	13-Oct	14-Oct		15-Oct	
8.30-17.00	Registration	Registration		Registration	
9:00-9:30	Tutorial Intro.	Opening remarks – Organizing Committee		Welcome Address by University and Greek Government Officials	
9:30-10:30	Lecture 1	Keynote 1		Keynote 3	
10:30-11:00	Coffee break	Coffee break	Coffee break	Coffee break	Coffee break
11:00-13:00	Lecture 2 &3	Session 1	Session 2	Session 5	Session 6
13:00-14:00	Lunch	Lunch	Lunch	Lunch	Lunch
14:00-15:00	Lecture 4	Keynote 2		Keynote 4	
15:00-15:30	Coffee break	Coffee break	Coffee break	Coffee break	Coffee break
15:30-17:30	Lecture 5 & 6	Session 3	Session 4	Session 7	Posters & PhD Forum
17:30-18:30	Panel Discussion with Lecturers			Closing	
18.30-20.30	-	Acropolis Museum Visit & Tour			
21:00-23:30	-	Banquet			

#### **Opening Remarks - Organizing Committee**

Tuesday, October 14, 2025, 9.00-9.30

John Baras, General co-chair GameSec 2025, Professor, University of Maryland, USA Symeon Papavassiliou, General co-chair GameSec 2025, Professor, National Technical University of Athens, Greece

#### **Welcome Address by University and Greek Government Officials**

Wednesday, October 15, 2025, 9.00-9.30

- 9.00-9.10 Welcome Address by Prof. Yannis Ioannidis, President of ACM, National and Kapodistrian University of Athens
- 9.10-9.15 Welcome address by Prof. Panagiotis Tsanakas, Dean of School of Electrical and Computer Engineering, National Technical University of Athens
- 9.15-9.30 Welcome Address by Mr. Dimitris Papastergiou, Minister of Digital Governance of Greece

#### Keynote 1 - Tuesday, October 14, 2025, 9.30-10.30

Chair: John Baras (University of Maryland College Park and Archimedes RC)

Title: Stochastic Games with Neural Perception Mechanisms: A Formal Methods Perspective

Speaker: Marta Kwiatkowska, Professor, University of Oxford, England

#### Keynote 2 – Tuesday, October 14, 2025, 14.00-15.00

Chair: Yannis Ioannidis (National and Kapodistrian University of Athens and Athena RC, President of ACM)

Title: A Collectivist, Economic Perspective on AI

Speaker: Michael Jordan, Professor, Inria Paris, France and University of California, Berkeley, USA

#### Keynote 3 – Wednesday, October 15, 2025, 9.30-10.30

Chair: Tamer Başar (University of Illinois Urbana-Champaign)

Title: Generative AI and Green Security Games for social impact: From conservation to public health

Speaker: Milind Tambe, Professor Harvard University and Google Deepmind, USA

#### Keynote 4 – Wednesday, October 15, 2025, 14.00-15.00

Chair: Symeon Papavassiliou (National Technical University of Athens)

Title: Trustworthy Al... for Systems Security

Speaker: Lorenzo Cavallaro, Professor, University College London (UCL), England

Sessions	Title	Date and Time	
Session 1	Game-Theoretic Foundations and Learning	Tuesday, October 14, 2025, 11.00-13.00	
Session 2	Game-Theoretic Cybersecurity Frameworks	Tuesday, October 14, 2025, 11.00-13.00	
Session 3	Deception and Adversarial Defense	Tuesday, October 14, 2025, 15.30-17.30	
Session 4	Applications in Security and Networks	Tuesday, October 14, 2025, 15.30-17.30	
Session 5	Strategic Defense and Robustness	Wednesday, October 15, 2025, 11.00-13.00	
Session 6	Al and LLMs in Security	Wednesday, October 15, 2025, 11.00-13.00	
Session 7	Emerging Threats and Anomaly Detection	Wednesday, October 15, 2025, 15.30-17.30	
	Posters & PhD Forum	Wednesday, October 15, 2025, 15.30-17.30	

### Session 1 - Game-Theoretic Foundations and Learning

Chair: Tansu Alpcan, University of Melbourne, Australia

- Tree Search for Simultaneous Move Games via Equilibrium Approximation Ryan Yu, Alex Olshevsky and Peter Chin
- Measuring Cooperation with Counterfactual Planning Samuel Barnett, Kathryn Wantlin and Ryan Adams
- Explore Reinforced: Equilibrium Approximation with Reinforcement Learning
  Mateusz Nowak, Qintong Xie, Emma Graham, Ryan Yu, Michelle Feng, Roy Leibovitz, Xavier Cadet and Peter Chin
- A Logic for Resource-sensitive Coalition Games
  Pinaki Chakraborty, Tristan Caulfield and David Pym
- Locally Optimal Solutions for Integer Programming Games in Cybersecurity Pravesh Koirala, Mel Krusniak and Forrest Laine

### Session 2 - Game-Theoretic Cybersecurity Frameworks

Chair: Mina Guirguis, Texas State University, USA

- CyQuaPro: A Stackelberg Game Framework for Cyberdefense for Distributed Systems Neil Kpamegan and Aryya Gangopadhyay
- Dynamic Shields: A Game-Theoretic RL Framework for APT Mitigation

  Aws Jaber, Gustaf Johansson, Florian Skopik, Max Landauer, Wolfgang Hotwagner and Markus Wurzenberger
- CyGym: A Simulation-Based Game-Theoretic Analysis Framework for Cybersecurity Michael Lanier and Yevgeniy Vorobeychik
- PoolFlip: A Multi-Agent Reinforcement Learning Security Environment for Cyber Defense Xavier Cadet, Simona Boboila, Sie Hendrata Dharmawan, Alina Oprea and Peter Chin
- PuRe Defender: A Game-Theoretic Pull Request Assignment with Deep RL
   Javad Mokhtari Koushyar, Mina Guirguis and George Atia

### Session 3 - Deception and Adversarial Defense

Chair: Mingyan Liu, University of Michigan, Ann Arbor, USA

Cooperative Deception in Swarms against a Smart Observer

Stanislas de Charentenay, Alexandre Reiffers-Masson, Caroline Lesueur, Gilles Coppin and Jacques Petit-Frère

Ransomware Negotiation: Dynamics and Privacy-Preserving Mechanism Design

Haohui Zhang, Sirui Shen, Xinyu Hu and Chenglu Jin

Adversarial Knapsack for Sequential Competitive Resource Allocation

Omkar Thakoor, Rajgopal Kannan and Viktor Prasanna

• A Continuous Strategy Space Adversarial Classification Game

John Musacchio

 Consistent Conjectural Approach to Adversarial Intent Tracking under Sensing Constraints in Multi-Target Defense Differential Games

Sharad Kumar Singh and Quanyan Zhu

### Session 4 - Applications in Security and Networks

Chair: Spiros Mancoridis, Drexel University, USA

Contested Route Planing

Jakub Cerny, Garud Iyengar and Christian Kroer

- When In Doubt, Abstain: The Impact of Abstention on Strategic Classification Lina Alkarmi, Ziyuan Huang and Mingyan Liu
  - Human Trafficking Interdiction Problem: A Game Theoretic Approach for Finding the Best Strategy for the Law Enforcement Agencies

Dev Patel, Suli Adeniye and Arunabha Sen

- contrastBERT: Behavioral Anomaly Detection for Malware using Contrastive Learning John Carter, Spiros Mancoridis, Pavlos Protopapas and Brian Mitchell
- Worst Case Assurance Guarantees for Black-Box Perimeter Defense Policies Richard Frost, Betty H.C. Cheng and Shaunak D. Bopardikar

### Session 5 - Strategic Defense and Robustness

Chair: Panagiotis Papadimitratos, KTH, Sweden

Empirical Mixnet Design

Yongzhao Wang, Tariq Elahi, Vasilios Mavroudis, Edward Plumb, Rahul Savani and Theodore Turocy

• Using Choice Overload to Degrade Cyber Attacks

Asif Rahman, Carlos Natividad, Md Abu Sayed, Palvi Aggarwal and Christopher D Kiekintveld

• Nash Q-Learning for Multi-Agent Cybersecurity Simulation

Qintong Xie, Edward Koh, Xavier Cadet and Peter Chin

- Theoretical Bounds on the Adversarial Robustness of Reduced-Rank Regression Soyon Choi and Scott Alfeld
- Strategic Defense Allocation in Cyber-Physical Sensor Systems under Dual-Domain Attacks
  Ahmad Bilal Asghar, Ahmed Hemida, Charles Kamhoua and Jon Kleinberg

### Session 6 - AI and LLMs in Security

Chair: John Musacchio, University of California, Santa Cruz, USA

- The Al Who Loved Me: Fundamental Bounds and Behaviors Under Human-Al Working Agreements Mark Bilinski and Ryan Gabrys
- A Multi-Resolution Dynamic Game Framework for Cross-Echelon Decision-Making in Cyber Warfare Ya-Ting Yang and Quanyan Zhu
- Generative-Conjectural LLM Equilibrium for Agentic AI Deception with Applications to Spearphishing Quanyan Zhu
- Balancing Act: Prioritization Strategies for LLM-Designed Restless Bandit Rewards
   Shresth Verma, Niclas Boehmer, Lingkai Kong and Milind Tambe
- Jailbreaking Large Language Models Through Content Concretization Johan Wahréus, Ahmed Hussain and Panos Papadimitratos

### Session 7 - Emerging Threats and Anomaly Detection

Chair: Stefan Rass, Johannes Kepler University Linz, Austria

 Secure and Power-Efficient Multi-User Scheduling in Semi-Grant-Free NOMA Networks: A Coalition Game Approach

Sofia Barkatsa, Panagiotis Charatsaris, Maria Diamanti and Symeon Papavassiliou

- A Gestalt Game-Theoretic Framework for Designing Agentic AI Workflows in Cyber Deception Quanyan Zhu and Muhammad Akram Al Bari
- Probabilistic and predictive strategies against zero-day advanced persistent threats in robotic systems Asim Zoulkarni, Sai Sandeep Damera and John S. Baras
- On Sequential Fault-Intolerant Process Planning
   Andrzej Kaczmarczyk, Davin Choo, Niclas Boehmer, Milind Tambe and Haifeng Xu
- Self-Supervised Time-Series Anomaly Detection with Temporal Logic Explanations Mahshid Noorani, Aniruddh Puranic, Jack Mirenzi and John Baras

#### Posters and PhD Forum

Chair: Vaslieios Karyotis, Ionian University, Greece

• Physics-Informed Value Approximation for Pursuit-Evasion Games (Poster)
Takuma Adams, Andrew Cullen and Tansu Alpcan

• Zero-Day Risk Estimation Using Security Games (Poster)

Stefan Rass, Víctor Mayoral Vilches and Beniamin Jablonski

• Adversarial Training under Data Exclusion Attacks: A Zero-sum Game Approach (PhD Forum) Zixin Ye, Shijie Liu, Tansu Alpcan and Christopher Leckie

### Tutorial on Game theory and Artificial Intelligence Methods for Security and Trust

Monday, October 13, 2025

Organizer: John S. Baras

Co-Chairs: John S. Baras and Tansu Alpcan

#### **Program**

9:00am - 9:30 am

Introduction and Goals of the Tutorial

John S. Baras

University of Maryland College Park, USA, and Archimedes Al Research Center, Greece baras@umd.edu

9:30am - 10:30am

An Introduction to Game-Theoretic Framework for Multi-Agent Decision-Making with Applications to Security Tamer Başar

University of Illinois Urbana-Champaign, USA basar1@illinois.edu

10:30am - 11:00am

**Coffee Break** 

11:00am - 12:00pm

Reward Schemes and Incentives in Proof of Stake Blockchain Protocols Vangelis Markakis

Athens University of Economics and Business and Archimedes Al Research Center, Greece markakis@gmail.com

12:00pm - 13:00pm

Posted Price Mechanisms for Combinatorial and Procurement Auctions Dimitris Fotakis

National Technical University of Athens and Archimedes Al Research center, Greece fotakis@cs.ntua.gr

13:00pm – 14:00pm Lunch

Luncn

14:00pm - 15:00pm

An Introduction to ML and Al methods for Networked Systems Security and Trust John S. Baras

University of Maryland College Park, USA, and Archimedes Research Center, Greece

15:00am – 15:30am

**Coffee Break** 

15:30pm - 16:30pm

**Constraints-Enforcing RL Solutions for Ensuring Safety and Security** 

Elena Stai

National Technical University of Athens, Greece <a href="mailto:estai@mail.ntua.gr">estai@mail.ntua.gr</a>

16:30pm – 17:30pm Resilient AI for Cyber F

Resilient AI for Cyber Physical Systems
Panagiotis Papadimitratos
Royal Institute of Technology (KTH), Sweden
papadim@kth.se

17:30pm - 18:30pm

Open Panel Discussion and Q&A with Lecturers

Moderator: Tansu Alpcan