Cyber for Training Modeling and Simulation

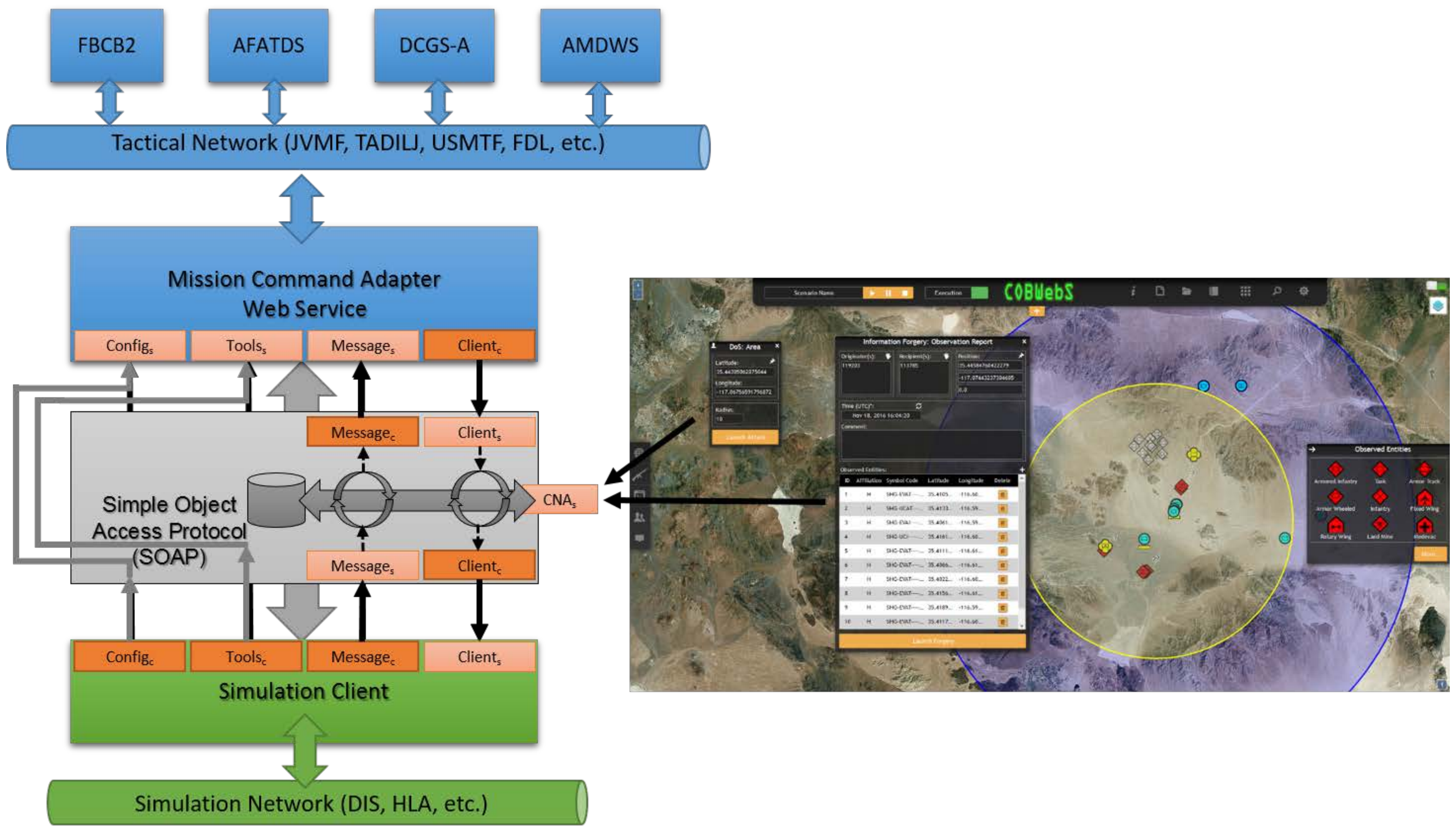
S&T Campaign: Assessment and Analysis
Tools, Techniques, & Methodologies
Complex Adaptive Systems

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.**
- **An end goal is to support mission training through responses to cyber attacks at all levels of interaction, from soldiers and leaders to Cyber protection teams.**

Current training simulations support many training objectives/tasks (like move, shoot, and communicate) but lack the ability to train Cyber-related tasks.



The Cyber Operations Battlefield Web Services (COBWebS) is an example of an ARL research prototype designed to model Cyber effects within current training simulations. It produces effects such as information delay, forgery, interception, and denial of service in Mission Command Systems.

ARL Facilities and Capabilities Available to Support Collaborative Research

- **ARL Orlando houses 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 Cyber attack prototype COBWebS is now part of the One Semi Automated Forces (OneSAF) baseline. Several papers on our researchwere awarded "Best Papers" for the Simulation Interoperability Workshop.**
- **ARL HRED has unique expertise in simulation and training technologies.**
- **ARL HRED Cyber prototypes are continuously demonstrated to the Army training community.**

Challenges

- **Cyber attacks are very asymmetrical, which complicates efforts to define training environments and requirements. Developing approaches that allow for this wide range of parameter flexibility is difficult and complex.**
- **Need to define Data Exchange Models for Cyber to allow exchange of Cyber operation information between simulations.**
- **Solutions must support the Information Assurance (IA) requirements required by training simulations.**
- **Doctrine and requirements in this area are not fully mature, so our prototypes are designed to demonstrate possible ways forward.**

Complementary Expertise / Facilities / Capabilities Sought in Collaboration

- **Innovative approaches to create a training environment that supports a wide-range of Cyber attacks**
- **Cyber and Cyber Electromagnetic Activities (CEMA) effects models**
- **Ways to best conduct data exchanges between cyber models**
- **Simulation editors and ways to represent Cyber events in training scenarios**

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED