CALL FOR PRESENTATIONS

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

Bordeaux, France and Online

October 25-26, 2022

Important Dates:
Deadline for Submissions: 19 September 2022
Notification of acceptance: 30 September 2022
Conference: October 25-26 2022

Human operators will increasingly need to contend with extremely complex networks, systems and infrastructures while simultaneously managing risks due to the fast anticipated growth of safety-critical autonomous systems on the other hand. Human operators will not be able to effectively monitor the cybersecurity of these assets and will struggle to respond to cyber-attacks at the speed, scale, and level of advanced adversaries employing automated or adaptive offensive tactics. For instance, in a future where Intelligent Things fight Intelligent Things on the battlefield, Autonomous Intelligent Malware (AIM) may seek to disable defence platforms, networks, and command and control systems. Complex networks, systems, and/or autonomous military systems and infrastructures will not be defensible 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 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 facilitate discussion of relevant issues, gaps, and challenges. Its conclusions will feed future research and contribute to creating a wider AICA research & technology community.

The AICA International Work Group developed and distributed, under an Open Source Licence, a prototype of an Autonomous Intelligent Agent. AICA 2022 intends to present and promote this result in a practical workshop and invites any contribution building on this work or any other prototyping development currently ongoing. AICA 2022 invites any research or industrial actor involved in AICA prototyping to propose sessions and contributions.

The prototype is available at https://github.com/aica-iwg/aica-agent.

The AICA 2022 conference additionally invites presentations and hands-on demonstrations in the following two topic areas:

1 - Methodologies for Building Autonomous Intelligent Cyber-defence Agents (AICAs)

AICA's 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- Methodologies for Autonomous Dynamic Decision-Making

In future highly-complex networks and systems, Intelligent Goodware will fight Intelligent Malware. In this context, robust and explainable Agent Decision-Making processes, based on effective learning models that enable them to gain knowledge about actions of hostile actors, is key to their trustworthiness. In cyber battles, AICAs will face many unpredictable situations to which their decisions will need to adapt. 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 autonomous decision-making capabilities; how to assure that automated decisions do not impede the safety of combat operations; communication and collaboration between autonomous agents 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 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 words. A slide deck to be shown during the conference (either onsite or virtually) will be appreciated. Submissions should be made electronically in PDF format and sent to aica22@aicaconfrence.org. At least one author of each accepted presentation must register for the conference and present (either onsite 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 on the mornings of Oct 25 and 26 and at least one author will be expected to lead the session onsite 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 aica22@aicaconference.org

CONFIRMED KEYNOTE SPEAKERS:

Mauro Conti, University of Padova, Italy

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)