ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

THURSDAY: SESSION 1, TRACK 2

SESSION CHAIRS/PRESENTER

Char Sample, Modern Technology Solutions

PRESENTERS

- Dr. James LaRue
- Dr. Char Sample

SESSION ABSTRACT

Artificial intelligence and machine learning (AI/ML) are already being used in various environments for differing applications. AI/ML are “black box” solutions and have been shown to be vulnerable to manipulation. AI/ML systems can be programmed to support resilience (robustness, resourcefulness, redundancy and recovery) but to date only re-enforcement learning is only sometimes used to improve robustness. For this session we seek the following topics and other related discussions.

Topics of Focus:

- Training data manipulation and countering techniques
- Malicious Use of AI (MUAI) and countering techniques
- AI/ML applications in supply chain resilience identification and repair
- Explainable AI (XAI)
- Trustworthy AI (TAI)
- AI implementations where resilience techniques were designed in and deployed.