Incorporation of Automated Cyber Adversaries to Improve Cyber-Kinetic Training

Omar Hasan, Ph.D., Derek Crane, Andrew Mendoza
W. Jeremy RiCharde
Dignitas Technologies
Orlando, Florida
ohasan@dignitastech.com, dscrane@dignitastech.com, amendoza@dignitastech.com, jricharde@dignitastech.com

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

ABSTRACT

In the modern battlespace, adversaries actively pursue Internet Protocol (IP)-based cyber attacks to affect operational missions in all warfighting domains. Cyber Mission Force (CMF) teams direct, synchronize, and coordinate cyberspace operations in defense of U.S. national interests. To maximize their effectiveness for Multi-Domain Operations (MDO), 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.

We previously developed a novel system architecture that automates the communication of cyber effects between a cyber range, used for CMF training, and Live, Virtual, and Constructive (LVC) systems, used for command staff training. That architecture, Cyberspace Battlefield Operating System Simulation (CyberBOSS), utilizes a cyber range adapter to determine cyber battle damage assessment (BDA) due to operator actions within the range that cause changes to network and system states. The cyber BDA is communicated to the LVC training environment using this architecture so that generated cyberspace effects have an operational impact on connected Command, Control, Communications, Computer and Intelligence (C4I) interfaces. This work extends our architecture by incorporating automated cyberspace adversaries that simulate cyber attack kill chains on networks and systems within cyber ranges and LVC environments. By running autonomously, the use of intelligent cyber adversaries such as the Intelligent Cyber Adversary Tool Suite (ICATS) reduces the manpower required to stimulate Blue Force (BLUFOR) training audiences with cyber attack inputs. The feasibility of this approach is demonstrated though a prototype that demonstrates how several ICATS-based cyberspace effects can automatically execute a cyber kill chain affecting systems within the cyber range and LVC environment. This approach represents a significant improvement for cyber-kinetic training since it reduces the cost and manpower required for live cyber role players to meet MDO training objectives.

ABOUT THE AUTHORS

Dr. Omar Hasan is the Chief Technology Officer (CTO) at Dignitas Technologies, where he serves as the principal investigator on cyberspace-related research efforts. Dr. Hasan has 25 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.

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 DEVCOM SC's Cyberspace Warfare for Training (CyWar-T) S&T research program. He has 20 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 B.S. degrees in Management Information Systems and Software Development from the University of Central Florida and 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 the International Information System Security Certification Consortium (ISC2). Mr. Strauss has earned a B.S in Information Technology-Security from Western Governors University.

Patrick J. Hart 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). Mr. Hart brings more than 30 years of experience in research and development and acquisition with the Army and Air Force. After serving in the Air Force, Mr. Hart received a B.S. in Electrical Engineering from the University of Central Florida and a M.S. in Program Management from the Naval Postgraduate School.

Incorporation of Automated Cyber Adversaries to Improve Cyber-Kinetic Training

Omar Hasan, Ph.D., Derek Crane, Andrew Mendoza
W. Jeremy RiCharde
Dignitas Technologies
Orlando, Florida
ohasan@dignitastech.com, dscrane@dignitastech.com,
amendoza@dignitastech.com, jricharde@dignitastech.com

J. Allen Geddes, Jason Strauss, Patrick Hart
US Army DEVCOM SC STTC
Orlando, Florida
james.a.geddes2.civ@army.mil,
jason.p.strauss.civ@army.mil,
patrick.j.hart.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. Denial of service (DoS) attacks, Advanced Persistent Threat (APT) operations, and other cyber attacks on military networks or systems can cause significant loss of life and damage to military assets. To counter these threats, the U.S. Cyber Command (USCYBERCOM) stood up Cyber Mission Force (CMF) teams to 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. The major efforts of cyber operations performed by the CMF focus on tight coordination of cyber operations to support the goals of kinetic military operations.

To maximize their effectiveness for multidomain operations (MDO), the CMF requires 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 includes communication of cyber effects between Live, Virtual, and Constructive (LVC) systems used for command staff training and cyber ranges used for CMF training. This provides an environment for training the coordination between these disparate teams to meet mission goals. Within the cyber-kinetic training environment, team members must continually train in the complex Tactics, Techniques, and Procedures (TTP) required for offensive and defensive military cyberspace operations to support mission objectives. For example, CPTs train on procedures to identify, mitigate, and defend threats against Blue Force (BLUFOR) systems or military or civilian Industrial Control Systems (ICS). In this training, cyber force threats are typically role-played by exercise support teams that must possess highly specialized skills in performing realistic cyber attacks within the training environment. This is a labor-intensive and costly method to introduce cyber actions and effects into the training environment to provide inputs for CPT trainees. What is needed is an automation approach at the cyber intent level that provides both offensive and defensive Opposing Force (OPFOR) cyber forces in support of training, reducing the manpower and costs to provide training to both command staff and CMF teams.

APPROACH

To facilitate cyber-kinetic training, this work provides an approach in which simulated automated cyberspace adversaries provide training inputs to BLUFOR teams using LVC systems or within cyber ranges. These adversaries perform simulated cyber attacks on simulated or live systems within the training environment, minimizing the cost and manpower required for threat cyber role players. In this use case, simulated adversaries perform threat TTPs which automatically cause changes to the functionality, configuration, or state of BLUFOR systems, providing realistic cyber injects into the training environment. The cyberspace adversaries provide coordinated cyber training stimuli that can be used to train CMF and command staff on the coordination of processes to identify and mitigate these threat cyber actions on BLUFOR systems to retain warfighting capabilities. This approach represents a significant improvement

over the current methods used for cyber-kinetic training, which relies heavily on unrealistic, out-of-game mechanisms such as *white-carding* and chat to communicate the presence of threat cyber effects to the trainees.

To support cyber-kinetic training that includes intelligent cyberspace adversaries, a novel system architecture was developed to integrate adversary models with LVC systems, cyber range systems, and Command, Control, Communications, Computers, and Intelligence (C4I) systems. The feasibility of this approach was demonstrated though a prototype that communicates and manifests cyber effects caused by simulated adversary models in a coordinated manner throughout the training environment. This approach can significantly improve cyber-kinetic training, reducing the manpower and costs to provide realistic cyber training inputs that increase warfighter readiness for conducting multidomain operations.

ARCHITECTURE

This section describes the high-level architecture developed to automate the communication of cyber effects between a cyber range, used for CMF training, and LVC systems, used for command staff training. This architecture builds on a previous cyber training architecture we have described [1] and expands that architecture to incorporate automated cyberspace adversaries that simulate cyber attack kill chains on networks and systems within cyber ranges and LVC environments. This architecture, depicted in Figure 1, consists of a cyber training environment containing a cyber range used for cyber offensive and defensive team training. It also contains a simulation environment containing constructive kinetic simulations and C4I systems used for command staff training. The simulation environment also contains simulated intelligent cyberspace adversaries that perform simulated cyber attacks on simulated or live devices within the training environment. Cyberspace domain-related information between the two environments is communicated using a cyberspace brokering architecture, which provides cyberspace effects and operations models as well as user interfaces (UI) utilized by exercise facilitators.

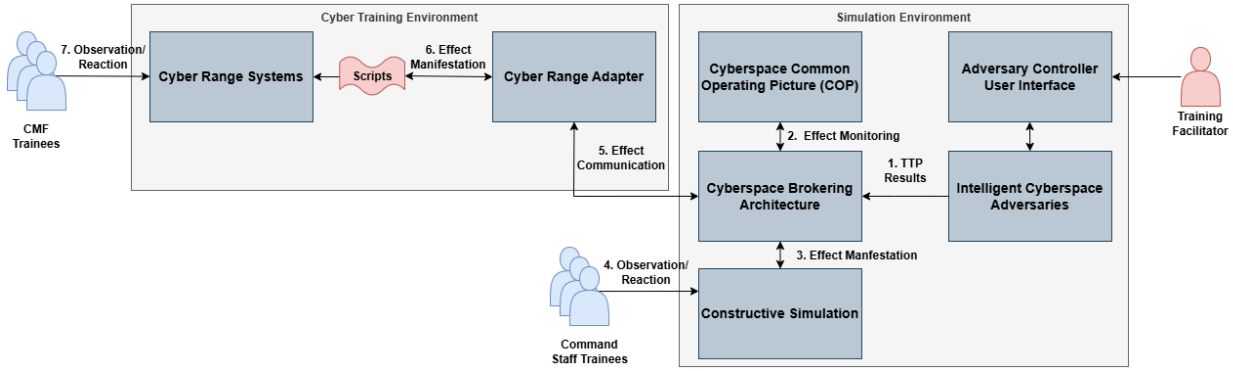

Figure 1. High-level architecture used to communicate simulated cyber adversaries TTP results to the cyber range and the simulation environment.

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 Systems	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 Adapter	Software application that receives cyber effects from the simulation environment and manifests those effects by changing the configuration or state of cyber range systems
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
Intelligent Cyberspace Adversaries	Simulated cyberspace adversaries that perform modeling of cyber-related operations, such as reconnaissance and attacks, and cause cyber effects
Adversary Controller UI	UI that allows control, configuration, and status monitoring of the intelligent cyberspace adversaries

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 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 BLUFOR systems or military or 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).

Cyber Range Adapter

The Cyber Range Adapter component receives cyber effects from the simulation environment and manifests those effects by changing the configuration or state of cyber range systems. These cyber range systems may represent C4I systems, operator workstations, and other systems relevant to the training scenario. Our previous work [1] described the use of cyber range sensors that provide 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. This work builds upon our previous research by expanding these sensors to include communication of cyber effects originating within the simulation environment to cause changes in cyber range systems. The ability to automatically cause changes to cyber range system configuration and states provides great benefits to the cyber-kinetic training environment since it reduces manpower requirements (i.e., white carding, swivel chair synchronization) and provides realistic and automated manifestation of cyberspace effects to the CMF trainees.

To communicate cyber effects originating in the simulation environment to the cyber range, the cyber range adapter utilizes a four-step process:

1. The cyberspace effect is communicated from the simulation environment to the cyber range adapter using the cyberspace brokering architecture.
2. The cyber range adapter determines the cyber range systems to affect and the appropriate changes to those cyber range systems to manifest the effect within the cyber range for CMF training inputs. These changes may affect 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. The cyber range adapter performs changes on the identified cyber range systems. Those changes may be performed using several mechanisms, including executing scripts or employing hypervisor services to change system configuration and/or state.
4. Cyber range operators (i.e., CMF trainees, threat cyber role players) identify and react to changes to cyber range systems that are results of cyber attacks or compromise.

As described in Step 2 above, once a cyber effect has been received by the cyber range adapter, changes to the state and configuration of affected cyber range systems is automatically performed. In our work, we developed mappings between the received cyberspace effect and the resulting changes that were made to cyber range systems to manifest the effect to provide realistic CMF training inputs. Our analysis found that there is a one-to-many relationship between a generated cyberspace effect and cyberspace attack manifestations. That is, a particular cyberspace effect can result in different changes to cyber range systems depending on their system type. For example, a data exfiltration cyberspace effect may result in different file system and log file changes depending on the particular operating system and installed software of the targeted system. For some example cyberspace effects, Table 2 shows possible manifestation of the results of the effect on cyber range systems. For each cyberspace effect, example attack vectors within the cyber range that would cause the effect are listed, providing changes to the cyber range systems to manifest the effect symptoms. There are various other combinations of possible ways to generate these cyberspace effects and their resulting changes to system state/configuration, however, and other attack vectors could be explored in future work.

Table 2. Examples of cyber range system affected state changes and user observed symptoms corresponding to cyberspace effects received from the simulation environment.

Received Cyberspace Effect	Detected Attack Types	Example Specific Attack Vector	Affected State	User Observed Symptoms
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
Data Exfiltration Effect	Payload Attack	Backdoor	• Filesystem ○ Logs • Network traffic • Running processes	• Possible degraded network bandwidth

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. [2] [3] Through on-going research efforts under the U.S. 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 [4]. The CyberBOSS system architecture contains services that

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] and 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 TTP modeling information between constructive simulations, C4I systems, simulated cyberspace adversaries, and a cyber range.

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.

Intelligent Cyberspace Adversaries

The intelligent cyberspace adversaries perform modeling of cyber-related operations and cause cyber effects. Those operations include interrogating networks and devices to identify vulnerabilities, performing cyber attacks on BLUFOR devices (simulated and real), or directly imparting cyber effects on BLUFOR devices and networks. These operations occur in a semi- or fully-automated fashion and rely on underlying models and supporting data. Simulated cyberspace adversaries may have varying degrees of skill level or effectiveness, mimicking real world actors and APTs who may utilize varying cyber techniques and who may possess cyber skills ranging from a novice up to expert level hacker. Cyber adversaries execute cyber TTPs in a controlled fashion to model specific APTs and threat profiles. Cyber threat TTPs can be informed by known attack libraries such as the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. [7]

Adversary Controller

The Adversary Controller is a web-based UI that allows the training facilitator to configure, control, and monitor the simulated cyber actions of cyberspace adversaries within the training environment. It also provides a real-time view into adversary cyberspace operations with insight into the adversary decision-making process.

PROTOTYPING EFFORTS

This section provides details on our prototyping efforts using the above architecture to demonstrate the use of automated cyberspace adversaries to provide the effects of simulated cyber operations within a cyber-kinetic training environment. Our prototyping activities focused on the design and development of automated cyberspace adversaries and their modeling of threat operation TTPs to affect systems within the training environment. We prototyped the mechanism by which adversary modeling information is communicated to two areas: 1.) to the simulation environment to affect Constructive simulations to alter stimulation of connected C4I systems, and 2.) to the cyber training environment to alter the state and configuration of cyber range systems.

Intelligent Cyberspace Adversaries

In our prototyping of this architecture, we used and enhanced our Intelligent Cyber Adversary Tool Suite (ICATS), which provides simulated intelligent, semi-automated OPFOR cyber adversaries that execute simulated cyberspace attacks and other operations on BLUFOR networks. We previously developed ICATS through a Phase II Small Business Innovation Research (SBIR) project under the U.S. Army DEVCOM SC STTC. ICATS automated adversaries simulate threat cyber operation TTPs within various networks and systems, including simulated networks and devices within LVC training systems, live military C4I systems used by the training audience, and emulated networks and systems within a cyber range.

One main reason we chose ICATS adversaries to model threat cyber operations is that ICATS models specific TTPs in a controlled fashion, guided by the TTP hierarchy defined in the ATT&CK database. Within ATT&CK, cyberspace operations are mapped to specific techniques, and those techniques are mapped to specific procedures used to execute each technique. As shown in Figure 2, ICATS adversaries decompose high-level cyberspace operations (tactics) into specific sets of cyberspace operation techniques and procedures that each adversary performs. Adversaries are assigned varying proficiencies of technique and procedure execution, modeling the variability of real-world cyber skill sets and supporting variation for modeling specific APTs. ICATS adversaries perform operations through manual user intervention or by automated means resulting from adversary goal planning algorithms.

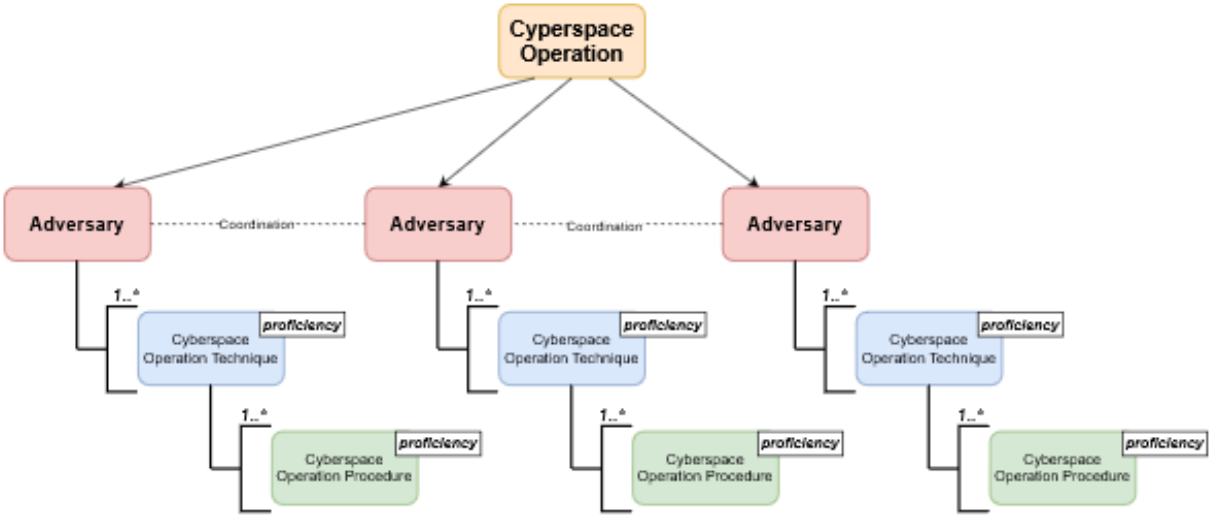

Figure 2. ICATS cyber adversary operations are decomposed to specific cyberspace technique and procedure models to support tailored adversary execution.

Communication of Adversary-Based Cyber Effects to C4I Systems

In our prototyping, we extended previously described system designs [8] to design a mechanism to communicate and apply the results of simulated adversary cyber TTP modeling on connected C4I systems. The goal of this prototyping was to communicate the results of the threat TTPs to connected BLUFOR C4I systems so those systems manifest

appropriate changes due to the TTPs. For example, the TTPs can result in the injection, alteration, or stopping of Position Location Information (PLI) sent by the C4I device due to the simulated threat actions. A high-level design of the communication of TTP operation results to connected C4I systems is shown in Figure 3.

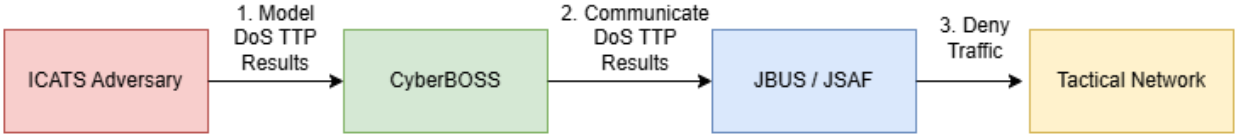

Figure 3. High-level design of the communication of adversary TTP operation results to connected C4I systems.

This design is shown for the use case of an ICATS adversary performing TTP modeling resulting in a DoS operation that affects a C4I system on the BLUFOR tactical network. This communication involves the following steps:

1. The ICATS adversary performs modeling of the threat TTPs resulting in a DoS attack against a BLUFOR C4I system. The results of the simulated TTP actions are periodically sent to the cyberspace brokering architecture. The cyberspace brokering architecture receives these results of the ICATS adversary TTP modeling. In our design, we used the CyberBOSS cyberspace brokering architecture since it provided a data model and mechanisms to communicate the TTP modeling results.
2. The TTP modeling results are communicated from the cyberspace brokering architecture to the Constructive simulation environment. In our design, we utilized Joint Semi-Automated Forces (JSAF) and Joint Bus (JBUS) as our Constructive simulation components since they contain representations of the platforms to be affected. JBUS also contains mechanisms to communicate with the connected BLUFOR tactical network.
3. JBUS stops (denies) sending messaging traffic for the affected device to the tactical network. This creates the trainee effect that PLI information for the attacked system becomes stale or times out from the network.

Communication of Adversary-Based Cyber Effects to Cyber Range Systems

In our prototyping, we also designed the mechanism to communicate and apply the results of simulated adversary cyber TTP modeling to connected cyber range systems. The goal of this prototyping was to communicate the results of the threat TTPs to connected BLUFOR cyber range systems so those systems manifest appropriate changes due to the TTPs. The Cyber Range Adapter can implement the cyber effect in two ways: 1. performing the actual cyber attack on target systems, or 2. mimicking the cyber attack by changing the configuration of the target systems, such as altering configurations, starting/stopping services or applications, or even completely disabling the systems. A high-level design of the communication of TTP operation results to connected cyber range systems is shown in Figure 4.

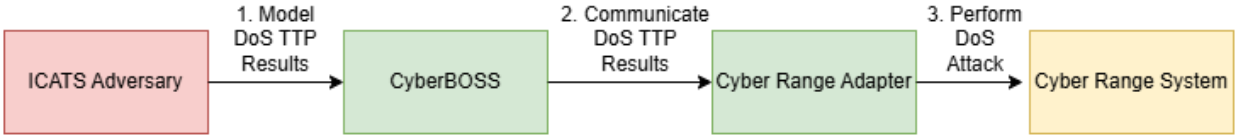

Figure 4. High-level design of the communication of adversary TTP operation results to connected cyber range systems.

This design is shown for the use case of an ICATS adversary performing TTP modeling resulting in a DoS operation that affects a cyber range system on the BLUFOR tactical network. This communication involves the following steps:

1. The ICATS adversary performs modeling of the threat TTPs that result in a DoS attack against a BLUFOR system emulated in a cyber range. The results of the simulated TTP actions are periodically sent to the cyberspace brokering architecture (CyberBOSS).
2. CyberBOSS periodically communicates the results of the DoS TTP actions to the cyber range adapter, which provides interfaces to communicate cyber effects between the simulation environment and the cyber range.
3. The cyber range adapter performs actions on the affected cyber range system corresponding to the received effect, such as performing the actual cyber attack or by mimicking the attack by changing system configuration files, starting or stopping services or applications on the system, or powering down the system. This creates conditions within the cyber range that can serve as inputs to CMF training.

EXPERIMENTAL RESULTS

In our work, we performed experiments to demonstrate the feasibility of our approach to communicate cyberspace effects generated from simulated cyberspace adversaries to C4I systems and to cyber range systems. For our experimentation, we developed and experimented with a representative scenario that was implemented across the systems depicted in the above architecture. Within this scenario, constructive BLUFOR ships provide self-reported PLI information to the BLUFOR C4I networks. The C4I devices for these constructive ships are also emulated in the cyber range, so they can be used for CMF defensive training. In this scenario, threat actors compromise a C4I device on a BLUFOR ship and perform a cyber attack that results in a DoS for that device, stopping the BLUFOR ship PLI information from being reported.

The system architecture used for experimentation is shown in Figure 5. This architecture consists of three enclaves, the cyber range, the simulation infrastructure, and the representative shipboard C4I network and systems. These enclaves are described as follows:

1. **Cyber Range.** A developmental and testing cyber range was deployed within our environment to emulate various BLUFOR shipboard C4I systems within the scenario. These emulated systems can be used by CPT trainees as representative systems within which cyber defensive tasks can be trained. They can also be used as targets of adversarial TTPs by our simulated cyberspace adversaries. Within the cyber range, we deployed an instance of our Cyber Range Adapter application which can receive adversary TTP results from the simulation infrastructure and apply those results to cyber range systems to produce configuration changes or changes to system state to reflect the results of the adversary TTPs. In our experimentation, the cyber range was comprised of a set of Podman containers, each of which represented a single shipboard C4I system.
2. **Simulation Infrastructure**. Within the simulation infrastructure, the Joint Semi-Automated Forces (JSAF) kinetic simulation was used to provide Constructive models of the BLUFOR and threat actors. JSAF is widely used for training by the U.S. Navy and Joint Staff. ICATS was used within the simulation infrastructure to simulate the cyberspace adversaries and their operational TTPs. CyberBOSS acted as the cyberspace brokering architecture to communicate cyberspace-related objects and effects between connected systems using the Advanced Message Queuing Protocol (AMQP). Finally, the Joint Bus (JBUS) was used to stimulate connected representative shipboard C4I systems using a variety of tactical protocols.
3. **Shipboard Systems**. A set of representative BLUFOR shipboard C4I systems and networks were used as targets of the threat cyberspace operation TTPs. The JBUS communicated with these systems using various tactical message protocols such as Link-16. Cyberspace effects on these systems were implemented by injecting, modifying, or dropping tactical messages communicated to the systems.

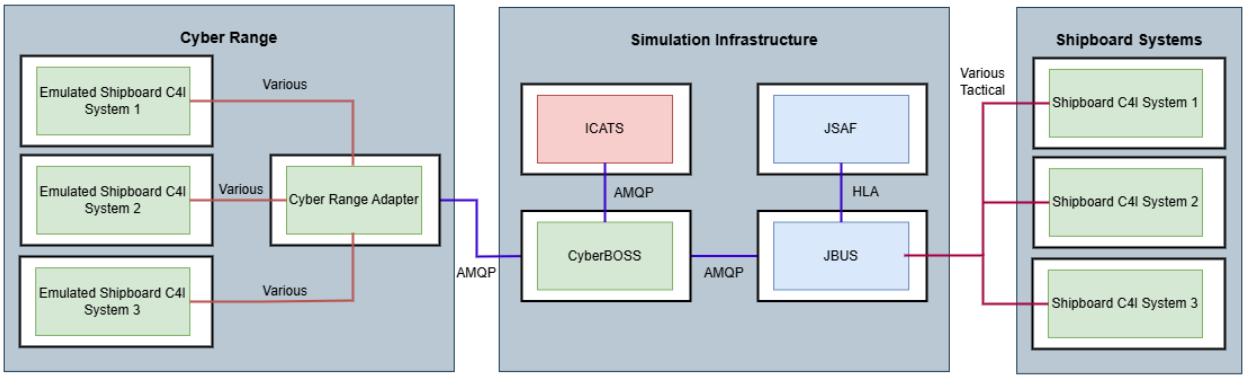

Figure 5. System architecture used for experimentation activities.

Communication of Adversary-Based Cyber Effects to C4I Systems

Using this system architecture, we experimented with communicating cyber effects based on simulated adversary TTPs to affect representative BLUFOR C4I systems. Those C4I systems were simulated in the JSAF constructive simulation and JBUS was used to send PLI information for the C4I systems to live C4I devices representing shipboard systems. In our experiments, ICATS cyberspace adversaries performed simulated cyber attacks against these C4I

systems, affecting their ability to correctly report PLI information. As an example, the ICATS adversaries were commanded to perform an Impact cyber operation tactic to affect BLUFOR C4I systems. MITRE ATT&CK defines the Impact tactic (TA0040) [9] as the goal of the adversary manipulating, interrupting, or destroying systems and data. ATT&CK describes various cyber techniques that adversaries can use to meet the goals of this tactic, including the techniques of Data Destruction (T1485), Data Manipulation (T1565), and Endpoint Denial of Service (T1499). Within our scenario, the Impact technique was performed to simulate a cyber attack on the BLUFOR C4I systems that interrupts their self-reporting capabilities. During this experiment, ICATS adversaries automatically decomposed the Impact tactic into various techniques and procedures, as guided by the ATT&CK framework. The simulation of a successful Endpoint Denial of Service technique by the cyberspace adversaries was communicated by the CyberBOSS framework to JBUS. JBUS then stopped PLI reporting for the affected C4I devices, causing their reporting information to stale out on receiving systems. This demonstrated that the cyberspace adversaries were able to run autonomously within the training environment and cause automated, realistic cyber effects that can serve as training inputs to Naval command staff.

Communication of Adversary-Based Cyber Effects to Cyber Range Systems

Using this system architecture, we also experimented with communicating cyber effects based on simulated adversary TTPs to affect cyber range systems that represent BLUFOR C4I devices. These systems were emulated in a developmental cyber range and were implemented as Podman containers. The C4I devices were also simulated in JSAF, as described above, and JBUS was used to send PLI information for the C4I systems to live C4I devices representing shipboard systems. In our experiments, ICATS cyberspace adversaries performed simulated cyber attacks against these cyber range systems, causing changes to the configuration or state of the systems. The results of these changes were communicated to JBUS using the CyberBOSS cyberspace brokering architecture. As above, we issued the ICATS adversaries a goal of the Impact technique to simulate a cyber attack on the BLUFOR C4I systems in the range that interrupts their self-reporting capabilities. During this experiment, ICATS adversaries automatically decomposed the Impact tactic into various techniques and procedures, as guided by the ATT&CK framework. The ICATS adversaries requested implementation of an Endpoint Denial of Service technique against a target cyber range system and this request was communicated by the CyberBOSS framework to the Cyber Range Adapter. Upon receipt of the request, the Cyber Range Adapter implemented the DoS technique by automatically performing a live DoS attack against the target system. When the DoS was effective, the sensors within the Cyber Range Adapter then communicated the on-going status of the DoS effect to JBUS, which stopped PLI reporting for the associated simulated C4I devices, causing their reporting information to stale out on receiving systems. This demonstrated that the cyberspace adversaries were able to automatically make changes to cyber range systems that can provide realistic cyber training inputs to CMF teams. Simultaneously, those inputs were automatically synchronized with the simulation systems within the training environment to provide coordinated training inputs to Naval command staff.

FUTURE WORK

This work represents a significant improvement to implement cyber-kinetic training since it provides an architecture to incorporate automated simulated cyberspace adversaries and communicate the results of their threat cyber TTPs across the training environment. Use of simulated adversaries reduces the costs and manpower required to provide realistic cyber training inputs to both CMF trainees and Naval command staff. Additionally, the automated coordination of the results of adversary TTP operations provides synchronized cyberspace effects between a cyber range and the simulation environment, reducing errors and improving 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 adversarial cyberspace effects and operation TTPs, and their associated changes to cyber range systems, on which to focus additional development.
- Incorporation of cyberspace adversary modeling to represent known APT operational TTPs, providing realistic inputs to cyber-kinetic training scenarios. Our prototype scenario focused on an endpoint denial of service attack on BLUFOR C4I systems; however, there are many other military and/or civilian scenarios that are applicable to this training architecture and can be affected by specific APT actions.
- Incorporation of Artificial Intelligence (AI) / Machine Learning (ML) into simulated cyberspace adversary capabilities to impart further realism to modeling threat cyber TTP operations.

- Development of additional cyber range adapter mechanisms and models by which changes to cyber range systems are performed due to cyber adversary TTPs. Our initial work utilized Linux shell scripts that performed a DoS operation on cyber range systems. However, other Open Source Software (OSS) and Commercial Off-the-Shelf (COTS) products could be used to make realistic changes to cyber range system files, configuration, and networking.
- Use of other communication protocols to communicate the cyberspace effect information between the cyberspace brokering architecture, and the cyber range. 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. 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 a Multi-Layer Security (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.

CONCLUSION

To maximize their effectiveness during multidomain operations, CMF 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. We previously described a novel system architecture that automates the communication of cyber effects between a cyber range, used for CMF training, and LVC systems, used for command staff training. This work extended our architecture by incorporating automated cyberspace adversaries that simulate cyber attack kill chains on networks and systems within cyber ranges and LVC environments. By running autonomously, the use of intelligent cyber adversaries such as ICATS reduces the manpower required to stimulate BLUFOR training audiences with cyber attack inputs. We demonstrated the feasibility of this approach though a prototype in which ICATS-based simulated cyber attacks automatically executed a cyber kill chain affecting systems within the cyber range and LVC environment. This approach represents a significant improvement for cyber-kinetic training since it reduces the cost and manpower required for live cyber role players to meet MDO training objectives.

REFERENCES

[1] Hasan, O., Crane, D., Welch, J., Truong, J., Evans, M., Geddes, J.A., Strauss, J., & Bogler, W.C. (2024). *Development of a Novel Architecture for Improving Cyber-Kinetic Training.* 2024 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Orlando, FL.
[2] Welch, J., Hasan, O., Burch, B., Vey, N., & Geddes, J.A. (2020). *CyberBOSS: An Approach for Control and Interoperation of Cyber for Training.* 2020 Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop (SIW), Orlando, FL.
[3] Hasan, O., Welch, J., Burch, B., Geddes, J.A., & Vey, N. (2021). *A Cyberspace Effects Server for LVC&G Training Systems.* 2021 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Orlando, FL.
[4] Hasan, O., Welch, J., Burch, B., Geddes, J.A., & Boyce, M. (2022). *Integration of Live and Synthetic Environments for Improved Cyberspace Training.* 2022 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Orlando, FL.
[5] Hasan, O., Welch, J., Burch, B., Vey, N., Geddes, J.A., & Hofstra, K. (2020). *CyberBOSS Common Data Model*. 2020 Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop (SIW), Orlando, FL.
[6] Wells, D., & Bryan, D. (2015). *Cyber Operational Architecture Training System Cyber for All.* 2015 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Orlando, FL.
[7] https://attack.mitre.org/
[8] Hasan, O., Crane, D., & Dukstein, G. (2024). *Incorporating Simulated Cyberspace Effects on Navy Shipboard Systems during Training*. 2024 Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop (SIW), Orlando, FL.

[9] https://attack.mitre.org/tactics/TA0040/