A Cyber Warfare Prototype for Live, Virtual, & Constructive Simulations

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

Nathan Vey
Army Research Laboratory (ARL)
Human Research and Engineering Directorate (HRED)
Simulation and Training Technology Center (STTC)
Orlando, Florida
nathan.l.vey.civ@mail.mil

J. Allen Geddes
Dynamic Animation Systems
Orlando, Florida
ageddes@d-a-s.com

Lawrence Elliott
Dynamic Animation Systems
Orlando, Florida
lelliott@d-a-s.com

ABSTRACT

Cyber warfare has quickly moved to the forefront of the Army's training needs. With the realization that cyberspace is now a warfighting domain, simulation and training program managers are left struggling to identify the best solution for implementing cyber warfare effects into the training domain. The term cyber itself can imply a broad range of possibilities including electronic warfare (e.g. jamming), kinetic warfare (e.g. destroying systems), hacking attacks, and insider threats. Current major training 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. It is necessary to train in this warfighting domain, but the requirements and best strategies for conducting cyber training have created a challenging technical gap for the simulation and training communities. Presently, the Army's Cyber Mission Force teams require cyber range training to provide the realistic data exchanges necessary to develop their skills. This type of training is commonly referred to as "cyber for cyber." The rest of the Army falls into another category of cyber training commonly referred to as "cyber for others." After talking with numerous stakeholders, we decided to develop a prototype system for training the "cyber for others" group to experience cyber-attacks on their tactical mission command systems and to make recovery decisions. This prototype, called Cyber Operations Battlefield Web Service (COBWebS), provides the capability to simulate the effects of various cyber-attacks on command and control communication between the synthetic entities and the Blue Force's mission command systems. Our prototype leverages the OneSAF Mission Command Adapter Web Service (MCA-WS) and adds cyber warfare effects modeling. We will share our experience developing and field testing this cyber warfare training capability.

ABOUT THE AUTHORS

HENRY MARSHALL is a Science and Technology Manager at the Army Research Laboratory, Human Research and Engineering Directorate, Advanced Training and Simulation Division (ARL HRED ATSD). 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.

NATHAN VEY is a Science and Technology Manager at the Army Research Laboratory, Human Research and Engineering Directorate, Advanced Training and Simulation Division (ARL HRED ATSD). He is a former Marine with operational experience in training Signals Intelligence (SIGINT) collection and analysis operations. Nathan's military training consisted of Electronic Intelligence (ELINT), Electronic Warfare (EW), and Geospatial Intelligence (GEOINT). He holds a Bachelor of Science (B.S.) in Electrical Engineering from the Milwaukee School of

Engineering and is currently pursuing a Master of Arts (M.A.) degree in Intelligence Studies with a concentration in Cyber from American Military University.

J. ALLEN GEDDES is a Software Engineer at Dynamic Animation Systems, Inc. He has over 12 years of Systems, Network, and Software Engineering experience and holds the following certifications: CompTIA A+, CompTIA Network+, CompTIA Security+, Microsoft Certified Professional (MCP), Microsoft Certified Systems Administrator (MCSA), Microsoft Certified Systems Engineer (MCSE). He has earned an Associate of Science (A.S.) degree in Computer Programming and Analysis, a Bachelor of Science (B.S.) degree in Management Information Systems, a Bachelor of Applied Science degree (B.A.S.) degree in Software Development, and is currently pursuing a Master of Science (M.S.) degree in Modeling and Simulation at the University of Central Florida. Mr. Geddes currently works on various projects sponsored by the Army Research Laboratory, Human Research and Engineering Directorate, Advanced Training and Simulation Division (ARL HRED ATSD).

LAWRENCE ELLIOTT is a Principal Software Engineer at Dynamic Animation Systems, Inc. He has over 15 years of Simulation Experience stemming from traditional programs of record such as WARSIM and CTIA to R&D efforts such as voice recognition, natural language processing, artificial intelligence, and space related technologies. He currently serves as the technical software lead for Cyber Operations Battlefield Web Service (COBWebS) which is sponsored by the Army Research Laboratory, Human Research and Engineering Directorate, Advanced Training and Simulation Division (ARL HRED ATSD). He received a Bachelor of Science in Computer Science degree from Florida State University and a Master of Engineering with Concentration in Management from University of Florida.

A Cyber Warfare Prototype for Live, Virtual, & Constructive Simulations

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

Nathan Vey
Army Research Laboratory (ARL)
Human Research and Engineering Directorate (HRED)
Simulation and Training Technology Center (STTC)
Orlando, Florida
nathan.l.vey.civ@mail.mil

J. Allen Geddes
Dynamic Animation Systems
Orlando, Florida
ageddes@d-a-s.com

Lawrence Elliott
Dynamic Animation Systems
Orlando, Florida
lelliott@d-a-s.com

Introduction

Cyber is a term that carries with it a variety of interpreted meanings depending on the context of discussion. Most often, cyber is analogous to the standard use-case of network security and protection (i.e. intruder detection, malware defense, etc.). In Joint Publication (JP) 3-12 (R) titled Cyberspace Operations, the Department of Defense (DoD) defines cyber in the context of cyberspace as, *"A global domain within the information environment consisting of the interdependent network of information technology infrastructure and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"* (Joint Staff Director of Operations, J-3, 2013). With the release of JP 3-12, cyberspace became the fifth warfighting domain, the others being the physical domains of air, land, maritime, and space (Joint Staff Director of Operations, J-3, 2013). Just as with the physical domains, the DoD seeks to control the cyberspace domain in order to freely conduct operations. Cyberspace superiority is the term that outlines this goal. It is defined as, *"The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary"* (Joint Staff Director of Operations, J-3, 2013). In order to achieve cyberspace superiority, it is necessary for warfighters and commanders who operate in the physical domains to have an understanding of cyberspace and its connection to their respective domains.

The goal of cyberspace superiority is further exemplified in the U.S. Army's newly released Field Manual (FM) No. 3-12, titled "Cyberspace and Electronic Warfare Operations," where Major General John B. Morrison Jr. states: *"We must anticipate that future enemies and adversaries will persistently attempt to infiltrate, exploit, and degrade access to our networks and data. A commander who loses the ability to access mission command systems, or whose operational data is compromised, risks the loss of lives and critical resources, or mission failure. In the future, as adversary and enemy capabilities grow, our ability to dominate cyberspace and the EMS will become more complex and critical to mission success."* (Headquarters, Department of the Army, 2017). This statement is profound and highlights the need to provide a robust training environment, adding Cyber and Electromagnetic Activities (CEMA) as an important part of the Army's training programs.

The Army's Cyber Training Program Model

The Army's current cyber training programs typically fall into one of two categories: *Cyber for Cyber* (CyforCy) or *Cyber for Others* (CyforO) (Seffers, 2015). CyforCy training programs target the training needs of the Army's cyber protection teams, who require very detailed low-level knowledge of how the Army's information systems communicate and share information across the network. CyforCy training typically occurs on cyber ranges where the cyber protection teams can practice in what could be the equivalent of a live exercise. In these training exercises, the cyber protection teams analyze network traffic and look for patterns indicative of a cyber-attack. They also train on executing the actions required to mitigate the cyber-attack once it has been detected. CyforO training programs on the other hand, do not require the same low-level technical expertise of the cyber protection teams, but need to make commanders aware of the potential threat of a cyber-attack against their mission command systems, and train them on what actions to take to mitigate a cyber-attack after it has been detected. A challenge in training CyforO is that the

training systems must comply with Information Assurance (IA) regulations and cannot subject the Army's Mission Command Information Systems (MCIS) to actual cyber-attacks that could compromise the security and integrity of the mission command system.

As a result of these CyforCy and CyforO training requirements and restrictions, it is our thesis that IA compliant Live, Virtual, and Constructive (LVC) simulations are best suited to focus on the training of the CyforO audience and cyber ranges are best suited for the CyforCy training audience. Based on this assumption, the focus of our research was to explore a possible CyforO training capability residing on a LVC system.

Evaluation of Current Cyber for Others Training Approach

Our research began by talking to stakeholders and reviewing the Army's existing CyforO training approach. Currently, when battle staff undergo MCIS training at a Mission Command Training Center (MCTC), training staff utilize Modeling and Simulation (M&S) solutions to stimulate the MCIS during the various training exercises. Current M&S solutions largely lack cyber-attack effect models, so in order to train cyber, the exercise controllers use manual workarounds (e.g. "white cards") to inject cyber-attack conditions into the training exercise. These manual injects are typically low fidelity and simply describe a denied or degraded condition that the battle staff must operate as-if their MCIS is now under, even though the cyber-attack effects do not appear on the MCIS.

There are two cyber capabilities that attempt to improve this CyforO training process: Cyber Operational Architecture Training System (COATS) and Network Effects Emulation System (NE2S). COATS provides a system called a Network Guard for bridging the cyber range environment networks with traditional battle staff training environment networks. COATS also provides a cyber data exchange model (DEM) that attempts to standardize the format for sharing cyber-attack data throughout the training environment network (Wells & Bryan, 2015). When a cyber-attack occurs on the cyber range, the details of that attack are transmitted from the cyber range through the Network Guard to the training environment in the format defined by the cyber DEM. The systems in the traditional battle staff training environment network each have an NE2S agent running on them listening for cyber-attacks and when the agent receives a cyber-attack message, NE2S creates the effects of the cyber-attack on that system (Wells & Bryan, 2015).

The limitation with this approach is that IA restrictions prevent the training staff from installing the NE2S agent on MCIS in the training environment network. As a result, we designed an IA compliant cyber training capability that does not alter the MCIS baseline, which provides the ability to create the effects of cyber-attacks on the MCIS in the training environment network, within the MCIS systems' IA restrictions.

Simulation of types of Cyber-Attacks

A challenge we encountered early in our research was how to best create a cyber effects simulation that covers the maximum number of possible cyber-attacks and possible effects that could be created on the mission command systems. Ideally, the training audience would come up with an attack script for an Opposing Force (OPFOR) attack on a mission command system, then the cyber training system would simulate the effects of the attacks within the training exercise. One of the most difficult tasks in modeling cyber-attacks is that they are very asymmetric and ever changing. This makes it hard to guess what the full effects were and what the next attack will be. Possible types of attacks include: Electronic Warfare (EW) attacks which cause mission command systems to lose contact with the network; kinetic attacks which could destroy nodes, computers, etc.; hacking attacks which the opposing force could use to gain access to the computer systems and monitor and manipulate information; and insider attacks which could have similar results to the hacking attacks.

The needs and requirements for cyber simulation within the CyforO training community were formulated through discussions with stakeholders and subject matter experts. Participants included representation from Army Research Laboratory (ARL); Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI); Army Cyber Center of Excellence; Army Training and Doctrine Command (TRADOC); Johns Hopkins University Applied Physics Laboratory (APL); and Army National Simulation Center (NSC). Based on these discussions, it was determined that the following subset of cyber-attacks would be best suited for CyforO training in LVC systems:

- *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 command and control (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.

Most of the major types of cyber-attacks can be simulated to some degree by the classes listed above.

Design of Cyber Operations Battlefield Web Service: COBWebS for Cyber Training

Our CyforO training capability 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 an IA compliant, web-based, Service-Oriented Architecture (SOA) software application that simulates the effects of cyber-attacks on C2 communications between synthetic entities and the MCIS in the tactical network. COBWebS improves the CyforO cyber training process by creating the actual effects of the cyber-attack on the MCIS in cyber training exercises, enabling the training exercise controllers to evaluate the battle staffs' ability to detect and react to the cyber-attack against their MCIS. See Figure 1 below for a high-level overview of the COBWebS architecture.

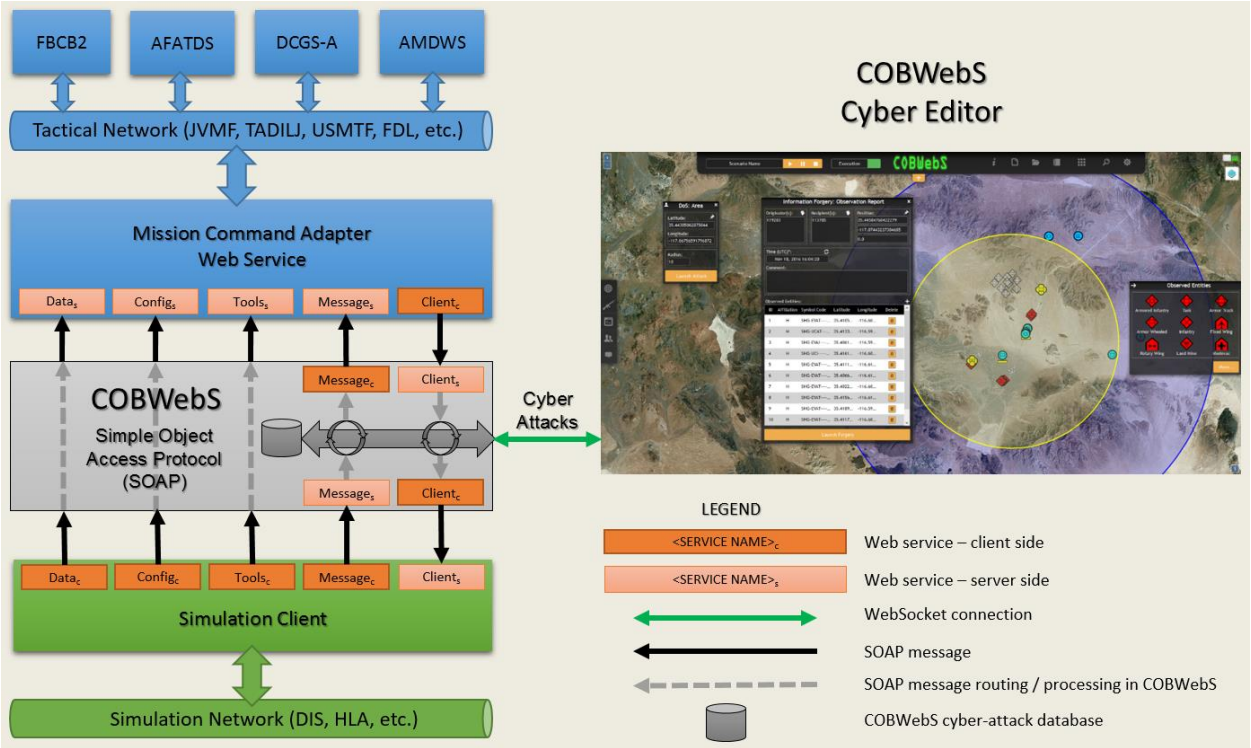

Figure 1 – COBWebS Architecture

COBWebS is able to remain IA compliant because it is a standalone web application and does not require any software or agents to be installed on the C2 devices. In addition, COBWebS does not launch actual cyber-attacks against the C2 device, and just creates the effects of cyber-attacks on the C2 devices by controlling the message flow from the simulation to the C2 device.

During our initial development phase, we focused on simulating effects of the attack classes described above (DoS, II, IF, and ID) that encompass most existing and future cyber-attack threats. When using COBWebS, the Cyber Attacker Role Player can launch II, ID, and DoS attacks by area (circular area or polygon shaped area) as well as by Originator and Recipient Uniform Reference Number (URN). See Figures 2 and 3 below for examples of URN and Area based attacks.

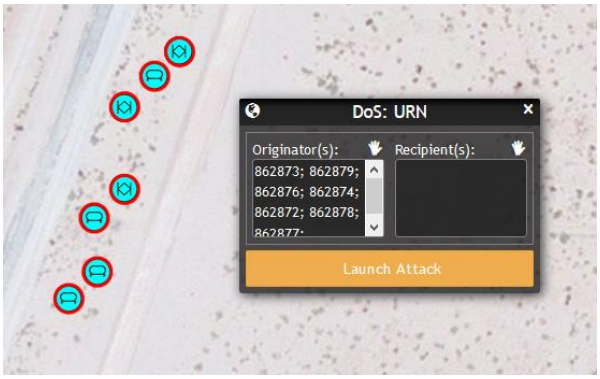

Figure 2 – URN Based Attack

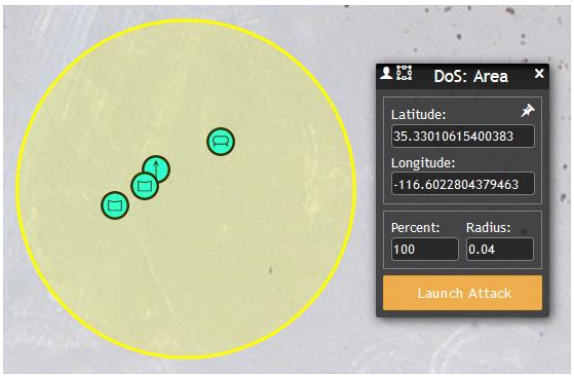

Figure 3 – Circular Area Based Attack

DoS attacks can be launched with a specified denial percentage, where COBWebS will deny anywhere from 0 to 100 percent of messages matching the DoS attack criteria.

The Cyber Attacker role player can inject forged Free Text messages, Entity Position Reports, and Observation Reports into the training exercise as well. COBWebS supports Forged Routes, where the Cyber Attacker role player can select a group of entities on the map and draw a route to forge. COBWebS will then schedule and dispatch forged Entity Position Reports along the route, to create the forged movement of the selected entities on the C2 devices. See Figures 4 through 7 below for an example of a Forged Route.

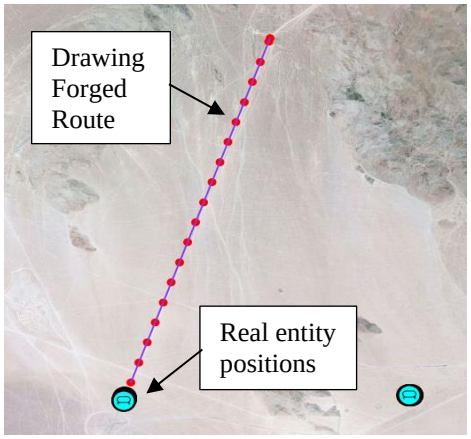

Figure 4 – Drawing Forged Route in Cyber Editor

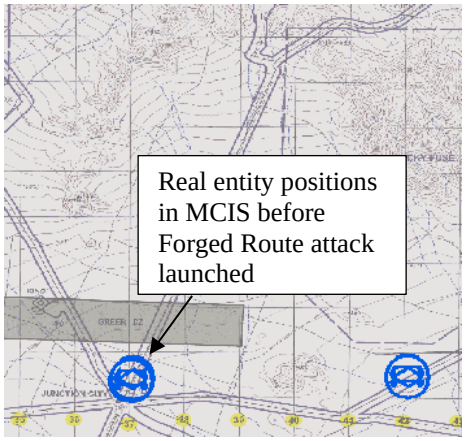

Figure 5 – Entity Positions in MCIS Before Forged Route

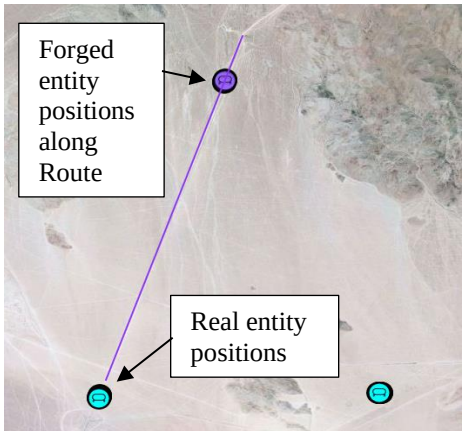

Figure 6 – Forged Route Executing in Cyber Editor

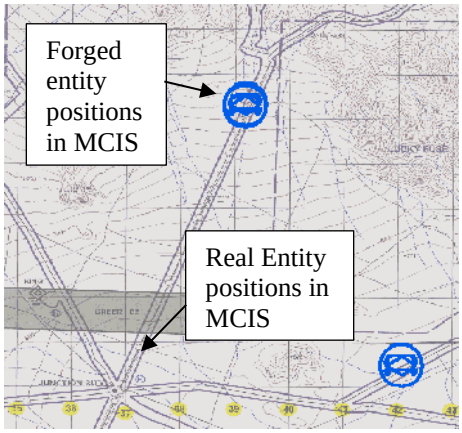

Figure 7 – Forged Route Effects in MCIS

COBWebS Development

COBWebS is able to generate cyber-attack effects on MCIS by intercepting and evaluating messages as they pass from the constructive simulation network to the live tactical network through the Mission Command Adapter Web Service (MCA-WS). COBWebS does not currently affect messages sent in the other direction, from the live tactical network to the constructive simulation, but could do so in the future if that became a requirement. As a result of leveraging the MCA-WS, COBWebS can work with any simulation that uses the MCA-WS to interface with the tactical network.

COBWebS communicates with the simulation MCA-WS client and the Mission Command Adapter (MCA) via Simple Object Access Protocol (SOAP). COBWebS communicates with the Cyber Editor, which is the Cyber Attacker role player user interface, via a bi-directional, full duplex WebSocket connection.

Each outbound (simulation to tactical network) message is intercepted by COBWebS and analyzed to determine if the message matches the criteria of any active cyber-attacks. If no cyber-attack effect is required, the message is forwarded on to the MCA-WS, which in turn dispatches the message to the appropriate C2 protocol(s) and sends it out to the designated MCIS.

If the message matches the area or URN criteria of an active cyber-attack, then COBWebS handles the message accordingly, based on the type of cyber-attack the message is under. For example, if the message is determined to be under a DoS attack, then COBWebS drops the message altogether, preventing it from reaching the tactical network, creating the effect of a DoS attack in the MCIS. If the message is under an ID attack, then COBWebS holds onto the message for the specified amount of time before forwarding it to the MCA-WS. If the message is under an II attack, then COBWebS dispatches the message to all registered cyber clients listening for II attacks. The Cyber Attacker role player can also launch IF attacks where COBWebS injects forged tactical messages directly into the MCA-WS that will appear on the MCIS as if they came from entities in the simulation.

The Cyber Attacker role player injects cyber-attacks into COBWebS using the Cyber Editor user interface. Using the Cyber Editor, the Cyber Attacker role player can launch URN based attacks by interacting directly with entities on the map, or they can launch Area based attacks (circular or polygon shaped attacks) by drawing the attack areas directly on the map. The Cyber Editor can also be used to script cyber-attacks into repeatable cyber scenarios.

When generating cyber scenarios, the Cyber Attacker role player can create cyber missions with scripted II, ID, DoS, and IF cyber-attacks. When adding a cyber-attack to a mission, the Cyber Attacker role player can specify what event will trigger the cyber-attack. Currently, COBWebS provides functionality for scheduling cyber-attacks with time triggers, phase line triggers, and completion triggers. When scheduling a cyber-attack with a time trigger, the cyber-attack will launch when the mission's elapsed time reaches the scheduled time for the cyber-attack. When scheduling a cyber-attack with a phase line trigger, the Cyber Attacker role player will draw a phase line on the map, and the cyber-attack will launch when any of the specified entities cross the phase line. When scheduling a cyber-attack with a completion trigger, the cyber-attack will launch when the completion of another specified event occurs, such as when a specific cyber-attack completes or when a specific cyber mission completes. Additional trigger types can be implemented in the future as requirements arise.

COBWebS Example Use Case

In a standard LVC mission command training exercise, Red and Blue forces conduct their missions according to training scenarios on a synthetic battlefield simulated by simulations with role players. The Blue and Red entities appear on the trainees' MCIS as Blue units report their position reports and observation reports. The trainee issues orders, and when the orders are successfully carried out, the updated Common Operating Picture (COP) is reflected on the MCIS.

The following fictional example shows how a Cyber Attacker role player can use COBWebS to inject a series of cyber-attacks into the training exercise to manipulate the trainee's perceived truth view of the battlefield.

Information Interception Attack

The Red Cyber Attacker role player first launches an Area based Information Interception attack and intercepts Blue position reports, creating a real-time view of the battlefield in the attack area. (Figure 8) This is a passive attack, and does not tip-off the Blue Commander that they are under any type of cyber-attack, as the Commander is still receiving all position report updates on their MCIS. (Figure 9 and Figure 10)

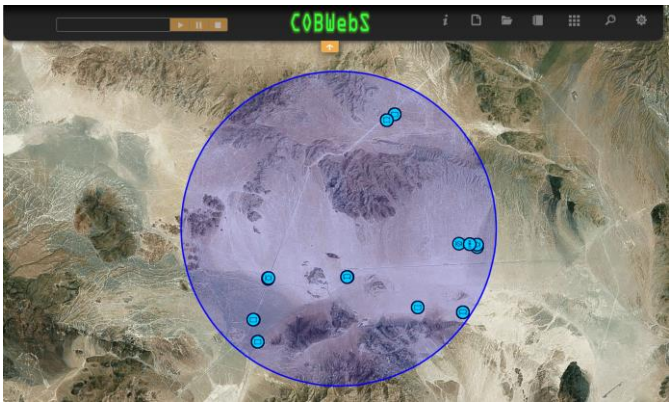

Figure 8 – Cyber Attacker Role Player Injects Area Based II Attack

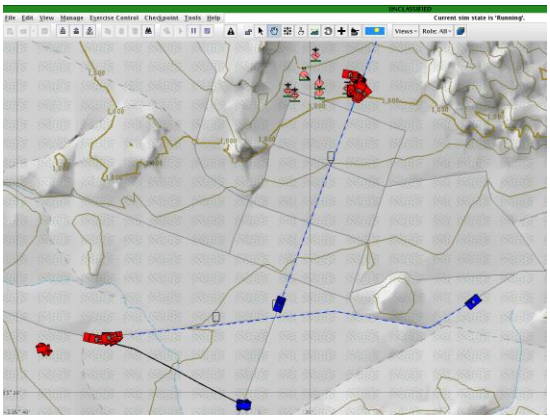

Figure 9 – Ground Truth

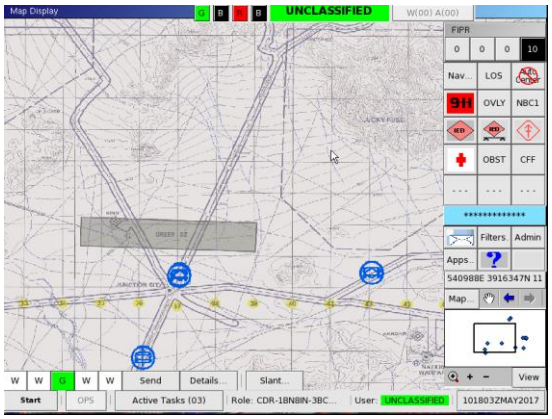

Figure 10 – Commander's Perceived Truth in MCIS

Information Forgery Attack

Now that the Cyber Attacker knows where Blue forces are positioned, they inject forged Free Text messages to the Commander's MCIS, alerting of possible enemy activity to the North and to the West, and requesting a Recon & Report mission. (Figure 11) The forged Free Text message appears in the Commander's MCIS. (Figure 12) If the Commander reacts to the intelligence message, he will be leading Blue entities directly into a Red ambush.

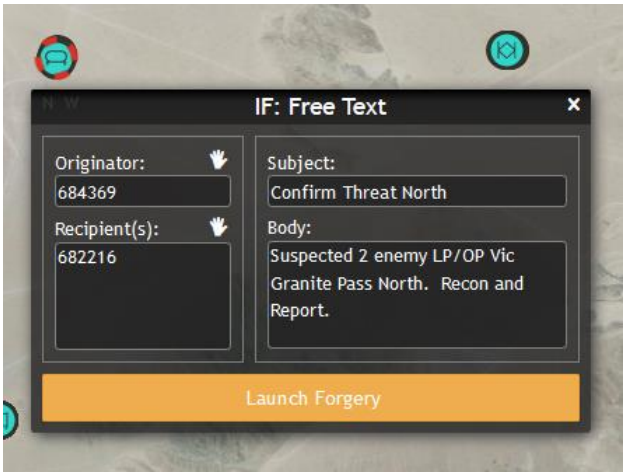

Figure 11 – Cyber Attacker Injects Forged Free Text Messages

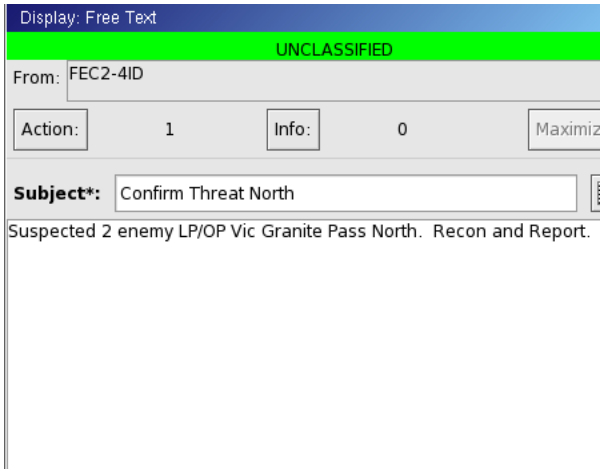

Figure 12 – Forged Free Text Message in MCIS

Denial of Service Attack

Once the Cyber Attacker has injected the forged intelligence messages, he observes Blue position reports and waits for movement to see if the Commander has ordered entities on the requested Recon & Report mission. As soon as the Cyber Attacker detects movement, they launch an Area based Denial of Service attack, so that anything the Blue forces see and encounter in the real world do not get transmitted back to the Commander. (Figure 13)

Forged Route

The Cyber Attacker has detected Blue entity movement North and West, but is suppressing all position report transmissions from those entities as a result of the DoS attack, so the Commander does not see the movement on their MCIS. The Cyber Attacker selects the moving entities on the map and launches Forged Route attacks, to forge the entities' movement along the North and West routes on the commander's MCIS device. (Figure 14)

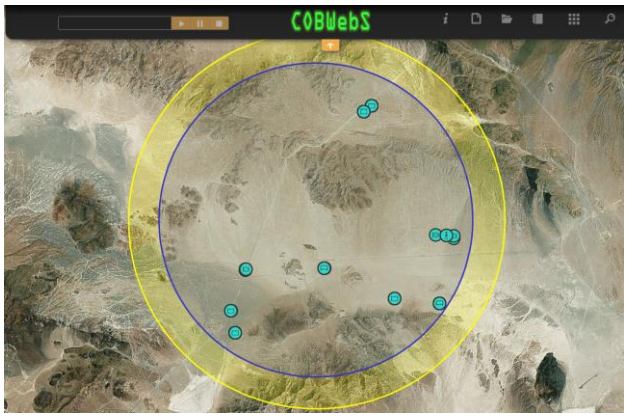

Figure 13 – Area based Denial of Service Attack

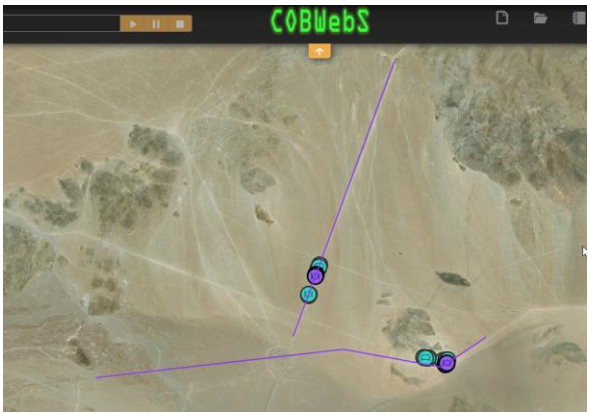

Figure 14 – Forged Route Attacks

As a result, the Commander sees entities moving North and West on their MCIS. But in the real world, those entities have stopped moving and are actively engaging hostile forces, sending Observation Reports, Personnel Status Reports, and Medevac Requests, all of which are being suppressed by the Cyber Attacker's DoS attack.

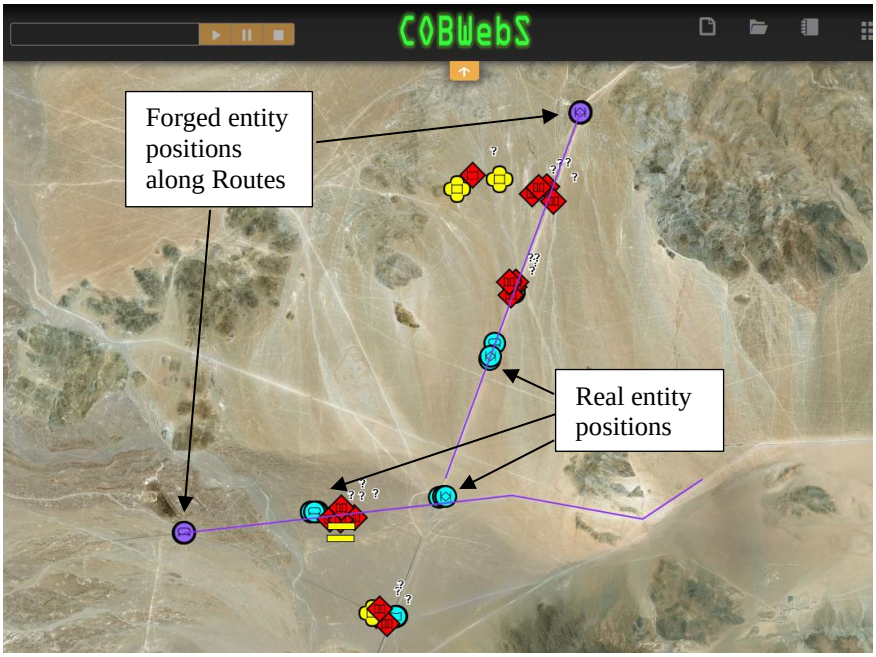

Figure 15 – Cyber Attacker Role Player Suppresses Real Entity Position Reports and Observation Reports, and Injects Forged Entity Position Reports along Routes

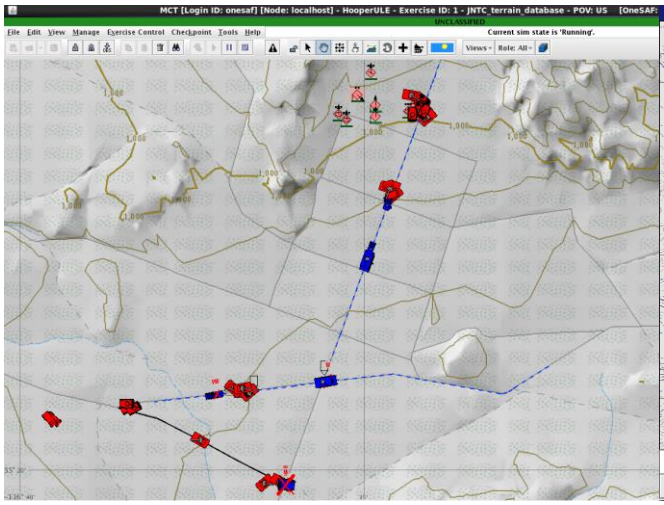

Figure 16 – Final Ground Truth

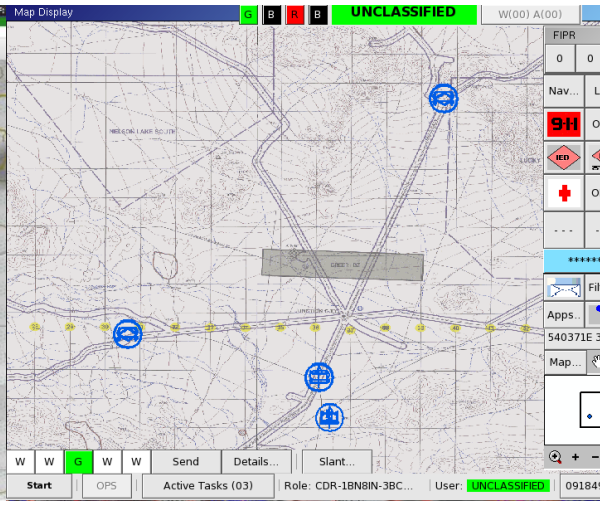

Figure 17 – Final Perceived Truth in MCIS

As you can see in this example, through a series of cyber-attacks the Red Cyber Attacker role player was able to manipulate the Commander's perceived truth view of the battlefield, deny critical information from the Commander, inject forged information to the Commander, and ultimately change the outcome of the mission. (Figures 16 and 17)

COBWebS Limitations

Currently, COBWebS only interfaces with simulations that utilize the MCA-WS, and does not interface with non-MCA-WS compatible simulations. Also, since COBWebS can only affect synthetic to live messages, COBWebS cannot currently affect live to live messages, which has been requested during our COBWebS demonstrations, in order to be able to use COBWebS in live training exercises.

Also, COBWebS can currently only conduct Red on Blue cyber, but cannot conduct Blue on Red cyber. In order to conduct Blue on Red cyber training, we would need Red tactical devices and an interface to those devices to be able to communicate with them.

Conclusion and Way Forward

Cyber warfare continues to be an important emerging concern of the Army. Many of the current LVC systems continue to struggle with cyber gap requirements and best strategies on how to train the CyforO community on reacting to cyber-attacks. When this research started, the goal was to develop a prototype that would show a possible implementation of a portion of the cyber training iceberg. Many users wanted "cyber" but did not have a concept to implement it in training simulations. By seeing a prototype rather than requirements in a spreadsheet, discussion on the prototype facilitated the development of the actual requirements and system design decisions.

COBWebS has been successful in that it shows an approach to simulating cyber-attacks, and the communities we have demonstrated COBWebS to have provided robust feedback. Presently, COBWebS is being considered to be part of future major constructive simulations development cycles. It is also planned for distribution with OneSAF 8.7, which is available to the simulation community. Talking to users, some issues they presented included how to create a cyber opposing force that would attack and be attacked. They also have interest in the development of a cyber server that would manage cyber events between the live ranges and simulations. Again, this is only a tip of this giant cyber iceberg so numerous research challenges remain for this extremely asymmetric and rapidly changing domain.

References

Headquarters, Department of the Army. (2017). *FM 3-12 Cyberspace and Electronic Warfare Operations.* Army Publishing Directorate.

Joint Staff Director of Operations, J-3. (2013). *Joint Publication 3-12 (R) Cyberspace Operations.* Department of Defense.

Seffers, G. I. (2015, December 1). Preparing Troops to Thrive in the Chaos of Combat. *SIGNAL*.

Wells, D. "., & Bryan, D. (2015). Cyber Operational Architecture Training System - Cyber for All. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*