



U.S. ARMY  
**RDECOM**

Cyber Battlefield Operating System Simulation Tools for  
Live-Virtual-Constructive (LVC) Training Simulations



## S&T Campaign: Human Sciences Human Capability Enhancement

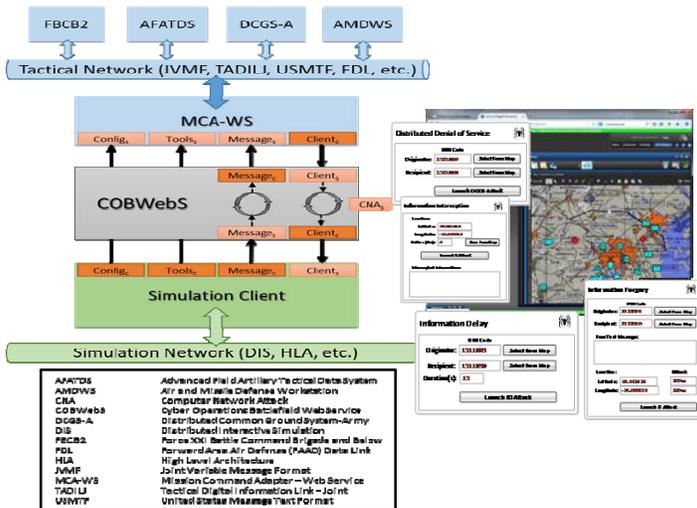
Henry Marshall, (407) 384-3820  
Henry.A.Marshall.civ@mail.mil

### Research Objective

- The Army proponents of Simulation and Training technology have identified Cyber as a major training technology gap.
- Our research proposes to develop prototypes with innovative solutions to train Cyber related tasks using current Army training simulations.



Current training simulations support many training requirements in the battlefield areas such as move, shoot, and communicate. However, the Army simulations lack the capability to train Cyber-related tasks.



The Cyber Operations Battlefield Web Services (COBWebS) is an example of an ARL research prototype designed to provide Cyber Simulation Effects in current training simulations. It produces Cyber operation attack effects like information delay, forgery, interception, and denial of service in Mission Command Systems.

### ARL Facilities and Capabilities Available to Support Collaborative Research

- The Advanced Simulation Systems Integration Modeling Interoperability Laboratory and Test Environment (ASSIMILATE) is a lab equipped with an unclassified instance of the Live, Virtual, and Constructive - Integrating Architecture (LVC-IA), selected Core Systems of the Integrated Training Environment (ITE), selected Army Mission Command systems, and a cloud server farm.
- Our most recent paper on COBWebS describes a Concept for a Tactical Cyber Warfare Effect Training Prototype. The document was selected as one of the "Best Papers" for the 2015 Fall Simulation Interoperability Workshop.
- ARL-HRED has unique expertise in simulation and training technologies.
- ARL-HRED prototypes are continuously demonstrated to the Army training community.

### Challenges

- Cyber attacks are very asymmetrical which makes it difficult to define the training environment and requirements. Developing approaches that allow for this wide-range of parameter flexibility is also difficult.
- There is a need to define Data Exchange Models for Cyber application in order to allow exchange of Cyber operation information between simulations.
- Solutions must support the Information Assurance requirements that are typically destroyed in attacks.
- Cyber doctrine and requirements in this area are not mature. Our prototypes will generate possible training solutions.

### Complementary Expertise/ Facilities/ Capabilities Sought in Collaboration

- Innovative approaches to create the effects and training environment for a wide-range of Cyber attacks.
- Ways to best conduct the data exchanges between Cyber models.
- Determine the correct doctrine for response to Cyber attacks at all levels of interaction, from Soldiers and leaders to Cyber protection teams.
- Ideas to integrate into our Cyber prototype so as to support the Army training community. The goal is to show a potential training way-forward to this complex and evolving research area.