A Cyberspace Effects Server for LVC&G Training Systems

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

J. Allen Geddes, Nathan Vey
US Army DEVCOM SC SED STTC
Orlando, Florida
james.a.geddes2.civ@army.mil, nathan.l.vey.civ@army.mil

ABSTRACT

The United States (U.S.) Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1 describes the concept of how Multi-Domain Operations (MDO)-capable Army forces, as part of the Joint Force, fight across all domains (land, sea, air, space, and cyberspace), the electromagnetic spectrum (EMS), and the information environment (IE). To achieve such an MDO-capable Army, the live, virtual, constructive, and gaming (LVC&G) training systems that the Army uses to train its forces must be able to replicate this emerging operational environment. However, the Army's current LVC&G systems were not originally developed to incorporate the actions and effects within and across the cyberspace domains, the EMS, and the IE.

Our work developing the Cyberspace Battlefield Operating System Simulation (CyberBOSS) focused on facilitating the representation and federation of cyberspace elements into existing and future LVC&G systems. Recent efforts have provided a framework to model cyberspace effects across these federated systems. We established an approach for the development, registration, and management of cyberspace effects models as a service within the CyberBOSS ecosystem. This paper discusses our approach to provide an architecture and protocol for federated systems to request cyberspace effects from the service.

There are three main concepts in the cyberspace effects service approach. First, we provide an architecture that allows for the incorporation of effects models that can be requested, instantiated, and provided as services. Second, we formalize a protocol and data model for control and status of these loosely coupled modeling services. Third, we provide a set of typical cyberspace effects models as exemplars. Finally, the paper describes how these cyberspace effects modeling services are provided within the CyberBOSS ecosystem using a loosely coupled effects server. We describe how the effects may be visualized within the environment and how CyberBOSS clients may allocate, control, and obtain information from the cyberspace effects models.

ABOUT THE AUTHORS

Dr. Omar Hasan is currently a chief software architect at Dignitas Technologies, where he serves as the software architect on two cyberspace-related research efforts, Cyberspace Battlefield Operating System Simulation (CyberBOSS) and the Intelligent Cyberspace Adversaries Tool Suite (ICATS). He also serves as the principal investigator on the cyberspace-related research efforts Geospatially Integrated Cyber Situational Awareness (GICSA) and Live, Virtual, and Constructive Cyber Battle Damage Assessment for Training (Cyber BDA). Dr. Hasan has 21 years of experience in software development, focusing on the modeling and simulation (M&S) areas of simulator interoperability, distributed simulation, and simulation architecture and infrastructure. He has extensive experience in object-oriented software analysis and design, open-source technologies and methodologies, and collaborative software development. Dr. Hasan has held architect and software engineering lead positions on both the One Semi-Automated Forces (OneSAF) and Joint Land Component Constructive Training Capability (JLCCTC) programs. He is currently supporting software development and cyber test event execution activities for the National Cyber Range (NCR). Dr. Hasan holds a B.S. and M.S. in engineering from Columbia University and a Ph.D. in engineering from Rutgers University.

Jeffrey Welch is a 20-year veteran of software development within the modeling and simulation industry. He is the current software development lead for the CyberBOSS program and related research efforts at Dignitas Technologies.

Approved for Public Release #PR2021_25792

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

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

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

Nathan Vey is a Science and Technology Manager at the U.S. Army Combat Capabilities Development Command Soldier Center (DEVCOM SC) Soldier Effectiveness Directorate (SED) Simulation and Training Technology Center (STTC). In his current role, Mr. Vey leads the DEVCOM SC SED STTC's Cyberspace Warfare for Training (CyWar-T) research program and is the organizational lead for S&T support to the Army's Synthetic Training Environment Cross Functional Team (STE CFT). Previously, he was the lead engineer for the STTC's Battlespace Visualization and Interaction (BVI) project wherein he led research and development activities focused on real-time, distributed mission planning using multi-modal devices. Mr. Vey is a Marine with operational experience training Signals Intelligence (SIGINT) collection and analysis operations. His military training consisted of Electronic Intelligence (ELINT), Electronic Warfare (EW), and Geospatial Intelligence (GEOINT). He holds a Bachelor of Science (B.S.) in Electrical Engineering from the Milwaukee School of Engineering.

A Cyberspace Effects Server for LVC&G Training Systems

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

J. Allen Geddes, Nathan Vey
US Army DEVCOM SC SED STTC
Orlando, Florida
james.a.geddes2.civ@army.mil, nathan.l.vey.civ@army.mil

INTRODUCTION

A quick scan of current news headlines is all it takes to observe that attacks in cyberspace are increasing in both frequency and impact. Two recent high-profile examples include the Colonial Pipeline ransomware attack, which disrupted fuel supply and distribution along the entire east coast of the United States (U.S.), and the SolarWinds supply-chain attack, which provided attackers with backdoor access to many U.S. Government agency networks and systems. The actors, motivations, sophistication, and techniques for these cyber attacks vary from attack to attack, but regardless of how and why the attacks occurred, the effects can be devastating.

To account for these types of cyberspace scenarios, the U.S. Army seeks to incorporate cyberspace attacks, effects, and their impacts into its live, virtual, constructive, and gaming (LVC&G) modeling and simulation (M&S) capabilities that it relies upon for training, analysis, experimentation, test and evaluation, intelligence, and acquisition programs. The Cyberspace Battlefield Operating System Simulation (CyberBOSS) research effort was initiated by the Army's Combat Capabilities Development Command - Soldier Center (DEVCOM SC) Soldier Effectiveness Directorate (SED) Simulation & Training Technology Center (STTC), to conduct research on innovative ways for replicating these cyberspace activities within existing M&S environments, and to help inform future M&S system requirements for the cyberspace domain.

Recent CyberBOSS development efforts have provided a framework to model cyberspace effects and cyberspace operations across federated LVC&G systems that may otherwise provide little to no native cyberspace modeling capabilities. The framework and models that we developed, and provide as a cyberspace Effects Server, enable rapid integration of modeling of these capabilities within those systems. We established an approach for the development, registration, and management of cyberspace effects models as a service within the CyberBOSS ecosystem. Our approach also can model the specific tactics, techniques, and procedures (TTPs) of the cyberspace operations employed to generate the attack effects, when that level of detail is necessary to meet the requirements of a particular exercise. This paper discusses our approach to provide an architecture and protocol for federated systems to request modeling of cyberspace effects and cyberspace operations from the service. The service, which uses an open framework and well-defined protocols, is designed to be extendible, so that additional cyberspace effect and operations models can be incorporated and offered for federation use to meet emerging training needs.

CYBERBOSS FEDERATION ARCHITECTURE

This section describes the overall CyberBOSS system architecture and its core components. The goal of the CyberBOSS architecture is to promote rapid integration of existing and emerging LVC&G systems, cyber ranges, and other cyberspace M&S tools to foster integrated training and analysis. The CyberBOSS system architecture, shown in Figure 1, is a Service Oriented Architecture (SOA) that uses well defined interfaces and protocols to facilitate system integration and future expansion. The architecture is flexible and extensible with an emphasis on adaptation to future cyberspace training and analysis needs. The goal of the CyberBOSS architecture is to support *cyber-for-others* training use cases, which represents leveraging cyber effects models and/or cyber ranges as a component in battle staff training against the impact of cyberspace operations on traditional kinetic operations, as well as training to use the cyberspace domain to enhance kinetic operations.

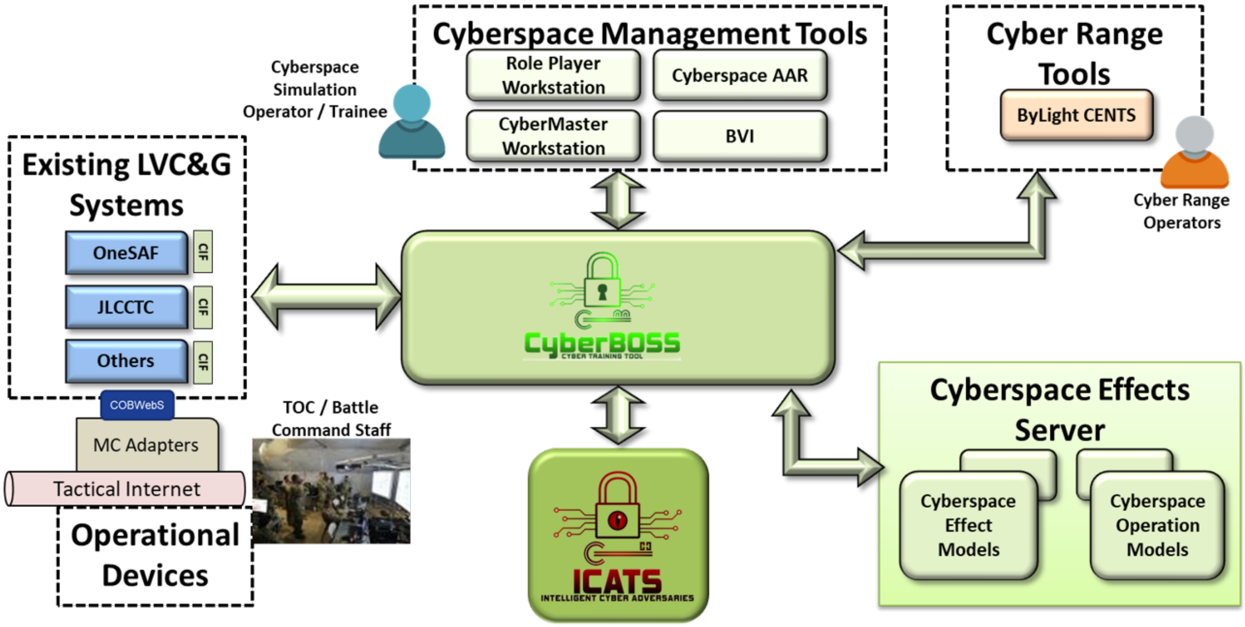

Figure 1. Flexible CyberBOSS system architecture based on SOA design patterns.

A wide variety of system types may interoperate through the CyberBOSS system architecture, including existing LVC&G systems (e.g., One Semi-Automated Forces (OneSAF) and Joint Land Component Constructive Training Capability (JLCCTC)), cyber ranges (e.g., ByLight CENTS), cyberspace effect and operation models (e.g., reconnaissance models, network models, or intelligent adversaries), and cyberspace effects tools (e.g., Cyber Operations Battlefield Web Services (COBWebS) [1] or Network Effects Emulation System (NE2S)). The CyberBOSS architecture delegates information between LVC&G systems and the cyber range to accomplish combined, cross-functional training using these disparate toolsets. CyberBOSS can also broker cyberspace effects across federated LVC&G systems during times when no cyber range is used. Additionally, tools such as cyber white cell controllers and after action review (AAR) data collection applications can integrate using the transparent nature of the system architecture. For example, the CyberBOSS Control Tool is a thin-client display solution that allows the cyber training facilitator to view and manage execution of the CyberBOSS scenario. Finally, adding external cyberspace effects models though an Effects Server may bring enhanced cyber functionality, such as automated cyber adversary modeling.

The CyberBOSS system architecture employs an open and transparent hub-and-spoke approach where client applications connect into a common, federated data bus that is managed by a centralized server. All client applications communicate using a common Cyberspace Data Model (CDM) representation to specify cyberspace-specific information (e.g., cyber attacks, cyber control, cyber status, etc.) [2]. The CDM builds upon existing cyber data models such as Cyber Operational Architecture Training System (COATS) [3] and the NE2S data models. CyberBOSS clients can send and receive CDM JavaScript Object Notation (JSON) messages directly using a messaging bus complaint with the open Advanced Message Queuing Protocol (AMQP) standard. Additionally, a Java library, termed the CyberBOSS Interface Framework (CIF), was developed that provides application programming interfaces (APIs) that clients may use to integrate with the CyberBOSS system architecture more rapidly. The CDM, and related CIF APIs, are extensible and are envisioned to grow as future systems are incorporated into the CyberBOSS architecture and new use cases emerge.

EFFECTS SERVER DESCRIPTION

The CyberBOSS Effects Server is a federate within the CyberBOSS federation. The Effects Server is used to model cyberspace effects that can be placed on simulated and real devices within the federation. The results of the cyberspace effects are delivered to the training audience through the interfaces of the simulation and through stimulation of tactical devices. The Effects Server utilizes an extensible architecture that allows for the incorporation of new cyberspace effects models that can be requested, instantiated, and provided as services to all CyberBOSS federates. The benefit to the approach is that the cyberspace effect modeling provided by the Effects Server can be reused across systems, minimizing the need to write additional code within each connected system.

Within the Effects Server, cyberspace effects can be modeled in two ways, as described below.

Direct creation of cyberspace effects

The Effects Server can directly create cyberspace effects on objects on behalf of CyberBOSS federates. Simulation systems connecting to CyberBOSS may not have internal modeling of cyberspace effects that they can apply to their associated simulated and real devices. When connected to the CyberBOSS federation, the simulation can request that a cyberspace effect, such as denial of service (DoS) or data injection, be applied to one or more of their simulated or real devices. The Effects Server can fulfill the request for cyberspace effects by modeling those effects directly and then providing the requesting simulation with the results of the effect modeling. Similarly, cyberspace effects may be placed on environmental objects such as buildings and utilities. Changes to the state of these objects due to cyberspace operations are modeled by the Effects Server, such as a cyber attack on a utility affecting connected buildings and devices. The resulting cyberspace effects are communicated to the federate modeling the environmental objects. A CyberBOSS federate can use this approach for direct modeling of cyberspace effects by the Effects Server if the federate does not need to model the specific steps of a cyberspace operation and is just interested in applying the resulting cyberspace effect to its modeled devices or environmental objects.

Creation of cyberspace effects through detailed modeling of cyberspace operation tactics, techniques, and procedures (TTP)

The Effects Server can also model cyberspace effects as a result of detailed modeling of the cyberspace TTPs that cause the effects. Simulation systems connected to CyberBOSS may require more detailed modeling of cyberspace operations, including modeling of the specific TTPs used to execute the cyberspace operation. For example, OneSAF may request a data exfiltration operation, but delegates modeling of the techniques and procedures associated with that operation to the Effects Server for modeling. Another example of this is found in the Intelligent Cyberspace Adversaries Tool Suite (ICATS), where simulated cyberspace adversaries may request that the Effects Server perform the modeling of the cyberspace techniques and procedures the adversaries use to execute their simulated cyberspace attacks. The models of cyberspace operation TTPs in the Effects Server are based on items from the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework [4]. Requests for modeling these cyberspace operations, along with their associated TTPs, can be sent to the Effects Server and the results of each TTP are communicated to the CyberBOSS federation. Upon completion of modeling each TTP comprising the cyberspace operation, the Effects Server will determine the resulting cyberspace effect. That effect is communicated to the federate modeling the target device. This approach is useful for simulation systems that require this detailed modeling of the specific TTPs used to produce the resulting effect.

The Effects Server and other CyberBOSS federates use well defined data interfaces to advertise cyberspace effect and operations modeling, request execution of models, and receive results of that modeling. The following section describes these data interfaces and the architecture of the Effects Server that supports their use.

EFFECTS SERVER ARCHITECTURE

The architecture of the Effects Server is shown in Figure 2. The Effects Server provides a framework for integration and execution of various cyberspace-related models. As described above, the Effects Server supports modeling of the specific TTPs of cyberspace operations and also supports modeling of cyberspace effects. As shown in Figure 2, the modeling framework in the Effects Server supports both classes of these cyberspace models. To support CyberBOSS clients that require detailed modeling of cyberspace operations, the Effects Server supports operational models at the tactic, technique, and procedure levels. To support CyberBOSS clients that require modeling at the effect level, the Effects Server supports cyberspace effect models for computer network operations and electromagnetic devices, and for environmental objects (e.g., power utilities, cellular towers). The Effects Server formalizes a protocol and data model for control, status, and reporting of its models, as described in the sections below. The modeling framework of the Effects Server is supported by a number of services. For example, the CyberBOSS client services allow communication of modeling requests and results between the Effects Server and other CyberBOSS federates.

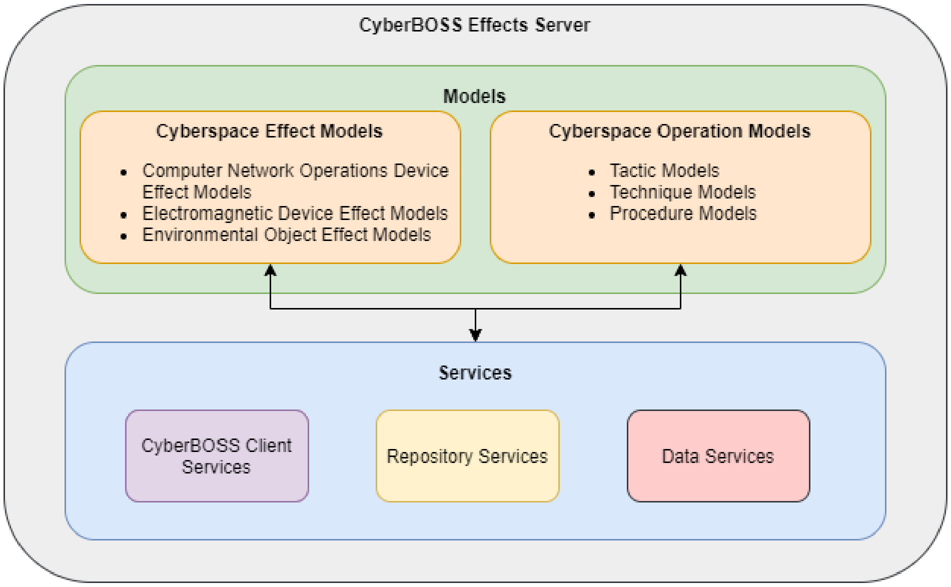
CyberBOSS Effects Server
Models
Cyberspace Effect Models
Computer Network Operations Device Effect Models
Electromagnetic Device Effect Models
Environmental Object Effect Models
Cyberspace Operation Models
Tactic Models
Technique Models
Procedure Models
Services
CyberBOSS Client Services
Repository Services
Data Services

Figure 2. Architecture of the CyberBOSS Effects Server, showing the cyberspace modeling framework and underlying supporting services.

INCORPORATION OF CYBERSPACE EFFECTS AND OPERATIONS MODELS

The Effects Server modeling framework allows for rapid development and integration of new cyberspace models to support emerging training and analysis use cases of CyberBOSS federates. The framework provides interfaces and services for incorporation of models, which can be provided as services across the federation. In this section, we describe the existing cyberspace effect and cyberspace operation TTP models provided by the Effects Server and show how each set of models can be expanded to meet future needs.

Cyberspace Effect Models

The Effects Server provides a set of cyberspace effect models for use within the CyberBOSS federation. As discussed above, these models do not consider individual cyberspace operation TTPs, but instead model the resulting effect of cyberspace actions on a simulated or real device. Examples of cyberspace effect models available in the Effects Server are shown in Table 1. These models all implement standardized interfaces within the Effects Server, promoting reuse and expansion as other effect models are added to the system.

Table 1. Example cyberspace effect models available in the Effects Server.

Cyberspace Effect Model	Description	Outputs
Delay of Service Effect Model	This models a delay of service cyberspace effect. This effect is the result of a cyber attack that degrades the functionality of a system, making that system's services unreliable for users. This type of effect may result from an attack where the attacker injects services onto the target system, such as a web server, and causes severe impact on legitimate services running on the system. Services such as inbound and outbound network traffic handling can be significantly delayed.	• Affected device(s) • Time and duration of effect • Inbound network traffic level • Outbound network traffic level • Duration of network traffic delay
Denial of Service Effect Model	This models a denial of service (DoS) cyberspace effect. This effect may be the result of a cyber attack that severely impacts a system, making that system's services unavailable to users. This type of effect may result from an attack where the	• Affected device(s) • Time and duration of effect

	attacker floods the target system, such as a web server, by sending massive amounts of traffic and the system is unable to be accessed by legitimate users.	• Inbound network traffic level • Outbound network traffic level
Eavesdropping Effect Model	This models an eavesdropping cyberspace effect. This effect may be the result of a man-in-the-middle (MitM) cyber attack, where the attacker intercepts communications between two parties to secretly eavesdrop on traffic traveling between the two. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.	• Affected device(s) • Time and duration of effect • Simulated intercepted data
Packet Manipulation Effect Model	This models a packet manipulation effect. This effect may be the result of an injection cyber attack, where the attacker gains access to the system and can inject falsified data to deceive users of the system. For example, attackers may inject packets with spoofed enemy location information so that the users of the system utilize incorrect information in determining courses of action.	• Affected device(s) • Time and duration of effect • Spoofed location • Spoofed location offset

Cyberspace Operations Models

The Effects Server also provides a set of cyberspace operations models for use within the CyberBOSS federation. As discussed above, these models consider individual cyberspace operation TTPs and the resulting effects of these actions on simulated or real devices. The Effects Server contains operation models at the tactic, technique, and procedure levels (based on the MITRE ATT&CK framework), with a hierarchical relationship between the models. Operation modeling is chained so that completion of lower-level procedure elements fulfill the larger goals of techniques, which in turn, fulfill goals of tactics. The operation procedure models are the lowest-level operation model. Examples of cyberspace operation procedure models available in the Effects Server is shown in Table 2.

Table 2. Example cyberspace operation procedure models available in the Effects Server.

Cyberspace Procedure Model	Description	Outputs
Login Attempt Procedure Model	This models a login attempt cyberspace operation procedure. This model considers the skill set of the simulated threat operator that is performing the operation, so that more skilled simulated operators will be more successful in gaining access to a targeted system. This modeled procedure can be categorized under the MITRE ATT&CK technique Brute Force: Password Guessing (ID: T1110.001), which falls under the ATT&CK tactic Credential Access (ID: TA0006). An example of this procedure is password guessing using the tool CrackMapExec.	• Device(s) attempted for login • Device(s) successfully compromised by login attempt
Malicious Payload Execution Procedure Model	This models a malicious payload execution cyberspace operation procedure. This model considers the skill set of the simulated threat operator that is performing the operation, so that more skilled simulated operators will be more successful in executing a malicious payload on the targeted system. This modeled procedure can be categorized under the MITRE ATT&CK technique System Services: Service Execution (ID: T1569.002), which falls under the ATT&CK tactic Execution (ID: TA0002). An example of this procedure using the PsExec module of Cobalt Strike to execute a payload on a remote host.	• Device(s) attempted for payload execution • Device(s) on which payload was deployed • Devices(s) on which payload was executed
Port Scan Procedure Model	This models a port scan cyberspace operation procedure. This model considers the skill set of the simulated threat operator that is performing the operation, so that more skilled simulated	• Device(s) that have active ports running

	operators will be more successful in executing a port scan on the targeted systems. This modeled procedure can be categorized under the MITRE ATT&CK technique Network Service Scanning (ID: T1046), which falls under the ATT&CK tactic Discovery (ID: TA0007). An example of this procedure using Cobalt Strike to perform port scans from an infected host.	common services (e.g., FTP, SSH, SQL)

Advertisement of Cyberspace Effect and Cyberspace Operation Models

For the Effects Server cyberspace effect and operation models to be used by other CyberBOSS federates, those models must first be advertised to the CyberBOSS federation. The Effects Server uses specific classes within the CDM that provide a well-defined protocol for this advertisement, so that the Effects Server modeling capabilities for cyberspace effects and operation TTPs are communicated to the CyberBOSS Server. As shown in Figure 3, these capabilities are stored by the CyberBOSS Server and used to delegate modeling of an effect or operation TTP when requested by a CyberBOSS federate (the Cyberspace Application Test Harness [CATH] in this example). Other federates may advertise modeling capabilities in a similar manner, and the CyberBOSS Server will delegate modeling according to the fidelity and parameters of the incoming modeling request. In this manner, federates may use models whose fidelities and implementations most closely match their use cases. Upon execution of the cyberspace effect model, the Effects Server returns the results of the model to the federate owning the simulated or real devices (One Semi-Automated Forces [OneSAF] in this example).

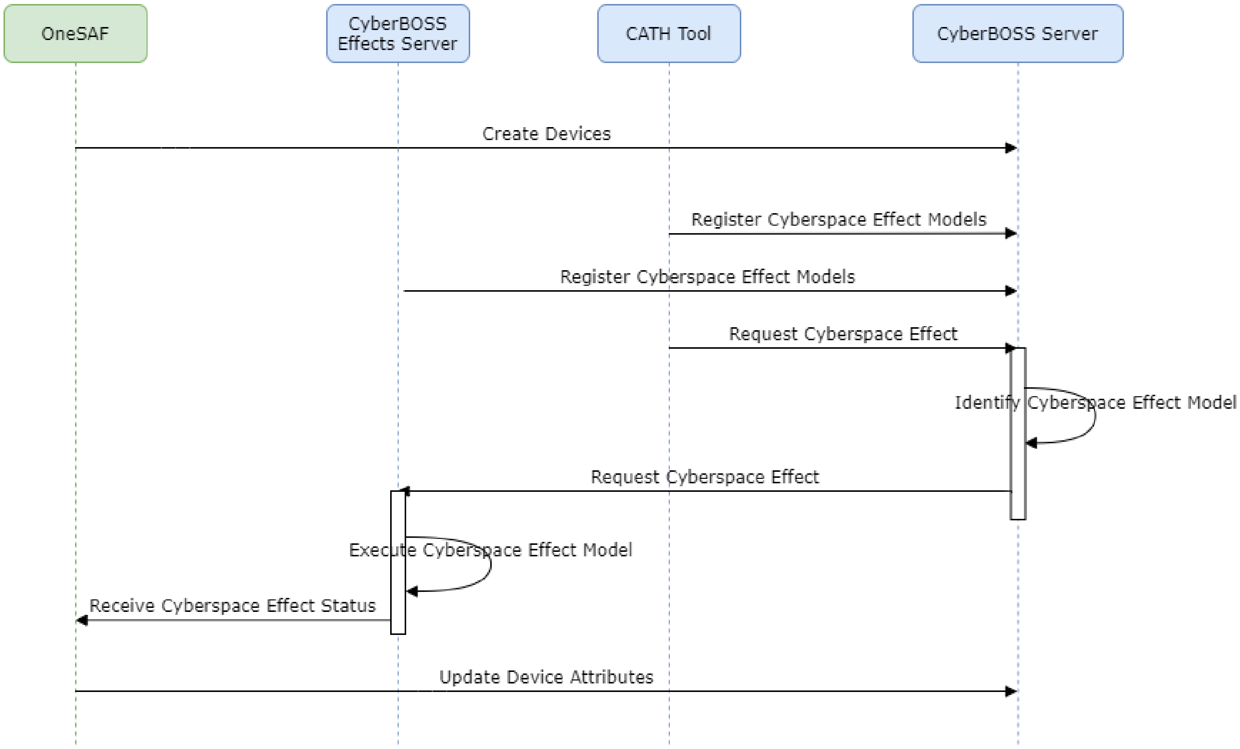
OneSAF
CyberBOSS Effects Server
CATH Tool
CyberBOSS Server
Create Devices
Register Cyberspace Effect Models
Register Cyberspace Effect Models
Request Cyberspace Effect
Identify Cyberspace Effect Model
Request Cyberspace Effect
Execute Cyberspace Effect Model
Receive Cyberspace Effect Status
Update Device Attributes

Figure 3. Advertisement and delegation of cyberspace effect models within the CyberBOSS federation.

Results of Cyberspace Effect and Operation Modeling

As the Effects Server models cyberspace effects and operations, it may periodically report back modeling results to the CyberBOSS federation. Those results may change over time, providing updates on device state, current operational information, and falsified or spoofed data to apply to the device. The Effects Server uses CDM classes for a well-defined protocol for communicating the effect and operation TTP modeling results to other CyberBOSS federates. As shown in Figure 3, the Effects Server publishes the results information, and that information is received by the federate owning the model for the affected devices. The receiving federate applies the effect results to its simulated or real devices and the resulting changes to the devices are published to the CyberBOSS federation. This mechanism of decoupling the modeling of the effect or operation TTP from application of the results of that modeling on the devices allows owning federates to apply the results according to what is most applicable to their use cases. For example, an owning federate may be interested in applying the results at a high fidelity or it may ignore the results altogether if the effect does not pertain to the level model modeling of that federate.

USING EFFECTS SERVER MODELS

This section describes examples of how the Effects Server modeling is used in within the CyberBOSS federation. We describe how the Effects Server's cyberspace effect and cyberspace operation TTP modeling are used to support more detailed modeling than is available in federated applications, and how these models can support simulation of cyberspace adversaries. We also discuss how the Effects Server supports visualization of cyberspace effects and operations within the simulated battlespace.

Detailed Modeling of Cyberspace Operations for OneSAF Devices

OneSAF contains some models of cyberspace operations and effects and these models are advertised to the CyberBOSS federation using the mechanism described above. However, some training use cases require modeling of cyberspace operation TTPs at a higher fidelity than these models provide. Higher fidelity modeling can take into account the specific techniques and procedures used to perform an operation, using results from each step as inputs to subsequent steps. For example, consider the case of a simulated data exfiltration attack on a simulated OneSAF device. In this example, requests may be made to the Effects Server to model various TTPs involved in the attack (e.g., initial threat access to the device, deployment of a rogue service on the device, engagement of that service to exfiltrate data to threat receivers). In this case, operation modeling requests for each TTP can be delegated from OneSAF to the Effects Server and the Effects Server returns results at each step of the TTP modeling chain. In this manner, OneSAF can incorporate the effects of each step in the TTP modeling chain if the training use case requires this high level of fidelity. This process can also be used to impart cyberspace effect and operations results on systems with no internal cyberspace models.

Support for Automated Cyberspace Adversaries

The ICATS capability provides semi-automated, intelligent cyberspace adversaries that act as a simulated cyberspace threat against simulated Blue Force (BLUFOR) networks and devices. ICATS simulated adversaries can use the CyberBOSS framework to interact with simulated and real devices controlled by OneSAF or other CyberBOSS federates. ICATS adversaries contain a planner, shown in Figure 4, which given an overall goal (e.g., discovery, compromise, exploitation), decides the detailed steps the adversary performs to accomplish the goal. The planner requests the modeling of specific cyberspace operation procedures in order to gather information and to gain required conditions to move through the goal-seeking process. Modeling requests can be made to models external to the ICATS adversary, such as to the cyberspace operation TTP models executing within the Effects Server. In the example shown in Figure 4, the Effects Server performs modeling of the cyberspace operation procedure and sends the results of that procedure to OneSAF for application to the affected device. The ICATS adversary will be notified of the device update and then move to its next stage of planning. This architecture allows ICATS to focus on the planning and execution aspects of adversary operations and leverages the existing external models of the Effects Server for modeling of the cyberspace operation details.

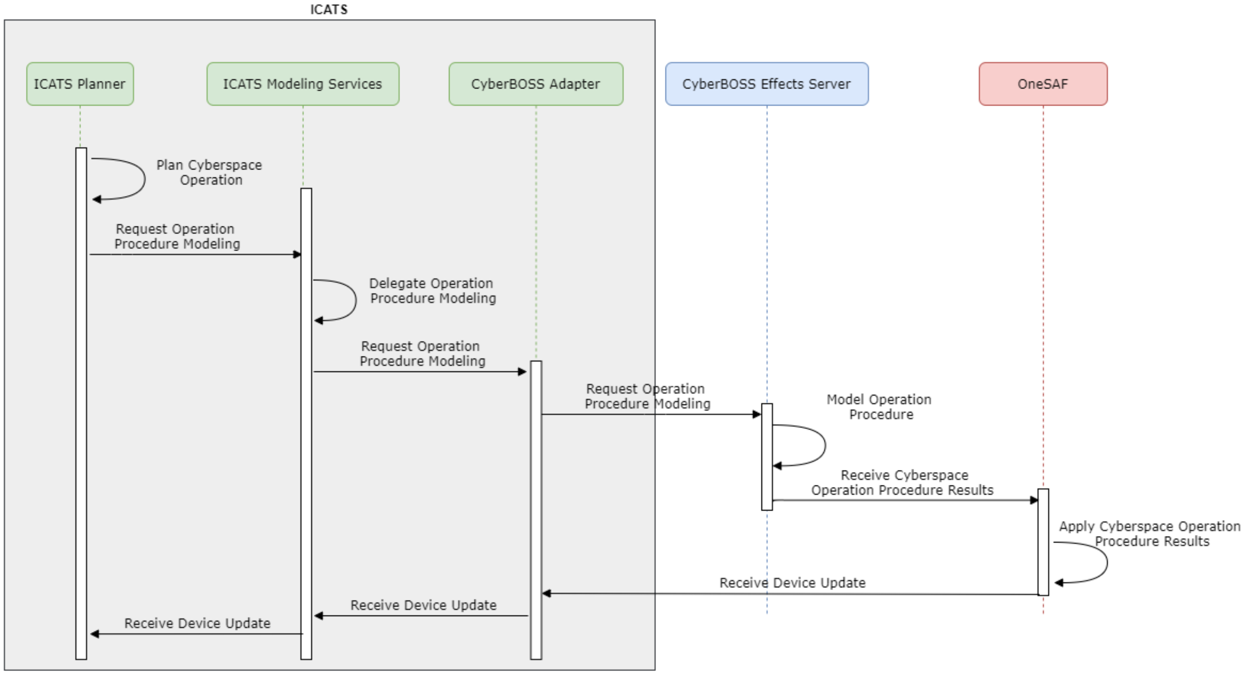
ICATS
ICATS Planner
ICATS Modeling Services
CyberBOSS Adapter
CyberBOSS Effects Server
OneSAF
Plan Cyberspace Operation
Request Operation Procedure Modeling
Delegate Operation Procedure Modeling
Request Operation Procedure Modeling
Request Operation Procedure Modeling
Model Operation Procedure
Receive Cyberspace Operation Procedure Results
Apply Cyberspace Operation Procedure Results
Receive Device Update
Receive Device Update
Receive Device Update

Figure 4. ICATS adversaries request modeling of cyberspace operation procedures by the Effects Server.

Visualization of Cyberspace Effects and Operations

As part of our CyberBOSS research effort, we designed and prototyped a cyberspace visualization scheme to visualize cyberspace-related information sent from the CyberBOSS federation to the STTC's Battlespace Visualization and Interaction (BVI) tool [5]. BVI provides both two- and three-dimensional visualization of the battlespace for training of mission planning and execution tasks. Our team designed and developed ways to visualize cyber information and effects and to develop control mechanisms in the BVI multi-modal ecosystem. An example of the visualization of cyberspace related objects and effects in BVI is shown in Figure 5. This example demonstrates how BVI uses 2525C symbology but decorates that symbology to indicate the state of cyberspace related elements. BVI is able to visualize the state of the cyberspace operations and effects in the scenario, such as those modeled by the Effects Server. For example, in Figure 5, labels placed above the 2525C symbology indicate the state of cyberspace operations or effects that have been applied to the actor. For example, a white label of IDENT indicates that the actor's device has been discovered by a reconnaissance operation. A red label of DOS indicates that the device is currently undergoing a simulated denial of service (DoS) operation from a threat actor. This visualization provides the training audience with a clear indication that entities and units under their control are impacted by cyberspace operations and improves mission readiness in understanding the relationship between these operations and kinetic domain tactics and operations.

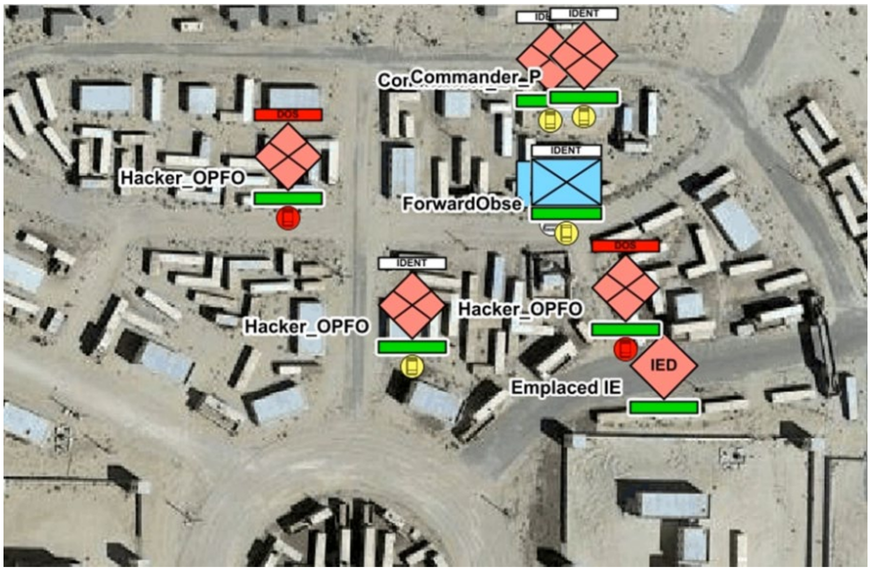

Figure 5. Visualization of cyberspace objects and effects in the BVI system.

FUTURE WORK

Research is continuing on CyberBOSS with plans to extend the cyberspace terrain modeling and representation for additional cyberspace related effects and devices. Below, we discuss a few of the most prominent additions.

- **Simulated Network Modeling** – Addition of status and control extensions to the CDM to incorporate simulated network models. This will allow for systems to accurately create, control, and simulate cyber-capable network models to incorporate accurate responses to cyber effects and events without investment in costly network model integration. Network modeling allows the creation and control of proxy network models for accurate cyberspace effects for kinetic simulation systems.
- **Radio Frequency (RF) Domain** – This entails the addition of cyberspace terrain representations to support RF-connected cyberspace elements. RF element representation is the basis for the planned addition of Global Positioning System (GPS) and Position, Navigation, and Timing (PNT) models and representations for LVC&G cyber based effects. In addition, it facilitates our addition of Cyber Electromatic Activities (CEMA) models and representation in order to encompass a larger range of cyberspace elements in support of MDO training.
- **Information Operations (IO)** – Addition of CDM extensions and services to support modeling of Information Operations information for LVC&G training tasks. This would serve to provide the IO domain to facilitate MDO training tasks.
- **AI/ML Assessments** – Addition of Artificial Intelligence/Machine Learning (AI/ML) analytics and modeling in order to incorporate cyberspace models, analytics, and operator control/status for cyberspace exercises.

RECOMMENDATIONS

We have several recommendations for continued research, development, and testing of the CyberBOSS Effects Server to promote its expansion to meet training needs within LVC&G environments. Those recommendations include:

1. As described in the Future Work section above, we recommend expanding the modeling and representations of the cyberspace terrain within CyberBOSS to several novel areas, including simulated network modeling, increased representation of RF devices, and IO. Each of these areas will require additional cyberspace effects and operations models to be developed within the Effects Server. Additionally, the architecture and underlying services of the Effects Server may need to be enhanced to meet any new dependencies of these models. For example, IO effect models may need additional services to correlate actors within the IO terrain.
2. We recommend validation of the cyberspace effects and operation models within the Effects Server. Our work has been focused on developing the architecture and underlying services of the Effects Server and the developed models have been used as basic representation of cyberspace effects and operations. Validated models should be developed and deployed within the Effects Server for more realistic modeling of the cyberspace domain. However, currently, these validated models are not yet available.

3. We recommend building more variability into the Effects Server cyberspace effects and operations models, to better model differences in behavior and abilities of threat adversaries. For improved realism, the models within the Effects Server should consider several levels of capabilities of the actors performing each modeled effect or operation. Skilled adversaries should have better results of modeled cyberspace operation procedures than amateur cyber attackers. The current Effects Server models do have some distinction in this area to consider the skill level of the threat, however this capability should be expanded in future work.

CONCLUSION

As described throughout this paper, the CyberBOSS research effort helps the U.S. Army incorporate cyberspace attacks, effects, and their impacts into its existing LVC&G M&S capabilities, and will help to inform future M&S system requirements for the cyberspace domain. With the addition of the CyberBOSS Effects Server, CyberBOSS can provide cyberspace attack effects to requesting CyberBOSS-connected systems. This allows CyberBOSS to model the specific techniques and procedures employed to generate the attack effects, when that level of detail is necessary to meet the particular exercise's requirements. By enabling the Army to incorporate cyberspace attacks, effects, and impacts into its LVC&G environments at the appropriate level of resolution and fidelity, the Army can better prepare its forces to operate and succeed in the constantly evolving complex modern battlefield facilitating MDO training.

REFERENCES

[1] 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).*

[2] Hasan, O., Welch, J., Burch, B., Vey, N., Geddes, J.A., & Hofstra, K. (2020). CyberBOSS Common Data Model. *Simulation Interoperability Standards Organization (SISO) Simulation Innovation Workshop (SIW).*

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

[4] The MITRE Corporation, 2020, <https://attack.mitre.org/>

[5] Vey, N., Markuck, C., Raby, Y., & Amburn, C. (2018). An Architectural Overview of the Augmented REality Sandtable (ARES). *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).*