Automated Coordination of Non-Kinetic Effects for Multi-Domain Operations Training

The Multi-Domain Operations (MDO) warfighting concept describes how U.S. forces fight across all domains - air, land, sea, space, and cyberspace. Within the cyberspace domain, adversaries conduct Internet Protocol (IP)-based cyber attacks and Electromagnetic Warfare (EW) operations to affect Army operational missions within every warfighting domain. U.S. Army Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*, describes how threats can identify and exploit critical cyberspace vulnerabilities to affect Army operations, often using commercial off-the-shelf (COTS) equipment that provides adversaries with flexible and affordable technologies that are adapted for military purposes. To create denied, degraded, intermittent and limited (DDIL) bandwidth conditions for U.S. forces, threats perform activities in cyberspace to affect a wide range of systems within the operational environment, including Command, Control, Communications, Computers and Intelligence (C4I) systems and Position, Navigation, and Timing (PNT) systems, as critical infrastructure (CI) components. For the Army to operate effectively under DDIL conditions, staff must train within environments that accurately replicate these conditions. However, current training venues have limited DDIL representations, limiting realism and training value.

For effective training of DDIL conditions, non-kinetic effects (NKE) - including cyber and EW effects - must be represented within and coordinated between all enclaves within the training environment, including Live, Virtual, and Constructive (LVC) simulations and live training ranges. Currently, effects within these training enclaves are often disjointed and communicated using manual means, limiting realism and training value. To address this gap, a novel system architecture was developed to automate the communication of NKE between LVC simulations, C4I systems, and live training range enclaves. This cyberspace brokering architecture defines interfaces that can be used by disparate systems to receive simulated NKE information and then apply those effects for realistic implementation in the live training environment. These effects, such as denial of service (DoS), jamming, and spoofing, are applied to real systems to cause tangible inputs for trainees, including communication disruptions, power outages, and misinformation.

The feasibility of this approach was demonstrated though a prototype that coordinates NKE between the simulation environment and live range components. We designed and developed a cyberspace brokering architecture that provides cyber and EW effect models and services that allow communication of these effects between constructive simulations and the live training environment. The feasibility of this approach to coordinate cyber and EW effects between LVC simulations and the live training environment was demonstrated using two NKE effects. First, we demonstrated a simulated cyber attack against power

plant critical infrastructure (CI), showing that simulation of the attack within an LVC simulation results in a corresponding power outage in the live training environment. Second, we demonstrated a simulated cyber attack against video surveillance systems, showing that simulation of the attack within the LVC simulation results in spoofed and degraded video feeds within the live training environment. These results show that the proposed cyberspace brokering architecture can automate and significantly improve the coordination of simulated NKE across LVC simulations and live ranges, thereby enhancing training realism and better preparing warfighters for MDO operations.