Integration of Live and Synthetic Environments for Improved Cyberspace Training

Omar Hasan, Ph.D., Jeffrey Welch, Bob Burch
Dignitas Technologies, LLC
Orlando, Florida
ohasan@dignitastech.com, jwelch@dignitastech.com, bburch@dignitastech.com

J. Allen Geddes, Michael W. Boyce, Ph.D.
US Army DEVCOM SC SED STTC
Orlando, Florida
james.a.geddes2.civ@army.mil, michael.w.boyce11.civ@army.mil

ABSTRACT

In the modern battlespace, Army forces must be Multi-Domain Operations (MDO)-capable, and as part of the Joint Force, must be prepared to fight across all domains (Land, Sea, Air, Space, and Cyberspace), the Electromagnetic Spectrum (EMS), and the Information Environment (IE). Increasingly, in conjunction with traditional kinetic operations, threats target the Army's Radio Frequency (RF) connected elements to gain an advantage in contested and competitive environments, such as the disruption of Global Positioning System (GPS) and other Position, Navigation, and Timing (PNT) systems, and jamming of radio communications. To support MDO training in this complex operational environment, the Army's Live, Virtual, Constructive, and Gaming (LVC&G) training systems need to incorporate these Cyberspace Electromagnetic Activities (CEMA) to produce realistic effects for the training audience. However, incorporating EMS elements in training environments is difficult due to regulations on spectrum interference and the lack of integration with existing Constructive and Virtual simulation systems. In this work, we describe our initial efforts to provide an architecture to coordinate training of EMS operations and effects between the Synthetic training environment and Live training participants. We established an architecture, toolset, and approach to communicate threat radio jamming effects from the simulated environment, producing actual jamming effects on participant radios in the Live environment. The Cyberspace Battlefield Operating System Simulation (CyberBOSS) system was used as an integrating architecture between simulated jammers in the One Semi-Automated Forces (OneSAF) system, stimulating software defined radios (SDR) in the Live environment. This resulted in actual jamming effects on tactical radios instrumented with Direct Injection Jammer (DIJ) devices, providing an emulated jamming effect without any open-air jamming in the operational environment. This paper describes the work to date for this effort and discusses the next steps to be taken to further coordinate CEMA training between Live and Synthetic training environments.

ABOUT THE AUTHORS

Dr. Omar Hasan is currently a chief software architect at Dignitas Technologies, where he serves as the software architect on two cyberspace-related research efforts: Cyberspace Battlefield Operating System Simulation (CyberBOSS) and the Intelligent Cyberspace Adversaries Tool Suite (ICATS). He also serves as the principal investigator on the cyberspace-related research efforts Geospatially Integrated Cyber Situational Awareness (GICSA) and Live, Virtual, and Constructive Cyber Battle Damage Assessment for Training (Cyber BDA). Dr. Hasan has 22 years of experience in software development, focusing on the Modeling and Simulation (M&S) areas of simulator interoperability, distributed simulation, and simulation architecture and infrastructure. He has extensive experience in object-oriented software analysis and design, open-source technologies and methodologies, and collaborative software development. Dr. Hasan has held architect and software engineering lead positions on both the One Semi-Automated Forces (OneSAF) and Joint Land Component Constructive Training Capability (JLCCTC) programs. He is currently supporting software development and cyber test event execution activities for the National Cyber Range (NCR). Dr. Hasan holds a B.S. and M.S. in Engineering from Columbia University and a Ph.D. in Engineering from Rutgers University.

Jeffrey Welch is a 21-year veteran of software development within the Modeling and Simulation industry. He is the current software development lead for the Cyberspace Battlefield Operating System Simulation (CyberBOSS)

 Approved for Public Release # PR2022_77084

program and related research efforts at Dignitas Technologies. He has worked on various research programs as well as directly on Virtual and Constructive simulation systems with emphasis on scenario generation, dynamic environments, interoperability, and complex system integration. His project involvements include direct support for JLCCTC, Brigade Combat Team Modernization (BCTM), Synthetic Environment (SE) Core, OneSAF, Combined Arms Command and Control Training Upgrade System (CACCTUS), and Joint Simulation System (JSIMS) programs. He holds an M.S. and B.S. in Computer Science from the University of Central Florida.

Bob Burch is Chief Technology Officer for Dignitas Technologies, with roles as technical advisor for Dignitas and principal investigator over a set of research programs including the U.S. Army Combat Capabilities Development Command Soldier Center (DEVCOM SC) Soldier Effectiveness Directorate (SED) Simulation and Training Technology Center's (STTC) Cyberspace Battlefield Operating System Simulation (CyberBOSS) and Intelligent Cyberspace Adversaries Tool Suite (ICATS). Mr. Burch has 38 years of experience in Modeling and Simulation. Mr. Burch has a wide range of Virtual simulation experience from vehicle platform systems modeling to simulation frameworks. Mr. Burch was the Chief Scientist for the Close Combat Tactics Trainer (CCTT) Semi-Automated Forces (SAF). For this role he was responsible for the overall architecture, technical approaches, frameworks, behavioral infrastructure, and integration and test of CCTT SAF. Mr. Burch was the Software Architect for One Semi-Automated Forces (OneSAF) and eventually System Architect. Mr. Burch has practical experience in the development of Product Line Architectures (PLA) in support of both Virtual and Constructive systems. He was a key contributor for PLA development for OneSAF, Synthetic Environment (SE) Core, and the United Kingdom's Combined Arms Tactics Trainer (UK CATT) programs. He holds a B.S. in Computer Science from the University of Central Florida.

J. Allen Geddes is a Science and Technology (S&T) Manager at the U.S. Army Combat Capabilities Development Command Soldier Center (DEVCOM SC) Soldier Effectiveness Directorate (SED) Simulation and Training Technology Center (STTC). In his current role, Mr. Geddes leads the DEVCOM SC's Cyberspace Warfare for Training (CyWar-T) S&T research program. He has over 15 years of Systems, Network, and Software Engineering experience and holds the following certifications: CompTIA A+, CompTIA Network+, CompTIA Security+, Microsoft Certified Systems Administrator (MCSA), and Microsoft Certified Systems Engineer (MCSE). He has earned a B.S. degree in Management Information Systems and a B.A.S. degree in Software Development from the University of Central Florida.

Dr. Michael W. Boyce is a Research Psychologist for the U.S. Army Combat Capabilities Development Command Soldier Center (DEVCOM SC) Soldier Effectiveness Directorate (SED) Simulation and Training Technology Center (STTC). Dr. Boyce is stationed at the Army Cyber Institute, West Point where he serves as a liaison for Modeling and Simulation within the Cyber Operations Research Element (CORE). His areas of focus include examining the human-system information requirements for Cyberspace and Electromagnetic Activities (CEMA) and presenting the complexities of the battlespace (including cyber) using Augmented & Mixed Reality. Dr. Boyce graduated with his Masters (M.S.) in Human-Computer Interaction from the Georgia Institute of Technology, and his Doctorate (Ph.D.) in Applied / Experimental Human Factors Psychology from the University of Central Florida.

Integration of Live and Synthetic Environments for Improved Cyberspace Training

Omar Hasan, Ph.D., Jeffrey Welch, Bob Burch
Dignitas Technologies, LLC
Orlando, Florida
ohasan@dignitastech.com, jwelch@dignitastech.com, bburch@dignitastech.com

J. Allen Geddes, Michael W. Boyce, Ph.D.
US Army DEVCOM SC SED STTC
Orlando, Florida
james.a.geddes2.civ@army.mil, michael.w.boyce11.civ@army.mil

INTRODUCTION

In the modern battlespace, Army forces must be Multi-Domain Operations (MDO)-capable, and as part of the Joint Force, must be prepared to fight across all domains (Land, Sea, Air, Space, and Cyberspace), the Electromagnetic Spectrum (EMS), and the Information Environment (IE). Increasingly, in conjunction with traditional kinetic operations, threats target the Army's Radio Frequency (RF) connected elements to gain an advantage in contested and competitive environments, such as the disruption of Global Positioning System (GPS) and other Position, Navigation, and Timing (PNT) systems, and jamming of radio communications. To support MDO training in this complex operational environment, the Army's Live, Virtual, Constructive, and Gaming (LVC&G) training systems need to incorporate these Cyberspace Electromagnetic Activities (CEMA) to produce realistic effects for the training audience. However, incorporating EMS elements in training environments is difficult due to regulations on spectrum interference with civilian infrastructure and the lack of integration with existing Constructive and Virtual simulation systems. Because of this, training of electromagnetic warfare (EW) effects currently relies on pre-scripted simulation events and *out-of-game* mechanisms (i.e., white cards, voice communication) to communicate the presence of these effects within the training environment. This does not provide a high level of realism and trainee stimulation during training, which prevents opportunities for the training audience to identify and diagnose the presence of the EW effect. Additionally, current training environments also do not automatically coordinate EW activities in the simulation with resulting effects in the Live training environment. Research and development activities are needed to more tightly integrate the EW activities within the simulation and Live domain so that training of both offensive and defensive EMS operations may be improved.

APPROACH

This section describes the high-level approach taken in our work to improve the coordination of EW effects between the Simulation and Live training environment to improve training realism. In our work, simulated threat actors in the Constructive simulation produce areal jamming effects and those effects are communicated by a cyberspace brokering architecture to the Live training environment. These jamming effects are then placed on Live tactical radios used by the Blue Force (BLUFOR) training audience to degrade or disrupt communication by participants, impacting their ability to execute their mission. The training goal is for the trainees to detect that their ability to communicate is degraded or denied and to trigger responses to determine mitigation strategies such as alternate communication paths or other methods to regain full operational capabilities. This approach is a significant improvement over current training in which exercise facilitators communicate the presence of EMS effects in a manual fashion.

In our work, we established an architecture, toolset, and approach to communicate threat radio jamming effects from the simulated environment, producing actual jamming effects on participant radios in the Live environment. The Cyberspace Battlefield Operating System Simulation (CyberBOSS) system [1, 2, 4] was used as an integrating architecture, providing communication between simulated jammer models in the One Semi-Automated Forces (OneSAF) system and Software Defined Radios (SDR) in the Live environment. This resulted in actual jamming effects on tactical radios instrumented with Direct Injection Jammer (DIJ) devices, providing an emulated jamming effect without any open-air jamming in the operational environment. This paper describes the work to date for this

effort and discusses the next steps to be taken to further coordinate CEMA training between Live and Synthetic training environments to support MDO.

ARCHITECTURE

This section describes the high-level architecture developed for bridging EW effects between the Simulation and Live training environments. This architecture, depicted in Figure 1, consists of components residing both within the Simulation environment (shown in blue) and components supporting communication with Live elements of the training environment (shown in green).

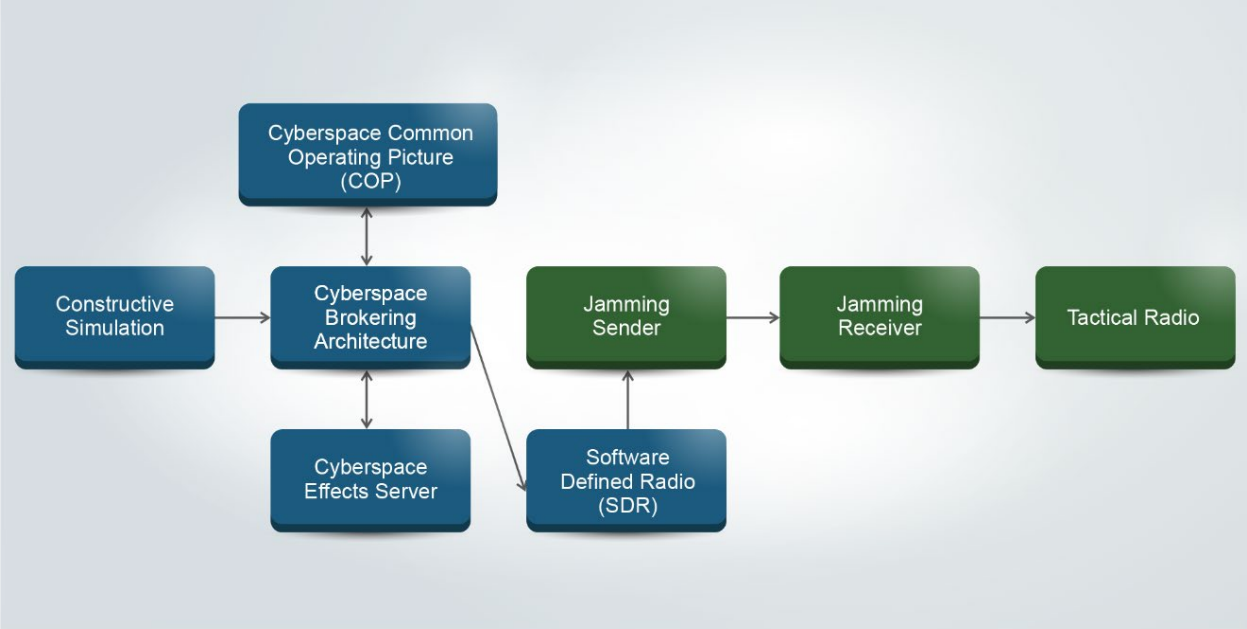

Figure 1. High-level architecture used for bridging EW effects between the Simulation and Live training environments.

A description of each of the components of this architecture is given in Table 1.

Table 1. Components within the EW effect bridging architecture.

Architecture Component	Description
Constructive Simulation	Provides models of friendly and threat actors, cyberspace devices, cyberspace operations and effects
Cyberspace Brokering Architecture	Provides data model and communication mechanism for communicating cyberspace-related information between the Simulation environment and the Live training environment
Cyberspace Effects Server	Provides modeling of jamming and other cyberspace and EW effects
Cyberspace Common Operating Picture (COP)	Provides exercise facilitator / white cell functionality to control and monitor cyberspace effects within the training environment
Software Defined Radio (SDR) Client / Jamming Sender	Receives effects from cyberspace brokering architecture and creates EW signals in Live environment for communication of effect to jamming receivers
Jamming Receivers	Devices connected to tactical radios which receive signals from jamming component sender and create emulated jamming effect on connected radios

We describe each of these components in more detail in the following sections.

 Approved for Public Release # PR2022_77084

Cyberspace Brokering Architecture

The cyberspace brokering architecture provides services and data models to promote integration of existing and emerging LVC&G systems, cyber ranges, and other cyberspace M&S tools to foster integrated training and analysis. In this work, we utilized the CyberBOSS system architecture and its core components to provide this functionality. The CyberBOSS system architecture, shown in Figure 2, is a Service Oriented Architecture (SOA) that uses well defined software interfaces and protocols to facilitate system integration and expansion to other systems. The architecture is flexible and extensible with an emphasis on adaptation to future cyberspace training and analysis needs. The goal of the CyberBOSS architecture is to support *cyber-for-others* training use cases, which represent leveraging cyber effects models and/or cyber ranges as a component in battle staff training against the impact of cyberspace operations on traditional kinetic operations, as well as training to use the cyberspace domain to enhance kinetic operations.

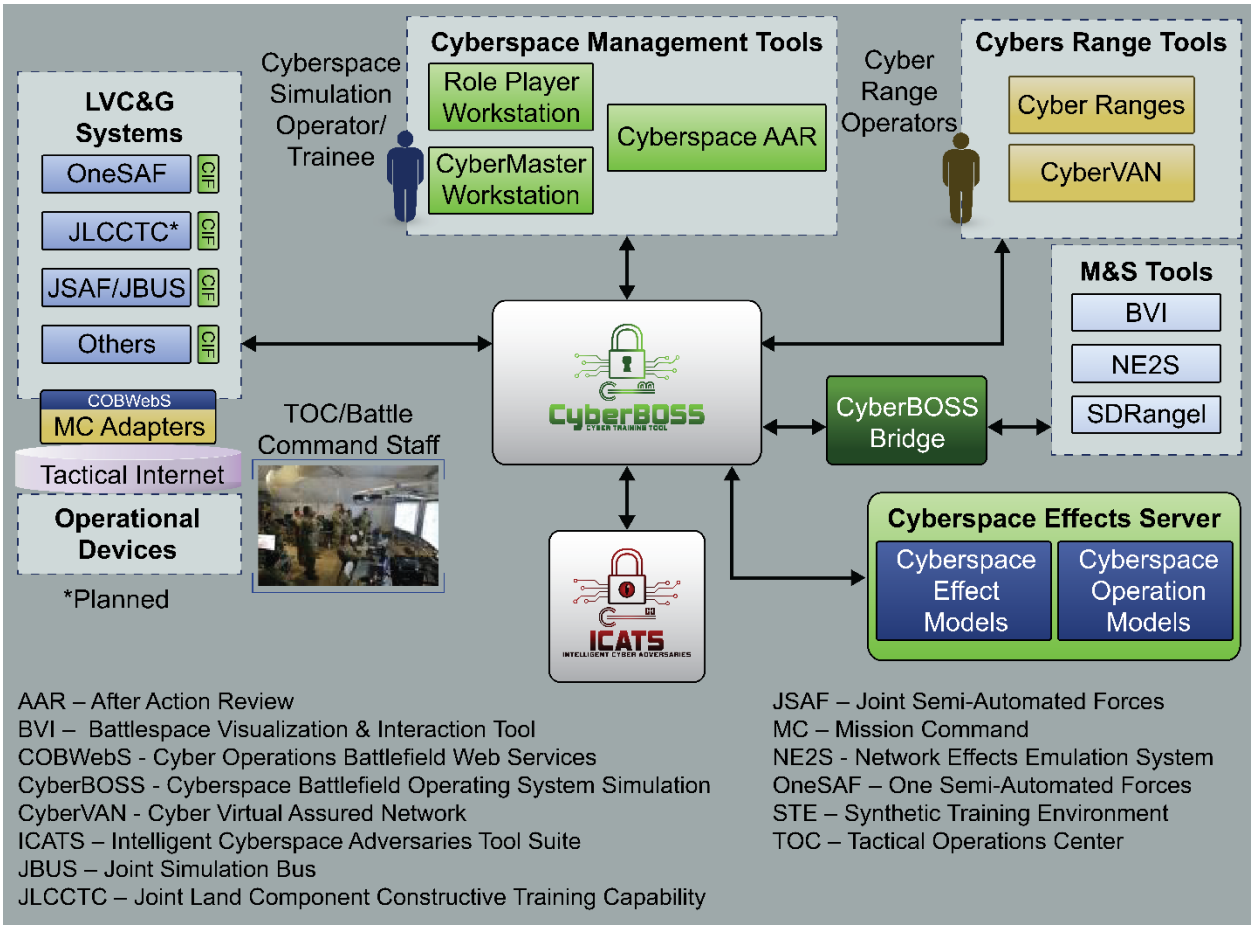

Figure 2. CyberBOSS cyberspace data model and brokering services are used to communicate EW effects between LVC&G simulations and other training systems.

The CyberBOSS system architecture employs an open and transparent hub-and-spoke approach where client applications connect into a common, federated data bus that is managed by a centralized server. [1] The group of connected client applications forms a CyberBOSS federation. All CyberBOSS client applications communicate using a common Cyberspace Data Model (CDM) representation to specify cyberspace-specific information (e.g., cyber attacks, cyber control, cyber status, etc.). [2] A wide variety of system types may interoperate through the CyberBOSS system architecture, including existing LVC&G systems (e.g., One Semi-Automated Forces (OneSAF) and Joint Land Component Constructive Training Capability (JLCCTC), Joint Semi-Automated Forces [JSAF]), cyber ranges (e.g., Cybersecurity Virtual Assured Network [CyberVAN], Cyberoperations Enhanced Network and Training Simulators [CENTS]), cyberspace effect and operation models (e.g., reconnaissance models, network models, intelligent

adversaries), and cyberspace effects tools (e.g., Cyber Operations Battlefield Web Services (COBWebS) [3] or Network Effects Emulation System (NE2S)). The CyberBOSS architecture delegates information between LVC&G systems and the cyber range to accomplish combined training of traditional warfighting functions and cyberspace domain operations using these disparate toolsets. CyberBOSS can also broker cyberspace effects across federated LVC&G systems during times when no cyber range is used. Additionally, tools such as cyber exercise facilitator / white cell controllers and After Action Review (AAR) data collection applications can integrate using the transparent nature of the system architecture. For example, the CyberBOSS CyberMaster Workstation is a thin-client display solution that allows the cyber training facilitator to view and manage cyberspace effects and operations within the training scenario. Adding external cyberspace effects models though a Cyberspace Effects Server brings enhanced modeling of cyberspace effects and cyberspace operation Tactics, Techniques, and Procedures (TTP). Automated cyberspace adversary modeling is performed using the Intelligent Cyberspace Adversaries Tool Suite (ICATS) services and tools. Finally, the CyberBOSS architecture contains the CyberBOSS Bridge application, used to communicate with external systems using a variety of protocols and standards. In our work, we extended the CyberBOSS Bridge to communicate with SDRs using Representational State Transfer (REST) Application Programming Interfaces (APIs).

Cyberspace Effects Server

Our architecture contains a cyberspace effects server which is used to model specific cyberspace actions and effects that affect simulated and Live devices within the training environment. In this work, we utilized the CyberBOSS Effects Server for this role. [4] The CyberBOSS Effects Server is a federate within the CyberBOSS federation. The Effects Server is used to model cyberspace effects that can be placed on simulated and real devices within the federation. The results of the cyberspace effects are delivered to the training audience through the interfaces of the simulation and through stimulation of tactical devices. The Effects Server utilizes an extensible architecture that allows for the incorporation of new cyberspace effects models that can be requested, instantiated, and provided as services to all CyberBOSS federates. The benefit to the approach is that the cyberspace effect modeling provided by the Effects Server can be reused across systems, minimizing the need to write additional code within each connected system. In this work, new models for areal- and point-based jamming EW effects were added to the CyberBOSS Effects Server. These models, which can be controlled by actions from the simulation or by cyber exercise facilitators / white cell operators, provide modeling of omnidirectional and directional jamming, and identify affected target systems within the training environment for application of the jamming effect.

Constructive Simulation

In the LVC&G training environment, the Constructive simulation provides modeling of *wrap-around* BLUFOR units that provide simulated actors to augment the Live BLUFOR training audience. It also provides modeling of threat actors that can perform simulated kinetic and non-kinetic attacks on both simulated and Live BLUFOR units. The simulated non-kinetic actions may result in effects in the cyberspace, EW, and Information Operations (IO) domains. In this work, we deployed One Semi-Automated Forces (OneSAF) as the Constructive simulation in our prototyping. OneSAF is a U.S. Army entity-based Constructive simulation and is extensible and composable for deployment in a wide variety of use cases. OneSAF was chosen for this work since it contains models of several threat jammer systems, originally developed by the U.S. Army Threat Systems Management Office (TSMO). These models were utilized in this work to provide stimulation of jamming effects within the Live training environment through the use of CyberBOSS. In previous work, we developed an adapter for OneSAF to communicate with the CyberBOSS federation. For this effort, we enhanced this adapter and provided mechanisms to communicate areal and point jamming effect requests from OneSAF to the Live training environment when jamming occurred in the simulation.

Software Defined Radio (SDR) Client

In the Live training environment, jamming of targeted tactical radios occurs through activation of DIJ devices that are physically connected to the radios. The DIJ system, also developed by TSMO, supports EW training by simulating jamming of radio signals used for electronic detection and communications. The DIJ jammer box is installed between the antenna and a target tactical radio. It can be programmed to digitally produce different kinds of jamming signals when cued by a simple line-of-sight signal sent remotely by an observer-controller-trainer (OC/T) or an Opposing Force (OPFOR) EW threat actor. Use of the DIJ eliminates the need for actual open-air transmissions of threat EW

jamming signals, which typically requires extensive military, Federal Communications Commission (FCC), and / or Federal Aviation Administration (FAA) approvals, if it is allowed at all.

In this architecture, we used a SDR to produce the activation signals that are received by the DIJ. A SDR system is a radio communication system which uses software for the modulation and demodulation of radio signals [5]. A SDR performs signal processing using general purpose computer hardware. This made it particularly useful for our work, since the SDR can both receive communications from the CyberBOSS infrastructure using standardized software interfaces and can create radio signals which can stimulate the DIJ jamming functionality. In this work, we used SDRangel (https://www.sdrangel.org/), an open source cross-platform SDR application for ham radio and general purpose SDR workloads. Written in C++ and designed around Qt5 and OpenGL 3.0, SDRangel supports a range of software defined radio platforms, from entry-level low-cost devices to more powerful units capable of both reception and transmission. SDRangel contains a REST API for external control.

The integration of SDRangel with the CyberBOSS federation is shown in Figure 3. In this integration, we enhanced the CyberBOSS Bridge application, which translates CyberBOSS CDM messages into various protocols and message formats communicated with external applications. Here, the CyberBOSS Bridge application receives CyberBOSS CDM messages communicating jamming effect information from the CyberBOSS federation. The CyberBOSS Bridge then creates and posts REST API calls to the SDRangel server, to communicate this jamming effect information to the SDR.

Figure 3. The CyberBOSS Bridge application is used for integration of the SDRangel with the CyberBOSS federation by translation of CDM messages to REST API calls to stimulate SDR functionality.

Jamming Components

As described above, the CyberBOSS Bridge invokes SDRangel REST API calls to activate / deactivate simulated jamming effects in the Live training environment. The communication of the simulated jamming between the SDRangel and the DIJ devices occurs through the production of RF signals. The SDRangel is connected to a HackRF One SDR that generates the appropriate RF signals in the Live training environment. Those signals are received by the DIJ, which in turns activates simulated jamming effects on the connected tactical radio. Once activated, the DIJ jams its connected radio, preventing the training audience from hearing or receiving all other radio transmissions on the same frequency, when the signals are weaker than the jamming signal injected by the DIJ.

PROTOTYPING EFFORTS

This section provides details on our prototyping efforts using the above architecture to communicate jamming effects between the Simulation and the Live training environments. During our prototyping, several aspects of our solution were refined, as described below:

Scheme for activation/deactivation of DIJ using RF signals. In our prototyping, we experimented with several schemes to initiate jamming with the DIJ through the transmission of RF signals. We attempted to reuse the existing architecture of the DIJ controller and receiver capabilities. Approaches we experimented with included broadcasting the same signal to activate/deactivate the HackRF One SDR, broadcasting separate frequencies for activation and deactivation of the HackSDR, and modulation of the SDR carrier signal via a frequency-shift keying (FSK) modulation scheme. Each approach had varying success in reliably activating or deactivating the jamming signal, mostly due to power and distance constraints between the SDR and the DIJ controller hardware. We also found that repeatedly toggling the SDR's transmitter on and off to generate or stop sending the DIJ activation signal tended to lock up the

SDR, and a full reset of the SDR was required to regain control. Ultimately, it was decided to configure SDRAngel to continuously broadcast a signal throughout the experiment's execution, but programmatically vary the frequency that the SDR transmits between the correct DIJ activation frequency and an alternate non-activation frequency, so that we could turn on and off the DIJ jamming effects without turning on and off the SDR transmitter. This scheme produced the most stable and reliable control of the DIJ from the SDR transmitter. Additionally, the SDR hardware and the DIJ Controller were physically positioned near each another, so that the limited transmutation power of the SDR would not be overcome by distance, line of sight, or buildings / material interference.

Determination of activation/deactivation RF frequencies. During our prototyping, we experimented with various signal frequencies used to activate and deactivate the DIJ controller receiver. The DIJ controller receiver is configured to listen for a broadcast signal at a specific frequency. We chose authorized frequencies that did not interfere with the expected spectrum of RF traffic in the training environment. The SDRangel was configured at a base frequency that was 1 Megahertz (MHz) greater than the DIJ activation frequency. This base frequency, referred to as the *neutral* frequency, was chosen so that it was distinct from the DIJ activation frequency, preventing unintended activation of the DIJ. When the simulated jammer was activated, the CyberBOSS Bridge invoked a REST API call to change the SDR's center frequency setting from the neutral frequency to the DIJ activation frequency. Upon receipt of a signal at this frequency, the DIJ controller applied the jamming effect to its connected SINCGARS radio. The jamming effect denied the radio's ability to receive incoming messages, but it did not affect its ability to transmit outbound messages. When the jamming effect was turned off, this invoked another REST API call to reset the SDR's center frequency back to the neutral frequency. The DIJ controller no longer received the activation signal and halted the jamming effect on the connected radio.

Coordination of simulated jamming and produced live effects. As described above, in our architecture the CyberBOSS Effects Server provided modeling of the jamming effect for the simulated jammer devices. Our prototyping investigated how the outputs of this modeling were coordinated with the request to apply the jamming effect on the Live radios in the training environment. We developed some simple areal jamming models which were used to identify the individual Live radios that were jammed as a result of the simulated jammer engagement. In our prototyping, we focused on the jamming area radius to determine which devices should be jammed. However, future work may enhance these models to include consideration of other modeling parameters, such as jamming frequency, radio type, and terrain effects.

EXPERIMENTAL RESULTS

To demonstrate its usefulness to provide coordinated EW training between Constructive simulations and the Live environment, we expanded upon our prototype and utilized it during the 2022 Army Expeditionary Warrior Experiment (AEWE) held at Fort Benning, Georgia. The annual AEWE event assesses Cross Domain Maneuver (CDM) concepts and capabilities at the lower tactical echelon in support of Multi Domain Operations (MDO). During the AEWE, we demonstrated that EW effects were successfully communicated across the distributed training environment, producing simulated jamming effects on Live tactical radios in the range.

The laydown of the simulation systems and Live systems used for our experimentation during AEWE is shown in Figure 4. The simulation systems were deployed at the Olive Hall simulation center at Ft. Benning. Within Olive Hall, a OneSAF simulation cluster was deployed. This cluster utilized a OneSAF v9.0 baseline with additional functionality maintained by the U.S. Army Combat Capabilities Development Command (DEVCOM) Data & Analysis Center (DAC). Within Olive Hall, a CyberBOSS federation was also deployed, consisting of one instance of the following components: CyberBOSS Server, CyberBOSS Control Tool, CyberBOSS Effects Server, and CyberBOSS Bridge.

The OneSAF simulation was provided with an adapter with which it communicated cyberspace and EW objects and events with the CyberBOSS federation.

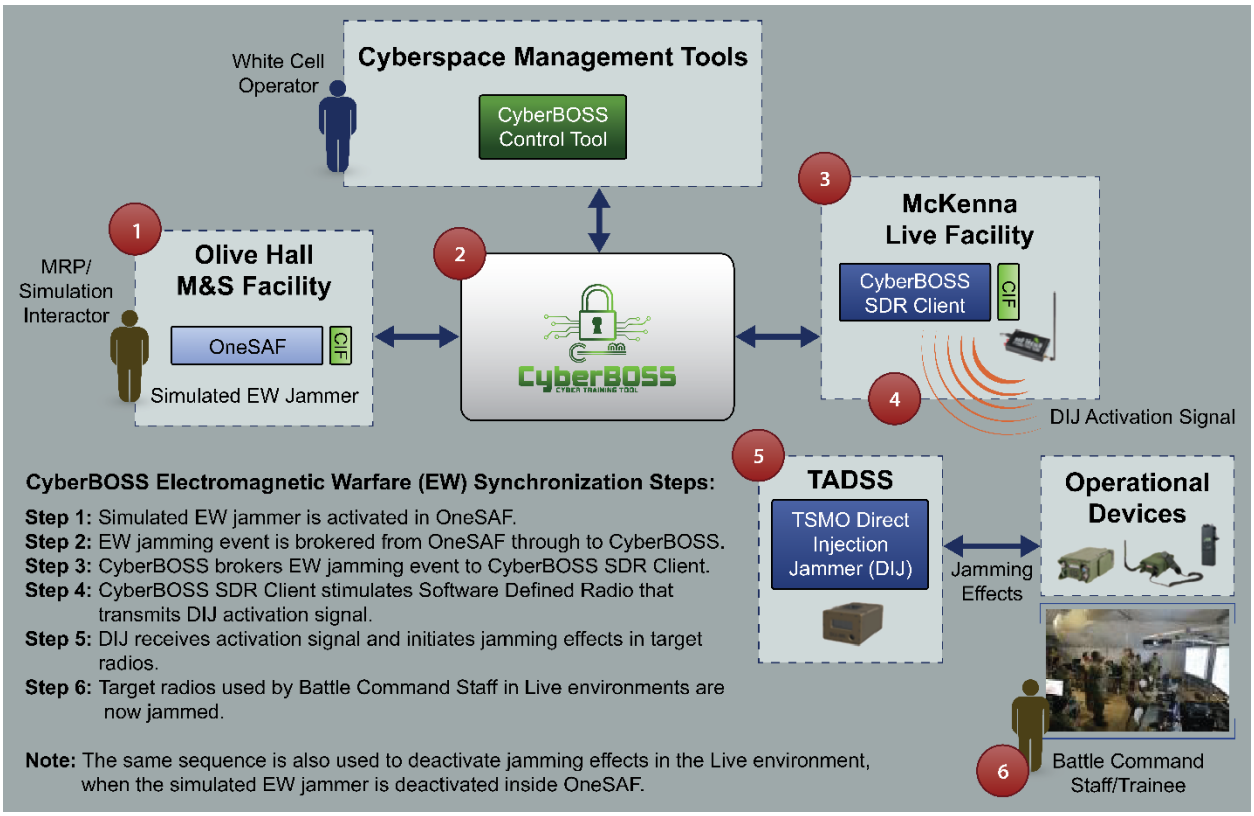

Figure 4. Laydown of simulation and live training systems used for experimentation of EW effects communication during the 2022 AEWE.

Upon activation of a simulated EW jammer in OneSAF, the jamming effect is modeled by the CyberBOSS Effects Server and the resulting jamming event is communicated from the simulation infrastructure to a CyberBOSS client application located at the McKenna Military Operations in Urban Terrain (MOUT) site. That site is in the vicinity of the Live training audience and RF signals from the McKenna site can reach the Training Aids, Devices, Simulations, and Simulators (TADSS) (i.e., DIJ controllers) attached to the tactical devices in the Live training environment. Communication between the CyberBOSS infrastructure at Olive Hall and the CyberBOSS client at the McKenna site performed using existing range instrumentation networks.

Throughout the course of the AEWE event, the coordination of jamming events within the Simulation environment with jamming of tactical radios in the Live environment was demonstrated multiple times. Successful experimental results were achieved each time, with activation of simulated jammers in OneSAF resulting in jamming of inbound radio communications of Live tactical devices. This experiment also demonstrated the ability to perform this jamming in the Live environment without emitting jamming signals. Because this solution does not interfere with existing military and commercial RF signals in the environment, it significantly facilitates the deployment of this technology within Live training ranges.

FUTURE WORK

This work represents a significant first step to provide automated coordination of EW effects between the Simulation and Live training environments. We demonstrated that this approach can be used for reliable coordination of jamming events within the Simulation environment with jamming of tactical radios in the Live environment. This approach does not require emitting jamming signals in the Live environment, facilitates the deployment of this technology within Live training ranges. Future work to build upon this capability includes the following:

- **Additional EW effects.** This work focused on jamming of tactical radio communications. However, other EW effects could be incorporated in future work. For example, in addition to jamming, deception effects could be introduced, producing confusing or contradictory signals for the training audience.
- **More sophisticated jamming effects**. This work used fairly rudimentary jamming models which did not take into consideration the effects of factors such as terrain or signal strength. In future work, more complex jamming effects could be introduced. For example, terrain and other geo-spatial elements can greatly affect jamming capabilities and these factors can be incorporated into the jamming models used by the Effects Server for improved realism. Additionally, jammers may use sophisticated patterns, pulsed jamming, and directionality and these factors may also be incorporated into the models used in this work. This may also require further development of the DIJ functionality to stimulate attached radios to incorporate these additional jamming factors.
- **More complex scenarios.** This initial work focused on an initial path to communicate jamming from the Simulation to the Live training environment. However, future work may incorporate not only *Simulated-to-Live* interaction, but also *Live-to-Simulated* interaction. For example, consider a scenario in which the BLUFOR triangulates the positioning of an OPFOR jammer in Live environment, then issues a Call-For-Fire back to the simulation in order to destroy the jammer in the simulation. Once destroyed, the Live jamming capability is disabled and BLUFOR RF communications are restored in the Live environment.
- **Stimulation of BLUFOR EW tools.** Future efforts could focus on stimulating the tools that the BLUFOR EW specialists use in the Live training environment to identify, locate, and ultimately target the source of the threat EW signals.
- **Simulation of BLUFOR EW operations**. In this work, we focused on simulated OPFOR EW operations producing jamming effects on Live BLUFOR units. However, this work could be extended to allow training of BLUFOR EW operations. For example, BLUFOR EW teams may use this architecture to train offensive operations that impact OPFOR RF communications.

RECOMMENDATIONS

Based on the work described here and the future work cited, we make some recommendations on how this capability can be utilized in Army training. As the Army considers deployment of this functionality for EW training, it should consider multiple different perspectives: the user, the performance, and the technology. For the user, when training with EW systems, prior knowledge and skillsets should be identified and relevant information with the appropriate level of detail should be conveyed. As an example, an EW officer will require a higher level of technical specification, while a commander will be focused on understanding how those EW capabilities can impact the ability to complete a mission. Frost, McClung, and Walls [6] describe key considerations that a commander needs to understand when working in the EMS, such as maintaining situational awareness of their unit's footprint in the EMS and what assets are available to them. This is different than being able to understand the when, where, and how of employing Electromagnetic Attack (EA), Electromagnetic Protection (EP), and Electromagnetic Support (ES). This drives curriculum development and training exercises so that when Modeling and Simulation is used to simulate EW, TTPs are put in place, such that the training value and return on investment to the to the trainees can be improved.

Assessment of performance is key to any military operation and is typically performed through a Battle Damage Assessment (BDA). To assess BDA due to EW effects and simulation, there needs to be Measures of Performance (MOP) and Measures of Effectiveness (MOE) which can determine the before and after state of an EW effect on a training audience. Researchers have already begun adapting the existing BDA models to incorporate EW effects. [7] One of the key takeaways from this research is that EW assets are of different types and cause varying effects on the battlefield. Assessment models need to accommodate for multiple asset types working simultaneously on the battlefield when providing information back to military commanders.

Finally, our adversaries are consistently developing new technological capabilities and the U.S. needs to keep pace in the EMS. One such example is Low Probability Interception and Detection (LPI / LPD) communication systems which, by minimizing their emission level and through making the signal less consistent, can stay hidden from detection. [8] Our research team is currently working with researchers from the Army Cyber Institute at West Point to investigate how we can effectively incorporate these emerging threat EMS capabilities in our training environments, using M&S systems such as CyberBOSS.

CONCLUSION

As described throughout this paper, incorporation of CEMA events and effects into M&S-driven environments is vital for Army training of modern battlespace operations. EMS and IE operations are an increasingly important part of the contested and competitive operational environments. Incorporating EMS elements in training environments is difficult due to regulations on spectrum interference with civilian infrastructure and the lack of integration with existing Constructive and Virtual simulation systems. Additionally, current training environments also do not automatically coordinate EW activities in the simulation with resulting effects in the Live training environment. This work has provided an architecture for integration of EW effects between simulation systems and radios within the Live training environment, allowing of automated coordination of those effects across the training exercise. We demonstrated this capability at the AEWE, where activation of simulated jammers in OneSAF resulted in successful jamming of inbound radio communications of Live tactical devices. This experiment demonstrated the ability to perform this jamming in the Live environment without emitting jamming signals. Because this solution does not interfere with existing military and commercial RF signals in the environment it significantly facilitates the deployment of this technology within Live training ranges. This initial work provides a basis for training using more sophisticated EW effects coordinated across the Simulation and Live environments though the architecture developed here.

REFERENCES

[1] Welch, J., Hasan, O., Burch, B., Vey, N., & Geddes, J.A. (2020). CyberBOSS: An Approach for Control and Interoperation of Cyber for Training. *Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop (SIW).*
[2] Hasan, O., Welch, J., Burch, B., Vey, N., Geddes, J.A., & Hofstra, K. (2020). CyberBOSS Common Data Model. *Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop (SIW).*
[3] Mize, J., Marshall, H., Hooper, M., Wells, R., & Truong, J. (2015). Cyber Operations Battlefield Web Services (COBWebS) – Concept for a Tactical Cyber Warfare Effect Training Prototype. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*
[4] Hasan, O., Welch, J., Burch, B., Geddes, J.A., & Vey, N. (2021). A Cyberspace Effects Server for LVC&G Training Systems. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*
[5] Akeela, R., & Dezfouli, B. (2018). Software-defined Radios: Architecture, state-of-the-art, and challenges. Computer Communications, 128, 106-125.
[6] Frost, P., McClung, C., Walls, C., & Huynh, D. (2018). Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum. *The Cyber Defense Review*, *3*(1), 15–26. http://www.jstor.org/stable/26427371
[7] Choi, S., Kwon, O. J., Oh, H., & Shin, D. (2020). Method for effectiveness assessment of electronic warfare systems in cyberspace. *Symmetry*, 12(12), 2107.
[8] Ricciardi, S., & Souque, C. (2021). Modern Electromagnetic Spectrum Battlefield. *PRISM*, *9*(3), 122-139.