manque de fiabilité.

**Réseaux de Neurones.** L'IA dite « connexioniste » consiste à mimer les mécanismes biologiques du raisonnement humain par les techniques du « Deep Learning » (réseaux de neurones). Ne pouvant retrouver que ce qu'elle connaît, l'IA se spécialise dans un seul usage comme la reconnaissance d'images, l'identification ou la prédiction de comportement en temps réel. Cela nécessite des normes pour établir une relation de confiance entre le concepteur de l'IA et son utilisateur. Il s'agit d'abord de montrer la robustesse et la sécurité de l'IA par une approche technique transverse. Ensuite, il convient de rassurer les citoyens sur son équité, sa transparence et sa confidentialité. Enfin, il faut constituer une barrière juridique contre la « colonisation numérique » (reconnaissance des données et leur traitement) par la responsabilisation des fabricants et vendeurs de systèmes.

**Course internationale.** L'IA suscite une compétition globale entre les Etats-Unis (entreprises privées) et la Chine (moyens étatiques). France, Allemagne, Grande-Bretagne, Irlande et Canada s'y intéressent de façon active. Russie, Italie, Israël, Japon, Inde et Corée du Sud se spécialisent sur certains sujets. Australie, Finlande, Suède et Luxembourg en observent les évolutions. En France, la Direction générale de l'armement suit l'ingénierie d'IA pour les armées. Au sein du comité ISO, le GICAT et Numalis présentent le projet français « Generate »,

norme de fiabilité du « Deep Learning ».

**Loïc Salmon**

Sécurité : l’intelligence artificielle, enjeu de souveraineté nationale

Drones : préparer le combat aérien de demain