

Chaire de cyberdéfense des systèmes Navals *Enjeux pour Thales*

www.thalesgroup.com



EN TANT QUE PARTENAIRE INDUSTRIEL

- > Maintenir un haut niveau de coopération entre le monde opérationnel, universitaire et industriel pour amener les meilleures réponses aux menaces cyber
- > Participer à la formation d'experts de haut niveau en cybersécurité pour anticiper les besoins de recrutement
- > Stimuler la réflexion et l'innovation

ADRESSER / CONSOLIDER LES THEMES CLES DE RECHERCHE

- > **Thème 1 : futures architectures logicielles et systèmes pour traiter et contenir l'érosion cyber**
- > **Thème 2: confiance conférée à l'IA pour la connaissance, l'aide au commandement et la gestion de crise cyber**
- > **Thème 3 : communications et résilience des systèmes et organisations**
- > **Thème 4 : intégrité et cybersécurité des systèmes industriels**
- > **Thème 5: exploration et continuité des perspectives identifiées dans les précédents doctorats: consolidation et capitalisation des expertises**



SUIVRE TROIS LIGNES D'EFFORT *(actuelles et futures)*

01



Axe Technologique

02



Axe métier Coalition
de circonstance

03



Axe métier
Cyberdéfense
embarquée



AXE TECHNOLOGIQUE

> Cyberprotection

Sécurisation des communications acoustiques (liaisons inter-UUAV et Porteur/UUAV)

> Data Centric Security (DCS)

Décentralisation au-delà du DCS-3

Prise en compte dynamique d'entités non planifiées dans l'action (traité par la chaire cyber Saint-Cyr)

> Application du Zero Trust (ZT) aux systèmes de combat naval

Fiabilité vs confiance dynamique

Intégration d'agents autonomes de cyberdéfense dans les sous-systèmes

Enrôlement d'un sous-système de circonstance

Standards d'interopérabilité

> Déploiement d'agents IA embarqués permettant de détecter des anomalies ou des attaques

Dans les systèmes de gestion de navire (SMS) et/ou de gestion de combat (CMS)

Dans les systèmes de supervision contrôle et acquisition de données (SCADA)



AXE MÉTIER : COALITION DE CIRCONSTANCE

Architecture sécurisée pour la confiance dynamique

> Echange de données tactiques dans un système de combat naval

Blue Force Tracking

Guidage d'armes

DCS 3

> Processus de gestion des droits et des éléments cryptographiques

Evolution des architectures de sécurité visant à intégrer les aspects comportementaux dans la gestion des droits d'accès et le besoin d'en connaître (traité par la chaire cyber Saint-Cyr)

Enrôlement et Révocation de sous-système sur opportunité

> Cybersurveillance & Cyberdéfense

Apprentissage fédéré pour la détection

Techniques de confidentialité différentielle

AXE MÉTIER : CYBERDEFENSE EMBARQUÉE (1/2)

> Cyberdéfense agentique en milieu naval

Cas d'usage cibles

- SMS/CMS
- Senseurs
- SCADA de puissance et propulsion / surveillance des cales

Menaces

- Spoofing GNSS
- Injection de malware
- Mouvements latéraux SCADA-PLC
- Nouvelles attaques facilitées par l'IA (empoisonnement de données, leurrage d'IA...)

Coopération des agents dans les systèmes de systèmes de plateforme ou de combats

Conditions de faisabilité, notamment la préservation de la fiabilité

AXE MÉTIER : CYBERDEFENSE EMBARQUÉE (2/2)

> Gestion des vulnérabilités

Evaluation de l'impact sur le système

- Conditionnalité de l'homologation
- Lien entre l'homologation et l'impact de la vulnérabilité (i.e. contournement d'authentification)

Priorisation des actions de MCS

- Système patchable par conception et exigences d'application des correctifs en phase opérationnelle
- Patchs virtuels ; filtrage actifs des éléments protocolaires pouvant générer le défaut

Configuration dynamique de la détection d'intrusion

- Actualisation des chemins d'attaques

Prise en charge par des agents autonomes



Merci

www.thalesgroup.com