SPRING**SIM'20**

2020 Spring Simulation Conference

AIMS AND SCOPE

Modeling and Simulation has the ability to improve our understanding and gain better insights into the exploitability and impact of threat landscape in cyber systems underpinning several critical infrastructures. The emergence of Internet of Everything has resulted in the growth in interactions between humans, physical and cyber systems and there is a increased need to understand how these interactions could be exploited by adversaries. Modeling and simulation provide a cost-effective means to support research, development, refinement, deployment, and evaluation of the next generation of security solutions for preventing, detecting, and recovering from cyber-attacks and failures. The goal of **Cybersecurity Engineering (CSE) Track** is to provide a forum to present and discuss advancements in research, tools, techniques, solutions, best practices, and heuristics related to the modeling and simulation of cybersecurity. The track will address all aspects of modeling, analyzing, design, simulation, implementation, deployment and management of security algorithms, protocols, architectures and systems. We encourage submissions related to all aspects of cybersecurity in a modeling and simulation context in a broad spectrum of application areas. Topics of interest include, but are not limited to:

- Formal models for cybersecurity simulation
- Cybersecurity evaluation and assessment approaches
- Testbeds and experimental infrastructure for cybersecurity simulation
- Simulation platforms for cybersecurity assessment
- Hybrid simulations for cyber physical system security
- Modeling and Analysis of Networked security systems
- Modeling security and privacy in mobile and cellular networks
- Modeling security for future Internet architectures
- Risk assessment and management
- Systems engineering for security