Training for the Combined Cyber / Kinetic Battlefield

Lloyd Wihl
SCALABLE Network Technologies
Los Angeles, CA
lwihl@scalable-networks.com

ABSTRACT

Training humans to recognize cyberspace operations and respond rapidly and effectively is imperative, because mistakes have immediate consequences. The ever-evolving complexity of the combined cyber / kinetic battlefield drives a need to simulate engagements in high fidelity where each domain affects the other. We present a new simulation approach that integrates real and simulated cyberspace operations, wired and wireless virtual networks, live and virtual equipment and applications, and traditional kinetic warfare training simulators into a full, instrumented, synthetic cyber warfare training environment. The system allows trainee performance centered on awareness, reaction time and correct action (at all levels), along with ability to work through a degraded cyberspace environment and complete a mission, to be monitored and evaluated. We include an example of how cyberspace operations, and human misunderstanding of the operations, can seriously affect a mission outcome.

ABOUT THE AUTHOR

Mr. Lloyd Wihl has over 30 years of experience in the Modeling, Simulation and Training industry. He has been a system architect for military simulation and training systems, and has led multi-million dollar projects in the areas of synthetic environments, network-centric systems, distributed mission training, air traffic management, space systems, visual systems, and flight simulation. He had the vision for, and guided the development of SCALABLE's new cyber warfare training system, the first live-virtual-constructive cyber training system in the world. Mr. Wihl graduated with distinction in Engineering from McGill University.

Training for the Combined Cyber / Kinetic Battlefield

Lloyd Wihl
SCALABLE Network Technologies
Culver City, CA
lwihl@scalable-networks.com

INTRODUCTION

Most modern military systems are network-centric, and they must protect vast amounts of sensitive data as it is stored on devices or transferred over a network. Warfighters whose lives depend on these systems depend on uncompromised data to arrive in a timely manner. It is clear that all future conflicts are going to involve attempts to disrupt information technology systems, which are necessary for communication and also for the operation of highly sophisticated weapons systems, most of which are computer driven. There is an urgent need for warfighters to train for cyber warfare as it can manifest itself in their operational environment.

Computer-based simulations have long been used to train troops and develop new warfighting techniques. Networked modeling and simulation systems realistically represent combat, from sensors and weapons systems to the tactical behavior of individual entities and military units. However, these traditional training systems assume that computer systems, communication nodes and networks are uncompromised, providing secure and perfect communications between entities in the virtual world. Changes to privacy, integrity, and availability of data due to cyber-attack are rarely if ever taken into consideration. Exercises have made clear the negative effects that result from such simplified modeling.

Cyber ranges, typically consisting of racks of hardware running virtual machines to represent an enterprise network, can be used to train network defenders. However, they lack a realistic representation of wireless battlefield networks with their increased vulnerabilities to disruption compared to wired environments. Nor do cyber ranges integrate with kinetic training systems, and they are thus unsuitable for training for the impact of cyber-attacks on classical warfare.

The current disconnect between kinetic training and cyber training is a challenging problem. Training for modern warfare requires integration across all domains: land, maritime, space, air, and cyber. There is a need to train to operate and complete missions regardless of cyberspace conditions (CJCS, 2014). How can mission rehearsal accurately include operations within cyberspace to avoid negative training?

In response to these challenges we present a system that integrates real and simulated cyberspace operations, wired and wireless virtual networks, live and virtual equipment and applications, and traditional kinetic warfare training simulators into a full, instrumented, synthetic cyber warfare training environment. The system allows cyber warriors, network administrators and command and staff to train as they fight, improving their awareness, reaction time and ability to take corrective action to work through a degraded cyber environment and complete a mission.

CYBERSPACE OFFENSE/DEFENSE

Unraveling the complexities of cyberspace operations requires a comprehensive understanding of information generation, distribution and consumption, as well as the recurring patterns that affect this information flow. Such patterns include information protection, information corruption, threat detection and response. Cyberspace Operations Analysis is a study of these patterns and their impact on the information itself.

A brief note on terminology used in this paper: '*blue force'* refers to those entities (human operators, weapon systems, communication assets, battlefield applications) that are the owners and primary users of the network infrastructure, whereas '*red force*' are those entities that attempt to disrupt the proper operation of the blue force's network.

The Arms Race Nature of Cyberspace Technology

There is a constant arms race struggle between the red and blue force cyberspace technology development. Red forces strive to defeat the protection strategies of blue forces' networks and disrupt their operations, whereas the blue forces defend both proactively and reactively by developing even further sophisticated intrusion prevention, detection and response systems. The technology, from both sides, therefore advances in generations, where a later generation has better attacks or defenses compared to previous ones, and it is highly unlikely that this technology escalation will ever arrive at a stalemate. Hence, there exists an urgent and ongoing need to train for vulnerabilities and resilience of military systems to cyberspace operations from multiple, diverse, and (possibly) coordinated threats on communication networks.

Note that the above discussion applies equally well when the blue force is in fact launching the cyberspace operations. The point is that the actions by either force, as an attacker or defender, are dependent on the actions of the other force. This sequence of attacker and defender actions makes the simulation and training of cyber warfare ideally suited to a role playing interactive environment.

Modeling and Simulation of Cyberspace Operations

The modeling and simulation of cyberspace operations requires some special features, which are dependent on the nature of the operations (Wihl, Varshney and Kong, 2010). A brief discussion of these follows.

Passive attacks, as the name suggests, do not actively influence the network. The intention is to glean information about the state of operational networks. Note that the information could be data itself (files, streaming video etc.), or other kinds of non-data information such as location and strength of troops, direction of movement, or identification of commanders. Prevailing strategies for passive attacks include wireless eavesdropping, packet sniffing and comprehensive network traffic analysis. To replicate these attacks in a synthetic environment, the latter must model information not only as packet data, but also as other attributes such as location, mobility, and operator roles. Authentication, trust management, and key management models must be included in the communications simulation.

Denial of Service (DoS) involves overwhelming networking or computation resources to render them incapable of servicing genuine operations. This is one of the most popular kinds of attack vector and includes attacks such as ICMP Smurf, TCP SYN flood etc. To model these attacks, the simulation must represent the protocol stack with high fidelity as well as packet level interactions (e.g. TCP sequence numbers, ICMP packet buffer allocation etc).

Malicious agents are software programs, such as viruses and worms, which leech themselves to a host computer to infect their resources and utilize the host computer's resources to propagate themselves further. Other examples include malware, trojans, backdoors, and rootkits. The role of these attacks on network performance can be investigated by connecting the network model to real hosts and real operating systems, so that the malicious agents propagate in a controlled testbed environment. The network model must interoperate with real configurable Intrusion Prevention Systems and Intrusion Detection Systems.

Topology misconfiguration applies to mobile ad-hoc networks (MANETs), which have a self-organizing nature to route traffic. A malicious agent could subvert the routing topology construction and maintenance protocol to force traffic to be routed along a preferred path. A well-known attack is Wormhole (Hu, Perrig and Johnson, 2003), where two or more collaborating nodes can influence the entire network topology such that all traffic is directed towards them. Simulating such attacks requires modeling the routing protocols and topology construction algorithms with high accuracy.

Code exploits utilize software vulnerabilities to execute malicious code. The victim software may be the operating system, applications, databases, web browsers and so on. Modeling these attacks requires that the simulation testbed must be able to interface with physical hardware and software. Such a technique is known is emulation, where the simulation models interact (by exchanging data and control information) with physical host machines.

Human error refers to that broad class of attacks where an operator makes an error, for example visiting a malicious web page, or clicking a harmful email link. Furthermore, there could be intentional actions by compromised personnel. Modeling this attack behavior requires a human-in-the-loop interface, where role players can actively participate in a training exercise to influence the state of the network.

Finally, wireless specific attacks target the specific characteristics of wireless communications, such as broadcast nature, hidden terminal effects, frequency hopping etc. For these attacks, the simulation must model the wireless specific details of communication, including detailed physical layer effects, jamming susceptibility, and mobile ad hoc network routing.

Attack Vector	Definition	Examples
Passive attacks	Gleaning information	Eavesdropping, sniffing, network traffic analysis
Denial of Service	Making service unavailable by overwhelming the computation or network resources	ICMP flood, Smurf ping flood, TCP SYN flood, Teardrop attack, Reflection attack, Blind DoS, Distributed DoS
Malicious Agents	A malicious undetected program executing on victim's computer	Virus, Worms, Malware, Trojans, Rootkits, Backdoor
Topology mis-configuration	Subverting the traffic flow paths	Wormhole attack, Rushing attack, Blackhole attack, Grayhole attack
Code Exploits	Exploiting software bugs to execute malicious code	Buffer overflows, OS / Services / Applications / Database exploits
Web Exploits	Exploiting the client-server interactions of Web protocols	Cross-site scripting, HTTP header injection
Human Error	Intentional or accidental operator actions	Phishing, Incorrect data entry, compromised personnel
Wireless Specific	Targeting the specific attributes of wireless communications	Jamming, RF signature identification

In summary of the above discussion, a cyber warfare communications effect model must provide the following features:

- Data communication at packet level and network security (for eavesdropping)
- Model information such as location, movement, roles (eavesdropping)
- Protocol stack operations (DoS), including routing (routing misconfiguration) and wireless (wireless specific)
- Emulation with real hardware and software (malicious agents and code exploits)
- Human-in-the-loop (human errors)
- Wireless detailed physical layer models and routing models

Impact of Attack

In a cyberspace operation analysis, three factors - privacy, integrity and availability - are the measures of performance. A key challenge for training is to evaluate how these come to play in the larger context of mission effectiveness. For this reason, we chose to develop an architecture that could be integrated into live virtual constructive environments, so that the effects of compromised data privacy, integrity or availability would affect operational systems, humans in the loop, or constructive entities, resulting in changes in battlefield outcome. To achieve this, the system would need to integrate with Distributed Interactive Simulation (DIS) or High Level Architecture (HLA) based simulations while also being able to bring live battlefield application traffic and communications into and out of the emulated communications network.

CURRENT APPROACHES TO CYBERSPACE TRAINING

White Carding

The simplest approach currently in use to introduce cyberspace effects is to "white card" participants in a training exercise to inform them that at that point in the scenario their system is deemed to be cyber-attacked and is nonoperational. The participant then stops using the capability that was attacked. White cards can be effective in reducing operational capabilities in a simulated mission, and have the benefit of being very low cost. However this simplistic approach provides no training in recognizing indications of a cyberspace operation, defending against it, containing it, or discovering compromised integrity or privacy of data and finding workarounds.

Effects-Based Simulation

An alternative approach to bridge the gap between traditional and cyberspace training is to introduce cyberspace effects simulation onto operator workstations. An example of this approach is the Network Effects Emulation System (NE2S) developed by Joint Staff J7 Joint Force Development (NE2S, 2014). It consists of a Master Control Station that allows an instructor to initiate host and network effects that appear to degrade operator workstations. Actual data transmission is not degraded; the effects on the operator workstation are only visually simulated.

While certainly more efficient and scalable than white carding, and with the added ability to "dial in" degradation, effects-based simulation nonetheless has similar limitations regarding cyberspace training – no way to defend against a cyberspace operation, contain it, nor discover and then deal with compromised integrity of data.

Cyber Ranges

Cyber ranges replicate a subset of hardware (or virtual machines) from an operational system and connect them on a wired network. The DoD Cyber (IA) Range is an example of this approach, providing an operational representation of today's Global Information Grid (GIG) Information Assurance (IA) architecture within a Network Operations (NetOps) construct (Powell, Holmes and Pie, 2010). The IA Range is an infrastructural platform designed to integrate distributed and heterogeneous IA architectural systems and solutions with the DoD Computer Network Defense (CND) operational hierarchy.

Current cyber ranges, though realistic representations, are limited in scale, costly, and time-consuming to configure. Importantly, wired ranges have little or no capability to model wireless tactical networks with their inherent vulnerabilities not found in wired networks. While these ranges can serve to train defenders of the network itself, they do not effectively model the impact of a cyberspace operation on an overall mission, which is essential for realistic training and mission rehearsal. Thus they do not train all users of the net-centric system, from commander to front line warfighter, on what to expect during cyber warfare and how to react.

IO PDU

Building on the long success of creating federations of interoperable simulations, there was a recent addition of an Information Operations Protocol Data Unit (IO PDU) to the DIS Standard (IEEE 1278.1-2012). The IO PDU would allow simulations to recognize when they are under a simulated cyber-attack, and change their behavior accordingly. This would be an improvement over effects-based simulation in that the data published by the simulations could be affected, which could in turn propagate to other simulations. The onus would be on each system's simulation to produce the appropriate response to each cyber-attack, and the fidelity of these responses could vary. However this approach would not simulate attacks against the network that connects the systems in the battlefield, which is itself a significant target of attack. Another limitation of this approach is the inability to launch real attacks within the synthetic environment making it difficult to quickly incorporate new threats.

IMPROVED APPROACH

All of these shortcomings can be improved upon with a new approach to integrating cyberspace operations into the kinetic training environment.

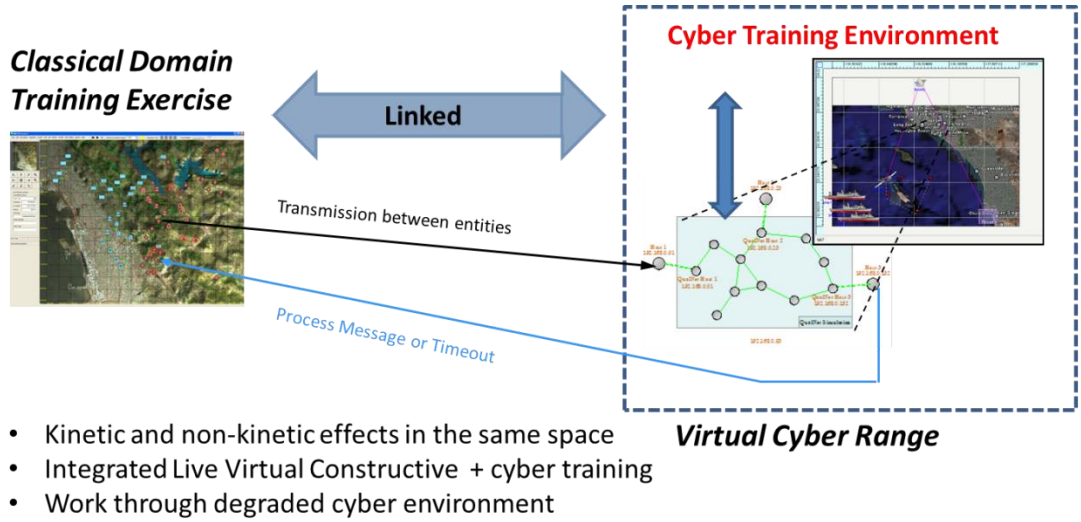

Figure 1: Linking Classical and Cyber Training

In classical domain training exercises, messages typically get passed directly between sender and receiver perfectly, without degradation. In cyber ranges, only host computers and networks are represented, without any kinetic battlespace representation. A new approach, shown in Figure 1, is to link these two disconnected training environments. Messages transmitted between entities in the classical domain are intercepted and sent through a software emulation of the battlefield network. As they traverse the emulated network, they are subjected to cyberspace operations which affect what gets delivered to the receiving entities. Messages that get through (which might have been delayed, eavesdropped or had selected information altered or dropped en route) are sent to the receiving entities in the classical domain. Compromised communications affect the entities' and trainees' situational awareness and decision-making, and therefore overall mission outcome.

The software emulation of the network, running in real-time, models the full network protocol stack on every emulated node and connects these nodes over simulated links that can be wired and wireless. Wireless communication effects include terrain, jamming, interference, fading, and other environmental factors. Actual packets are passed up and down the emulated protocol stack on every node and across the simulated physical layer between nodes. The emulated network thus reacts the same way as a real network, and can be subjected to real or simulated cyberspace operations.

A suite of simulated cyberspace attacks and defenses can interact with every layer of the emulated network. These include network security protocols, firewall models, port and network scanning, eavesdropping, jamming and silent jamming, denial of service, stimulation of intrusion detection systems, SIGINT, vulnerability exploitation, virus and worm propagation and defense, backdoors, rootkits, botnets, and others. Host models can be configured with memory, CPU cycles, vulnerabilities, processes, and shared files which can get infected. Security logs are generated to assist with forensics. Adaptive attack scripts can be used which will modify attack vectors depending on the success of previously attempted attacks.

The real-time software emulation of the network makes it possible to represent the communication infrastructure at sufficiently high levels of fidelity that live equipment, devices, and applications—such as sensor feeds, streaming video, and voice communications—can be deployed unmodified across it, and thus be subjected to cyberspace operations (Figure 2).

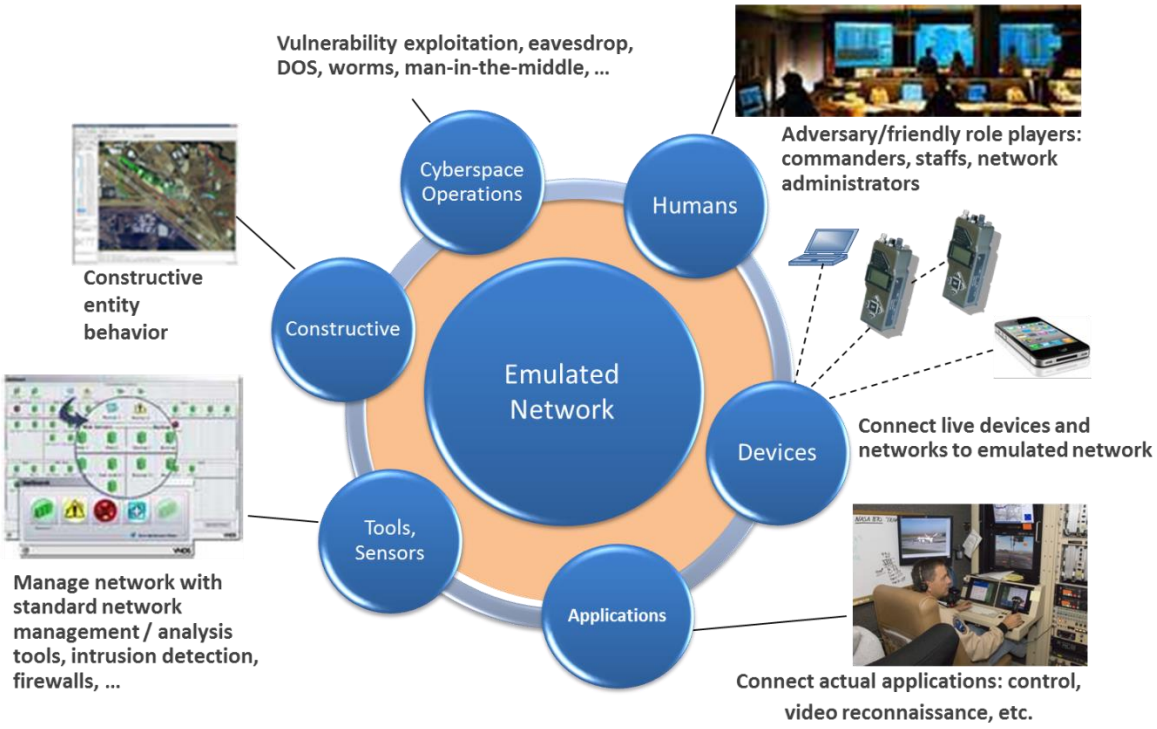

Figure 2: The Cyberspace / Kinetic Training System

The trainees can include everyone from commander to network administrators in the same exercise. Trainees can use their real battlefield applications and network defense tools on role player stations that are mapped to virtual nodes in the scenario. The training is fast paced for operational speeds, and is centered on awareness, reaction time, correct action, workarounds and countermeasures, along with the ability to work through a degraded cyber environment at all levels to complete a mission. Trainees learn how to act individually and as part of a team. Teams learn to work together effectively as they attempt to thwart cyberspace operations. The system logs all trainee actions and attack successes, then reinforces lessons learned with After Action Reviews that show trainees and observers what actually happened and why.

SYSTEM DEPLOYMENT

A typical deployment of the training system is illustrated in Figure 3:

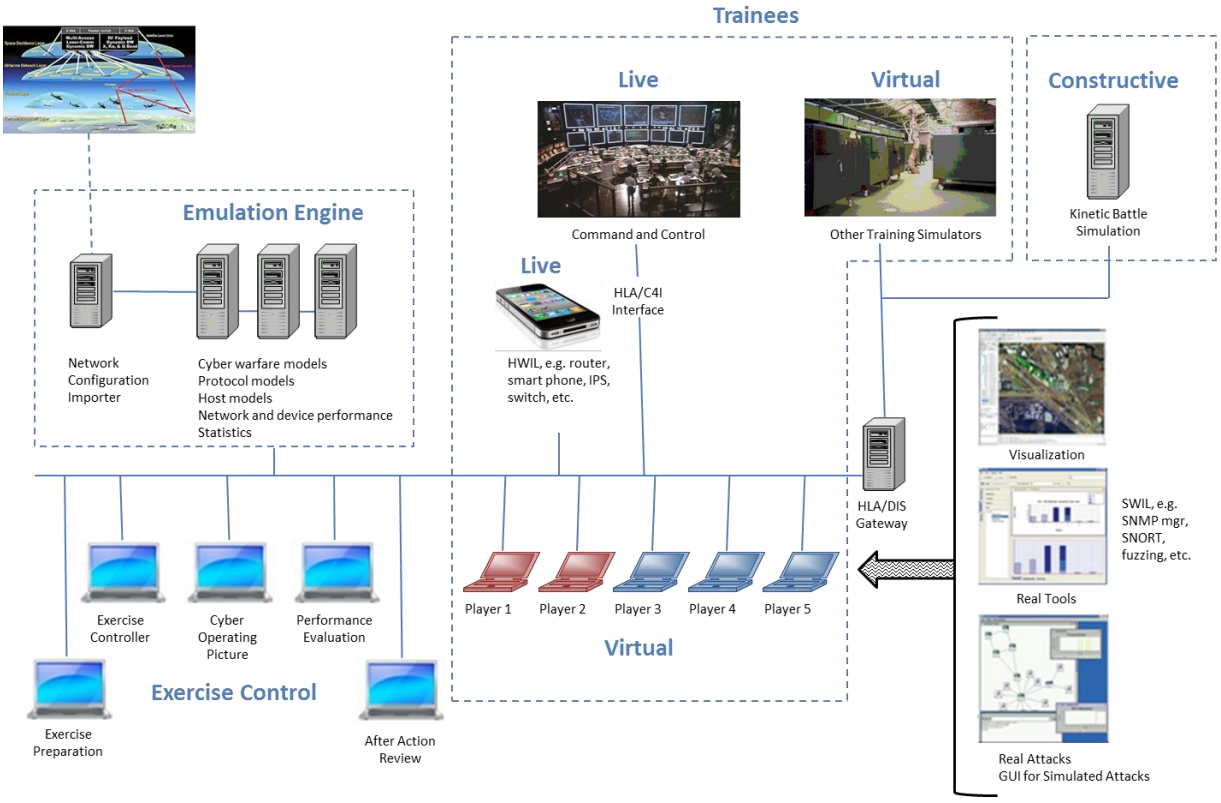

Figure 3: Typical Training System Deployment

Emulation Engine

The Emulation Engine replicates the network in software and contains cyber warfare models that are used to attack or defend the network as well as the connected equipment and applications. Real devices, virtual machines, and role players connect and exchange data from live applications over the emulated network. The privacy, integrity, or availability of these data can be compromised by cyber-attack, with resulting effects observed on the live equipment.

Role Player Stations

Role players participate in the exercise at friendly or adversary stations, using their own repertoire of real discovery, attack, monitoring, and defense tools. That is, the tools embraced by the thick arrow in Figure 3 can be launched from the role player stations. Adversary players can use real malware and exploitations, as well as launch simulated attacks, to attack the emulated network and the connected live components. The friendly role players try to accomplish their mission while monitoring and defending the network using their actual tools. The trainees are not limited to the Role Player stations. Trainees could also be at a live system such as a C2 station, or participating from another kinetic training simulator.

Exercise Control

Exercise Preparation allows the creation, modification, or selection of Lesson Plans, mission scenarios, network configurations, cyber-attacks, host models, user behavior models, real to virtual device mapping, role and trainee assignments, and sides and teams.

Exercise Control is used to load and unload an exercise, control federation execution, freeze and unfreeze, launch cyber-attacks, take snapshots during the exercise and restore them (in case a trainee made an unrecoverable mistake), reset attacks, and communicate with trainees using chat and VoIP.

The Cyber Operating Picture gives an indication of the state of the network and devices, traffic, routing, entity position, mapping of trainees to entities, and it can be used to launch preconfigured or new cyber-attacks.

Performance Evaluation keeps track of trainees' progress. Exercise Controllers can monitor trainees' screens. The launching of attacks is logged, and trainee's responses (views, keystrokes, clicks, and communication with others) are logged along with their response times, and whether attacks were successful, to assist with scoring. It maintains databases of trainees and the exercises they have completed along with their scores.

After Action Review plays back any players' screenshots ("perceived truth") and all their actions (clicks, keystrokes, chat messages and voice calls) on a moving timeline along with attacks, other players' views, and the actual state of the network (the "ground truth").

EXAMPLE USAGE

With the integration of kinetic and cyber warfare effects into a unified live virtual constructive training environment, we are now able to better simulate a classical battlespace subject to cyberspace operations. The following example using this training environment illustrates some of the unique capabilities of this new approach, showing how cyberspace operations, along with human misunderstanding of these operations, could affect a mission.

The kinetic battlefield scenario is modeled by a commercial-off-the-shelf or government-supplied constructive simulation. The behavior of trainees and constructive entities is influenced by the orders and messages they receive, the timing of their delivery, and whether these messages get through at all. Sensor feeds and voice communications are routed through the emulated network and subjected to cyberspace operations, influencing what is seen or heard at the receiving end. Real battlefield applications communicate over the emulated network. The emulated network is attacked by red teams using simulated and/or real attacks, while blue role players must defend the network and complete the overall mission.
.
The friendly forces patrol a residential area, using a UAV which is sending imagery to a platoon commander in a headquarters (HQ). The UAV video feed, simulated using an image generator, is transmitted through the emulated network to a physical display used by the commander. The HQ contains servers and a wired network to workstations running battle command systems (BCS). The commander gives orders to his lower command and receives reports using voice and data over tactical radios on a mobile ad hoc network. The UAV is controlled over VHF radio and its downlink video stream is unencrypted. Several specialists in the HQ are responsible for keeping the BCS's and the network operational.

The adversary forces are able to eavesdrop the unencrypted UAV video. The emulated network routes this video to a red role player station where it is viewed. The adversary forces want to disrupt this video feed at a critical moment. They use a silent jammer (modeled) which disrupts only the high-bandwidth video without affecting the lower bandwidth control channel. Since they are able to view the video, they test their jammer for 3 seconds. The video freezes, then resumes. This also happens at the HQ, but no one pays much attention, since it resumes quickly.

Soon, the adversary forces again jam the UAV video, while attacking and capturing hostages. They speed off in a vehicle, unseen by the friendly forces. Their destination is unknown to the friendly forces.

Later, the adversary forces make use of an existing vulnerability in the UAV's onboard computer (modeled) to surreptitiously send packets to the UAV Ground Control Station. They get through the firewall (modeled) which has been incorrectly configured. They then launch a zero day attack (modeled) on the commander's workstation. This exploit allows them to modify the content of orders sent from the commander.

The friendly forces locate the building where the hostages are. They plan a rescue using dismounted soldiers. The adversary forces become aware of the plan by eavesdropping the unsecured communications. Using the exploited computer at the HQ, they modify the geographical coordinates of the building that will be stormed. If this data change goes undetected, the command to start the rescue will indicate the wrong building.

If the soldiers head toward the wrong building, they will be ambushed by adversary soldiers waiting for them, and the friendly side will suffer losses. If the commander is able to discover that the orders were changed, and can get the real orders to his soldiers by other means, they will succeed in rescuing the hostages.

The following are sample learning objectives for the commander in this combined kinetic/cyber scenario:

1. Notice the momentary glitch on the UAV video feed and investigate the cause. Review SIGINT data to determine if enemy radio transmissions coincided with this glitch and pinpoint the source of the transmissions. Destroy the silent jammer.

2. When the UAV gets jammed, investigate the cause. If possible, switch to an alternate downlink channel. Quickly order alternate surveillance from another UAV. Find and destroy the jammer.

3. Discover that the soldiers are heading toward the wrong building. Understand that the orders were tampered with, and the implication on the trustworthiness of the computer and/or communication network. Rapidly find an alternate way to communicate, and get the real orders to them before they are ambushed.

These unique integrated cyber / kinetic training capabilities are enabled by the:

• Live video feed from an external source subject to disruption
• Integration with constructive simulation
• Difference between ground truth (video sent by UAV) and perceived truth (what gets to commander)
• Network emulation integrating wired, tactical radios, and satellite
• Ability to produce a real transient effect on a role player station which must be noticed by a trainee
• SIGINT model integrated with cyberspace operations
• Ability to model a future unknown (zero day) vulnerability
• Outcome of the mission affected by cyberspace operations

As this example indicates, with the tight integration of cyber warfare models into a classical training exercise, the capability to train for the effects of cyber warfare on mission outcome is dramatically improved.

BENEFITS

The benefits of this new approach are many-fold:

- Accurate modeling of the network produces high-fidelity responses to cyberspace operations including attacks to the network's control plane or exploitation of wireless vulnerabilities.

- The ability to mix real equipment, virtual machines, and host models allows the incorporation of existing and future vulnerabilities and their effects on systems.

- Routing real traffic through the emulated network allows integration with deployed live and virtual training systems.

- Real exploitation tools can be used side by side with simulated cyber-attacks in a safe environment.

- Interfaces to constructive simulations allow messages between their entities to be subjected to cyber-attack, affecting entity behavior.

- The system integrates cyberspace and kinetic environments and allows training for the impact of cyberspace operations on overall missions.

CONCLUSION

We have architected and developed a new approach that integrates real and simulated cyberspace operations, wired and wireless virtual networks, live and virtual equipment and applications, and traditional kinetic warfare training simulators into a full, instrumented, synthetic cyber warfare training environment. The combined LVC kinetic / cyberspace environment provides improved, higher fidelity training for the combination of cyberspace operations with traditional warfare, with damage in one domain affecting performance in the other.

The approach allows trainees to learn individually and as teams to detect when something is wrong, assess what is happening, contain the attack, take countermeasures, and modify operations to assure the mission. The ability to train command and staff to work around the cyberspace operations and complete a mission, while network administrators learn to detect and react to threats as they occur, in the same exercise, can provide a true "train as you fight" environment to help warfighters prepare for future conflicts.

REFERENCES

Chairman of the Joint Chiefs of Staff (CJCS) Notice 3500.01. 2015-2018 Chairman's Joint Training Guidance. 30 October 2014.

Wihl L., Varshney M., Kong J. (2010). Introducing a Cyber Warfare Communications Effects Model to Synthetic Environments. *Proceedings of the Inter-service / Industry Training, Simulation and Education (I/ITSEC) Conference 2010.*

Hu Y., Perrig A., Johnson D. (2003). Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, *Proceedings of the 22nd IEEE INFOCOM, 2003.*

Network Effects Emulation System (NE2S) / Cyber Operational Architecture Training System (COATS) (2014), http://www.navair.navy.mil/nawctsd/Programs/Files/5-2014%20COATS%20NE2S.pdf

Powell R., Holmes T., Pie C. (2010). The Information Assurance Range. *International Test and Evaluation Association (ITEA) Journal 2010; 31: 473-477.*

IEEE Standard 1278.1-2012. IEEE Standard for Distributed Interactive Simulation--Application Protocols. IEEE Computer Society, 2012.