Cyber Operations Battlefield Web Services (COBWebS) – Concept for a Tactical Cyber Warfare Effect Training Prototype

Henry Marshall  
Army Research Laboratory (ARL)  
Human Research and Engineering Directorate (HRED)  
Simulation and Training Technology Center (STTC)  
Orlando, Florida  
henry.a.marshall.civ@mail.mil

MAJ. Jerry R. Mize  
Army Research Laboratory (ARL)  
Human Research and Engineering Directorate (HRED)  
Simulation and Training Technology Center (STTC)  
Orlando, Florida  
jerry.r.mize.mil@mail.mil

CPT. Michael Hooper  
U.S. Army Cyber Command (ARCYBER)  
Fort Meade, Maryland  
michael.j.hooper2.mil@mail.mil

Robert Wells  
Dynamic Animation Systems  
Orlando, Florida  
rwells@d-a-s.com

Jeff Truong  
Effective Applications Corporation  
Orlando, Florida  
jeff@effectiveapplications.com

ABSTRACT: As the Army continually develops a force capable of meeting the challenges of 2025 and beyond, the domain of Cyberspace is exponentially important. The United States (U.S.) Army Operating Concept states that “Enemies and adversaries collaborate as contests in space and cyberspace extend to and affect tactical operations.” The realization that Cyberspace is a warfighting domain has simulation and training program managers struggling to identify the best solution to implementing cyber warfare effects into the training domain. Current simulations among the Live, Virtual, Constructive, and Gaming (LVC&G) domains lack a cyber implementation with the exception of a low fidelity cyber warfare effects simulation in the One Semi-Automated Forces (OneSAF) program. While the Test community progressed, the Training community lacked clear implementation progression. The cyber domain transverses all other warfighting domains, and impacts the conduct of all other warfighting functions, thereby forcing us to determine the best focus to meet an Army use case towards a multi-domain cyber training solution via gap analysis. Amongst stakeholders, a clear missing capability emerged: a cyber warfare mission command service that would work in a LVC&G training environment. Our goal is to build a prototype of a simulated mission command cyber effects capability, using defined user requirements with an ability to scale across training simulation domains. The Combat Training Centers (CTC) leverage Army Cyber expertise to execute cyber training pilots that integrate cyber effects into the operational environment, largely for and/or against Brigade Combat Teams (BCTs). From an Opposing Forces (OPFOR) perspective these exercises demonstrate, through actual effects, potential adversary mission command system compromise, while other emerging efforts provide friendly forces, or Blue Forces (BLUFOR), with cyber capabilities. These scenarios are groundbreaking, and force trainees to recognize system compromise while simultaneously planning offensive operations of their own. However, a simulated training environment is currently lacking at all echelons. Adding cyber effects to the simulated training environment is a first step towards allowing Soldiers and Battle Staffs the ability to develop battle drills against cyber-attacks in a LVC&G construct. To address these issues we are developing a loosely coupled software service, called Cyber Operations Battlefield Web Services (COBWebS), that provides the capability to simulate the effects of various cyber-attacks on command and control communication between the synthetic entities and the Blue mission command systems. Our prototype leverages the One Semi-Automated Forces (OneSAF) Mission Command Adapter Web Service and adds cyber warfare effects modeling. Incorporating COBWebS in a LVC&G training event allows the trainee to recognize and make decisions that will minimize attack effects on overall mission command. Over the past year our team made significant additional domain contacts and progressions in the design. This paper provides an overview of our front end requirements including
interactions with the cyber training community, training system architecture analysis, example COBWebS scenario cyber-attack event flows based on our design progress and interactions with users, and our conceptual prototype design. Our goal is to solicit feedback from the Simulation Interoperability Workshop (SIW) community and seek developmental collaboration.

1. Introduction

During a lecture delivered to the audience at Stanford University (California, USA) in April 2015 [1], the United States (U.S.) Defense Secretary Ashton Carter unveiled the new Department of Defense (DoD) Cyber Strategy [2] and discussed the ever-increasing cyber threat that our country, business enterprises, as well as individuals face. In order to maintain ready forces and capabilities to conduct cyberspace operations, one of the tasks outlined in the DoD Cyber Strategy is to establish an enterprise-wide cyber modeling and simulation (M&S) capability. As quoted in the 2015 DoD Cyber Strategy the Director of National Intelligence named the cyber threat as the number one strategic threat to the U.S. from 2013-2015, placing it ahead of terrorism for the first time since the 11 September 2001 attacks.

The current Army Training community needs a non-intrusive way of incorporating cyber operations M&S in their training exercises. To address these issues our research led to the development of a loosely coupled software service that provides the capability to simulate the effects of various cyber-attacks on Command and Control (C2) communication between the synthetic entities and the U.S./Coalition Forces’ Mission Command Systems (MCS).

2. Why Cyber Warfare Training?

The first phase of our research consists of tasks to understand the cyberspace domain and the gaps in cyber warfare M&S. We reviewed several Joint and Army publications to understand the doctrine related to cyber warfare. We also analyzed capability gaps from the Army’s acquisition organizations to scope and drive our research.

2.1 DoD/Army Drivers

Other than the DoD Cyber Strategy, there are other DoD, Joint, and Army publications that drive the doctrine and requirements for cyber training M&S.

The Joint Publication (JP) 3-12R “Cyberspace Operations” [3] provides fundamental constructs and guidance for planning, preparing, executing, and assessing joint cyberspace operations across the range of military operations. The JP 3-12 describes various cyberspace operations and how to integrate them into joint operations. It also covers the roles and responsibilities of the joint forces and discusses planning and coordination of cyberspace operations among them.

The Army Field Manual (FM) 3-38 “Cyber Electromagnetic Activities (CEMA)” provides overarching guidance and direction for conducting cyber electromagnetic activities [4] from the Army’s perspective. FM 3-38 provides an overview of principles, tactics, and procedures to integrate CEMA as part of Army operations. It also defines the roles and responsibilities from commanders to soldiers in the area of CEMA. Cyberspace operations are explained in details including cyber offense and cyber defense operations. The FM describes cyberspace that consists of the following three layers: 1) Physical Network Layer; 2) Logical Network Layer; and 3) Cyber-Persona Layer. The operational environment and the area of operations for each layer are described.

The Army FM 3-36 “Electronic Warfare” provides Army doctrine for Electronic Warfare (EW) planning, preparation, execution, and assessment in support of unified land operations [5]. This FM serves as a reference for doctrine and training developers as well as for those who plan, prepare, execute, and assess EW.

The Army Training and Doctrine Command (TRADOC) Pamphlet 525-7-8 “Cyberspace Operations Concept Capability Plan 2016-2028” includes a conceptual framework for integrating cyber operations (CyberOps) into Full Spectrum Operation, thereby providing the basis for follow-on doctrine development efforts [6]. This conceptual framework describes how commanders integrate CyberOps to gain advantage over adversaries and to place adversaries at a disadvantage. It establishes a lexicon for Army CyberOps and describes the relationship between cyber domain and the other four domains (air, land, maritime, and space).

2.2 CAC-T/PEO STRI/TRISA Drivers

The U.S. Army Combined Arms Center – Training’s (CAC-T’s) vision for a Future Holistic Training Environment – Live/Synthetic (FHTE-L/S) is an environment that encompasses the land, sea, air, space, and cyber domains in a single synthetic environment accessible from anywhere in the world and is integrated with the Live training environment [7]. FHTE-L/S will be realized through sets of required and desired capabilities which are grouped under six focus areas. Cyber security/warfare training was one of the gaps listed under the Point of Need focus area.
The U.S. Army Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) listed Threat Cyber Capabilities as one of the Science and Technology (S&T) Focus Areas [8]. The document specifies the following needs for an ongoing or emerging/future Program of Record (PoR):

- Enhance threat Computer Network Operations
- Threat Computer Network Attack & Computer Network Defense
- Remote mission command of multiple cyber platforms
- Modeling & execution of cyber activities
- Virtualization of threat networks
- Threat cyber tools developed as Software as a Service (SaaS)

We met with the team from the U.S. Army Training and Doctrine Command (TRADOC) G-2 Intelligence Support Activity (TRISA) Operational Environment Lab (OEL) to discuss cyber operations M&S gaps. They provided excellent insight in what’s lacking in cyber offense and defense modeling for training, particularly in Constructive simulations. Although there are some CyberOps effects implemented in OneSAF, there are still many more gaps remaining to be fulfilled; e.g., Global Positioning System (GPS) cannot be corrupted or exploited; intelligent network cannot be corrupted or exploited, etc. The biggest gap, per the TRISA OEL team, with the current implementations of CyberOps modeling is that it does not affect the actual operational C2/MCS.

3. Cyber Operation Terms

Various DoD [2], Joint publications [3] [9] [10], or industry resources [11] have defined different cyber operations terminologies as summarized below.

**Cyberspace Operations (CO)** are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

**Computer Network Operations (CNO)**, in concert with Electronic Warfare (EW), are used primarily to disrupt, disable, degrade or deceive an enemy’s command and control, thereby crippling the enemy’s ability to make effective and timely decisions, while simultaneously protecting and preserving friendly command and control.

Military CNO or CO consists of two main types:

**Computer Network Attacks (CNA), or Offensive Cyberspace Operations (OCO)**, include actions taken via computer networks to disrupt, deny, degrade, deceive, or destroy the information within computers and computer networks and/or the computers/networks themselves.

**Computer Network Defense (CND), or Defensive Cyberspace Operations (DCO)**, include actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks.

CNA can further decomposed into the following types of attacks:

- **Denial of Service (DoS)**, or **Distributed DoS (DDoS)**, is an attempt to make a targeted machine or network resource unavailable to its intended users. DoS is an attempt to disrupt, degrade, deny, or destroy the target computer or network’s ability to send or receive information.

- **Information Interception (II)** is an attempt to intercept, or eavesdrop, on a targeted machine or network resource to gather information that may be used to the attacker’s advantage.

- **Information Forgery (IF)** is an attempt to forge (i.e., fake) information sent on behalf of a known entity to a targeted machine or network resource in order to deceive the target’s C2 situational awareness (SA).

- **Information Delay (ID)** is an attempt to intercept and delay the information sent/received by a targeted machine or network resource in order to deceive and obstruct the target’s C2 SA.

Typically many of the CNA attack types are carried out concurrently or sequentially to result in greatest damages to the targets as illustrated later in the example use cases section.

4. Cyber Training at Army Combat Training Centers

The stated vision of the Combat Training Centers (CTCs) is to “…generate ready units and agile leaders who are confident in their ability to operate in complex environments. The CTCs will lead the Army’s transition to unified land operations as described in Army Doctrine Publication (ADP) 3–0. This transition includes a bridging period when CTCs sustain the Army’s seasoning in irregular warfare and re-establish training superiority in major combat operation skills. Success is defined as growing the next generation of adaptive Army leaders and providing relevant land forces for Army Force Generation (ARFORGEN) requirements; both equally skilled and trained to standard in offense, defense, and stability operations. The CTC Program has led Army cultural changes throughout its history. The challenge in this period is to identify innovative training methods to reduce overhead without sacrificing training quality, standards, or outcomes.” In order to evaluate the relative readiness of a unit and areas for improvement, they rotate through
CTCs which provide realistic, intensive training for Soldiers and commanders. The main tool for receiving feedback includes detailed after action reviews by observer/coach/trainers, known as OCTs, who rate soldiers’ performance and tactics. The scenarios unfold, and often include mock villages to enhance a complete picture of readiness by injecting “actors” for heightened realism.

In the same measure of adding actors for realism, the emerging necessity for the modern and future battlefield to represent Cyber at CTCs caused the implementation of OCTs to realistically implement the Cyber threat for rotating units. The U.S. Army Cyber OPFOR has been responsible for emulating national level adversary attacks against U.S. Army Battle Command Systems at the Combat Training Centers since as early as 2011. This training has been critical in teaching end-users, systems administrators, and commanders the importance of protecting their mission command systems.

This training has evolved in degree of difficulty over the years, and the Rotational Training Units have been thoroughly challenged. While this OPFOR unit has conducted events in support of Corps, Division, and Brigade level exercises, a capabilities gap has been identified in the modeling and simulations capabilities at echelons above Brigade. How will higher echelon battle staffs react to wide-ranging cyber-attacks affecting the spectrum of mission command systems?

It is difficult to emulate attacks of that scale without the resources of the modeling and simulation community. A standard Warfighter exercise will test the Mission Essential Task List (METL) of a battle staff across a multi-echelon spectrum, and cyber-warfare effects simulation will assist that training.

5. COBWebS for Cyber Warfare Training

Based on the finding from our domain and gap analysis we compiled a list of capability needs for cyber warfare training. The list was then vetted with our stakeholders to prioritize and scope our research. The initial phase is focused on CNA/OCO M&S, specially the II, DoS, ID, and IF cyber-attacks. Future phases will address the CND/DCO M&S.

Our prototype is called Cyber Operations Battlefield Web Service (COBWebS). By definition a cobweb is something that entangles, obscures, or confuses, which is characteristic of the effects of cyber-attacks. COBWebS is a Service Oriented Architecture (SOA) based software application that simulates the effects of C2 communication between synthetic entities and the MCS.

The initial phase of COBWebS is designed to address the “low hanging fruit” gaps raised by our stakeholders, specifically:

- Lack a way to simulate cyber operations that affect the Blue (U.S. and Coalition) MCS
- Enhance threat Computer Network Operations
- Threat Computer Network Attack
- Remote mission command of multiple cyber platforms
- Modeling & execution of cyber activities
- Threat cyber tools developed as Software as a Service (SaaS)

5.1 Design Rational and Approach

Typical CNA implementation at cyber ranges and in the operational test environment provides the ability to train forces and conduct equipment testing. However, these systems lack the ability to integrate with traditional M&S simulation training environments such as battle staff training that require simulation of the training environment and stimulation of the MCS systems. An additional concern is training systems require Information Assurance (IA) validation to operate. Our approach would provide an IA-safe environment without corrupting the MCS computers or its network infrastructure.

To build a service based application that simulates cyber-attacks on the Blue MCS, our application would need to first map the data exchanged between the synthetic entities from the simulation and the MCS. This Sim-MCS SOA-based gateway already exists, it’s called the Mission Command Adapter – Web Service (MCA-WS). MCA-WS is a product of the Project Manager (PM) for OneSAF. It is a SOA-based application that bridges the C2 communication between simulated/synthetic entities and MCS. It supports a wide variety of C2 protocols and MCS. We decided to leverage the MCA-WS for the mapping of simulation-C2 messages and for interfacing with the MCS in COBWebS.

We also needed a set of drivers to test the CNA services offered by COBWebS. These test drivers will also be used to initiate and manage the various cyber-attacks. We decided to leverage the Ozone Widget Framework (OWF) currently used in Command Web Command Post Computing Environment (CPCE) to provide users with a common map and graphical user interface that is familiar to warfighters.

5.2 Design Overview

The COBWebS server leverages the MCA-WS to provide a series of CNA services that other simulation models can
use to trigger the effects of cyber-attacks on mission command devices. Figure 1 shows a high-level view of the COBWebS architecture.

![Figure 1 - COBWebS Architecture](image1.png)

COBWebS works with any simulation that uses MCA-WS to interface with the MCS. Each outbound (simulation-to-MCS) message is intercepted and examined. If no cyber-attack effect is required, the message is forwarded on to the MCA-WS which in turn maps it to the appropriate C2 protocol(s) and sends it out to the destination MCS(s). Otherwise, COBWebS applies the appropriate cyber-attack effects; e.g., if the sender or recipient is under the DoS attack, COBWebS would simply discard the message and not forward to the MCA-WS.

COBWebS configuration and status information can be accessed using a standard web browser such as Firefox. The Configuration page allows user to connect to different simulation clients and MCA-WS. The Status page (showed in Figure 2) displays the connected simulation client and cyber clients (test widgets), a list of current cyber-attacks, and logs of the most recent messages calls.

![Figure 2 - COBWebS Status Page](image2.png)

In order to test and mature COBWebS’s CNA services, we also implemented a set of CPCE OWF widgets. There is an OWF widget for each type of CNA. A 3D map widget is used to display the intercepted entities on a Google Earth map. All widgets are running in an OWF browser. The widgets interface with the COBWebS server via web services to invoke the various CNA services. Each widget includes common fields, e.g., Originator and Recipient Uniform Reference Number (URN), as well as fields that are unique to the attack type, e.g., Delay Time for the Information Delay attack or text field for the Information Forgery Free Text message. As data is input by the user, the widget performs some validation to ensure required information is captured before sending the request to COBWebS. The following figures show the current version of our prototype widgets.

![Figure 3 – 3D Map Widget](image3.png)
6. Example COBWebS Use Cases

Our intent was to develop a service based software application that allows any cyber client to invoke the support CNA services modeled by COBWebS. Depending on the training objectives and scenarios, individual cyber-attack can be launched to simulate different attacks. Some example use cases are listed below.

Before CNA Attack

Red and Blue forces conduct their missions, according to training scenario, on a synthetic battlefield simulated by simulations with role players. The Blue and Red entities appear on the trainee’s Force XXI Battle Command Brigade and Below (FBCB2) system as Blue units report their position reports and observation reports. The trainee can issue orders for a fire mission, using a fire support C2 system such as the Advanced Field Artillery Tactical Data...
System (AFATDS), from Blue to Red. The order is carried out successfully and the updated Common Operating Picture (COP) is reflected on FBCB2 and other MCS.

DoS Use Cases
The cyber-attacked Blue units’ positions and observed information stop updating on FBCB2 and other COP systems, become stale, and eventually disappear.

A call for fire order issued to the cyber-attacked unit was ignored and the targeted Red unit still shows up as healthy on the COP system.

IF Use Cases
Fake entity and observation reports were generated by the Red cyber-attack unit on behalf of Blue units. These reports deceive the COP as seen by the trainee and cause him/her to take actions that would otherwise not be taken.

A fake call for fire was generated by the Red cyber-attack unit on behalf of a Blue commander unit to fire at another friendly Blue unit causing a friendly kill.

II Use Cases
The cyber-attacked Blue units’ position and heading information was intercepted by the Red force and was used to launch an ambush on the Blue units or to launch subsequent DoS, ID, and IF attacks.

ID Use Cases
A call for fire order, issued by the trainee to a Blue unit to fire at a location where Red units were observed, is intercepted and delayed for a period of time then forward on. This allows the Red units to move out of harm’s way. When the fire mission is finally launched at the predetermined location, the Red units are no longer there and therefore remain unharmed.

Combined Use Cases
Different cyber-attacks can also be combined to simulate more realistic cyber-attack use cases. Here’s an example “Man-in-the-Loop” use case of Red cyber-attacker using the COBWebS’s II, DoS, ID, and IF services to deceive and disrupt Blue units’ SA while launching an ambush to destroy the Blue units.

1. Red cyber-attacker uses II to intercept, discover, and gain knowledge of the Blue entities ground truth
2. Red cyber-attacker uses DoS to denied Blue units’ C2 communication so their position reports and observation reports are blocked
3. Red cyber-attacker uses ID to delay critical Blue C2 communication
4. Red assault units move in and destroy the Blue units
5. Red cyber-attacker uses IF to send fake C2 communication on behalf of Blue units as if everything is fine
6. Once the Red assault units have moved out of the area, Red cyber-attacker stop the IF messages

As a result of these coordinated cyber-attacks, the COPs can be quite different between the ground truth (shown in Figure 10) and perceived truth as seen on the Blue MCS (shown in Figure 11). Please note that the graphics and units are fictional for demonstration purpose.

Figure 10 – Ground Truth simulated by Constructive simulation

Figure 11 – Perceived Truth as seen of MCS as a result of cyber-attacks

7. COBWebS Limitations
During the course of our research project, we’ve held several in-progress reviews (IPR) where we demonstrated
the capabilities of COBWebS to various stakeholders. Some of the feedback received from the IPRs has been incorporated in the initial phase of development while others are captured for consideration as potential future product enhancements. Since the initial IPR we’ve added a “mass attack” capability that enables the Red cyber role player to quickly launch large scale CNA. This is accomplished via a Master Scenario Event List (MSEL). Below are some of the limitations and potential future capabilities.

- Simulate CNA effects on in-bound C2 communication, i.e., from MCS to simulation clients
- Simulate CNA effects on C2 communication between live entities/C2 devices, i.e., live to live
- Simulate proactive and reactive CND measures after the realization of being cyber-attacked.

8. Conclusion and Way Forward

In recent years there have been increasing occurrences and severity of cyber-attacks on U.S. interests, to include DoD networks, information, and systems. Cyberspace is a domain that lacks the necessary M&S tools to properly evaluate, experiment, and train the warfighter to recognize and utilize cyber operations as a part of the mission. In recent years various DoD and Army publications have indicated the need for better cyber operations training. In response to this need we’ve researched and developed an initial service-based application prototype to be used in cyber warfare training. The initial phase of COBWebS allows training managers to incorporate CNA/OCO injection into their training exercises so that the trainees can recognize cyber-attacks and make decisions accordingly. There are, however, other gaps and limitations that remain to be addressed, some of which are listed in the section above. In the long run we see CobWEBS as web based service that could be accessed and managed by any simulation to generate effects based on their cyber scenarios as they unfold. We also are looking into similar simulation cyber data exchange models as they mature [12] to see their usability in extending the prototype. We’re working with various military subject matter experts (SME) to develop several Combat Training Center (CTC) like scenarios to demonstrate in simulation various possible cyber-attacks against the Blue MCS. Our goal is through these IPRs, demonstrations, and conference presentations, we’ll continue to engage our stakeholders to solicit feedback that will enhance COBWebS in order to provide the Army with a better cyber warfare simulation for training. We see COBWebS transitioning to the OneSAF baseline when it matures.

9. References

[10] “Joint Communications System,” JP 6-0, June 2010

Author Biographies

HENRY MARSHALL is a Science and Technology Manager at the Army Research Lab, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC). His assignment experience spans across several agencies including Army, Department of Homeland Security (DHS), and Navy. His 30+ years with the Government have been spent assigned to leading edge simulation technology efforts in Modeling and Simulation (M&S) Architecture, cyber training, law
enforcement training, embedded training technology, Semi-Automated Forces (SAF), and simulation software development and acquisition. He received a Bachelor of Science in Engineering (B.S.E.) degree in Electrical Engineering and a Master of Science (M.S.) degree in Systems Simulation from the University of Central Florida.

JERRY MIZE is a Science and Technology Assistant Program Manager/Acquisition Officer at the Army Research Lab, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC). His assignment experience spans across several Army functions including Signal, Military Intelligence, Air Defense, Operations, Logistics, Officer Training, and Army Acquisition. His 25+ years with the Army give him keen insight into various functions affecting Warfighter processes and requirements which now are focused on leading edge simulation technology efforts in Modeling and Simulation (M&S) and acquisition. He received an: Associate of Applied Science in Electronics from Cochise College, Arizona, Bachelor of Science in Technology from Jacksonville State University, Alabama, and a Master of Arts in Procurement and Acquisition Management degree from Webster University.

MICHAEL HOOPER is a Cyberspace Operations planner at the 780th Military Intelligence Brigade. He enlisted into the Army in September of 2001 as a Network Switching Systems Operator, and deployed to Baghdad, Iraq throughout 2004. Following the deployment, CPT Hooper completed schooling and commissioned as a signal officer while serving an infantry branch detail in Afghanistan from 2008-2009. He later served as the squadron signal officer for an armored reconnaissance squadron in Baghdad and Al' Kut, Iraq in 2011. Following that assignment, CPT Hooper served as a Team Leader for the United States Army Cyber Opposing Forces (OPFOR), and later as a company commander in the 780th Military Intelligence Brigade. He received a Bachelor of Science in Information Systems Management from the University of Maryland's University College, and is currently pursuing a Master of Science in Security Informatics (MSSI) from Johns Hopkins University.

JEFF TRUONG is a Principal Systems Engineer at Effective Applications Corporation. He has over 25 years of Systems/Software Engineering and Technical Management experience in distributed Modeling & Simulation systems, telephony/telecommunication systems, networking systems, and network management systems. Mr. Truong is currently a Systems Engineer working on various projects sponsored by the Army Research Lab, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC) and Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) Project Manager for Constructive Simulation (PM ConSim).

ROBERT A. WELLS is a Project Engineer at Dynamic Animation Systems, Inc. He has led the development of the Risk Reduction Test Bed (RRTB) as part of the Advanced Simulation Systems Integration Modeling Interoperability Laboratory and Test Environment (ASSIMILATE) research effort. Mr. Wells has over 17 years of experience in the Modeling & Simulation (M&S) community and has managed a wide range of training systems within the industry. He has integrated Live, Virtual, and Constructive (LVC) components from the LVC Integrating Architecture (LVC-IA) program as well as core-system components from the LVC domains to include Homestation Instrumentation System (HITS), Aviation Combined Arms Tactical Trainer (AVCATT) & Close Combat Tactical Trainer (CCTT) Semi-Automated Forces (SAF), and Joint Land Component Constructive Training Capability (JLCCCT) within the RRTB. He earned his Bachelor of Science degree in Computer Science from the University of Central Florida and his Master of Business Administration from the Crummer Graduate School of Business at Rollins College.