1st International Workshop on Symbiotic AI for Cyber-Social Security (SAI4CSS'26): Human–AI Collaboration for Social Resilience and Trustworthy Digital Ecosystems

Vita Santa Barletta[1], Danilo Caivano[1], Antonietta Curci[2] and Annita Larissa Sciacovelli[3]

[1]*Department of Computer Science, University of Bari Aldo Moro, Italy*
[2]*Department of Education, Psychology, Communication, University of Bari Aldo Moro*
[3]*Department of Law, University of Bari Aldo Moro*

Abstract

The growing interdependence between digital technologies and social systems calls for a new paradigm in cybersecurity, capable of addressing not only technical vulnerabilities but also social, psychological, and ethical risks. Symbiotic Artificial Intelligence (SAI) represents a step forward in this direction, promoting a collaborative ecosystem in which humans and AI systems co-evolve to enhance collective security, resilience, and trust. This workshop aims to explore the convergence between Cyber-Social Security (CSS) and Symbiotic AI, fostering multidisciplinary dialogue among computer scientists, social scientists, psychologists, legal experts, and policy-makers. The goal is to design and discuss human-centered, explainable, and ethically aligned AI frameworks that can detect, interpret, and mitigate emerging social-cyber threats such as hate speech, misinformation, online gender-based violence, and digital manipulation. Through contributions combining theoretical models, empirical studies, and demonstrative applications, the workshop seeks to define the foundations of a Symbiotic AI for Cyber-Social Security (SAI4CSS) framework. This includes the integration of human-in-the-loop learning processes, multimodal social sensing, and transparent decision-making to support trustworthy digital ecosystems.

Keywords

Cyber-Social Security, CSS, Social-Threats, Cybersecurity, Digital Society, SAI, Artificial Intelligence

1. Preface

The rapid convergence of digital technologies, artificial intelligence, and interconnected socio-technical ecosystems is profoundly reshaping the cybersecurity landscape. Contemporary cyber threats no longer target only information systems and digital infrastructures; instead, they increasingly exploit the complex interactions between technology, information, human cognition, and the physical world. Consequently, the impact of cyber incidents extends well beyond technical consequences, propagating across four interconnected domains that characterize the **Cyber-Social Security (CSS)** paradigm: the *Cyber* domain, where attacks originate and affect digital assets; the *Informational* domain, where information is created, manipulated, and disseminated; the *Cognitive* domain, where perceptions, decisions, trust, and human behavior are influenced; and the *Physical* domain, where cyber events ultimately generate tangible consequences on critical infrastructures, organizations, and society.

Addressing these multidimensional challenges requires moving beyond traditional technology-centric approaches toward human-centered and interdisciplinary security models. In this context, **Symbiotic Artificial Intelligence (SAI)** emerges as a promising paradigm that promotes effective collaboration between humans and intelligent systems. Rather than replacing human expertise, Symbiotic AI augments

1st Workshop on Symbiotic AI for Cyber Social Security: Human–AI Collaboration for Social Resilience and Trustworthy Digital Ecosystems (SAI4CCS 2026), co-located with the 2nd Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09–13, 2026, Cagliari, Italy

vita.barletta@uniba.it (V. S. Barletta); danilo.caivano@uniba.it (D. Caivano); antonietta.curci@uniba.it (A. Curci); annitalarissa.sciacovelli@uniba.it (A. L. Sciacovelli)
0000-0002-0163-6786 (V. S. Barletta); 0000-0001-5719-7447 (D. Caivano); 0000-0002-0932-7152 (A. Curci); 0000-0003-4795-9238 (A. L. Sciacovelli)

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-14

CEUR-WS.org/Vol-4329/preface-sai4css26.pdf

human capabilities through transparency, explainability, shared decision-making, and continuous mutual adaptation, enabling more resilient, trustworthy, and socially aware security ecosystems.

The **Symbiotic AI for Cyber Social Security (SAI4CSS)** workshop is conceived as a multidisciplinary forum to explore the convergence between CSS and SAI, bringing together researchers and practitioners from computer science, artificial intelligence, cybersecurity, social sciences, psychology, law, ethics, and public policy. By fostering dialogue across these disciplines, the workshop aims to advance innovative methodologies, frameworks, and technologies capable of strengthening resilience against emerging cyber-social threats while placing human values, trust, and societal well-being at the center of future cybersecurity research.

Therefore, the workshop includes interdisciplinary contributions that explore theories, methods, technologies, and case studies related to SAI and CSS. Suggested topics include, but are not limited to:

- Cyber Intimate Partner Violence (C-IPV) and gender-based digital abuse.
- Detection of hate speech, sexism, and disinformation.
- Bias mitigation and fairness in NLP and vision models.
- Cognitive and affective modeling of online aggression.
- Automated annotation and classification of harmful content.
- Detection–Response–Prevention paradigms in social cyber risk management.
- Integration of AI, psychology, and law in socio-technical security.
- Social Sensor Data extraction and fusion.
- Multimodal and semantic analysis for behavioral interpretation.
- Emotion and sentiment analysis for threat detection.
- AI-driven situational awareness in urban and social contexts.
- Symbiotic AI architectures for human–machine collaboration.
- Human-in-the-loop and human-on-the-loop decision models.
- Explainable and transparent AI for critical social systems.
- Hybrid intelligence and cognitive symbiosis in cyber defense.
- Adaptive and self-evolving AI in social and ethical contexts.
- Ethical, legal, and socio-political implications of Symbiotic AI.
- Governance models for trustworthy digital ecosystems.
- Case studies and prototypes of Symbiotic AI systems for social resilience.
- Simulation, digital twins, and cyber range environments for social risk training.
- Human factors and psychological profiling in AI-mediated security.
- International and geopolitical dimensions of cyber-social security.

The paper submission deadline was December 05, 2025, followed by acceptance notifications on December 20, 2025, and the camera-ready submission deadline on January 10, 2026. The workshop took place on February 9, 2026.

A total of 13 papers were submitted to the workshop. The review process was conducted under a double-blind policy, with each submitted paper evaluated by three members of the Program Committee. Following this peer-review process, 12 papers were accepted for presentation at the workshop and inclusion in the proceedings.

2. Program Committee

- Mario Angelelli - University of Salento (Italy)
- Valentina Antoniol - University of Bologna (Italy)
- Fabiana Battista - Università Pegaso (Italy)
- Vito Bavaro - University of Bari Aldo Moro (Italy)
- Alessia Anna Catalano - University of Salento (Italy)

- Teresa Catalano - University of Bari Aldo Moro (Italy)
- Miriana Calvano - University of Bari Aldo Moro (Italy)
- Antonio Curci - University of Bari Aldo Moro (Italy)
- Samuele del Vescovo - IMT School for Advanced Studies of Lucca (Italy)
- Luca Mainetti - University of Salento (Italy)
- Antonio Piccinno - University of Bari Aldo Moro (Italy)
- Alfonso Pio Pretorino - University of Bari Aldo Moro (Italy)
- Corrado Aaron Visaggio - University of Foggia (Italy)
- Manuel A. Serrano - University of Castilla-La Mancha (Spain)

Acknowledgments

This work was partially supported by the following projects: SERICS - “Security and Rights In the CyberSpace - SERICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU; CYBER-PREDICT: Cyber vulnerability ranking prediction by prescription, Avviso “Reti - Sostegno alla ricerca collaborativa”, - Codice Progetto DUQVKW0; SMART: System for Matching and Ranking Talents, Avviso “Reti - Sostegno alla ricerca collaborativa” - Codice Progetto CGGUBN6.

Declaration on Generative AI

The authors have not employed any Generative AI tools.