Development of a Novel Architecture for Improving Cyber-Kinetic Training

Omar Hasan, Ph.D., Derek Crane, Jeffrey Welch

Dignitas Technologies
Orlando, Florida
ohasan@dignitastech.com, dscrane@dignitastech.com, jwelch@dignitastech.com

J. Allen Geddes, Jason Strauss

US Army DEVCOM SC STTC
Orlando, Florida
james.a.geddes2.civ@army.mil, jason.p.strauss.civ@army.mil

Jeff Truong, Mark Evans

MITRE Corporation
Orlando, Florida
jtruong@mitre.org, mwevans@mitre.org

W. Cory Bogler

US Army PEO STRI PM CT2 PdM CRT
Orlando, Florida
william.c.bogler.civ@army.mil

ABSTRACT

In the modern battlespace, the traditional fight within the warfighting domains of air, land, sea, and space has expanded to the cyberspace domain. Within the cyberspace domain, adversaries actively pursue Internet Protocol (IP)-based cyber attacks to affect operational missions in all domains. Cyber Mission Force (CMF) teams direct, synchronize, and coordinate cyberspace operations in defense of U.S. national interests. Within the CMF, Cyber Protection Teams (CPT) defend critical infrastructure and key resources from threat actions, while Cyber Combat Mission Teams (CCMT) conduct military cyber operations in support of combatant commands. To maximize their effectiveness for multidomain operations, these cyber teams require collective cyber-kinetic training to ensure they work effectively with commanders across the Services and Joint Force to accomplish their assigned missions and achieve information advantage in the battlespace.

Cyber-kinetic training is currently hindered because existing Live, Virtual, and Constructive (LVC) systems used for command staff training are not developed to communicate directly with cyber ranges used for cyber team training. Coordination of cyber effects between these training environments is performed manually. This paper describes a novel system architecture developed to automate the communication of cyber effects between a cyber range and LVC systems. The system utilizes cyber range sensors for cyber Battle Damage Assessment (BDA) due to operator actions within the range that cause changes to network and system states. This cyber BDA is communicated to the LVC training environment using the Cyberspace Battlefield Operating System Simulation (CyberBOSS) architecture so that generated cyberspace effects have an operational impact on simulation models and connected Command, Control, Communications, Computers, and Intelligence (C4I) interfaces. The feasibility of this approach is demonstrated though a prototype that coordinates several cyberspace effects between the cyber range and LVC environment. This approach represents a significant improvement for cyber-kinetic training, increasing warfighter readiness for conducting multidomain operations.

ABOUT THE AUTHORS

Dr. Omar Hasan is the Chief Software Architect at Dignitas Technologies, where he serves as the principal investigator on cyberspace-related research efforts. Dr. Hasan has 24 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 has also supported 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.

Derek Crane is the technical lead for this research. He has 15 years of experience with system/software development for military modeling, simulation, and training systems. He has significant experience with Development Operations (DevOps) principles, including containerization using Docker and Podman, automation using Ansible, and is experienced with Linux variants. Mr. Crane has leveraged containerization to run infrastructure monitoring tools, host web services, and to create build environments for large Army Programs of Record (PoR), including the Aviation Combined Arms Tactical Trainer (AVCATT). Mr. Crane holds a B.S. in Computer Science with a minor in Mathematics from the University of Central Florida.

Jeffrey Welch has 23 years of software development experience within the modeling and simulation industry. He is the current software development lead for the CyberBOSS 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.

Jeff Truong is a Lead Modeling & Simulation Engineer with the MITRE Corporation. He has over 30 years of Systems/Software Engineering and Technical Management experience in telecommunication/networking systems, network management systems, and Modeling and Simulation (M&S) training systems. Mr. Truong has worked as Systems Engineer and Technical Lead in various DoD Programs including Future Combat Systems (FCS), Modeling Architecture for Technology, Research, & EXperimentation (MATREX), Cyber Operations Battlefield Web Service (COBWebS), Joint Land Component Constructive Training Capability (JLCCTC), and Synthetic Environment Core (SECORE), and Synthetic Training Environment (STE). Since 2023, Mr. Truong serves as the LVC Systems Engineer and the Product Owner for Infrastructure and Continuous Integration and Continuous Delivery (CI/CD) for the Persistent Cyber Training Environment (PCTE) Program. He holds a B.S. in Computer Science from the University of Central Florida.

Mark W. Evans is a Lead Simulation and Training Engineer at the MITRE Corporation and currently serves as MITRE's Associate Project lead for the Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) and the Task lead for the Persistent Cyber Training Environment (PCTE). In support of PCTE, Mr. Evans has aided in integration with US Cyber Command's (CYBERCOM's) Joint Cyber Warfighting Architecture (JCWA), early development of operations and exercise support procedures, and capability shaping. Since joining MITRE in 2015, Mr. Evans has contributed to various simulation and training programs including the Squad Overmatch Study and the Joint Nonlethal Weapons Directorate. He holds a B.S. in Physics from Principia College and a M.S. in Modeling and Simulation 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) 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 18 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 and is currently pursuing an M.S. in Systems Engineering and Program Management from the Naval Postgraduate School.

Jason Strauss is an Information Technology Specialist at the U.S Army Combat Capabilities Development Command Soldier Center (DEVCOM SC) Simulation and Training Technology Center (STTC). Mr. Strauss, in his current role, provides research and technical assistance to DEVCOM SC's Cyberspace Warfare for Training (CyWar-T) S&T research efforts. He has 16 years of Systems, Network, and Security Engineering experience and currently holds a Certified Information Systems Security Professional (CISSP) certification from ISC2. Mr. Strauss has earned a B.S in Information Technology-Security from Western Governors University.

W. Cory Bogler works at US Army PEO STRI as the Senior Test & Integration Officer for the Persistent Cyber Training Environment (PCTE). His teams are responsible for monitoring & maintaining PCTE production platforms

as well as conducting Developmental, Operational, and Cybersecurity testing. Prior to working for PCTE, Mr. Bogler served as a software developer on the Paladin self-propelled howitzer and as a product manager for Multiple Integrated Laser Engagement System (MILES), the Army's live training system product line. Much of his career has focused on enabling technical or doctrinal interoperability between disparate military systems and organizations; this experience has served him well in pulling together PCTE Operations & Test staff to execute a coordinated Ops/Test mission supporting for the Cyber Mission Force's training objectives.

Development of a Novel Architecture for Improving Cyber-Kinetic Training

Omar Hasan, Ph.D., Derek Crane, Jeffrey Welch
Dignitas Technologies
Orlando, Florida
ohasan@dignitastech.com, dscrane@dignitastech.com, jwelch@dignitastech.com

J. Allen Geddes, Jason Strauss
US Army DEVCOM SC STTC
Orlando, Florida
james.a.geddes2.civ@army.mil, jason.p.strauss.civ@army.mil

Jeff Truong, Mark Evans
MITRE Corporation
Orlando, Florida
jtruong@mitre.org, mwevans@mitre.org

W. Cory Bogler
US Army PEO STRI PM CT2 PdM CRT
Orlando, Florida
william.c.bogler.civ@army.mil

INTRODUCTION

In the modern battlespace, the traditional fight within the warfighting domains of air, land, sea, and space has expanded to the cyberspace domain. Within the cyberspace domain, adversaries actively pursue Internet Protocol (IP)-based cyber attacks to affect operational missions in all domains. Cyber Mission Force (CMF) teams direct, synchronize, and coordinate cyberspace operations in defense of U.S. national interests. Within the CMF, Cyber Protection Teams (CPT) defend critical infrastructure and key resources from threat actions, while Cyber Combat Mission Teams (CCMT) conduct military cyber operations in support of combatant commands. To maximize their effectiveness for multidomain operations, these cyber teams require collective cyber-kinetic training (combined cyber training with kinetic-focused training) to ensure they work effectively with commanders across the Services and Joint Force to accomplish their assigned missions and achieve information advantage in the battlespace.

Cyber-kinetic training is currently hindered because existing Live, Virtual, and Constructive (LVC) systems used for command staff training are not developed to communicate directly with cyber ranges used for cyber team training. Coordination of cyber effects between these training environments is performed manually (i.e., white cards, swivel chair). This manual coordination is cumbersome, error-prone, and limits the realism for the training audience. To better prepare for the multidomain operations required in the current battlespace, systems need to be developed to automatically communicate cyberspace information across the training environment, so a unified operational picture is provided to all trainees (cyber and non-cyber).

APPROACH

This work provides an approach to develop an architecture supporting *cyber-kinetic* training, in which actions within a cyber range result in the communication of cyberspace effects within a connected simulation environment. This allows command staff to train against threat cyberspace activities affecting their operational systems. In this use case, cyber range operators acting as a CPT or CCMT, attack or defend emulated systems that represent operational systems within the training scenario. Those systems are also represented as simulated or real devices within the simulation environment. Cyber battle damage is assessed from the results of activities within the cyber range and that damage is injected into the simulation environment as a cyberspace effect on the simulated or real devices within the simulation environment. This use case represents *multidomain* cyberspace training, where the cyber range environment is used to train CPT or CCMT operators and the simulation environment is used to train military command staff and systems operators. This approach represents a significant improvement over the current methods used for cyber-kinetic training, which are error prone and limit training realism due to manual coordination between the two training environments.

To support cyber-kinetic training, a novel system architecture was developed to automate the communication of cyber effects between a cyber range and a simulation environment comprised of LVC systems and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces. The system utilizes cyber range sensors for cyber Battle Damage Assessment (BDA) due to operator actions within the range that cause changes to network and system states. This cyber BDA is communicated to the simulation environment using a cyberspace brokering architecture, so that generated cyberspace effects have an impact on connected LVC simulations and C4I interfaces. The feasibility of this approach was demonstrated though a prototype that coordinates cyberspace effects between the cyber range and simulation environment. This approach can significantly improve cyber-kinetic training, increasing warfighter readiness for conducting multidomain operations.

ARCHITECTURE

This section describes the high-level architecture developed to communicate cyberspace effects between a cyber range and the simulation environment. This architecture, depicted in Figure 1, consists of a cyber range, used for cyber offensive and defensive team training, and constructive simulations and C4I systems, used for command staff training. Cyberspace domain-related information between the two simulation systems is communicated using a cyberspace brokering architecture, which provides cyberspace effect models as well as user interfaces utilized by exercise facilitators. A network guard is optionally used to restrict the data flow between the cyber range and the simulation environment.

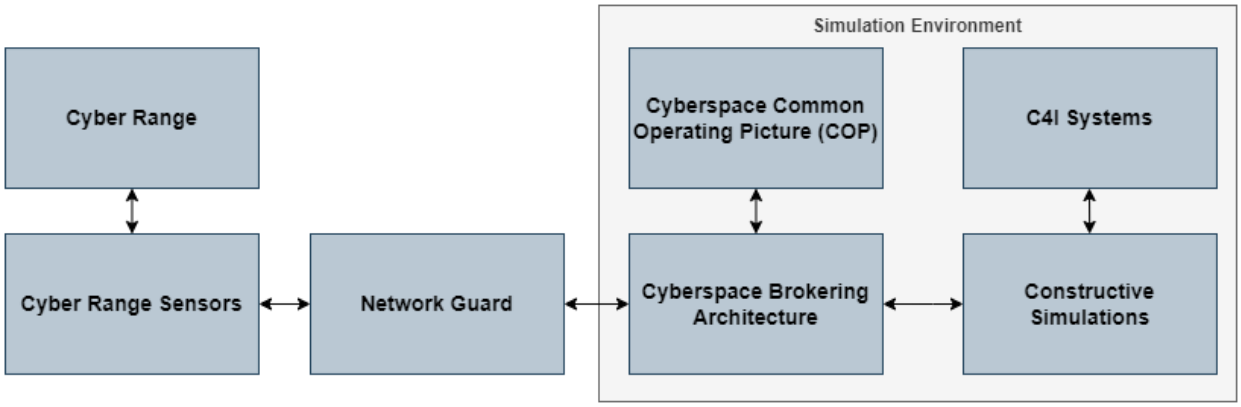

Figure 1. High-level architecture used to communicate cyberspace effect information between a cyber range and the simulation environment.

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

Table 1. Components within the combined cyber range and simulation environment architecture.

Architecture Component	Description
Cyber Range	Provides a virtual environment that contains emulated systems and networks, as well as training content used for training Cyber Protection Teams and Cyber Combat Mission Teams
Cyber Range Sensors	Provides software applications that assess changes within cyber range systems, assess corresponding cyber battle damage, and communicate resulting cyberspace effects to simulation environment
Network Guard	Optional component which limits communication between the cyber range and simulation environment based on preconfigured rulesets
Cyberspace Brokering Architecture	Provides data model and communication mechanism for communicating cyberspace-related information between connected systems
Cyberspace Common Operating Picture (COP)	Provides exercise facilitator / white cell functionality to control and monitor cyberspace effects within the training environment

Constructive Simulations	Provides models of friendly and threat actors, cyberspace devices, cyberspace operations and effects
C4I Systems	Tactical interfaces utilized by the command staff during training

Each of these components is described in more detail in the following sections.

Cyber Range

Cyber ranges are comprised of interactive, emulated platforms and representations of networks, systems, tools, and applications. They emulate an organization's network, systems, and services in a safe and controlled virtual environment for cybersecurity training. Utilized within Department of Defense (DoD) service branches, CPTs and CCMTs utilize cyber ranges for training on complex Tactics, Techniques, and Procedures (TTPs) required for offensive and defensive military cyberspace operations to support mission objectives. For example, a cyber range may be used by trainees role playing as a threat cyber red team to perform cyberspace operations against emulated Blue Force (BLUFOR) systems or military or civilian Industry Control Systems (ICS). These emulated systems, implemented as Virtual Machines (VM) or software containers within the cyber range, can represent a variety of real-world systems pertinent to military missions, including tactical systems in a command post or on a Navy ship, Network Operation Center (NOC) workstations, or power facility control systems. Trainees within the cyber range perform offensive or defensive cyberspace operations on the emulated devices and software-defined networking within the range to simulate those actions on corresponding real-world systems. Cyber ranges used for DoD training include dedicated infrastructure such as the National Cyber Range Complex (NCRC) and the Persistent Cyber Training Environment (PCTE), as well as testing and experimentation environments comprised of digital twins, such as the Army Research Lab's (ARL) Cyber Virtual Assured Network (CyberVAN).

Cyber Range Sensors

Currently, there are no automated mechanisms used within cyber-kinetic training exercises to analyze actions occurring within the cyber range and to programmatically impart related cyberspace effects on the simulation and C4I systems used by the battle staff being trained. During our investigation, we analyzed technologies that can act as cyber range sensors, automatically mining the cyber range for information about ongoing operator activities against range systems that emulate C4I systems, operator workstations, and other systems relevant to the military scenario. The sensors perform cyber BDA on those emulated systems and derive appropriate cyberspace effects based on range operator activities. The sensors automatically communicate the cyberspace effect information between the cyber range and the constructive simulation system, reducing manpower requirements (i.e., white carding, swivel chair synchronization) and providing more realistic cyberspace effects to the trainees.

To assess cyber BDA and communicate the resultant cyber effect, the cyber range sensors utilize a four-step process:

1. Cyber range operators, role playing as threat cyber actors or executing BLUFOR offensive cyber operations, perform actions (attacks) against systems in the cyber range that represent C4I systems, operator workstations, and other systems relevant to the scenario.
2. These actions change the state of the emulated systems (e.g., increased network usage, central processing unit (CPU) spikes, service disruptions) and/or leave *breadcrumbs* within the filesystem on the emulated systems (e.g., system logs, added malware).
3. Cyber sensors within the range detect these state changes and filesystem changes and perform cyber BDA by determining the appropriate cyberspace effect, if any, that results from these changes.
4. The resultant cyberspace effect is communicated to the simulation systems and C4I systems for implementation of the appropriate cyberspace effect.

Our work considered various means by which the cyber range sensors can determine cyber BDA due to changes in the range systems. The cyber range sensors can query and monitor the range systems directly, or they can utilize existing Open Source Software (OSS) and/or Commercial-Off-The-Shelf (COTS) tools such as Network Security Monitoring (NSM) systems, Intrusion Detection Systems (IDS), and Security Information and Event Management (SIEM) systems. For example, these systems can perform Network Behavior Anomaly Detection (NBAD) by examining individual network packet signatures for anomalies to help detect attacks such as spoofing. Even using

these systems, detecting BDA due to a cyber attack is challenging. For example, since the number of attack vectors per cyber attack type varies, several implementations of detection may be required for a cyber attack type. For instance, consider a Synchronized (SYN) flood based Denial of Service (DoS) attack. For this attack type, the Linux socket statistics (ss) command can be used to query the number of connections in the SYN_RECV state as a form of network traffic analysis. A high number of connections in the SYN_RECV state from the same IP address could indicate that a DoS attack is occurring. However, this only indicates one particular DoS attack vector. Detection of cyberspace attacks using range sensors must be done carefully, since detection methods are highly dependent on specific attack vectors and circumstances.

Once a cyber attack has been detected, cyber BDA is performed to generate an appropriate cyberspace effect which is communicated to the simulation and C4I systems. Mappings were developed between cyberspace attack operations within the cyber range and the cyberspace effect that is generated upon cyber BDA. Our analysis found that there is a one-to-many relationship between a generated cyberspace effect and cyberspace attack types. That is, multiple types of cyberspace attacks may result in the generation of the same cyberspace effect. For some example cyberspace effects, Table 2 shows possible cyber attacks that can be detected. For the bolded cyber attack, example attack vectors within the cyber range that would cause the effect are listed, providing input to the symptoms the cyber range sensors should monitor for that effect. There are many more combinations of possible ways to generate these and other cyberspace effects, however, and other attack vectors could be explored in future work.

Table 2. Cyberspace effects generated upon BDA of cyberspace attacks within the cyber range.

Generated Cyberspace Effect	Detected Attack Types	Example Specific Attack Vector	Affected State	User Observed Symptoms
Data Exfiltration Effect	Payload Attack	Backdoor	• Filesystem ○ Logs • Network traffic • Running processes	• None
Denial of Service Effect	Denial of Service Attack	TCP SYN Flood	• Filesystem ○ Logs • System performance • Network traffic • Service connectivity • Network connectivity • System uptime	• Degraded system performance • Blocked network communication to the machine or its services • System rendered inoperable
Packet Manipulation Effect	Active Eavesdropping Attack	IP Spoofing	• Network interface mode • Network traffic • Service connectivity • Running processes	• Degraded, disrupted, or modified network communications

Network Guard

An optional component in this architecture is a network guard. Network guards allow simulation systems operating within different enclaves or at different security levels to interoperate within a common, synthetic environment. Often, network guards function as Cross-Domain Solutions (CDS), acting as a Multi-Level Security (MLS) appliance that supports distributed simulation training systems interoperating at different security levels; for example, within a Distributed Interactive Simulation (DIS) or High Level Architecture (HLA) environment. Network guards contain hardware and software that provide security mechanisms to address the transfer of data between systems executing at different security levels. In addition to its ability to support MLS, in this architecture a network guard can also provide

tight control of the information communicated between the cyber range and the simulation environment. Even when operating at the same classification level, rulesets and schemas within the network guard can be used to ensure that only approved data flows between the cyber range and the simulation environment.

Cyberspace Brokering Architecture

The cyberspace brokering architecture provides services and data models to promote integration of existing and emerging LVC systems, cyber ranges, and other cyberspace M&S tools to foster integrated training and analysis. In this work, the Cyberspace Battlefield Operating System Simulation (CyberBOSS) system architecture was used to provide this functionality. [1] Through on-going research efforts under the US Army Combat Capabilities Development Command – Soldier Center (DEVCOM SC) Simulation and Training Technology Center (STTC), we continue to develop CyberBOSS to provide a Cyberspace Data Model (CDM), software interfaces, cyberspace operations and effects models, and user interfaces to communicate cyberspace elements and effects between simulation systems and other cyberspace toolsets [2]. The CyberBOSS system architecture is a microservices based system in a Service Oriented Architecture (SOA) that uses well-defined software interfaces and protocols to facilitate system integration and expansion to other systems. [3] [4] This 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. Services maintain the model of the state of the cyberspace terrain across the training environment to provide a common and consolidated view for all connected client applications. Client applications communicate using CDM representations to specify cyberspace-specific information (e.g., cyber attacks, cyber effects, cyber status). [5] The CDM builds upon previous cyberspace data models such as Cyber Operational Architecture Training System (COATS) [6] is compliant with emerging cyberspace data standards, such as the recently released Simulation Interoperability Standards Organization (SISO) Cyber Data Exchange Model (CyberDEM) (SISO-STD-025-2023). A wide variety of system types may interoperate through the CyberBOSS system architecture, including LVC systems, cyber ranges, cyberspace operations and effects models, and cyberspace effects tools. For the purposes of this work, this architecture was utilized to broker cyber effects from the cyber range to Constructive simulation and C4I systems.

Cyberspace COP

The cyberspace COP provides user interfaces and other tools that exercise facilitators and white cell controllers use to inject and monitor cyberspace and Electromagnetic Warfare (EW) effects within the training environment. The cyberspace COP can provide a visualization of cyberspace domain objects and effects using map and table views. In this architecture, the cyberspace COP provides two main areas of functionality: 1. visualizing the state of simulated and emulated devices across the training environment (i.e., cyber range VMs, constructive device models), and 2. monitoring of cyberspace effects resulting from actions within the cyber range.

Constructive Simulations

Within the simulation environment, the Constructive simulations provide modeling of BLUFOR, threat, and civilian actors and organizations. These simulations provide modeling of kinetic activities (i.e., moving, sensing, shooting) of these forces during simulated military operations. Our work focused on interfacing with Constructive simulations, however a similar approach could be taken for Virtual or Live training systems. Within this architecture, interfaces were developed between the Constructive simulations and the cyberspace brokering architecture to communicate cyberspace and EW effects. Depending on the effect type, each effect is applied in specific ways to models within the Constructive simulation to affect the modeling of kinetic activities within the simulation. For example, for effects disrupting or altering simulated Global Positioning System (GPS) signals used by constructive actors, simulated GPS signal data was removed or modified within constructive mobility or firing models, changing the output of those models within the simulation and causing differences in the simulated movement or firing capability of the simulated actors.

C4I Systems

Within the simulation environment, C4I systems are stimulated with simulated data from the Constructive simulations. This simulated data is communicated using a variety of military protocols, depending on the targeted C4I system. During training, C4I system operators, including military command staff, view the kinetic operations modeled within the simulation using C4I system interfaces. In this architecture, cyberspace and EW effects received by the

Constructive simulation from the cyberspace brokering architecture can be applied to tactical messages communicated to the C4I systems to have an operational impact on those systems. [7] For example, a jamming effect can cause information to disappear from the C4I system interface, while a data injection effect can cause erroneous information to be displayed on the C4I system interface. These effects are typically manifested by adding or removing tactical messages sent between the constructive simulation and the C4I systems, or by altering specific fields in those tactical messages to change the information received by the C4I systems.

PROTOTYPING EFFORTS

This section provides details on our prototyping efforts using the above architecture to demonstrate the communication of cyberspace effect information between a cyber range and the simulation environment. Our prototyping activities focused on the design and development of the cyber range sensors and associated applications used to assess changes to cyber range systems, determine resulting cyber BDA, and communicate that BDA to the connected cyberspace brokering architecture.

Cyber Range

The cyber range infrastructure used in our prototyping was the PCTE. PCTE is the United States Cyber Command (USCYBERCOM) Virtual Combat Training Center for the Joint CMF. It serves as a training platform for standardized Joint Cyberspace Operations Forces individual sustainment training, team certification, mission rehearsal, and collective training exercises. A cyber range was built within an unclassified PCTE Regional Compute and Storage (RCS) data center comprised of a set of VMs and Software-Defined Networking (SDN). This cyber range is a simplified representative power plant control system modeled after a larger range used by previous cyber events (e.g., Cyber Flag).

Cyber Range Sensors Design

For our prototyping efforts, we developed a design for the cyber range sensors used within our architecture. This design builds upon our initial cyber range sensor design and prototyping performed under the Office of Naval Research (ONR). As described above, sensors connected to the cyber range monitor the state of the systems in the range and the activity of operators as inputs for determining cyber BDA. Figure 2 depicts our overall design of the cyber range sensors. In this design, a cyber range operator role plays the actions of a cyber red team, performing actions and cyber attacks on emulated systems within the cyber range. A sensor host machine runs within or is connected to the cyber range environment and contains various components that collect information, perform BDA, and transmit cyberspace effect data to CyberBOSS based on the assessed battle damage. Within our design, two types of applications run within the sensor host machine:

1. **Cyber Range Sensor application(s).** One or more cyber range sensor applications run within the sensor host machine to monitor the state of VMs within the cyber range. These various monitoring applications sense changes in the state of the emulated systems due to range operator actions, assessing for system damage. In Figure 2, the OSS LibreNMS is shown as a representative monitoring tool (sensor). However, our architecture uses open Application Programming Interfaces (API) to support various sensor back-end implementations to work in tandem. These back-ends act as a plugin architecture, allowing various configurations of monitoring services to run depending on the desired functionality. This also provides loose coupling between the specific sensor technology back-ends (e.g., LibreNMS) and the other components of our architecture, promoting flexibility and scalability.
2. **Cyber Effect Generator application.** If the sensors detect a significant change in an emulated system, an alert is sent to the cyber effect generator component. The cyber effect generator collects information from the sensors, performs cyber BDA, and transmits corresponding cyberspace effects to CyberBOSS. CyberBOSS then communicates the effects to connected simulation or C4I systems. The cyber effect generator application contains two main components: 1. an alert bus, used to receive and normalize alerts from the sensor applications, and 2. the cyber effect resolver, used to perform cyber BDA based on the sensor alerts, generate a resulting cyberspace effect, and communicate that effect to the simulation environment. The cyber effect resolver contains cyber BDA models and a CyberBOSS Interface Framework (CIF) connection for communication with the CyberBOSS infrastructure.

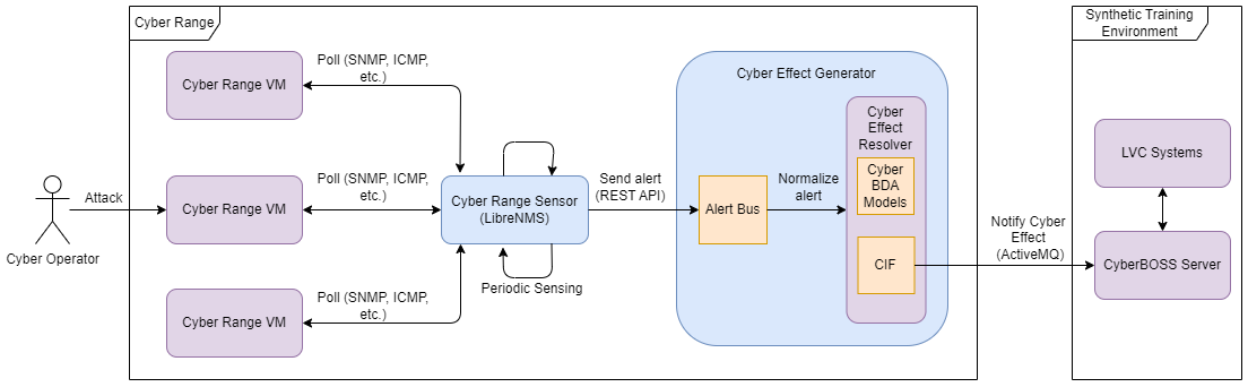

Figure 2. Design of cyber range sensors, showing LibreNMS as an example monitoring tool.

Prototyping of Cyber Range Sensor Applications

In our work, we prototyped the use of cyber range sensor applications described in the above design. As mentioned, if the sensors detect a significant change in an emulated system, an alert is sent to the cyber effect resolver application. In our prototyping, LibreNMS [8] was used as a cyber range sensor. LibreNMS was chosen since it is OSS and there is community support for development of a library of alert rules [9] and supporting macros [10] that can be reused or extended for this work. In our prototyping, these existing alert rules were utilized to monitor cyber range VMs that were not responsive to Internet Control Message Protocol (ICMP) messages (pings). These alert rules were also used to monitor cyber range VMs for which a particular service was not responsive. These alerts were sent from the cyber range sensor application (LibreNMS) to the Alert Bus component of the Cyber Effect Resolver application. The Alert Bus contains a REpresentational State Transfer (REST) endpoint that receives Hypertext Transfer Protocol (HTTP) POST messages from the LibreNMS alert transport capability when an alert occurs. The type of alerts, along with various settings and other meta data, can be configured within LibreNMS.

Prototyping of Cyber Effect Generator Component

In our prototyping, components within the Cyber Effect Generator application were developed to receive the alerts from the cyber sensors (LibreNMS), normalize the alerts, and convert them into a format that is consumable by the cyberspace brokering architecture (CyberBOSS). As mentioned above, the Alert Bus contains a Java Spring Boot REST endpoint that receives HTTP POST messages from the LibreNMS alert transport capability when an alert occurs. After receiving an alert from a sensor, the Alert Bus passes the alert to one of the cyber BDA models within the Cyber Effect Generator. The receiving cyber BDA model normalizes the alert information into a common data model. Normalizing the alerts allows for future flexibility and scalability if other types of sensors are utilized in future work.

After normalization of the alert, cyber BDA models then utilize information in the alert to determine what, if any, cyberspace effect should result based on the alert. The cyber BDA models are responsible for analyzing the normalized sensor alert data and assessing battle damage. The cyber BDA models are stateful components that track the history of sensor alert data, as well as on-going cyberspace effects, to determine if cyberspace effects should be created or removed from the training environment. If a cyber BDA model determines the emulated system is damaged (e.g., disabled, compromised, disrupted), a corresponding request for a cyberspace effect is generated. In our prototyping, cyber range systems not responding to ICMP messages (pings) were mapped as being under a hardware damage cyberspace effect. Additionally, cyber range systems for which a particular service was not responsive were mapped to a DoS cyberspace effect. These cyberspace effects were used to communicate the cyber BDA to other systems in the training environment as described in the next section.

Prototyping the Communication of Cyber Effects to the Cyberspace Broker

As described above, the cyber BDA models send the cyberspace effect status messages to the cyberspace brokering architecture (CyberBOSS) for communication to connected simulation and C4I systems. Those systems can receive

the cyberspace effect information and implement the effect in a manner applicable to the receiving system. For example, upon receipt of a DoS effect, an adapter to the C4I systems, such as the Cyber Operations Battlefield Web Services (COBWebS) [11] or the Joint Bus (JBUS), may stop tactical messaging corresponding to the targeted system from being communicated to the C4I system, resulting in the targeted system disappearing as a track on the C4I system. The cyberspace effect is also received by the CyberBOSS Control Tool, where it can be monitored by exercise facilitators or white cell personnel. In our prototyping, a mechanism was developed to communicate the cyberspace effect information between the cyber BDA models and the cyberspace brokering architecture. The CyberBOSS CDM was utilized to communicate cyberspace effect information as JavaScript Object Notation (JSON) messages over an ActiveMQ message bus. These messages were received by the CyberBOSS Server, which communicated the cyberspace effect message to other CyberBOSS federates, including the Constructive simulation (OneSAF) used in our prototype to model the cyberspace effects within the synthetic battlespace.

EXPERIMENTAL RESULTS

To demonstrate the feasibility of our approach to communicate cyberspace effects between a cyber range and the simulation environment, we developed and experimented with a representative scenario that was implemented across the systems depicted in the above architecture. As an example of combined cyber-kinetic operations, this scenario involves coordination between a BLUFOR CPT and command staff to mitigate a cyber threat against host nation Critical Infrastructure (CI) to support mission objectives. In this scenario, a threat has cyber attacked a power plant generating power for a nearby hospital. Spear-phishing emails were sent to power plant personnel to gain a foothold within the power plant network. The threat performs a cyber attack within power plant network to disable power generation by affecting Supervisory Control and Data Acquisition (SCADA) systems or Industrial Control Systems (ICS) within the power plant. The threat affects connected Programmable Logic Controllers (PLC) and/or Runtime Units (RTU) to stop power generation by the power plant, cutting off power to the hospital. In this scenario the CPT coordinates with command staff and conducts a Hunt/Clear/Harden/Assess operation to locate and fix the problem in the power plant network, restoring power to the hospital.

The system architecture used for experimentation is shown in Figure 3. This architecture consists of two enclaves, the cyber range (PCTE) and the simulation infrastructure. These enclaves are described as follows:

1. **Persistent Cyber Training Environment (PCTE).** A virtual range was deployed within PCTE as a representative power plant control system that included emulated components such as a SCADA Human-Machine Interface (HMI) and PLCs. These emulated systems contained software including OpenSCADA and OpenPLC, and are utilized by CPT operators to perform cyber reconnaissance and defensive operations. Within the PCTE environment, we also deployed an instance of the cyber range sensors (LibreNMS), used to monitor the state of the emulated range systems, and an instance of the Cyber Effect Generator application, used to perform cyber BDA and communicate resulting cyberspace effects to the cyberspace brokering architecture (CyberBOSS).
2. **Simulation Infrastructure**. Within the simulation infrastructure, the One Semi-Automated Forces (OneSAF) kinetic simulation was used to provide Constructive models of the BLUFOR and threat actors and the power plant CI. 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 an existing OneSAF model could be extended to simulate power plant conditions that turn lights on and off in a city block to demonstrate how cyber effects can affect the outcomes of kinetic operations. CyberBOSS acted as the cyberspace brokering architecture to communicate cyberspace-related objects and effects between the cyber range and OneSAF. The CyberBOSS Control Tool functioned as the cyberspace COP, providing a web-based interface to view and control cyberspace effects across the training environment.

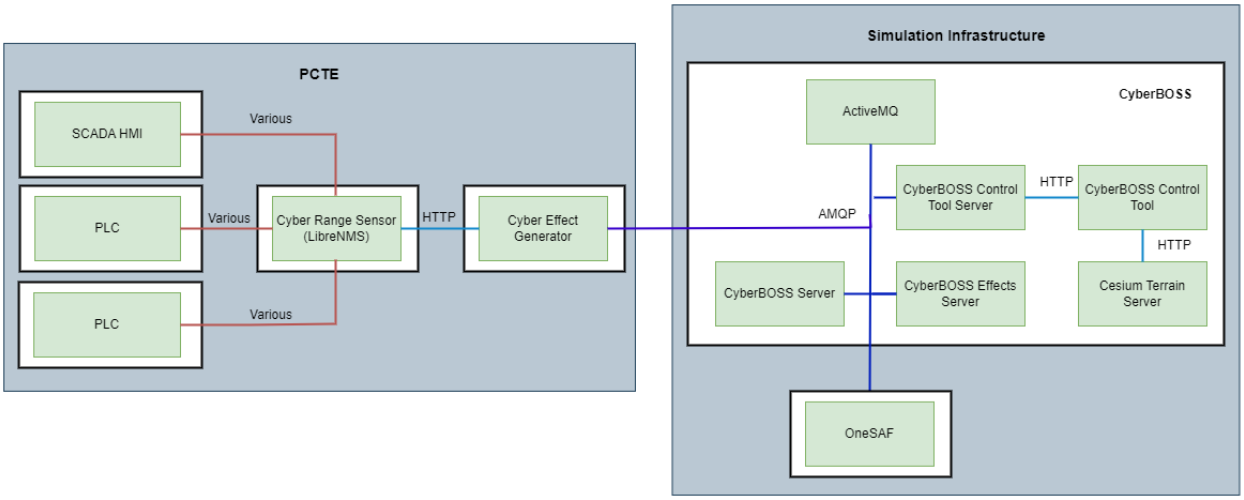

Figure 3. System architecture used for experimentation activities.

Using this prototyping architecture and scenario, we demonstrated the coordination of cyberspace effects between the PCTE cyber range and the OneSAF simulation models due to operator actions within the cyber range. This demonstration involved the following steps: 1. Within PCTE, a simulated cyber attack occurred on an emulated PLC within the emulated SCADA system, causing the PLC to no longer be responsive to ICMP (ping) requests messages. The action to simulate this attack can be performed manually by cyber range operators or using scripts. 2. The LibreNMS monitoring system deployed within PCTE alerted since the sensor could no longer communicate with the PLC VM through ICMP (ping). 3. The cyber effect generator received the alert and its cyber BDA models created and sent a corresponding DoS cyberspace effect to CyberBOSS, which was forwarded to the OneSAF simulation. 4. OneSAF, also representing the SCADA system, changed its internal status for that system to reflect this cyberspace effect, resulting in disabling all simulated streetlights and building lights within an area controlled by that SCADA system.

In this demonstration, actions or scripts within the cyber range were then used to mitigate the initial cyber attack on the PLC devices and restore them back to operational state. Following the steps listed above, power to the OneSAF-simulated power plant was restored and the simulated streetlights in the area were reactivated. This demonstration provided an initial proof of feasibility of our concept to coordinate cyberspace training between cyber ranges and the simulation environment.

FUTURE WORK

This work represents a significant improvement to implement cyber-kinetic training since it provides an architecture to automatically communicate cyberspace information across the training environment, so a unified operational picture is provided to all trainees (cyber and non-cyber). This automated coordination minimizes manual methods to communicate and synchronize cyberspace effects between a cyber range and the simulation environment, which are error-prone and limit training realism. Future work to develop this architecture to support cyber-kinetic training may include:

- Further analysis, in conjunction with Information Warfare (IW) subject matter experts (SME) to determine other cyberspace effects and target systems on which to focus additional development. These effects can be due to both offensive and defensive actions performed within the cyber range by CCMTs and CPTs.
- Development of additional scenarios that are applicable for cyber-kinetic training. Our prototype scenario focused on a critical infrastructure (power plant) attack; however, there are many other military and/or civilian scenarios that are applicable to this training architecture.
- Development of additional cyber range sensors and cyber BDA models. Our initial work utilized the OSS LibreNMS to provide alerts to our cyber range sensors; however, other OSS and COTS products could be used as a sensor front-end to provide inputs to the cyber BDA models. Additionally, other cyber BDA models

can be developed to support additional cyberspace effects, such as data infiltration, data exfiltration, or spear-phishing.

- Use of other communication protocols to communicate the cyberspace effect information between the cyber BDA models and the cyberspace brokering architecture. In our prototyping, the CyberBOSS CDM was used for this communication; however, future work could utilize alternative methods to communicate cyberspace effect information between the cyber BDA models and CyberBOSS. For example, the emerging SISO Cyber DEM standard (SISO-STD-025-2023) structured Distributed Interactive Simulation (DIS) Protocol Data Units (PDU) could be used to communicate cyberspace effect information. Future work can develop capabilities in the CyberBOSS Bridge application to receive these PDUs and create corresponding CDM cyberspace effect messages based on the received PDU data. An advantage to this alternative method to communicate cyberspace effect information is that many network guards can scan DIS PDUs, so this method may be preferred when passing information within an MLS environment or for tight control of data passing between the cyber range and the simulation environment. A similar approach using the upcoming SISO HLA Cyber Federation Object Model (Cyber FOM) could be taken to support interoperability of cyber ranges with HLA-based federations.
- Expanded integration with the Live training environment. For example, in our prototype, cyber attacks carried out against CI in the cyber range causes effects in connected constructive simulations but does not cause effects in the Live training environment. Future development could also introduce effects into the Live training environment, where the power disruptions in the cyber range could also disrupt power to buildings, physical systems, and infrastructure in the Live training environment.
- Bi-directional effects synchronization, where kinetic events occurring in the LVC training environment could have an impact on the cyber range environment. For example, if physical network nodes are destroyed by a kinetic event in the simulation or Live training environment, the effects could be synchronized with the cyber range, impacting the network and connectivity between nodes in the cyber range environment.

CONCLUSION

To maximize their effectiveness during multidomain operations, the Cyber Mission Force teams, such as CPTs and CCMTs, require collective cyber-kinetic training to ensure they work effectively with commanders across the Services and Joint Force to accomplish their assigned missions and achieve information advantage in the battlespace. However, cyber-kinetic training is currently hindered because existing LVC systems used for command staff training are not developed to communicate directly with cyber ranges used for cyber team training, and coordination of cyber effects between these training environments is performed manually. In this paper, we described a novel system architecture developed to automate the communication of cyber effects between a cyber range and LVC systems. This architecture utilizes cyber range sensors for cyber BDA due to operator actions within the range that cause changes to network and system states. The feasibility of this approach was demonstrated though a prototype that coordinated cyberspace effects between the cyber range and LVC environment during a simulated cyber attack on a power plant. This approach represents a significant improvement for cyber-kinetic training, increasing warfighter readiness for conducting multidomain operations.

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., Geddes, J.A., & Vey, N. (2021). A Cyberspace Effects Server for LVC&G Training Systems. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*

[3] Hasan, O., Welch, J., Burch, B., Geddes, J.A., & Boyce, M. (2022). Integration of Live and Synthetic Environments for Improved Cyberspace Training. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*

[4] Hasan, O., Mendoza, A., Welch, J., Burch, B., & Geddes, J.A. (2023). Incorporating Navigation Effects into Synthetic Environments for Improved Cyberspace Training. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*

[5] 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).*

[6] Wells, D., & Bryan, D. (2015). Cyber Operational Architecture Training System Cyber for All. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*
[7] Hasan, O., Crane, D., & Dukstein, G. (2024) Incorporating Simulated Cyberspace Effects on Navy Shipboard Systems during Training. *Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop (SIW).*
[8] https://www.librenms.org/
[9] https://github.com/librenms/librenms/blob/master/misc/alert_rules.json
[10] https://github.com/librenms/librenms/blob/master/misc/macros.json
[11] 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).*