AAAI Summer Symposium 2026

Human-Aware AI Agents for the Cyber Battlefield: From Human Models to Autonomous Defense

June 22–24, 2026

Dongguk University | Seoul, South Korea, Room: 337

Session 1: Reasoning, Coordination, and Defense in Cyber Systems

Date: June 22, 2026
Time: 9:00 AM – 12:30 PM
Session Chair: Dr. Quanyan Zhu

Time	ID	Authors	Title
9:00	Keynote Talk	Dr. Tao Li	From Automation to Autonomy: Decision-Theoretic Cyber Defense Agent in the Age of LLMs
10:00	Discussion		
10:30	Break		
11:00	14	Samuel Addington	From Playbooks to Decisions: Coordination Protocol for Cyber Agents
11:30	52	Shin et al.	The Illusion of Optimal Defense: Static Interdiction under Adaptive Attackers
12:00	12	Yiming Bai, Sheng Zhong	Beyond Common Knowledge: A Belief-Reasoning Framework for Non-Equilibrium Games

Session 2: Human-Aware Cyber Defense and Security Games

Date: June 22, 2026
Time: 2:00 PM – 5:00 PM
Session Chair: Dr. Quanyan Zhu

Time	ID	Authors	Title
2:00	Keynote	Dr. Kai	Security Games With Layered Defenses
3:00	Discussion		

3:30	Break		
4:00	74	Delgado et al.	Human-Aware Multi-Agent Cyber Defense for Nuclear OT Systems + Demo
4:30			
5:00	Reception		

Session 3: Deception

Date: June 23, 2026
Time: 9:00 AM – 12:30 PM
Session Chair: Dr. Tao Li

Time	ID	Authors	Title
9:00	Keynote	Dr. Quanyan Zhu	Deception in the Age of Generative Intelligence: The Dialectics of Trust and the Formation of Agency for Resilience
10:00	17	Tim Pappa, Darin Roberts	HoneyContent: Deception Storyline Content
10:30	Break		
11:00	36	Sai Puppala et al.	Agent-Fence: Mapping Vulnerabilities in Deep Research Agents
11:30	18	Tim Pappa, Teja Sane	Deceptive Misuse of Low-Code Platforms
12:00	76	Acosta et al.	Cyber-Agent-Flow: Execution Trace Instrumentation + Demo

Session 4: Operational Deployment and Security of Agents

Date: June 23, 2026
Time: 2:00 PM – 5:00 PM
Session Chair: Dr. Tao Li

Time	ID	Authors	Title
2:00	57	Yiran Gao et al.	Autonomous Network Incident Response via LLM Agents
2:30	72	Tim Pappa, Chris Williams	Agentic AI Army That Never Was (Swarm Narratives)

3:00	11	Samuel Addington	Bounded Autonomy: Resilient Human-AI Teaming in SOCs
3:30	Break		
4:00	55	Emilia Rivas, Aritran Piplai	Contrastive Adversarial Agents for IDS Drift
4:30	75	Md Jahangir Alam et al.	HALLPERM: Privilege Escalation in LLM Tool Use

Session 5: Future and Grand Challenges of Human-Aware AI Agents for Cybersecurity

Date: June 24, 2026
Time: 9:00 AM – 12:30 PM
Session Chair: Dr. Quanyan Zhu

Time	ID	Authors	Title
9:00	30	Hung Nguyen, Tu Vu	Human-Aware Active Directory Defense with Fine-Tuned LLMs
9:30	Discussion		
10:00	73	Tanzim Ahad et al.	Semantic Intent Fragmentation Attack
10:30	Break		
11:00	70	Ismail Hossain et al.	Safety Geometry Collapse in Agentic Guard Models
11:30	Panel: Human-Aware AI Agents for the Cyber Battlefield: From Human Models to Autonomous Defense		
12:15	Concluding Remarks		