CYB'AIR
CHAIRE
CYBER RÉSILIENCE
AÉROSPATIALE



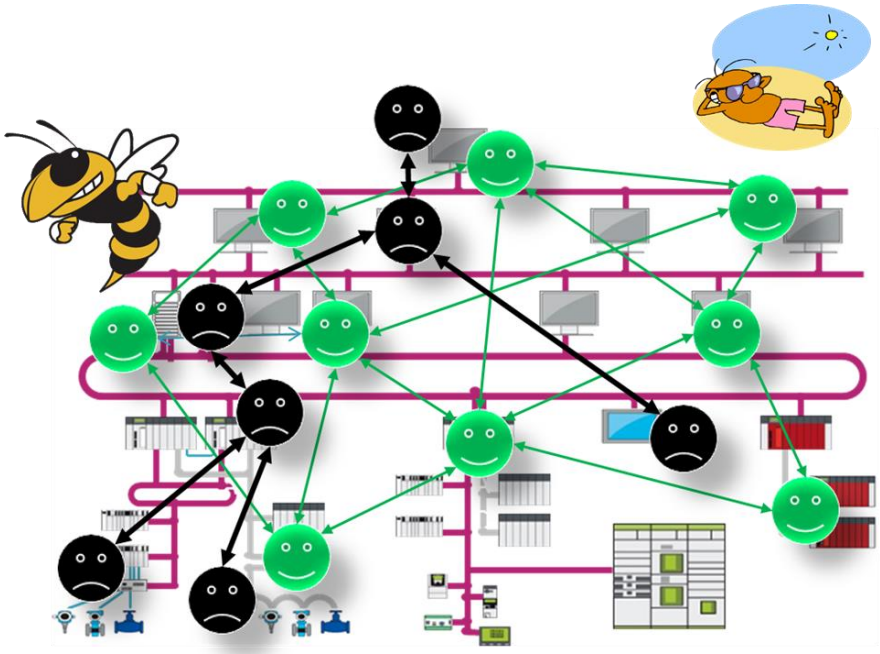


La cyber défense autonome : Clé du succès des futures technologies connectées ?

Dr Paul THERON, Thales, Directeur de la chaire Cyb'Air, Chairman AICA IWG
Deuxième journée de la chaire C3S, 11 décembre 2020

Sponsors THALES DASSAULT AVIATION

La cyber défense autonome ?



1. La cyber défense autonome comme hypothèse
2. Principes des agents AICA
3. Applications des agents AICA : Défense & systèmes civils
4. État de l'art
5. Défis scientifiques et techniques
6. Un premier prototype en construction
7. La prise de décision des agents
8. AICA International Work Group
9. La chaire Cyb'Air
10. Thèses, Post-docs, Master & Projets collaboratifs « AICA agents »

CYB'AIR

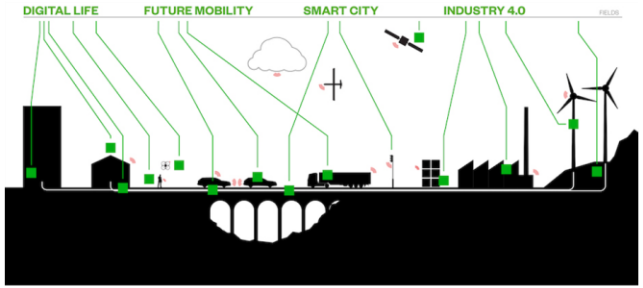
La cyber défense autonome comme hypothèse

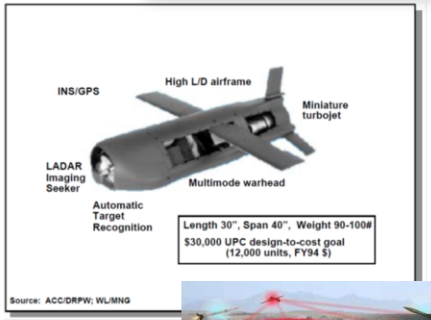
AUTONOMOUS CYBER-ATTACKS

5G

COMPLEXITY

AUTONOMY

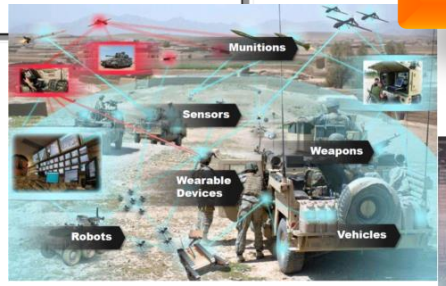




Quantum

LAWS

SAFETY & RAPIDITY



HUMAN COGNITIVE LIMITS

SDN

AI

Cloud

...

EFFICIENCY & RESILIENCE

Intelligent Things will fight intelligent Things

Kott, A., 018. *Bonware to the Rescue: the Future Autonomous Cyber Defense Agents.* Washington DC, Conference on Applied Machine Learning for Information Security, October 12, 2018, CAMLIS.

CYB'AIR

Principes des agents AICA

Autonomous Intelligent Goodware will fight Autonomous Intelligent Malware

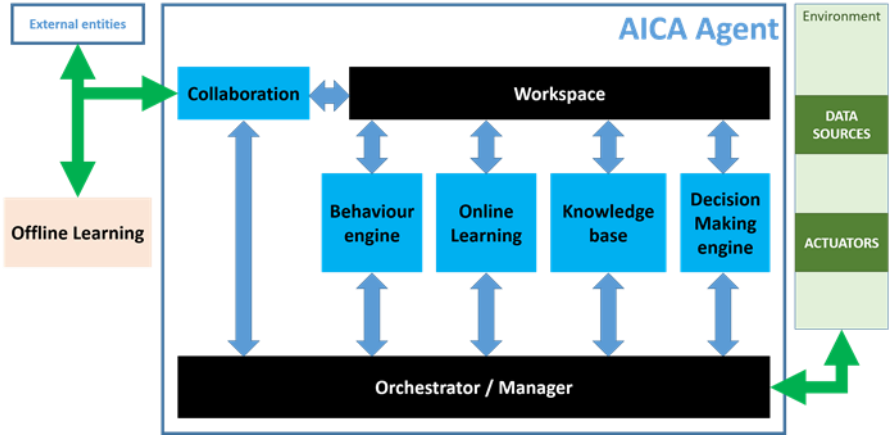
- Humans out of the loop
  - A major paradigm shift

Trustworthiness

Fitting the host architecture's constraints

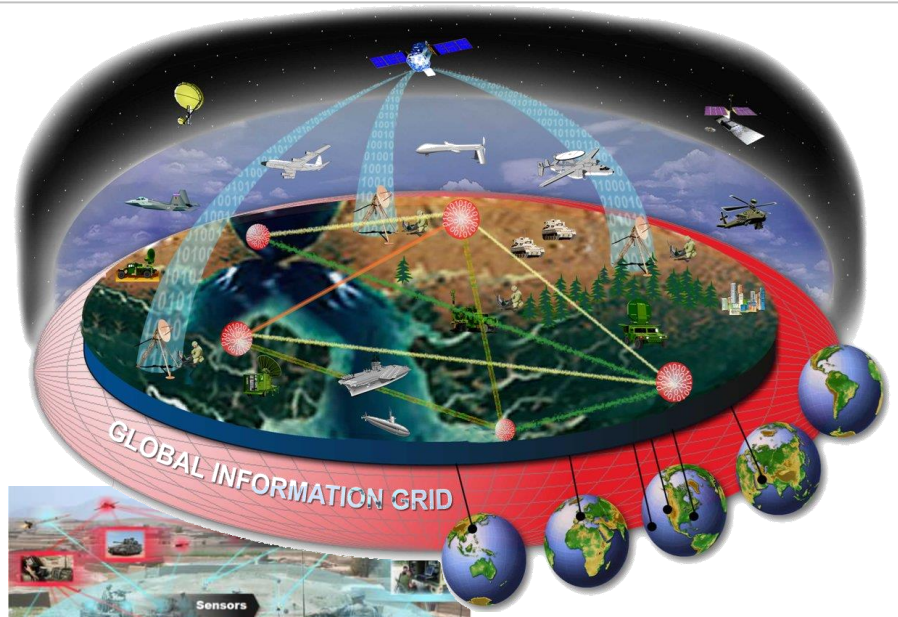
Interoperability

Autonomous Intelligent Cyber-defence Agents (AICA)



CYB'AIR

Applications des agents AICA : Défense & systèmes civils



Intelligent Things will fight intelligent Things

Kott, A., 018. *Bonware to the Rescue: the Future Autonomous Cyber Defense Agents.* Washington DC, Conference on Applied Machine Learning for Information Security, October 12, 2018, CAMLIS.

No Automation (Level 0)

- The human driver must complete all driving tasks even with warnings from vehicles.

Driver Assistance (Level 1)

- The automated system shares steering and acceleration/deceleration responsibility with the human driver under limited driving conditions (e.g., high speed cruising), and the driver handles the remaining driving tasks (e.g., lane change).

Partial Automation (Level 2)

- The automated system fully controls the steering and acceleration/deceleration of vehicles under limited driving conditions, and the human driver performs remaining driving tasks.

Conditional Automation (Level 3)

- The automated system handles all driving tasks under limited driving conditions, and expects that the human driver will respond to requests to intervene (i.e., resume driving).

High Automation (Level 4)

- The automated system handles all driving tasks under limited driving conditions even if the human driver does not respond to requests to intervene.

Full Automation (Level 5)

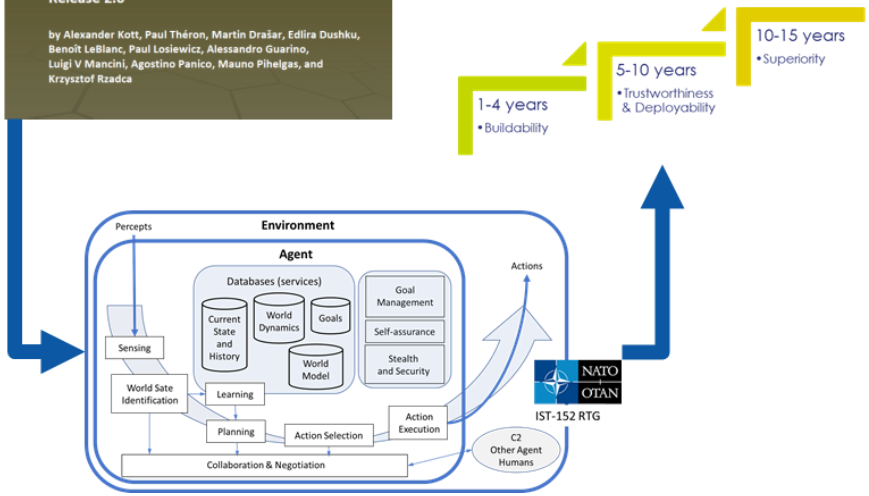
- The automated system takes full control of all driving tasks under all driving conditions that can be managed by a human driver.

MIN

MAX

CYB'AIR

État de l'art



A really new research current

The heart of AICA agents is their Decision Making "engine"

- Trustworthiness ➔ Smart DM
- Many algorithmic bricks but…
  - No DM techniques integration framework

Implementing AICA agents

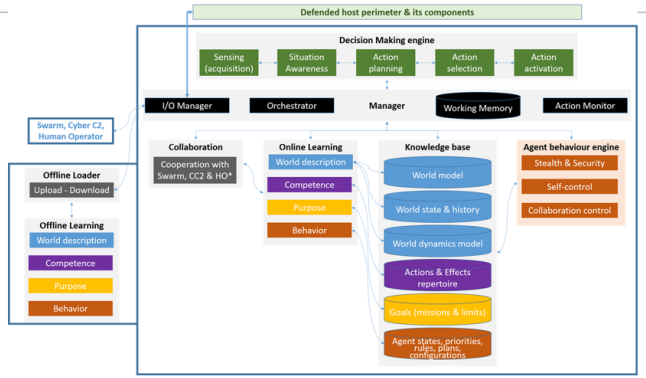
No doctrine yet

CYB'AIR

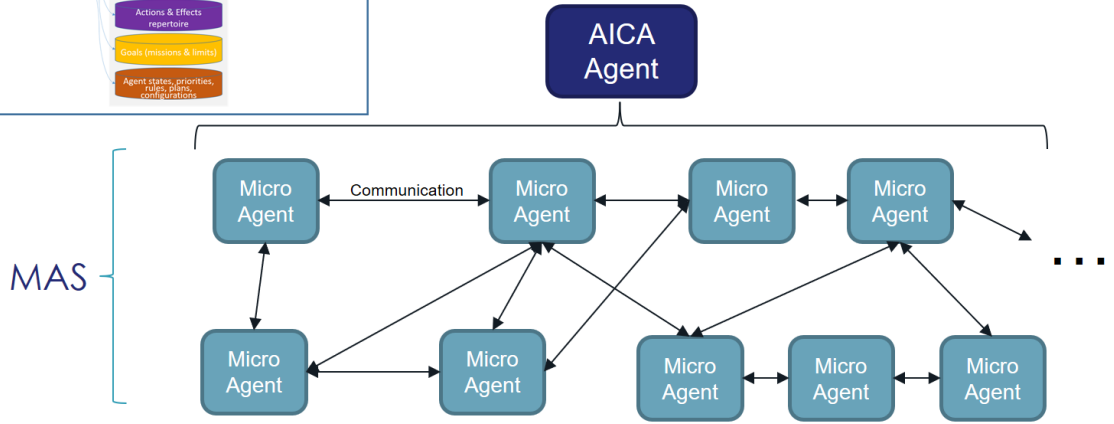
Défis scientifiques et techniques

Un premier prototype en construction

The MASCARA architecture: Each agent is a MAS



MASCARA: **M**ulti **A**gent **S**ystem **C**entric **A**ICA **R**eference **A**rchitecture



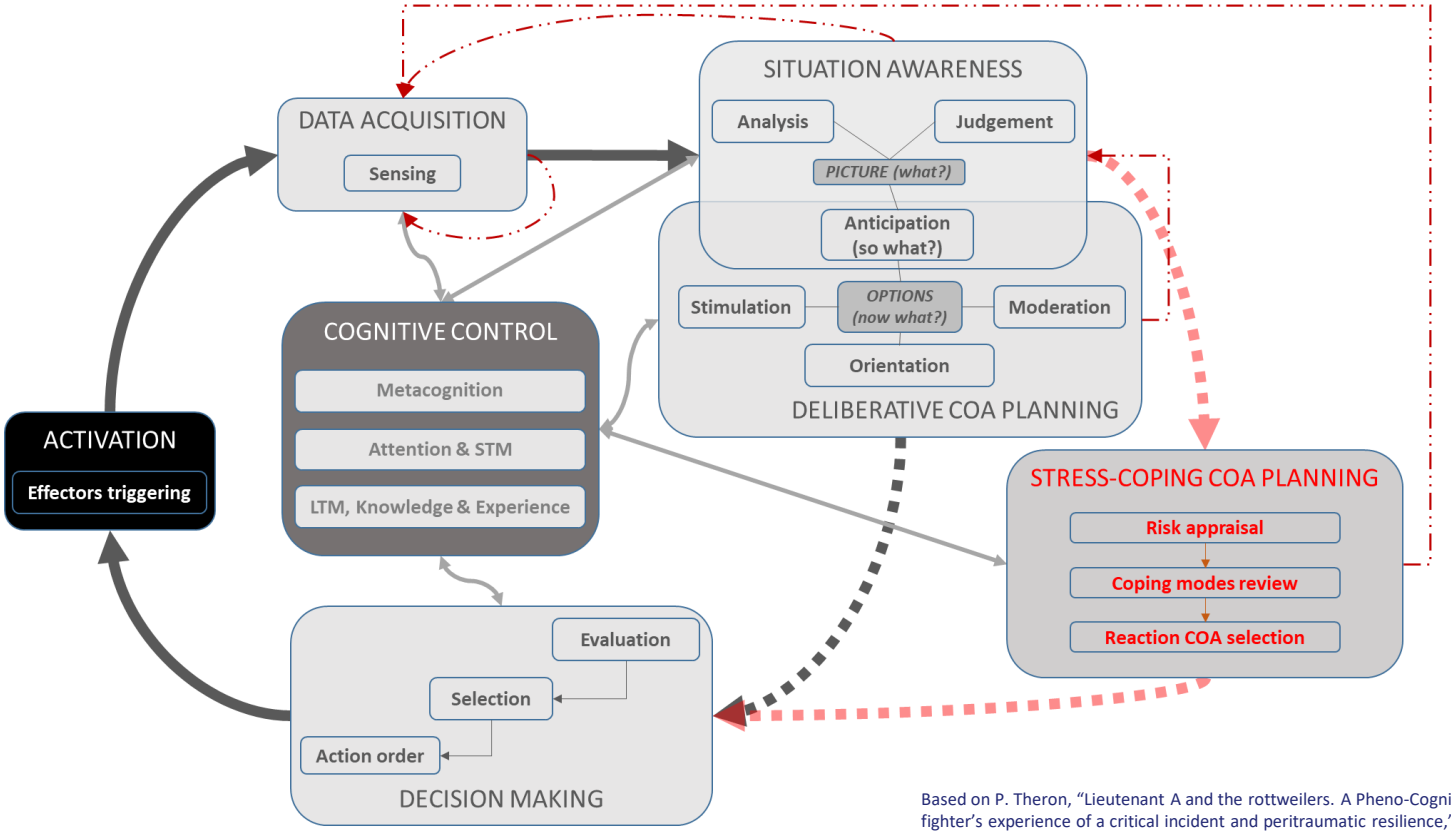
PUBLIC

CYB'AIR

PUBLIC

CYB'AIR

La prise de décision des agents



Based on P. Theron, "Lieutenant A and the rottweilers. A Pheno-Cognitive Analysis of a fire-fighter's experience of a critical incident and peritraumatic resilience," PhD Thesis, available at https://sites.google.com/site/cognitionresiliencetrauma, University of Glasgow, Scotland, 2014.

CYB'AIR

AICA International Work Group

DEFENSE

- **OTAN** (NCIA)
- **OTAN** (CCDCOE)
- **US Army Research Laboratory**, USA;
- **US Army Corps of Engineers**, Boston, USA;
- **US Navy, Center for Naval Analyses**, USA;
- **Netherlands Defence Academy**;
- **Westpoint Academy**, USA;
- **Ministry of Defence,** UK;

UNIVERSITE & RECHERCHE

- **MIT**, USA;
- **Dartmouth College**, USA;
- **Indiana University,** USA;
- **Vanderbilt University**, USA;
- **Rochester Institute of Technology**, USA;
- **Pennsylvania State University**, USA;
- **Bordeaux INP**, ENSC, France;
- **Grenoble INP**, LCIS, France;
- **Universita di Roma La Sapienza**, Italie;
- **Universität der Bundeswehr München**, Allemagne;
- **University of Liechtenstein**;
- **Imperial College**, UK;
- **Masarick University**, Tchèquie
- **Czech Technical University**, Tchèquie;

INFRAS CRITIQUES & RECHERCHE

- **Pacific Northwest National Laboratory**, USA;
- **Argonne National Laboratory**, USA;
- **Idaho National Laboratory**, USA;

ETUDES AMONT/PRE-NORMALISATION

- **MITRE Corporation**, USA;

INDUSTRIES DE DEFENSE & ICT

- **Thales**, France ;
- **Raytheon Technologies,** USA;
- **Northrop Grumman**, USA;
- **Cythereal Predictive Cyber**, USA;
- **Boston Fusion,** USA;
- **Culmen, LLC**, USA;
- **PWC,** Norvège;
- **Riskaware,** UK;
- **NORSECON,** Suède;
- **StAG srl,** Italie.

CYB'AIR

La chaire Cyb'Air

CYB'AIR
CHAIRE
CYBER RÉSILIENCE
AÉROSPATIALE

AICA
AUTONOMOUS INTELLIGENT CYBERDEFENCE AGENTS
INTERNATIONAL WORK GROUP
Chapter

2017-2022, et au-delà…

Programme scientifique axé sur la cyber défense autonome (AICA agents)

Priorités (*Projets collaboratifs, Thèses, Post-docs, Projets de Master*)

- Développement d'un prototype d'agent AICA
- Environnement de simulation et d'essai
- Coopération Cyber Cognitive
- Cadres d'emploi

Collaborations académiques

- Grenoble INP / LCIS, Bordeaux INP / ENSC, Ecole de l'Air
- Autres chaires

Sponsors THALES DASSAULT AVIATION

Thèses, Post-docs, Master & Projets collaboratifs « AICA agents »

Thèses financées (CIFRE) & Post-docs

- Thales, Dassault, …
- École doctorale
  - Selon sujet de la thèse

Projets de Master

- Projets techniques ponctuels
- Formations dans les Masters

Et aussi les projets collaboratifs (longitudinaux)

- Études amont
- Études techniques
  - Prototypage et architecture des agents; Plateformes de simulation, test, entrainement…

Contact: paul.theron@thalesgroup.com

CYB'AIR

CYB'AIR
CHAIRE
CYBER RÉSILIENCE
AÉROSPATIALE

Merci pour votre attention…

Et à votre disposition.





Quelques références

- https://arxiv.org/abs/1803.10664 (IST-152 RTG's AICA Reference Architecture final report)
- https://arxiv.org/abs/1804.07646 (Report of Oct 2017 Prague workshop)
- http://ceur-ws.org/Vol-2057 (proceedings of Oct 2017 Prague workshop)
- https://arxiv.org/abs/1806.08657 (ICMCIS conference paper, Warsaw, May 2018)
- https://www.springer.com/fr/book/9783030334314 (2020 Springer book chapter)
- https://ieeexplore.ieee.org/abstract/document/9091352 (2020 IEEE Security & Privacy paper)