Présentation « Projets » Chaire Cyber résilience aérospatiale

Les activités réalisées dans le milieu aérospatial reposent à la fois sur un nombre important de ressources techniques distribuées et intégrées dans de multiples réseaux physiques et numériques (systèmes cyber-physiques, Contrôle Commande, …), et sur des opérateurs humains.

L'essor de nouvelles technologies (communications à haut débit, Drones (véhicules (agents intelligents) autonomes), Essaim de drones (Multi-agents intelligents autonomes) , optimisation des tâches par l'utilisation de ressources à distance (Nuage numérique), capacités prédictives/d'aide à la décision dues au développement de programmes d'analyse (apprentissage ou intelligence artificielle) de banque de données en masse (Big Data)) inspire aujourd'hui de nombreux nouveaux cas d'utilisation dans le domaine aérospatiale (civil et militaire).

La Cyber résilience aérospatiale est une aptitude utile en temps de « crise » dont les mécanismes (Prévision de la cyber menace, Prévention de cette menace, Protection des systèmes contre les menaces résiduelles, Reconnaissance des signes d'une attaque en cours, Réponse à une attaque détectée, Rétablissement de la performance nominale des missions) sont le fruit d'une ingénierie (Theron, 2013).

Cet essor pose une question centrale : comment assurer la continuité des activités aérospatiales au regard des nouvelles stratégies de déploiement et de missions militaires et civiles, et plus largement de l'utilisation grandissante des systèmes cyber-physiques (avec /ou sans autonomie) sous la menace de cyber attaques ?

Les principales questions sont :

- A quels types de menaces les systèmes cyber-physiques de l'aérospatial doivent-ils se préparer à faire face ?
- Qu'est-ce qu'être résilient à la cyber menace dans de nouveaux contextes d'utilisation ? Dans ce cadre, quelles compétences et quelles aides cognitives individuelles et collectives faut-il développer pour réagir à de possibles cyber-attaques, aussi bien au niveau des centres de décision et/ou de commandement qu'au niveau des ressources exécutantes (utilisateurs, opérateurs) ?
- Quelles dispositions techniques mettre en œuvre pour assurer la résilience des systèmes cyber physiques ?
- Comment prendre en compte la cyber-menace dans les processus d'acquisition, de développement, d'utilisation et de maintenance des systèmes aérospatiaux ?
- Comment former et entraîner le personnel concerné à la résilience ?

L'objectif de la chaire « Cyber résilience Aérospatiale » de l'armée de l'air est d'étendre la connaissance du comportement des systèmes sociotechniques aérospatiaux confrontés à la cyber menace. Il s'agit d'en préciser l'ontologie et de développer des modèles permettant d'explorer et de comprendre les rôles, les comportements et les interactions des acteurs humains, des composantes technologiques et des facteurs organisationnels qui sont impliqués tant dans la cyber attaque que dans la cyber défense des systèmes cyber-physiques du milieu aérospatial. Son projet est donc interdisciplinaire, à l'interface des sciences cognitives, des sciences de l'ingénieur et de l'informatique, et des sciences de l'organisation.

La chaire « Cyber résilience aérospatiale » de l'armée de l'air propose ainsi de soutenir les travaux de recherche visant à :

- Explorer, décrire et modéliser la dynamique, les mécanismes, les moyens et les performances possibles des nouvelles cyberattaques et des nouvelles techniques de cyberdéfense sur les futurs systèmes aérospatiaux. Développer une plateforme technique de simulation, de recherche et de démonstration ad hoc.
- Mieux comprendre la prise de décision (individuelle et collective) située dans des environnements décisionnels numérisés où la performance opérationnelle et décisionnelle dépend de l'intégrité et de la fiabilité des informations stockées, diffusées et partagées
- Explorer les processus cognitifs individuels et collectifs face à une cyber attaque sur les futurs systèmes aérospatiaux
- Contribuer au développement de l'ingénierie de formation, de préparation et d'entraînement des opérateurs et des décideurs confrontés à la menace cyber dans le domaine aérospatial
- Mieux comprendre comment améliorer la Cyber résilience aérospatiale au fil des étapes de la chaîne de valeur et du cycle de vie des systèmes (chaîne de production, supply chain, Maintenance).