CALL FOR PRESENTATIONS

2nd International Conference on Autonomous Intelligent Cyber-defence Agents (AICA 2022)

Bordeaux, France and Hybrid

May 2-3, 2022

Important Dates:
Deadline for Submissions: 31 March 2022
Notification of acceptance: 14 April 2022
Camera-ready: 30 April 2022
Conference: May 2-3 2022

Faced with future hugely complex networks, systems and infrastructures on one hand, and with the anticipated huge growth of safety-critical autonomous systems on the other hand, human operators will not be in a position to monitor the cybersecurity of these assets and will not be able anymore to respond to cyber-attacks at the speed, scale and level of complexity needed. For instance, on the battleground, when Intelligent Things fight Intelligent Things in the future, Autonomous Intelligent Malware (AIM) will seek to disable our defence platforms, networks and command and control systems. Our complex networks and systems and/or autonomous military systems and infrastructures will not work without embedding trustworthy autonomous cyber-defence technology that will fight enemy autonomous intelligent malware and other forms of cyber-attacks, at speed and scale.

Autonomous Intelligent Cyber-defence Agents – AICAs – are being recognized as a key enabler of present and future military networks, devices and combat doctrines. AICAs are also being developed for the cyber defence of civil networks and systems (critical infrastructures, manufacturing, connected vehicles).

AICA 2022 will present the state of the art in Autonomous Cyber Defence. It will allow to discuss issues, gaps and challenges. Its conclusions will feed future research and contribute to creating a wider AICA research & technology community. The AICA 2022 conference invites presentations and hands-on demonstrations focused on the two topics:

1 - Best Methodologies to build Autonomous Intelligent Cyber-defence Agents (AICAs)

AICAs' architecture(s) must allow autonomous agents to be deployed within host systems aimed for military combat, as well as for civil applications. Host systems generate many constraints such as those due to operational missions' fast pace or changes, differences in computing and memory capacities between systems, distributed resources and networking, AI and software-defined networks and radio communications, systems and data classification, embarked cybersecurity, complexity, autonomy, stealth, self-healing systems or software, validation, certification and qualification for security. Speakers are expected to present ongoing research on the building of AICAs, architectural designs and their rationales, novel methods for creating AICAs that can be embedded in and compatible with host systems, models for the security accreditation process of autonomous agents in the context of allied operations.

2- AICAs' Dynamic Decision-Making

In future highly-complex networks and systems, Intelligent Goodware will fight Intelligent Malware. In this context, Agents' Decision-Making processes, based in effective learning models that enable them to gain knowledge about actions of hostile actors, is key to their trustworthiness. In these cyber battles, AICAs will face many unpredictable situations to which their decisions will need to adapt. AICAs' smart decisions will be those that win the battle, not

those that counter single adversary moves and risk the enemy gaining the initiative. Speakers are expected to present: cognitive architectures for AICAs and the need for analogies with human reasoning; novel uses of Machine Learning (ML) for making smart decisions in the fight against enemy malware; cooperation of formal knowledge bases and ML to enhance AICAs' decision-making capacities; how to assure that AICAs' decisions do not impede the safety of combat operations; communication and collaboration between AICAs and with human operators; designs of agent-agent and agent-human cooperation frameworks; methods by which agents can measure progress in their collaboration; advantages of multi agent collective decision-making; methods to make agents capable of diverse forms of reasoning needed to both achieve their mission and survive in a battlefield where enemy agents target them through a variety of cyber-attacks and deception strategies.

PRESENTATIONS SUBMISSION

Authors are invited to submit extended abstracts or short papers related to the above topics, written in English, with a minimum length of 1000 words and a maximum of 4000 thousand words. A slide deck to be showed during the conference (either on site or virtually) will be appreciated. Submissions should be made electronically in PDF format and sent to the following email address: aica22@aicaconfrence.org. At least one author of each accepted presentation must register for the conference and present (either on site or remotely).

WORKSHOP OR DEMONSTRATION SESSIONS SUBMISSIONS

Authors are also invited to submit free form proposals for hands-on workshops or demonstrations of AICA prototypes and related development. These sessions will be held in the mornings of May 2 and 3 and at least one author will be expected to lead the session on site, in Bordeaux. Submissions should include a description of the software/environment to be presented and of the infrastructure that will be needed. Systems and support will be provided by the venue and will be discussed with the authors. Please send your proposals to the address aica22@aicaconference.org

CONFIRMED KEYNOTE SPEAKERS:

Alexander Kott, USARL, USA

STEERING COMMITTEE

Alexander Kott, USARL, USA
Paul Theron, Thales, Cyb'Air Research Chair, France
V.S. Subrahmanian, Northwestern University, USA

CONFERENCE CHAIRS

Bênoit LeBlanc, École Nationale Supérieure de Cognitique, Bordeaux, France
Alessandro Guarino, StAG srl, Italy
S. Jay Yang, Rochester Institute of Technology, USA. (TBC)