Incorporating Simulated Cyberspace Effects on Navy Shipboard Systems during Training

Omar Hasan, Ph.D., Derek Crane, Gregory Dukstein
Dignitas Technologies, LLC
3626 Quadrangle Blvd., Suite 100
Orlando, FL 32817
ohasan@dignitastechnologies.com, dscrane@dignitastechnologies.com, gdukstein@dignitastechnologies.com

Keywords:
Cyber, Cyberspace, Cyber Effects, Training, Information Operations, Shipboard Applications, Electronic Warfare

ABSTRACT: Increasingly, Great Power Competitor’s (GPC) Signal Intelligence (SIGINT) teams are focusing on the disruption of intelligence, surveillance, and reconnaissance (ISR) capabilities as one step in a complex kill chain used to track, target, manipulate, and disable U.S. Navy assets. To disrupt Navy mission operations, adversaries actively pursue methods in cyberspace and electronic warfare (EW) such as internet protocol (IP)-based cyber attacks and electromagnetic spectrum (EMS)-based attacks, including jamming and spoofing. For example, recently, adversaries spoofed shipboard identification system tracks for North Atlantic Treaty Organization (NATO) and Swedish warships, causing them to appear in Russian waters. Naval battle staffs need training which considers cyberspace effects as warfare threats, in line with the traditional kinetic effects that affect warfighting operations.

Existing live, virtual, constructive, and gaming (LVC&G) systems are not developed to incorporate offensive and defensive cyberspace operations as a part of combined training. During Fleet Synthetic Training (FST) events, trainees within virtual and live ships interact with actors simulated by constructive systems within the Navy Continuous Training Environment (NCTE). This paper describes a novel system architecture, termed the Cyber Simulation TRaining for Impacts to Kinetic Environment (CyberSTRIKE), we developed to incorporate simulated cyberspace effects within this complex environment using a flexible integration approach. CyberSTRIKE communicates cyberspace effects to Navy simulation systems and shipboard command, control, communications, computers, and intelligence (C4I) systems. We describe the CyberSTRIKE architecture’s data models, services, and interfaces to communicate cyberspace effects to NCTE systems so that generated cyberspace effects have an operational impact on the shipboard C4I interfaces through which the Naval trainees interact. This approach represents a significant improvement over current methods used to communicate cyberspace effects to the training audience since it does not rely on out-of-game communications and promotes identification and mitigation of cyberspace effects by the targeted training audience.

1 Introduction

Increasingly, Great Power Competitor’s (GPC) Signal Intelligence (SIGINT) teams are focusing on the disruption of intelligence, surveillance, and reconnaissance (ISR) capabilities as one step in a complex kill chain used to track, target, manipulate, and disable Naval assets. To disrupt Navy mission operations, adversaries actively pursue methods in cyberspace and electronic warfare (EW) such as internet protocol (IP)-based cyber attacks and electromagnetic spectrum (EMS)-based attacks, including jamming and spoofing. For example, recently adversaries spoofed shipboard identification system tracks for North Atlantic Treaty Organization (NATO) and Swedish warships, causing them to appear in Russian waters, disrupting battlespace situational awareness (SA). It is imperative that Naval commanders understand and train against SIGINT threats by including the cyberspace domain in their operational approach to the modern Naval battlespace. Adequate training is necessary to ensure that Naval commanders are prepared to make offensive and defensive decisions that incorporate the cyberspace domain to achieve information advantage.

Naval battle staffs require training which considers cyberspace effects as warfare threats, in line with the traditional kinetic effects that affect warfighting operations. This type of cyberspace training, termed cyber-for-others, does not
focus on training tasks that are performed by cyber warriors to detect, defend against, or conduct cyber attacks. Instead, it represents leveraging cyber effects models and/or cyber ranges as a component in battle staff training against the impact of cyber on traditional kinetic operations, as well as training to use cyber to enhance kinetic operations. Existing Naval live, virtual, constructive, and gaming (LVC&G) systems are not developed to incorporate offensive and defensive cyberspace operations as a part of combined training. During Fleet Synthetic Training (FST) events, trainees within virtual and live ships interact with actors simulated by constructive systems within the Navy Continuous Training Environment (NCTE). However, these NCTE systems have limited representation of the cyberspace domain. Our work seeks to improve current Naval command staff cyberspace training by providing cyberspace effects directly on the shipboard systems through which the training audience interacts, improving realism and promoting the use of cyberspace offensive and defensive tactics as part of a multi-domain operations (MDO) battlespace strategy.

2 Approach

To meet this training need, we developed a system architecture, termed the Cyber Simulation TRaining for Impacts to Kinetic Environment (CyberSTRIKE), which incorporates simulated cyberspace effects within this complex environment using a flexible integration approach. Our team is developing and prototyping the CyberSTRIKE architecture through a Small Business Innovation Research (SBIR) effort under the Navy’s Office of Naval Research (ONR). CyberSTRIKE is government purpose rights (GPR) software that communicates cyberspace effects requested by the white cell or due to cyber range battle damage assessment (BDA) to Navy simulation systems and connected shipboard command, control, communications, computers, and intelligence (C4I) systems.

Our approach uses the CyberSTRIKE architecture’s data models, services, and interfaces to communicate cyberspace effects to NCTE systems so that generated cyberspace effects have an operational impact on the shipboard C4I interfaces through which the Naval trainees interact. This approach represents a significant improvement over current methods used to communicate cyberspace effects to the training audience (i.e., white cards, chat) since it does not rely on out-of-game communications. Instead, it injects, modifies, or stops information flow to shipboard C4I systems, allowing realistic visualization of effects and promoting identification and mitigation of cyberspace effects by the targeted training audience. In the sections below, we describe our design and development of the CyberSTRIKE architecture to affect tactical messaging sent to connected Naval C4I systems to create a range of EW and cyberspace effects, visible to the training audience on the C4I interfaces. We describe our prototyping efforts with this architecture to demonstrate its feasibility to provide effects on two C4I interfaces. Our prototyping has shown that realistic cyberspace effects can be manifested on these systems and provides the groundwork for future efforts to incorporate additional effects and other Naval C4I systems into this architecture. This approach will greatly improve Naval command staff training of offensive and defensive cyberspace domain operations in the modern warfighting environment.

3 Analysis

In our initial work [1], we identified several cyberspace effects applicable to Navy shipboard C4I systems used during FST. For each identified cyberspace effect, we described the effect, its outputs, and the expected experience for the shipboard training audience. The identified cyberspace effects provide varying experiences for the training audience. Some of these effects produce results that are obvious to the training audience, such as missing or misidentified tracks, so they are suited to novice trainees. Other effects have more subtle perceivable results for the training audience and are therefore better suited to more experienced trainees. For each effect we considered, we classified the system interfaces used by the training audience to determine the effect applicability to those systems. We described the possible impact to Navy C4I system interfaces and assigned a severity level to the effect, where high severity effects have a greater impact on the shipboard training audience. We also suggested some possible training goals and responses for the training audience for each effect.

In this initial work, we also analyzed shipboard C4I system interfaces used by the training audience and considered how each of these effects could be applied. Due to the large number of possible effects and target C4I systems, there
are many combinations of effects/systems that can be targeted. Effect sub-categories magnify the possible development options. For example, data manipulation effects can result in a vast number of perceived changes on targeted devices since various fields within C4I message protocols can be altered. This analysis served as input to our initial prototype design and development. For each identified effect and shipboard system, we designed the implementation of the effect across all elements of the CyberSTRIKE prototype to ensure the effect is perceivable in a realistic manner on the target virtual C4I systems. In this paper, we describe how this analysis was used to support the design of cyberspace and EW effects against two C4I-related Naval systems. For each of these systems, we designed and prototyped a variety of effects, including jamming, data injection, and data manipulation, as described in the sections below.

4 Architecture

During FST events and other training exercises, trainees interact with platforms and entities simulated by constructive systems within the NCTE. The NCTE connects Navy Training Baseline (NTB) applications, such as the Joint Semi-Automated Forces (JSAF) system and the Joint Simulation Bus (JBUS), to affect shipboard trainees located within vessels located pier-side (termed a virtual ship) or located at sea (termed a live ship). We developed the CyberSTRIKE technical architecture, which integrates cyberspace effects within this complex environment based on the use of a flexible integration approach. This architecture is used to produce and communicate cyberspace effects to various systems within the NCTE, so that cyberspace effects injected using a white cell interface have an operational impact on the shipboard command C4I interfaces through which the Naval trainees interact during the exercise. At the heart of this architecture is the Cyberspace Battlefield Operating System Simulation (CyberBOSS) cyberspace integration framework [2, 3]. Through ongoing research efforts under the US Army Combat Capabilities Development Command (DEVCOM), we continue to develop CyberBOSS to provide a cyberspace data model (CDM), software interfaces, cyberspace models, and user interfaces to communicate cyberspace domain elements between simulation systems and other cyberspace toolsets [4].

The high-level architecture for the CyberSTRIKE prototype is shown in Figure 4.1. CyberSTRIKE consists of several components, including the cyberspace integration framework (CyberBOSS) and its applications and NCTE applications (e.g., JSAF, JBUS). This architecture does not modify shipboard C4I systems, and instead injects, modifies, or stops tactical messages between those systems and the simulation to produce a resulting cyberspace effect. In Figure 4.1, existing components of the NTB baseline are shown in orange, while components new to the NTB baseline are shown in green. NTB components modified for CyberSTRIKE are shown in blue. Black boxes indicate system boundaries and depict how this solution can be deployed across multiple host systems. Descriptions of components that include additions or modifications to the NTB baselines versions are given in Table 4.1. This architecture employs various mechanisms for communication between components. First, the JSAF and JBUS components communicate over High-Level Architecture (HLA) Runtime Infrastructure (RTI) services using the Navy Training Federation (NTF) version 7.0 federation object model (FOM). This communication mechanism and protocol currently exists within the NTB and is used commonly in training exercises. Second, ActiveMQ is used as a messaging bus to support communication within the CyberSTRIKE federation. This allows CyberSTRIKE federates (e.g., CyberBOSS Server, the CyberBOSS Effects Server, JBUS) to communicate using Advanced Message Queuing Protocol (AMQP) to exchange JavaScript Object Notation (JSON) formatted messages. Third, the CyberSTRIKE Control Tool communicates with the CyberBOSS Server using Hypertext Transfer Protocol (HTTP) using a web socket connection.
In this architecture, various shipboard C4I systems can be connected to JBUS to visualize tracks associated with JSADF constructive ships. In our current prototyping, we are focusing on two C4I systems for incorporation of cyberspace effects. First, Over-The-Horizon Targeting Gold (OTH-GOLD) messages are sent to shipboard systems for visualization of JSADF-simulated Naval vessel tracks. Second, Distributed Interactive Simulation (DIS) messages can be sent to the Automated Scriptor Simulator Exercise Trainer (ASSET) to communicate shipboard identification information for JSADF-simulated commercial vessels. Cyberspace effects communicated from CyberSTRIKE to JBUS are implemented on the message protocols sent to these systems for visualization of cyberspace effects by the training audience. Additional shipboard C4I systems will be included in this architecture in future work.

Table 4.1. Prototype development involves additions/modifications to various systems within the NCTE.

<table>
<thead>
<tr>
<th>Description</th>
<th>Additions or Modifications within NCTE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CyberBOSS Server</strong></td>
<td>Provides the integrating cyberspace data model, architecture, and services used to communicate cyberspace effect requests and results between systems within the federation</td>
</tr>
<tr>
<td><strong>CyberBOSS Control Tool</strong></td>
<td>Allows visualization of the cyberspace terrain for the common operating picture (COP). Provides user interfaces for injecting cyberspace effect requests into the simulation.</td>
</tr>
<tr>
<td><strong>CyberBOSS Effects Server</strong></td>
<td></td>
</tr>
</tbody>
</table>
Provides modeling of cyberspace effects. Receives cyberspace effect requests from federates and provides effect results as effects are on-going.

Potential additions/modifications to cyberspace effect models to support identified set of effects and target Navy C4I systems

**JBUS**

Instance of JBUS running a new JBUS CyberBOSS plugin, which allows JBUS to function as a federate within the CyberSTRIKE federation. JBUS may contain new and modified filters and manipulators to provide implementation of cyberspace effects prior to sending messages to C4I and combat system JBUS plugins.

New JBUS CyberBOSS plugin development. Potential additions/modifications to JBUS filters and manipulators to support identified cyberspace effects. Potential updates to existing JBUS plugins.

5 Prototyping Efforts

This section describes some of the CyberSTRIKE prototype activities we performed to demonstrate the feasibility of this approach to introduce cyberspace effects into the Navy training environment. In our prototyping, we performed development of various areas of functionality within our architecture, including: 1.) communication of simulated platforms from JSAF to JBUS and CyberSTRIKE, 2.) communication of simulated C4I devices from JSAF to JBUS and CyberSTRIKE, 3.) communication of cyberspace effect information from CyberBOSS to JBUS, and 4.) communication of cyberspace effects from the CyberBOSS JBUS plugin to JBUS C4I-related plugins. Our prototyping used JSAF scenarios that contain Navy and threat ships and aircraft, as well as commercial vessels, that provide simulated platforms and their associated simulated C4I devices. In the sections below, we describe examples of our prototyping of simulated cyberspace effects against both Naval systems and commercial systems.

5.1 Simulated Cyberspace Effects on Naval Command and Control (C2) Systems

In our initial prototyping [1], we designed the mechanism to communicate simulated command and control (C2) devices from JSAF to CyberBOSS. In this design, information about JSAF simulated C2 devices is received by the CyberBOSS JBUS plugin and communicated to the CyberSTRIKE federation using CDM objects. JSAF-simulated C2 devices appear as CDM computer network operations (CNO) devices within the CyberSTRIKE federation and are visualized within the CyberSTRIKE Control Tool user interface. This allows the user to select a particular JSAF C2 device as the target of a cyber attack. We also designed and developed methods to communicate cyberspace effect information between the CyberSTRIKE federation and JBUS. Within our new CyberBOSS JBUS plugin, CDM cyberspace effect status messages are received from the CyberSTRIKE federation and information in those messages is communicated to C4I-related JBUS plugins to implement the effect on messages sent to connected C4I systems. This occurs through translation of the CDM messages into JBUS Common Data Definition (CDD) messages or through changes to JBUS filters and manipulators associated with the C4I-related JBUS plugins. These communication mechanisms between the CyberBOSS JBUS plugin and C4I-related JBUS plugins allow implementation of a wide range of cyberspace effects, including data injection, data manipulation, denial of service (DoS), and jamming.

The C2 system we targeted for cyberspace effects in this work is used to communicate battlespace SA across various echelons during warfighting. In this section, we describe our use of these mechanisms to produce cyberspace effects on JSAF-simulated C2 devices which affects the OTH-GOLD messages communicated to the shipboard C2 systems used by the trainees. To implement cyberspace effects on messages output by the C2 plugin, various JBUS filters and manipulators are utilized. The specific filter or manipulator used depends on the cyberspace effect to be implemented. We prototyped the use of JBUS filters and manipulators to implement various specific cyberspace effects on simulated C2 systems, including data injection, data manipulation, and DoS, to affect the OTH-GOLD messages communicated to shipboard C2 devices. Upon execution of a cyberspace effect though altering or stopping OTH-GOLD messages received by the shipboard C2 device, a range of results can be visualized by the trainee, including stale, duplicated (ambiguous), or mis-located tracks.
As an example, we prototyped packet manipulation cyberspace effects on simulated C2 devices. The packet manipulation effect used in our prototyping is a specific class of data manipulation effect that alters fields in the OTH-GOLD messages sent by the devices, such as its location, force identifier, or track category. For example, in the OTH-GOLD POSITION (POS) set, our prototype currently alters the fields shown in Table 5.1 during a packet manipulation effect and additional fields may be added in future work. Similarly, fields in the OTH-GOLD CONTACT (CTC) set can also be altered during this effect. This effect simulates a man-in-the-middle (MitM) attack, in which a cyber threat force alters information sent within Navy tactical networks. The operational result of this effect is that tracks from the affected simulated C2 device are incorrectly communicated to the C2 network, appearing with modified locations or with incorrect symbology on the receiving C2 system. Figure 5.1 shows the CyberSTRIKE Control Tool during execution of a packet manipulation cyberspace effect in which the reported location of the sending ship is being modified by the threat actor. The actual (ground truth) position of the simulated USS Mahan (using call sign MAHAN) destroyer is shown on the right side of the figure, and a purple line is drawn between the position and the altered reported position of the ship to the south west. This map view provides a clear indication for exercise facilitators to understand the ship currently targeted by this cyberspace effect and graphically indicates the difference between the ships ground truth and reported positions. While this effect is on-going, the track for the MAHAN appears as a valid track on the C2 user interface, however located at the manipulated position specified in the cyberspace effect. This is a significant improvement over current cyber-for-others training for the command staff since it provides an opportunity for the trainee to identify anomalous track positions and consider if those anomalies are the result of a threat attack against Naval systems. Additionally, this provides stimulation by which the command staff can train to mitigate this type of cyber attack against shipboard systems.

![Figure 5.1. CyberSTRIKE Control Tool map displays both ground truth and altered ship reported location during OTH-GOLD packet manipulation effect execution.](image)

### Table 5.1. Fields in the OTH-GOLD POS message set altered during packet manipulation effects.

<table>
<thead>
<tr>
<th>Field Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Latitude of Center</td>
</tr>
<tr>
<td>4</td>
<td>Longitude of Center</td>
</tr>
<tr>
<td>9</td>
<td>Course</td>
</tr>
<tr>
<td>10</td>
<td>Speed</td>
</tr>
<tr>
<td>11</td>
<td>Altitude/Depth</td>
</tr>
</tbody>
</table>

5.2 Simulated Cyberspace Effects on Commercial Shipboard Identification Systems

Another set of C4I-related systems we targeted in this work is commercial shipboard identification systems. These systems act like a transponder, operating in the Very High Frequency (VHF) spectrum, communicating information
such as the ship name, course, speed, classification, call sign, and registration number. In this work, we simulate
cyberspace attacks against commercial shipboard identification systems, including jamming, data injection, and data
manipulation. These attacks seek to provide the Naval trainee with a confusing or inconsistent picture of commercial
maritime traffic, impeding their ability to execute battlespace operations.

Similar to the methods described above to implement cyberspace effects on shipboard C2 systems, we used JBUS
filers, manipulators, and CDD messages to produce cyberspace effects on JSAF-simulated shipboard identification
devices for commercial vessels. Within the NCTE, commercial shipboard identification messages are
communicated to the training audience by adding tracks within the C2 network. DIS Entity State Protocol Data Units
(PDU) are produced by JBUS for JSAF commercial ships and those PDUs are received by ASSET. ASSET then
creates OTH-GOLD messages based on the PDU data and adds those messages to the Navy C2 network so that
commercial vessel tracks are viewed on shipboard C2 devices. To implement various cyberspace effects, we altered,
stopped, and injected DIS Entity State PDUs sent by JBUS to ASSET utilizing JBUS filters and manipulators. The
specific filter or manipulator used depends on the cyberspace effect to be implemented. We prototyped the use of
JBUS filters and manipulators to implement various specific cyberspace effects on simulated shipboard identification
systems, including point and areal jamming, packet manipulation, and packet injection, to affect the OTH-GOLD
messages communicated to shipboard C2 devices representing commercial vessel tracks. As described above, upon
execution of a cyberspace effect though altering or stopping OTH-GOLD messages received by the shipboard C2
device, a range of results can be visualized by the trainee, including stale, duplicated (ambiguous), or mis-located
tracks.

As an example, we prototyped areal jamming cyberspace effects on simulated shipboard identification devices by
stopping the sending of DIS Entity State PDUs for commercial vessels within a jammed area. This simulates actions
in the battlespace in which a cyber threat force jams shipboard identification signals within a geographic region,
disrupting the Naval view of commercial vessel traffic in that area, potentially affecting the ability to conduct Naval
operations. The operational result of this effect is that tracks from the affected simulated shipboard identification
devices are not communicated to the C2 network, causing missing or stale (time-late) tracks on the receiving C2
system. Figure 5.2 shows the CyberSTRIKE Control Tool during execution of an areal jamming cyberspace effect
that is affecting shipboard identification reporting for commercial vessels within a geographic region. Jammed
shipboard identification devices are shown with a yellow label. This map view provides a clear indication for exercise
facilitators to understand the ships currently targeted by this cyberspace effect. While this effect is on-going, tracks
for the jammed commercial ships appear stale (time-late) on the shipboard C2 system and stop periodically updating
their positions. This provides an opportunity for the trainee to identify issues with commercial track reporting as a
potential cyber threat to Navy systems.
Future Work

This work represents a significant improvement to current Naval battle staff training by incorporating the cyberspace domain into the traditional kinetic training environment. This provides opportunities for command staff to identify and mitigate the effects of threat cyberspace and EW attacks against Navy shipboard systems. It also allows training to use cyber and EW operations to enhance current Naval offensive tactics. To meet current and emerging training needs, the CyberSTRIKE system is envisioned to be expanded and refined over time to incorporate other and more complex cyberspace and EW effects, additional targeted shipboard systems, and new training use cases. Future work to develop CyberSTRIKE to incorporate cyberspace domain effects during Navy training may include:

- Further analysis, in conjunction with Fleet Information Warfare (IW) subject matter experts (SME) to determine specific cyberspace and EW effects and ships’ systems on which to focus additional development
- Refinement of CyberSTRIKE system and software designs to support identified cyberspace effects and connected systems, including the communication of cyberspace effects using additional tactical message protocols
- Further development of the CyberSTRIKE prototype, to include additional connected shipboard C4I systems and Naval simulation components
- Investigation of application of cyberspace effects on shipboard combat systems
- Design and development of interfaces to cyber ranges, promoting coordinated training of Naval cyber teams and Naval command staff in offensive and defensive cyberspace operations

Conclusion

Existing Naval LVC&G training systems are not developed to incorporate offensive and defensive cyberspace operations as a part of combined training. This work seeks to improve current Naval command staff cyberspace domain training by providing cyber and EW effects directly on the shipboard systems through which the training audience interacts, improving realism and promoting the use of cyberspace offensive and defensive tactics as part of a MDO battlespace strategy. To meet current and emerging cyberspace training needs, we developed the CyberSTRIKE system architecture that incorporates simulated cyberspace and EW effects within the complex Naval training environment using a flexible integration approach. CyberSTRIKE communicates cyberspace and EW effects injected by exercise facilitators or due to cyber range BDA to Navy simulation systems and connected shipboard C4I systems. Our approach uses the CyberSTRIKE architecture’s data models, services, and interfaces to communicate
cyberspace effects to NCTE systems so that generated cyberspace effects have an operational impact on the shipboard C4I interfaces through which the Naval trainees interact. This approach represents a significant improvement over current methods used to communicate cyberspace effects to the training audience (i.e., white cards, chat) since it does not rely on out-of-game communications. Instead, it injects, modifies, or stops information flow to shipboard C4I systems, allowing realistic visualization of effects and promoting identification and mitigation of cyberspace effects by the targeted training audience.

In this paper, we described our design and development of the CyberSTRIKE architecture to affect tactical messaging sent to connected Naval C4I systems to create a range of EW and cyberspace effects, visible to the training audience on the C4I interfaces. In our prototyping efforts with this architecture, we demonstrated its feasibility to provide effects on two C4I-related systems. Our prototyping has shown that realistic cyberspace effects can be manifested on these systems and provides the groundwork for future efforts to incorporate additional effects and other Naval C4I systems into this architecture. This approach will greatly improve Naval command staff training of offensive and defensive cyberspace domain operations in the modern warfighting environment.

8 Acknowledgements

We would like to thank Ms. Natalie Steinhauser and her team at the Office of Naval Research (ONR) for their assistance with this paper and for their support of our research efforts.

9 References


Author Biographies

DR. OMAR HASAN is currently the chief software architect at Dignitas Technologies, where he serves as the principal investigator on cyberspace-related research efforts. Dr. Hasan has 23 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.

MR. DEREK CRANE is the technical lead for this research. He has 13 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.

MR. GREGORY DUKSTEIN has over 25 years of experience in modeling and simulation applications, with a focus on terrain services, terrain databases, and modeling behaviors. Mr. Dukstein has worked CGF applications, SAF database formats, and terrain services for CCTT, UKCATT, Warfighters Simulation (WARSIM), and Synthetic Environment Core (SE Core). Mr. Dukstein has been involved in large programs and smaller efforts filling roles such as software developer, systems engineer, team lead, and Chief Engineer. Mr. Dukstein is currently the Director of Engineering at Dignitas Technologies where he manages research and development projects for PEO STRI, U.S Army DEVCOM, and the Office of Naval Research. Mr. Dukstein holds a B.S. in Electrical/Computer Engineering from Kansas University.