SCALABLE
NETWORK TECHNOLOGIES

Network Defense TRAINER

Integrate Cyber Warfare Into Kinetic Training Systems

The SCALABLE Network Defense Trainer (NDT) is a live-virtual-constructive (LVC) simulator for training all types of cyber warriors. It can be implemented as a stand-alone system to deliver hands-on experience in the behavior of a wide range of cyber attacks.

NDT can also be integrated with computer generated forces (CGF) and semi-automated forces (SAF) tools to add realistic cyber warfare effects into kinetic mission planning and mission rehearsal exercises.

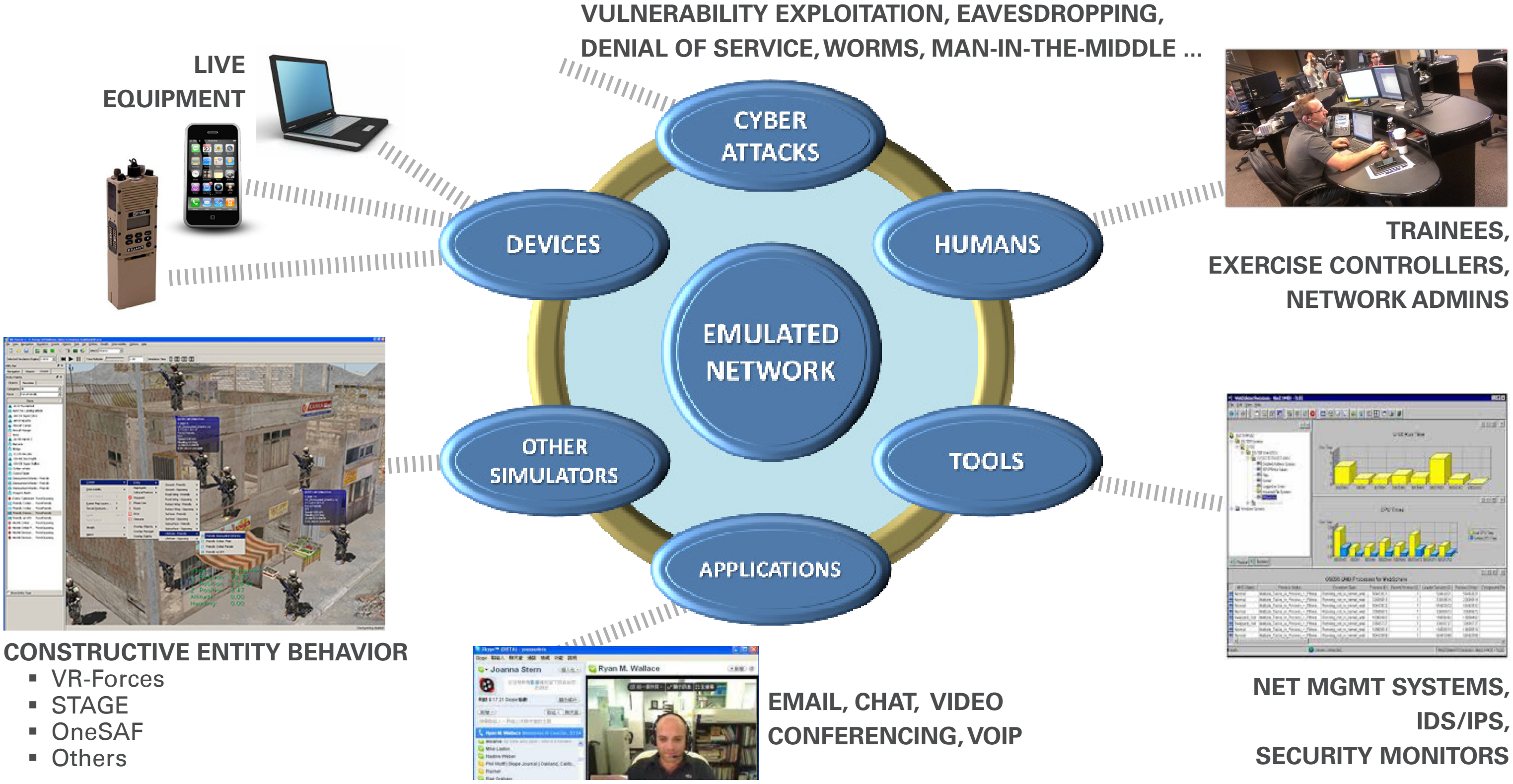
An NDT system leverages virtual network models which are configured to accurately emulate networks comprised of thousands of wired and wireless nodes. Live and virtual hosts can be connected to the virtual network models, and a system can be federated with other simulators to create powerful training solutions.

The unique advantages of an NDT system are:

- Effectively represent mobile wireless equipment and applications (and the vulnerabilities they include)
- Accurately model the information transport fabric between servers and end-point systems in high fidelity to illustrate the effects of cyber-attacks
- **Seamlessly federate with other military training systems such as kinetic battlefield simulators (e.g. MAK VR-Forces, Presagis STAGE, OneSAF and others)**

Network Defense Trainer delivers a comprehensive hands-on experience in a cost-effective training environment.

THE LIVE-VIRTUAL-CONSTRUCTIVE INTEGRATED TRAINING ENVIRONMENT



VULNERABILITY EXPLOITATION, EAVESDROPPING, DENIAL OF SERVICE, WORMS, MAN-IN-THE-MIDDLE ...

LIVE EQUIPMENT

TRAINEES, EXERCISE CONTROLLERS, NETWORK ADMINS

CONSTRUCTIVE ENTITY BEHAVIOR

- VR-Forces
- STAGE
- OneSAF
- Others

EMAIL, CHAT, VIDEO CONFERENCING, VOIP

NET MGMT SYSTEMS, IDS/IPS, SECURITY MONITORS

ROLES & COMPONENTS

A Network Defense Trainer exercise is comprised of multiple role players: **Blue Force** defenders (the trainees), **Red Force** attackers and **Exercise Controllers**.

Trainee systems are "mapped" onto nodes in the virtual network model via the **Trainee Agent** clients. To the trainees, the virtual environment "looks and feels" like they are connected to an actual physical network. Exercises can be run multiple times with trainees playing different roles connected to different nodes.

Exercise Controllers manage the overall training process, observing and guiding the trainee behavior as appropriate. Cyber attacks can be scripted to occur at specific times or under specific conditions during an exercise, and can be launched ad hoc by the Exercise Controller or a designated attacking force in response to trainee actions.

System Management, comprised of **exercise preparation** (EXPREP), **exercise control** (EXCON), and **after action review** (AAR) is performed via browser-based applications. Elements include:

- **Library Management:** a database of lesson plans, device definitions, cyber attacks, virtual network model configurations, and user profiles
- **Exercise Management:** a facility for combining library elements into specific exercise descriptions
- **Exercise Control:** the interface for running exercises
- **Trainee Management:** profiles and scoring
- **Performance Evaluation:** metrics and AAR with key stroke, mouse click and screen display capture

Red Force and Blue Force "classic" and "advanced" GUIs provide role-based views of **Cyber Operating Pictures**.

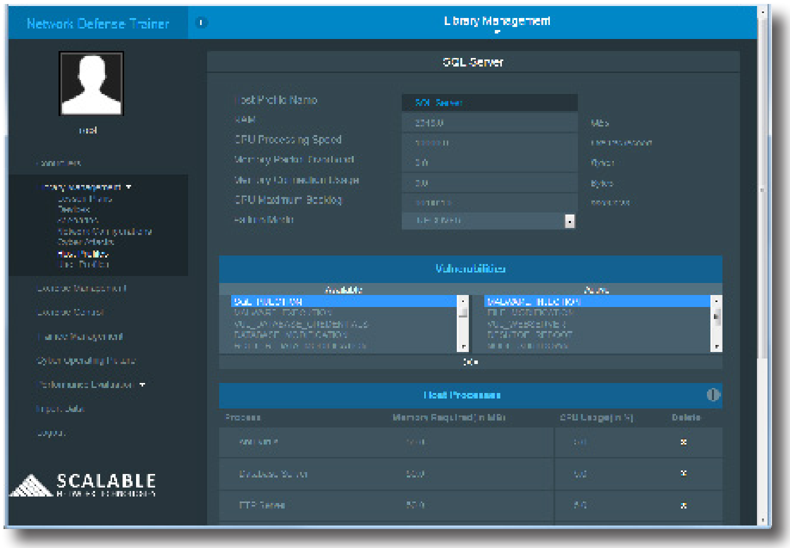
Live third-party network and systems monitoring and management tools can be used by trainees to determine network status and identify cyber attacks.

Virtual network model topology can be generated from structured Microsoft Visio diagram files.

ENHANCE CURRENT TRAINING SYSTEMS FOR CYBER

By integrating / federating with an NDT system:

- Train everyone from commanders down to network administrators in the same exercise
- Personnel can fully understand and experience how cyber-attacks will affect a mission
- Train to work through a degraded cyber environment to complete a mission



SQL Server

Host Profile Name: SQL Server

RAM: 2048.0 MBs

CPU Processing Speed: [illegible]

Memory Perfor. Threshold: 0.0 Bytes

Memory Connection Usage: 0.0 Bytes

CPU Maximum Backlog: [illegible]

Failure Mode: [illegible]

Vulnerabilities

Available	Active
SQL INJECTION	MALWARE INJECTION
[illegible]	FILE MODIFICATION
[illegible]	[illegible]
DATABASE MODIFICATION	[illegible]
[illegible]	[illegible]

Host Processes

Process	Memory Required (in MBs)	CPU Usage (in %)	Delete
Antivirus	[illegible]	[illegible]	×
Database Server	50.0	[illegible]	×
FTP Server	50.0	5.0	×

KEY CAPABILITIES

- Integrate physical hardware and live applications seamlessly into virtual network models
- Accurately represent attacks and vulnerabilities in mobile wireless networks
- Federate with other LVC simulation systems
- Experience customizable cyber attacks at real-time speeds against realistic network simulations
- Combine both simulated and real cyber attacks in an exercise
- Capture and replay trainee behavior for After Action Review

CYBER THREAT MODELS

- Network security
- Firewalls
- Port and network scanning
- Eavesdropping
- Jammers
- Denial of Service
- Intrusion Detection System Stimulation
- Signals Intelligence
- O/S resource models
- Vulnerability exploitation
- Virus attacks
- Worm and virus propagation
- Antivirus
- Backdoors and rootkits
- Host models
- Botnets
- Security logs and audit trails
- Coordinated and adaptive attacks

PN DST0141129