CALL FOR PAPERS

CyberAIS 2027

International Workshop on Artificial Intelligence and Agentic Systems for Cybersecurity

In conjunction with the 19th International Conference on Agents and Artificial Intelligence (ICAART 2027)

February 26, 2027 | Valletta, Malta

Workshop website: https://icaart.scitevents.org/CyberAIS.aspx

Artificial Intelligence (AI) is reshaping the cybersecurity landscape, enabling new approaches to threat detection, security analysis, and cyber defense. Recent advances in machine learning, large language models (LLMs), and agentic AI offer promising opportunities to develop intelligent, adaptive, and increasingly autonomous security solutions. These advances also introduce challenges related to reliability, explainability, robustness, and the safe deployment of autonomous security agents.

CyberAIS 2027 aims to bring together researchers, scientists, engineers, and practitioners working at the intersection of artificial intelligence and cybersecurity. The workshop will provide a forum for presenting original research findings, discussing emerging challenges, and exchanging innovative ideas on AI-driven cybersecurity, intelligent security operations, and agentic cyber defense.

Contributions are invited on novel methods, algorithms, models, architectures, and frameworks, as well as experimental studies, prototypes, datasets, and benchmarks. Research addressing the practical deployment and evaluation of AI-based and multi-agent security solutions is particularly welcome.

TOPICS OF INTEREST

Area 1: AI-Based Intrusion and Threat Detection

- Machine learning and deep learning for intrusion and anomaly detection
- Advanced detection of malware, botnets, and emerging cyber threats

Area 2: AI-Driven Threat Intelligence, Security Analysis, and Digital Forensics

- AI-assisted threat intelligence, threat hunting, and attack-chain analysis
- LLMs and retrieval-augmented generation for security analysis and reasoning
- AI-assisted digital forensics, incident reconstruction, and evidence analysis

Area 3: Agentic AI and Multi-Agent Systems for Cyber Defense

- Autonomous security agents and collaborative multi-agent architectures
- Agent reasoning, planning, coordination, and tool use for cyber defense

Area 4: Intelligent Security Operations and Incident Response

- AI-driven alert triage, investigation, and SOC automation
- Agent-based response orchestration, decision-making, and automated containment

Area 5: Adaptive and Proactive Cyber Defense

- AI-driven cyber deception and adaptive defense strategies
- Reinforcement learning and intelligent decision-making for proactive defense

Area 6: Security, Robustness, and Trustworthiness of AI-Based Defense

- Adversarial attacks against AI models, LLMs, and defensive agents
- Explainability, robustness, human oversight, and safe autonomous operation

Area 7: Evaluation of AI and Agentic Cyber Defense

- Datasets, benchmarks, and cyber ranges for intelligent cyber defense

- Evaluation of detection effectiveness, autonomous decision-making, reliability, and operational performance

Application domains include, but are not limited to, enterprise networks, cloud and edge infrastructures, IoT and Industrial IoT, 5G/6G networks, satellite communications, cyber-physical systems, ICS/SCADA, critical infrastructures, connected and autonomous vehicles, UAVs, and healthcare systems.

PAPER SUBMISSION GUIDELINES

Authors are invited to submit original and unpublished research papers in English for double-blind peer review.

- **Regular Papers** must be submitted as anonymized PDF files containing 10,000 to 50,000 characters (excluding spaces), including references, tables, figures, and appendices.
- Following peer review, accepted Regular Papers will be classified as Full Papers or Short Papers:
- **Full Papers:** up to 12 pages in the proceedings; 25-minute oral presentation.
- **Short Papers:** up to 8 pages in the proceedings; 20-minute oral presentation or poster presentation.
- Up to 4 additional pages may be allowed for an extra fee.
- All papers must follow the official conference templates and be submitted electronically through the online submission system.

Submission guidelines: https://icaart.scitevents.org/Guidelines.aspx

Paper templates: https://icaart.scitevents.org/Templates.aspx

Workshop and submission information: https://icaart.scitevents.org/CyberAIS.aspx

PUBLICATION AND INDEXING

Accepted papers will be published in a dedicated section of the ICAART 2027 Conference Proceedings, published by SCITEPRESS (ISBN), with individual DOIs. Papers must be presented at the event to be made available online through the SCITEPRESS Digital Library.

The proceedings will be submitted for indexing in Scopus, Web of Science (Conference Proceedings Citation Index), DBLP, Google Scholar, Semantic Scholar, EI, and other indexing services.

IMPORTANT DATES

Paper submission deadline	December 3, 2026
Authors notification	December 21, 2026
Camera-ready and registration	January 8, 2027
Workshop date	February 26, 2027

KEYNOTE SPEAKER

Prof. Axel Sikora
Offenburg University of Applied Sciences, Germany

Keynote title: “Legacy, Intelligent, and Agentic Security for Networked OT-Systems in the Era of Intelligent Cybercrime”

ORGANIZING COMMITTEE

Workshop Co-Chairs

- Slim Rekhis, SUP'COM, University of Carthage, Tunisia
- Nejla Essaddi, ISTIC, University of Carthage, Tunisia

Technical Program Committee

- Walid Abdallah, Aviation School of Borj El Amri, Tunisia
- Giampaolo Bella, University of Catania, Italy

- Nihel Benyoussef, University of Tunis El Manar, Tunisia
- Adnane Cabani, IRSEEM, France
- Nesrine Kaaniche, Telecom SudParis, France
- Yvon Kermarrec, IMT Atlantique, France
- Rida Khatoun, Independent Researcher, France
- Yosra Lakhdhar, University of Carthage, Tunisia
- Maryline Laurent, Telecom SudParis, France
- Wojciech Mazurczyk, Warsaw University of Technology, Poland
- Aref Meddeb, University of Sherbrooke, Canada
- Mohamed Mejri, Laval University, Canada
- Henrich C. Pöhls, University of Passau, Germany
- Axel Sikora, Offenburg University of Applied Sciences, Germany
- Bruno Silva, University of Beira Interior, Portugal
- Maha Sliti, University of Carthage, Tunisia
- Hajer Tounsi, University of Carthage, Tunisia
- Mark Vella, University of Malta, Malta
- Wiem Zemzem, University of Carthage, Tunisia

More members to be announced.

CONTACT AND FURTHER INFORMATION

Workshop website: https://icaart.scitevents.org/CyberAIS.aspx

Workshop Secretariat: icaart.secretariat@insticc.org

We look forward to receiving your contributions to CyberAIS 2027. Please feel free to distribute this Call for Papers among your colleagues, research groups, and professional networks.