# Chaire Cyb'Air™

## Chaire Cyber Résilience Aérospatiale

## Armée de l'Air - Dassault - Thales

## Appel à candidats

**Intitulé proposé** : De l'organisation d'un système multi-agent de cyberdéfense : application aux agents AICA

**Ecole doctorale** : Ecole Doctorale MSTII – Université Grenoble Alpes

**Directeur de thèse** : Pr J.-P. Jamont et Pr M. Occello

**Co-encadrants académiques** :

**Tuteur en entreprise** : Dr P. Théron

**Entreprise sponsor** : THALES

**Lieu(x) de réalisation** : LCIS – Valence

**Temps plein / partiel** : ☑ Temps plein (3 ans) ☐ Temps partiel (6 ans)

**Echéances** : Dépôt des dossiers : 30/06/2021 Démarrage : Septembre / Octobre 2021

**Langues de rédaction** : ☑ Français ☐ Anglais

**Confidentialité de la thèse** : ☐ Classifiée ☑ Publique

**Présentation du sujet**

**Problématique générale** :

Dans un contexte dans lequel le nombre d'incidents de sécurité croît continuellement et dans lequel la complexité des attaques est de plus en plus importante, la thèse se penchera sur le choix d'une organisation pour des systèmes multi-agents (SMA) de cyberdéfense. Elle aura pour objectif la production d'une architecture de SMA/Agent multi-dimensionnelle répondant aux contraintes de la cyberdéfense.

**Background** :

La création d'une application de cyberdéfense prend la forme d'un déploiement de composants logiciels sur une plateforme cible. Ce déploiement se fait en fonction de différents critères qu'il faut clairement identifier et hiérarchiser en faisant souvent appel à l'expérience des spécialistes.

Pour l'analyse et la conception de systèmes requérant ces propriétés, l'exploitation du concept de SMA semble la bienvenue car elle permet l'intégration d'objectifs/contraintes globaux/locaux et rend possible une délégation de la prise de décision aux entités logicielles elles-mêmes au plus près de leur contexte d'exécution [Calo2017].

Alliant de grandes capacités de décision adaptatives basées sur des connaissances complexes et une décentralisation apportant une sureté de fonctionnement, les SMA sont capables de mettre en œuvre les facteurs évolués à prendre en compte dans la prise des décisions du contexte cyberdéfense.

Les fonctionnalités requises pour un agent de cyber défense ont été étudiées au sein de l'OTAN et exposées dans le méta-modèle AICA (Autonomous Intelligent Cyber-defence Agents [Théron 2018, Kott 2019, Kott 2020]). Les agents AICA auront la charge de protéger collectivement des systèmes hôtes complexes. Dans l'architecture MASCARA (Multi Agent Centric AICA Reference Architecture [Théron 2020]), chaque agent est conçu comme un système multi-agents (les agents sont alors

nommés micro-agents). Un agent AICA est lui-même un système complexe opérant dans le cadre d'un système hôte complexe, par exemple un Internet of Battle Things (IoBT [CCDC 2017]).

Cette notion de SMA introduit une "rupture de technologie" qui vise à voir le déploiement comme le choix d'une structure organisationnelle. Plus loin, l'adaptation du système peut être renforcée en délégant aux entités logicielles elles-mêmes une partie relative à leur déploiement en rendant la structure adaptative par une organisation dynamique. Des mécanismes de réorganisation ou d'auto-organisation peuvent alors permettre de commuter entre plusieurs organisations [Wester-Ebbinghaus 2008].

Il s'agit alors d'établir une caractérisation des critères de partitionnement et de déploiement de ces systèmes afin de construire ces organisations et leur dynamique dans le contexte cyberdéfense.

[Calo2017] Calo, S. B., Touna, M., Verma, D. C., & Cullen, A. (2017, December). Edge computing architecture for applying AI to IoT. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 3012-3016). IEEE.
[CCDC 2017] Internet of Battlefield Things (IOBT), CCDC Army Research Laboratory. February 7, 2017.
[Jamont2015] J.-P. Jamont, M. Occello: Meeting the challenges of decentralized embedded applications using multi-agent systems. Int. J. Agent Oriented Software. Eng. 5(1): 22-68 (2015)
[Kott2019] Kott, A., Theron, P., Drašar, et al. (2019). Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture, Release 2.0. Adelphi, MD: US Army Research Laboratory
[Kott2020] A. Kott, P. Théron: Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience. IEEE Secur. Priv. 18(3): 62-66 (2020)
[Théron2018] P. Théron et al. : Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture, Int. conf. on military communications and information systems (2018)
[Théron2020] P. Théron; J.-P. Jamont et al. : A first prototype of the Multi Agent System Centric AICA Reference Architecture (MASCARA), 1st NCIA – AICA IWG Technical Workshop, AICA Agents' reference architecture session, (2020)
[Wester-Ebbinghaus 2008] Wester-Ebbinghaus, M., Moldt, D., & Köhler-Bußmeier, M. (2008, September). From multi-agent to multi-organization systems: Utilizing middleware approaches. In International Workshop on Engineering Societies in the Agents World (pp. 46-65). Springer, Berlin, Heidelberg.

**Question(s) de recherche** :

Ce travail propose d'étudier les modalités possibles de déploiement et les stratégies d'auto-organisation / réorganisation d'un SMA de cyberdéfense autonome intelligent, compte tenu des contraintes (environnement technique de déploiement, environnement protecteur de cybersécurité, …) et de la présence de malware intelligent.

Un objectif essentiel consiste à déterminer les critères de déploiement des fonctionnalités de l'agent AICA en une organisation multi-agent multi-dimensionnelle adaptative.

**Méthodologie envisagée** :

La thèse mènera de front un travail méthodologique, l'étude d'un cadre fondamental et une approche expérimentale.

Le travail méthodologique aura pour objectif d'analyser les contraintes de décision, de déploiement, de sécurité, de dimensionnement, de communication, imposées par un système de cyber défense.

Un état de l'art sera dressé qui analysera les organisations de SMA disponibles, mono ou multi-niveaux, hiérarchiques, récursives, pures ou hybrides. Il fixera le cadre fondamental de l'étude.

L'approche expérimentale consistera dans un premier temps l'analyse des fonctionnalités du méta-modèle AICA et la réalisation d'une implémentation d'étude.

Elle la projettera ensuite sur chacune des catégories de contraintes établies et en tirera des préconisations pour le choix d'une organisation multi-agent AICA et de sa dynamique.

**Contribution / Utilité envisagée** :
La contribution attendue est double.

(1) Il s'agit d'élaborer d'une part un modèle flexible d'organisation pour un système multi-agent de cyberdéfense autonome intelligent du type « AICA ».

(2) Il faut d'autre part produire les éléments d'accompagnement méthodologique pour l'ingénierie et le déploiement d'un tel SMA.

**Défis théoriques ou pratiques** :

Un premier défi, qui relève de la démarche de recherche, est de réaliser ce travail de choix d'organisation tout en garantissant la couverture des fonctionnalités de cyber défense autonome de l'agent AICA.

Un défi pratique technique est lié à la déployabilité des systèmes composés de plusieurs agents de type AICA dans un environnement hôte équipé de dispositifs de protection cyber (firewalls, antivirus, etc.) susceptibles de contrecarrer l'action de ces agents.

**Attentes particulières** :

Ce travail de thèse devra livrer un prototype qui pourra ultérieurement être réutilisé par d'autres chercheurs notamment, et sa documentation de base.

**Attentes vis-à-vis du/des candidat(s) & Description des acquis**

**Niveau d'étude requis** : ☑ Master (Recherche préféré) ☐ Doctorat ☐ Autre :

**Spécialisation** : Informatique, Intelligence Artificielle, Systèmes Multi-agents

**Connaissances et compétences préalables (attendues)** :

- des compétences en architecture logicielle seront nécessaires,
- une sensibilisation à la cybersécurité serait un plus.

**Langues maîtrisées** : ☑ Français ☑ Anglais ➔ Niveau : ☑ scientifique

**Nationalité** : ☑ Française ☐ Autre

**Dossier de candidature**

☒ Pour candidater, envoyer si possible la copie du mémoire de Master (ou d'un article ou travail de synthèse bibliographique)
☒ Copie des diplômes