# Florida Center for Cybersecurity (FC²) University of South Florida (USF) Adaptive Immersion Technologies (AIT)

**"Advancing cybersecurity through outreach, research and collaboration with academia, industry and government."**

## Unique Qualifications & Capabilities:

**FC²:**

- Access to researchers across **12 institutions in Florida's State University System (SUS)**
- Academic and Research Outreach **across Florida**
- **Top Secret Facility Clearance**

**USF:**

- **Cyber Intelligence** – collection and analysis of information concerning the intentions, capabilities, activities of adversaries and competitors in the cyber domain
- Using analytic and visual cognition (through data visualization) to enhance **human sensor capabilities** for cyber anomaly detection and forecasting
- Combining information analytics and structured intelligence analytic techniques to develop **operationally relevant threat actor profiles** in the cyber domain (e.g., categories, database)
- Discerning attack/activity trends within an industry or sector to develop **probabilistic risk/threat assessments** (e.g., targets, tactics)
- Integrating collection and knowledge management technologies **to improve the efficiency of cybersecurity operations**

**AIT:**

- **Novel machine learning applications** to complex human performance prediction problems
- **Computational modeling of human performance**
- Technology-enabled **performance assessment and diagnosis**
- **Computer-adaptive assessment and training** employing modern psychometric theory
- **Algorithm development, optimization, and benchmarking** for real time, simulation-based assessment

Open to collaborative research, to include:

- Cyber Intelligence
- Human Sensors
- Machine Learning
- Computational Modeling of Human Performance

## CAUSE-specific Capabilities & Interests:

- Developing novel methodologies for **measuring behavioral signatures** of individual operators and networks of operators
- **Pattern recognition** of complex patterns of free **cyber attack activities** within distributed, networked environments
- Evolution and application of machine learning algorithms for **complex pattern recognition** within the cyber domain
- Algorithm boosting for enhanced detection accuracy with low base rate events useful for **forecasting critical cyber events**
- Develop database to **categorize cyber threat actor profiles** based on capabilities, intentions, targets, activities
- **Predictive cyber threat analysis** for threat/risk assessments
- Using analytic and visual cognition (through data visualization) to enhance **human sensor capabilities** for cyber anomaly detection and forecasting
- Cyber threat actor **trend analysis**

## Key Members – Experience (Clearance Status):

- **"Scuba" Steve Gary** – Former Chief of Cyber Intelligence, US Special Operations Command. MS in Cyber Operations. (Cleared)
- **Dr. Randy Borum** – Psychologist. Intelligence analytic methods in the cyber domain. Strategy and decision making. (Cleared)
- **Dr. Phillip Mangos** – President and Chief Scientist of Adaptive Immersion Technologies, a Florida-headquartered small business. (Pending)
- **Adam Sheffield** – Program Manager, FC² & HUMINT Targeting Analyst. (Cleared)

"Scuba" Steve Gary
Assistant Professor of Practice
School of Information, University of South Florida
sgary@usf.edu
813-974-3520